Quiz with prizes!!

Polynomial Commitments from Lattices

Ngoc Khanh Nguyen

Joint work with: *Valerio Cini, Giulio Malavolta and Hoeteck Wee*

Outline

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

SNARKs

ethereum

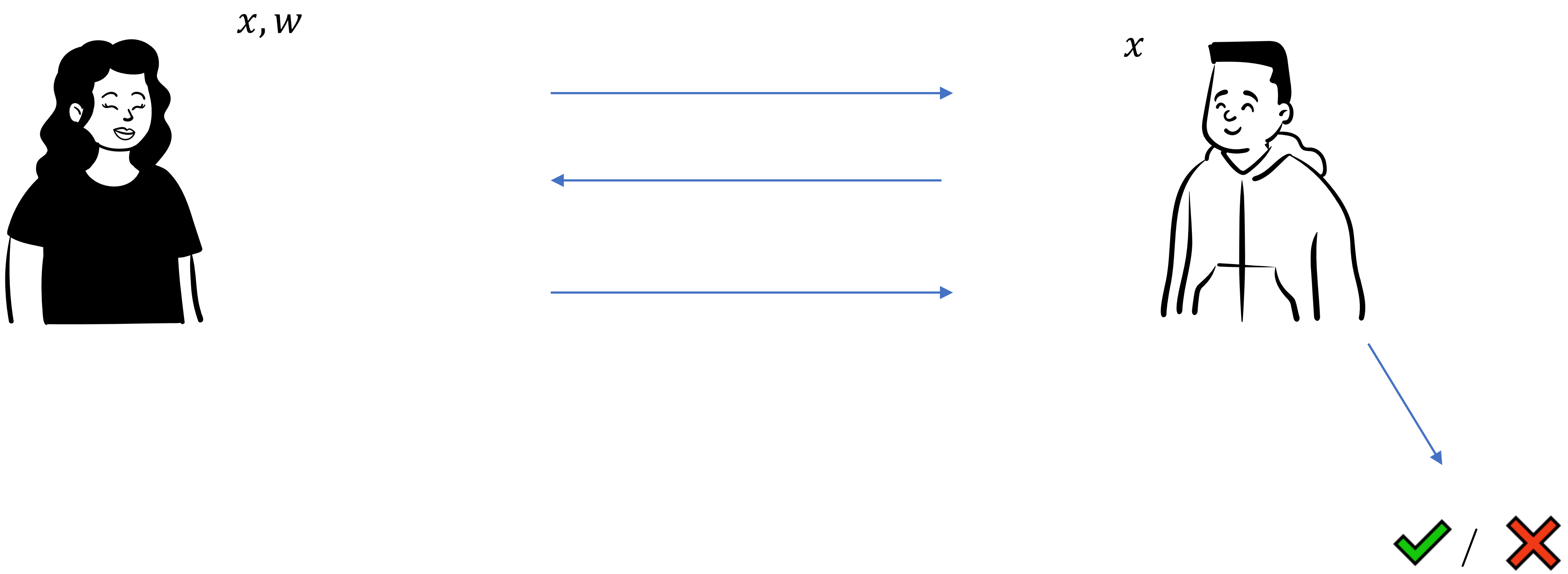
SNARKs

- Succinct
- Non-interactive
- ARgument (of)
- Knowledge

ethereum

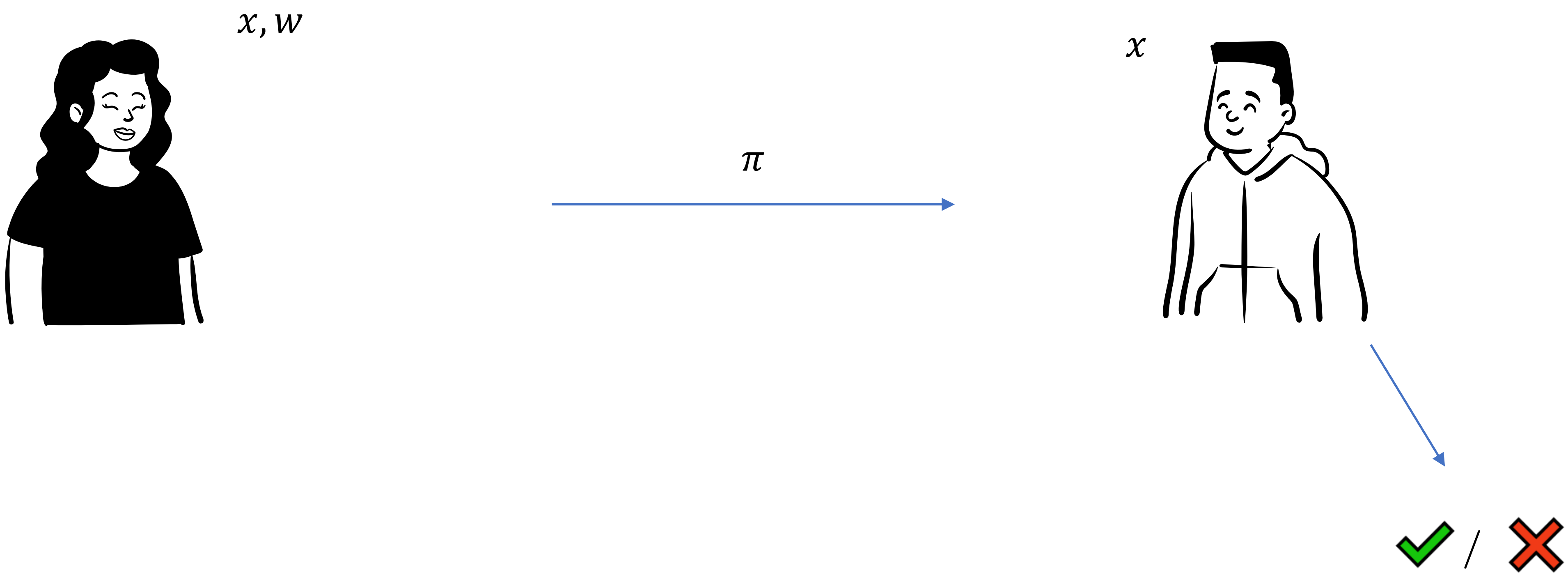
Interactive Proof

$$R(x,w) = 1$$



Non-Interactive Proof

$R(x, w) = 1$



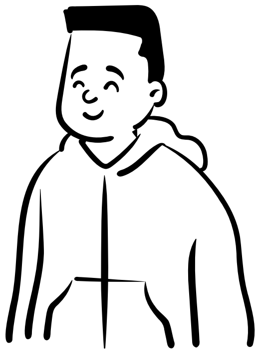
Succinct Non-Interactive Proof

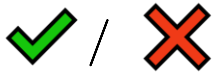
$R(x, w) = 1$

x, w

π

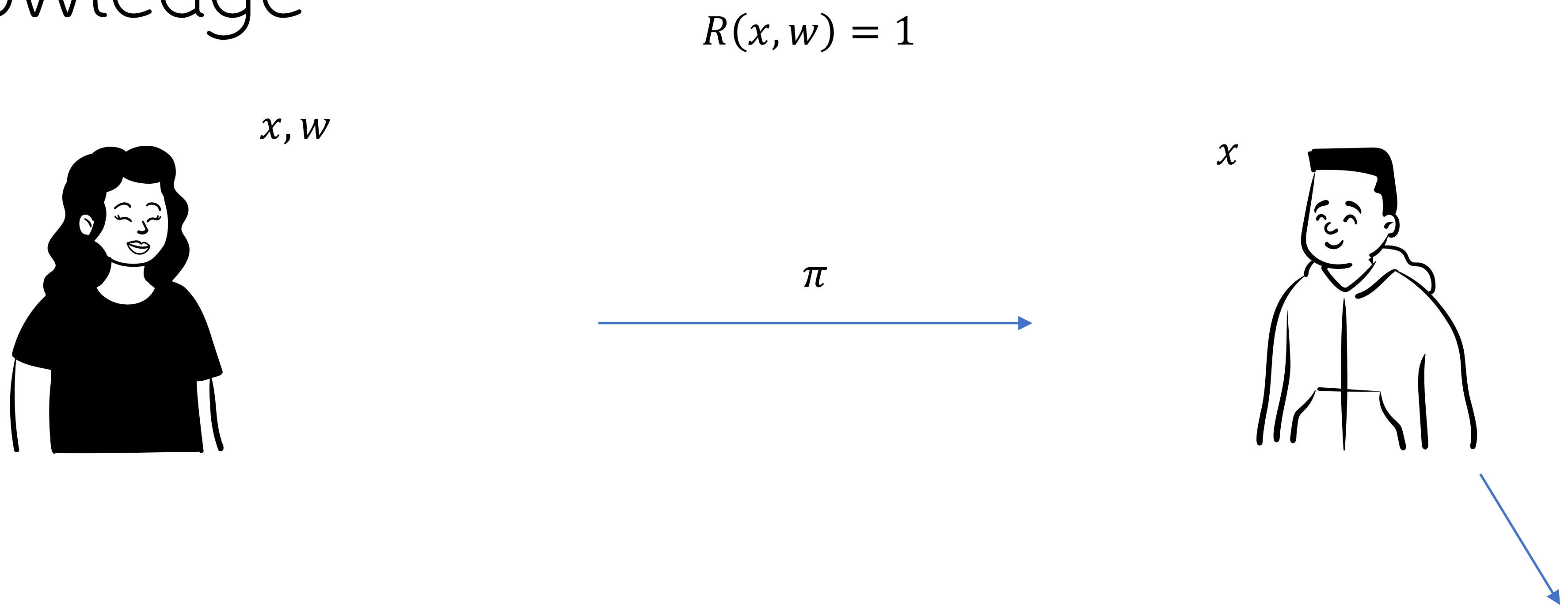
x

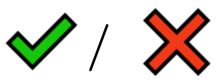




Succinct: $|\pi| \ll |w|$ + fast verifier

Succinct Non-Interactive Argument of Knowledge

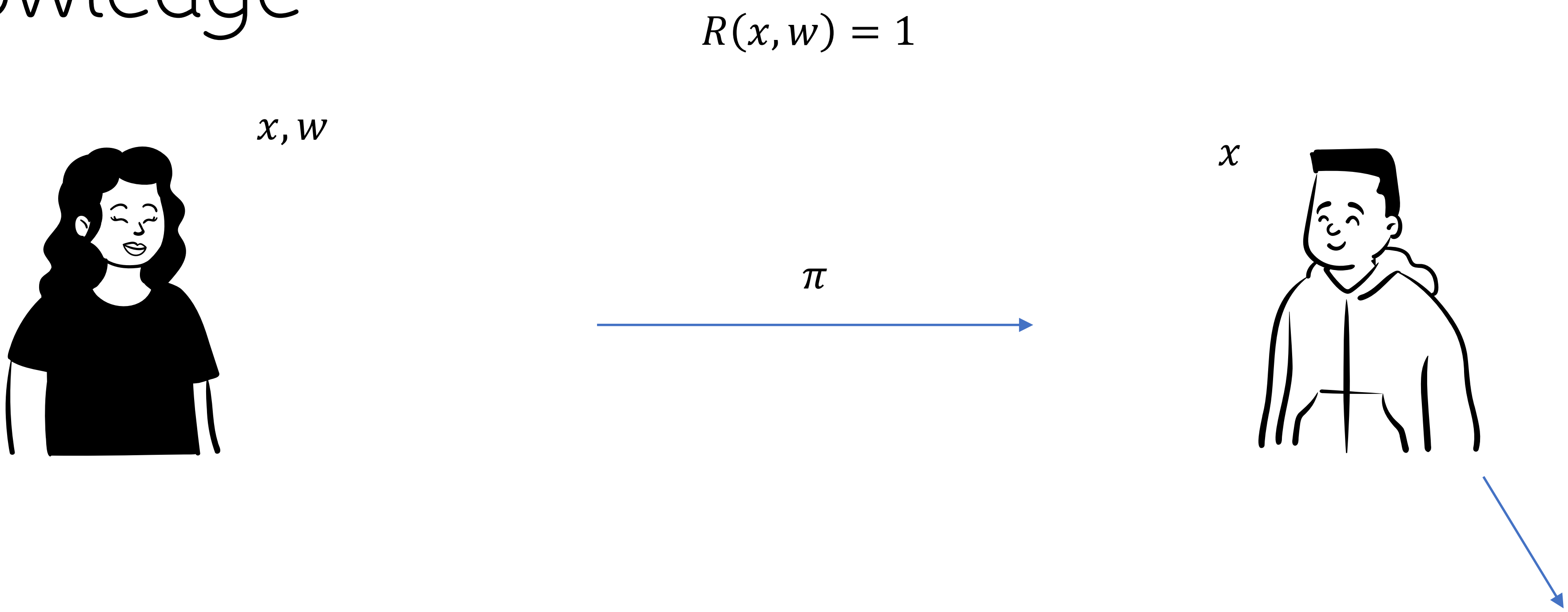


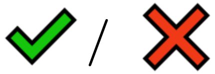


Succinct: $|\pi| \ll |w|$ + fast verifier

Knowledge soundness: If a prover can convince the verifier with high probability, then it ``must know w''.

Succinct Non-Interactive Argument of Knowledge





Succinct: $|\pi| \ll |w|$ + fast verifier

Knowledge soundness: If a prover can convince the verifier with high probability, then it ``must know w''.

Argument: knowledge soundness holds under a computational assumption.

Applications of polynomial commitments

Polynomial commitments + Polynomial IOPs = (zk)-SNARKs

Polynomial Commitments [KZG10]

Polynomial $f \in R[X]$ of degree $< L$

$t = Com(f; r)$

Polynomial Commitments [KZG10]

Polynomial $f \in R[X]$ of degree $< L$

$t = Com(f; r)$

Binding:
It's hard to find two different openings (f, r) and (f', r') such that $Com(f; r) = Com(f'; r')$.

Polynomial Commitments [KZG10]

Polynomial $f \in R[X]$ of degree $< L$

$t = Com(f;r)$

Binding:
It's hard to find two different openings (f,r) and (f',r') such that $Com(f;r) = Com(f';r')$.

Hiding:
The adversary can't learn any information about (f,r) from t

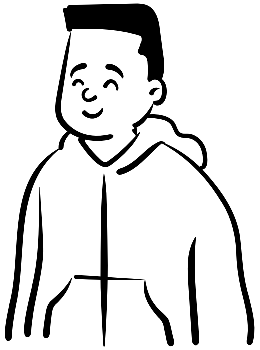
Polynomial Commitments [KZG10]

Polynomial $f \in R[X]$ of degree $< L$

$t = Com(f;r)$ →

$x \in R$ ←

$(y, \pi$=proof that $f(x) = y$ and $t = Com(f;r))$ →



✓ / ✗

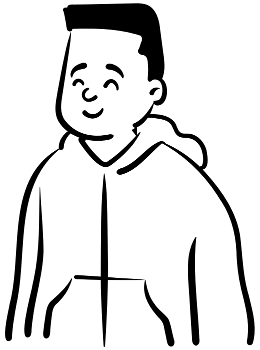
Polynomial Commitments [KZG10]

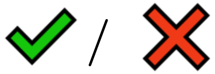
Polynomial $f \in R[X]$ of degree $< L$

$t = Com(f; r)$ →

$x \in R$ ←

$(y, \pi$=proof that $f(x) = y$ and $t = Com(f; r))$ →





Completeness:
For an honest prover the verifier accepts

Knowledge soundness:
If a prover can convince the verifier with high probability, then it ``must know f''.

Zero-knowledge/hiding:
the verifier does not learn anything about f from the interaction

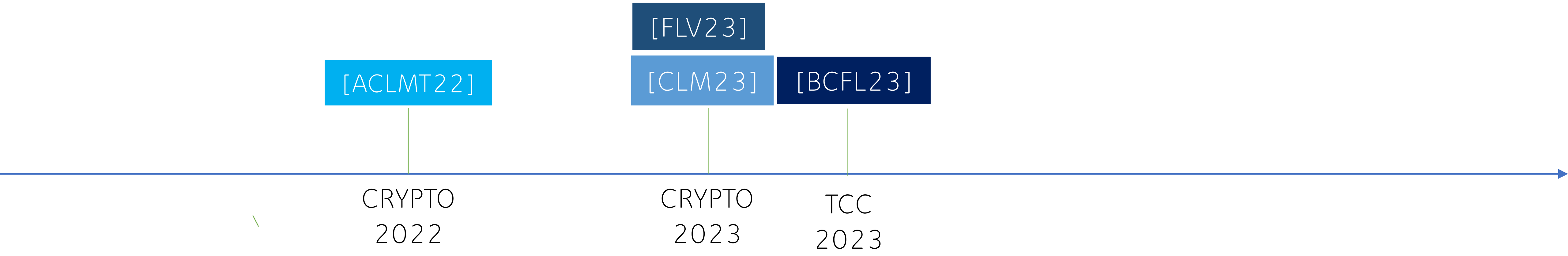
Succinctness:
The proof size and verifier runtime are $\ll L$, i.e. $poly(\lambda, \log L)$

Outline

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

Prior works

Functional commitment [LRY16]: commit to input x. Next, given a function f, output $y \coloneqq f(x)$ and prove that $f(x) = y$.



Prior works

Functional commitment [LRY16]: commit to input x. Next, given a function f, output $y \coloneqq f(x)$ and prove that $f(x) = y$.

💀 $polylog(L)$ [ACLMT22] — CRYPTO 2022

💀 $polylog(L)$ [FLV23] [CLM23] — CRYPTO 2023

💀 $polylog(L)$ [BCFL23] — TCC 2023

💀 [WW23] Knowledge K-R-ISIS — ASIACRYPT 2023

[DFS24] Quantum attack on knowledge K-R-ISIS and more (!) — Eprint 2024

Prior works

Functional commitment [LRY16]:
a
rove

Provide an **interactive** split-and-fold evaluation proof and make it non-interactive via Fiat-Shamir transform.

$polylog(L)$ $polylog(L)$

[DFS24]
Quantum attack on knowledge K-R-ISIS and more (!)

$polylog(L)$

[FLV23]

[ACLMT22]

[CLM23]

[BCFL23]

[WW23]
Knowledge K-R-ISIS

CRYPTO 2018	CRYPTO 20-21	CRYPTO 2022	CRYPTO 2023	TCC 2023	JoC	ASIACRYPT 2023	Eprint 2024	EUROCRYPT 2024
[BBCGL18]	[BLNS20] [ACK21] [AL21] [BCS21]	[NS22]	[CLM23] [BCS23] [BS23]		[FMN23]			[AFLN23]
$O(\sqrt{L})$	$polylog(L)$	$O(\sqrt{L})$	$polylog(L)$		$polylog(L)$			$polylog(L)$

Prior works

Functional commitment [LRY16]: … a … rove

Provide an **interactive** split-and-fold evaluation proof and make it non-interactive via Fiat-Shamir transform.

CRYPTO 2018: [BBCGL18] — $O(\sqrt{L})$

CRYPTO 20-21: [BLNS20], [ACK21], [AL21], [BCS21] — $polylog(L)$

CRYPTO 2022: [ACLMT22] 💀 $polylog(L)$; [NS22] — $O(\sqrt{L})$

CRYPTO 2023: [FLV23], [CLM23] 💀 $polylog(L)$; [CLM23], [BCS23], [BS23] — $polylog(L)$

TCC 2023: [BCFL23] 💀 $polylog(L)$

JoC: [FMN23] — $polylog(L)$

ASIACRYPT 2023: 💀 [WW23] Knowledge K-R-ISIS

Eprint 2024: [DFS24] Quantum attack on knowledge K-R-ISIS and more (!)

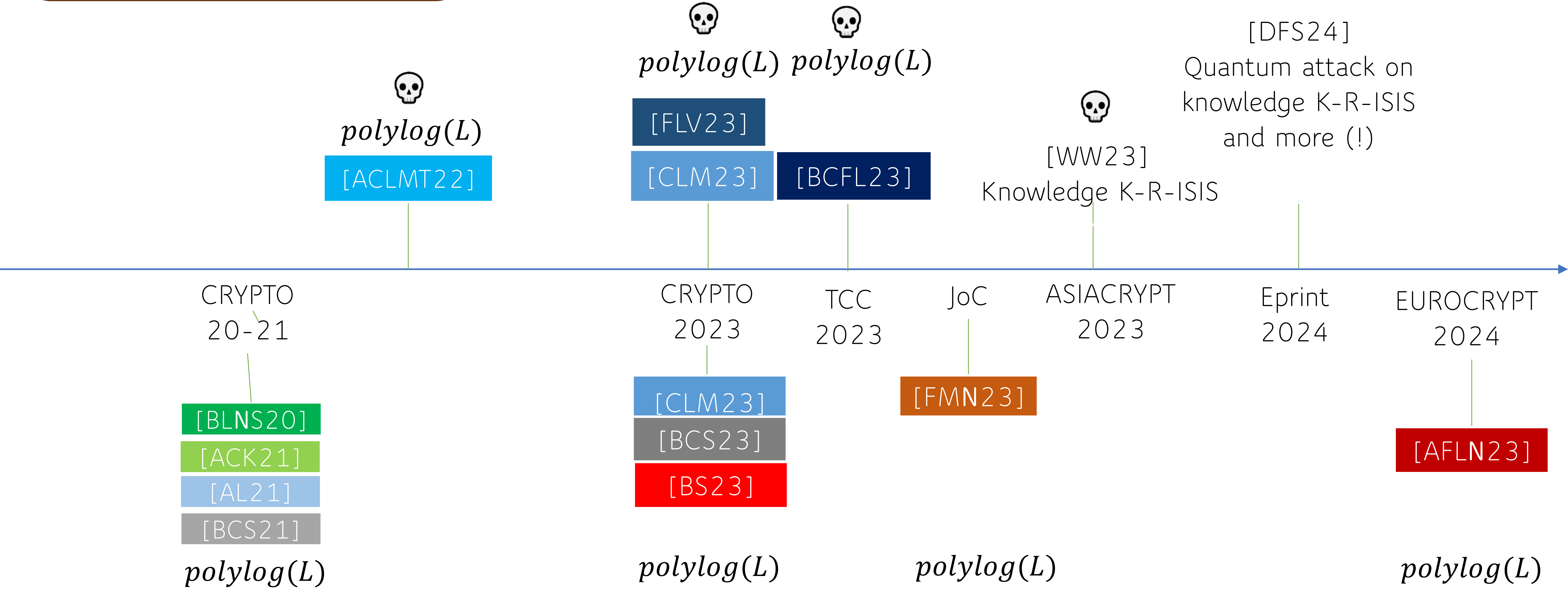
EUROCRYPT 2024: [AFLN23] — $polylog(L)$

Prior works

Functional commitment [I

Provide an **interactive** split fold evaluation proof and mak non-interactive via Fiat-Shamir transform.

✓ succinct (polylog) sizes



Prior works

Functional commitment [L

Provide an **interactive** split fold evaluation proof and mak non-interactive via Fiat-Shamir transform.

✔ succinct (polylog) sizes

[ACLMT22] — 💀 $polylog(L)$

[FLV23] [CLM23] — 💀 $polylog(L)$

[BCFL23] — 💀 $polylog(L)$

💀 [WW23] Knowledge K-R-ISIS

[DFS24] Quantum attack on knowledge K-R-ISIS and more (!)

CRYPTO 2023

TCC 2023

JoC

ASIACRYPT 2023

Eprint 2024

EUROCRYPT 2024

[CLM23] [BCS23] — $polylog(L)$

[FMN23] — $polylog(L)$

[AFLN23] — $polylog(L)$

Prior works

Functional commitment [...

Provide an interac... fold evaluatio... non-interac... tr...

✓ succinct (polylog) sizes

✓ fast verifier

$polylog(L)$
[ACLMT22]

$polylog(L)$ $polylog(L)$
[FLV23]
[CLM23] [BCFL23]

[WW23]
Knowledge K-R-ISIS

[DFS24]
Quantum attack on knowledge K-R-ISIS and more (!)

CRYPTO 2023

TCC 2023

JoC

ASIACRYPT 2023

Eprint 2024

EUROCRYPT 2024

[CLM23]
[BCS23]

[FMN23]

[AFLN23]

$polylog(L)$ $polylog(L)$ $polylog(L)$

Prior works

ent [

Pr
fold evalu
non-interac
tr

✓ standard assumptions (+ROM)

✓ succinct (polylog) sizes

✓ fast verifier

CRYPTO 2023

[BCS23]

$polylog(L)$

EUROCRYPT 2024

[AFLN23]

$polylog(L)$

Prior works

- ✓ standard assumptions (+ROM)
- ✓ succinct (polylog) sizes
- ✓ fast verifier
- ✓ transparent setup

CRYPTO 2023

[BCS23]

$polylog(L)$

Prior works

ent [

Pr

✓ standard assumptions (+ROM)

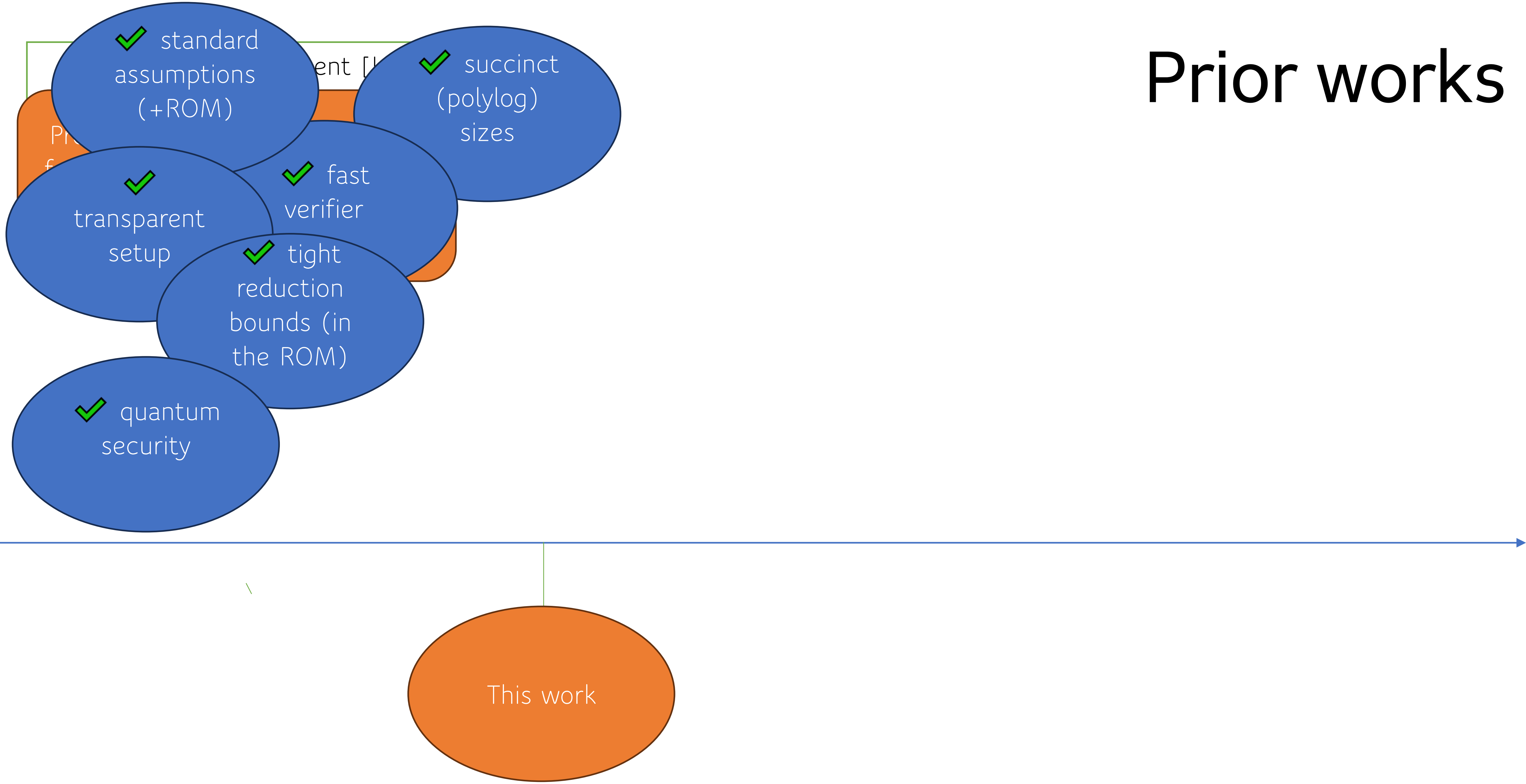
✓ succinct (polylog) sizes

✓ fast verifier

✓ transparent setup

✓ tight reduction bounds (in the ROM)

Prior works



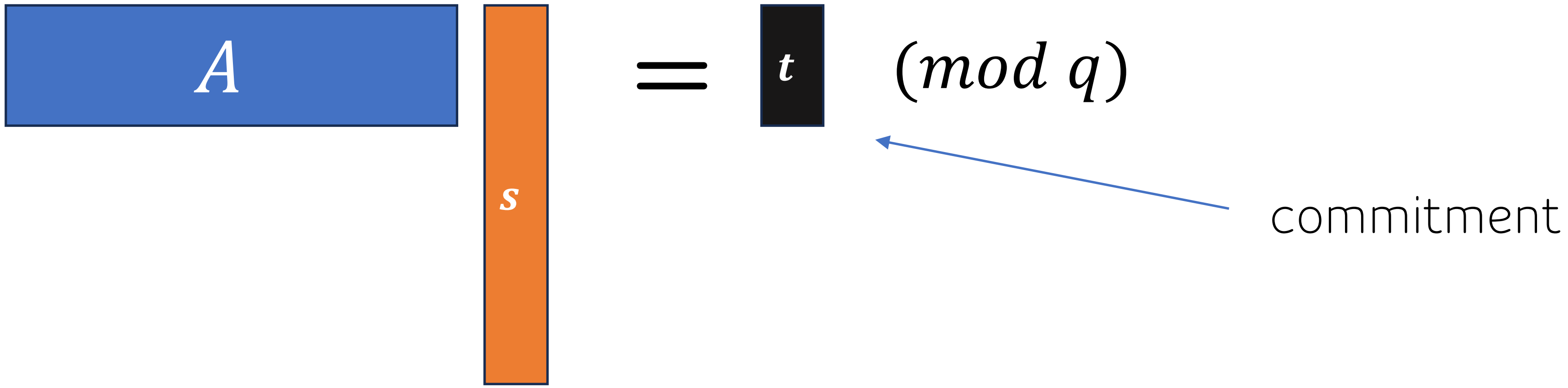
✓ standard assumptions (+ROM)
✓ succinct (polylog) sizes
✓ fast verifier
✓ transparent setup
✓ tight reduction bounds (in the ROM)
✓ quantum security
This work

Outline

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

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:



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:

$$A \, \boldsymbol{s} = \boldsymbol{t} \quad (mod\ q)$$

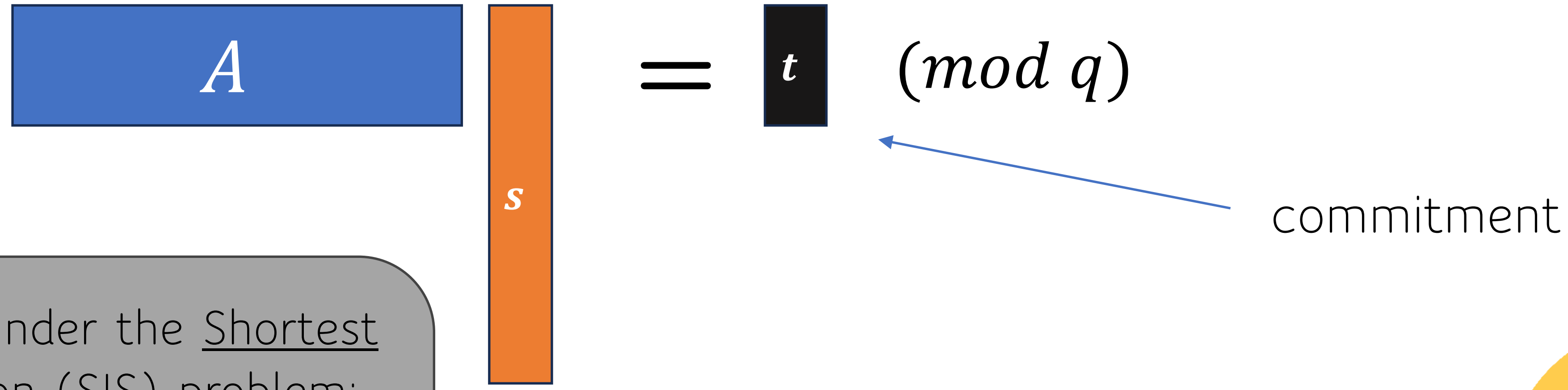
commitment

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

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

Can we build a polynomial commitment from this?
- More structure to $\boldsymbol{A}$ [CLM23]?
- Preprocessing [BCS23]?

Ajtai commitment for large messages

- Let $G_n = \begin{bmatrix} [1\ 2\ 4\ \ \ldots 2^{\log q}] & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & [1\ 2\ 4\ \ \ldots 2^{\log q}] \end{bmatrix} \in \mathbb{Z}_q^{n \times n \log q}$

- The binary decomposition function $G_n^{-1}\colon \mathbb{Z}_q^n \to \mathbb{Z}_q^{n \log q}$ satisfies for any $\boldsymbol{f} \in \mathbb{Z}_q^n$:

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

We will ignore the subscript.

Ajtai commitment for large messages

- Let $G_n = \begin{bmatrix} [1\ 2\ 4\ \ldots\ 2^{\log q}] & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & [1\ 2\ 4\ \ldots\ 2^{\log q}] \end{bmatrix} \in \mathbb{Z}_q^{n \times n \log q}$

- 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

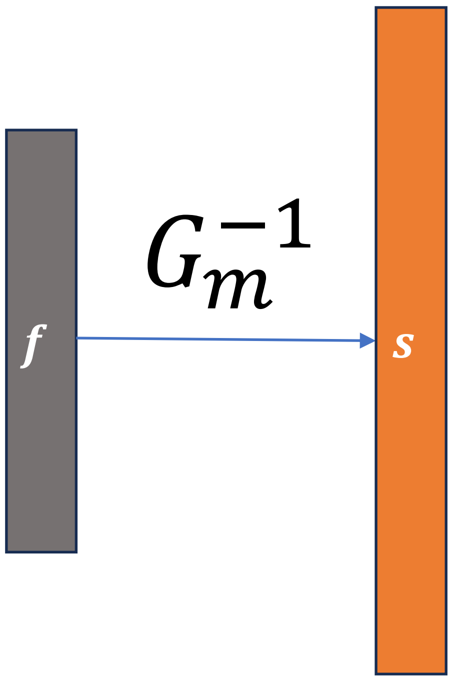
We will ignore the subscript.

Ajtai commitment for large messages

To commit to any message vector $\boldsymbol{f} \in \mathbb{Z}_q^m$, we compute:

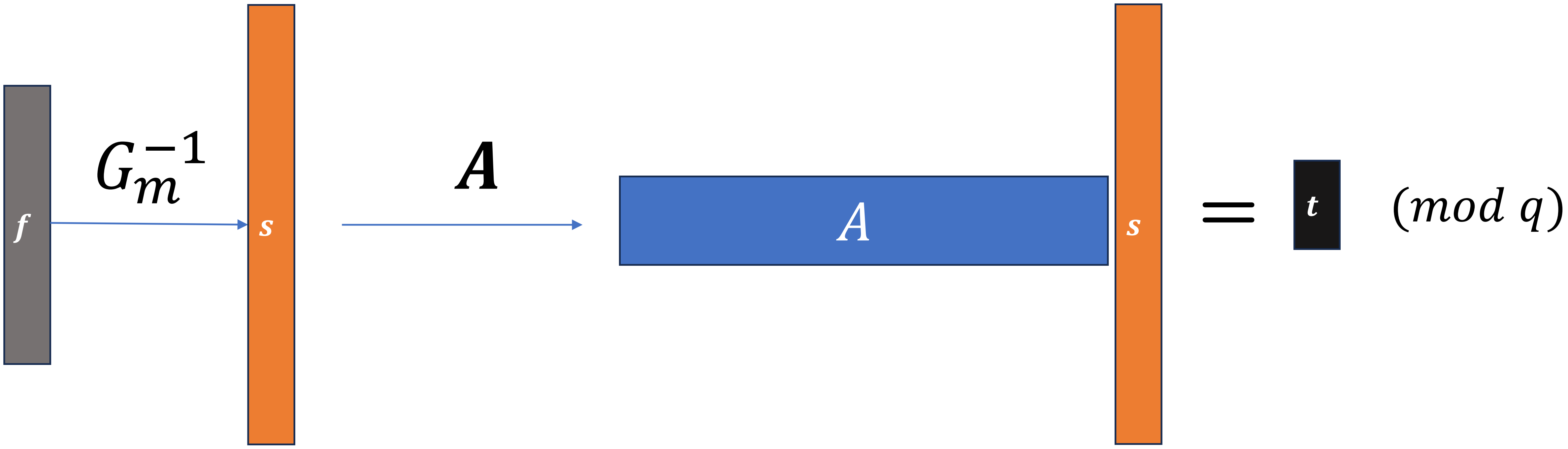
Ajtai commitment for large messages

To commit to any message vector $\boldsymbol{f} \in \mathbb{Z}_q^m$, we compute:



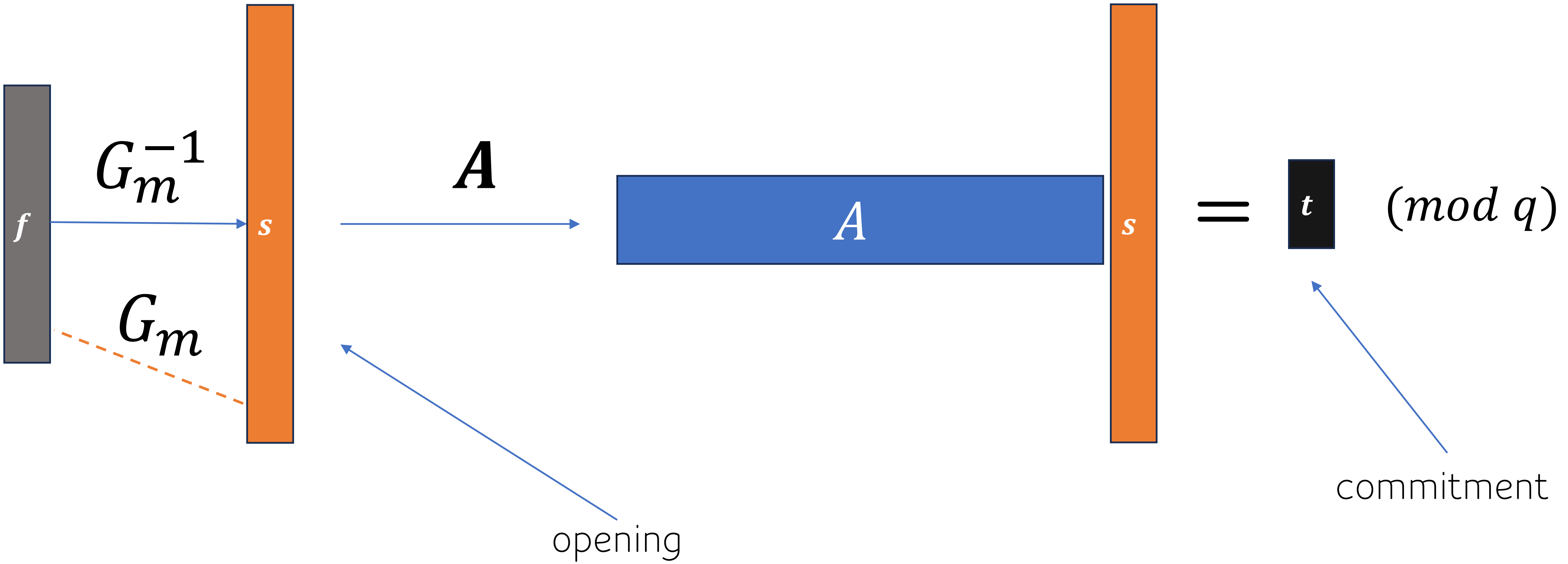
Ajtai commitment for large messages

To commit to any message vector $\boldsymbol{f} \in \mathbb{Z}_q^m$, we compute:



Ajtai commitment for large messages

To commit to any message vector $\boldsymbol{f} \in \mathbb{Z}_q^m$, we compute:

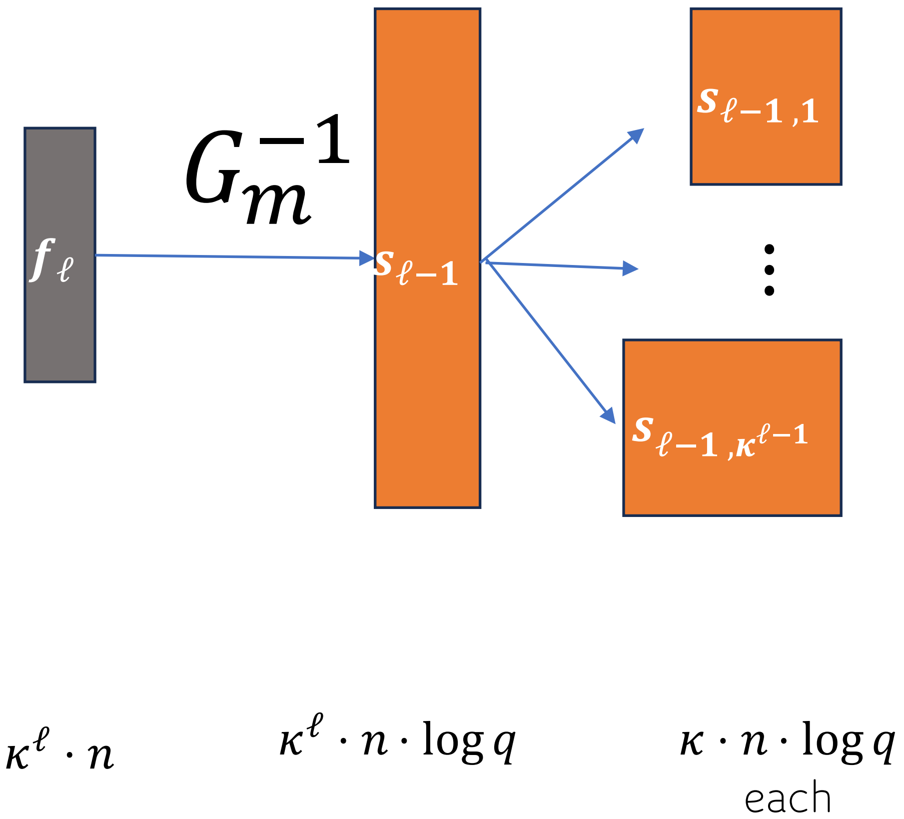


Many-to-one Ajtai commitment

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

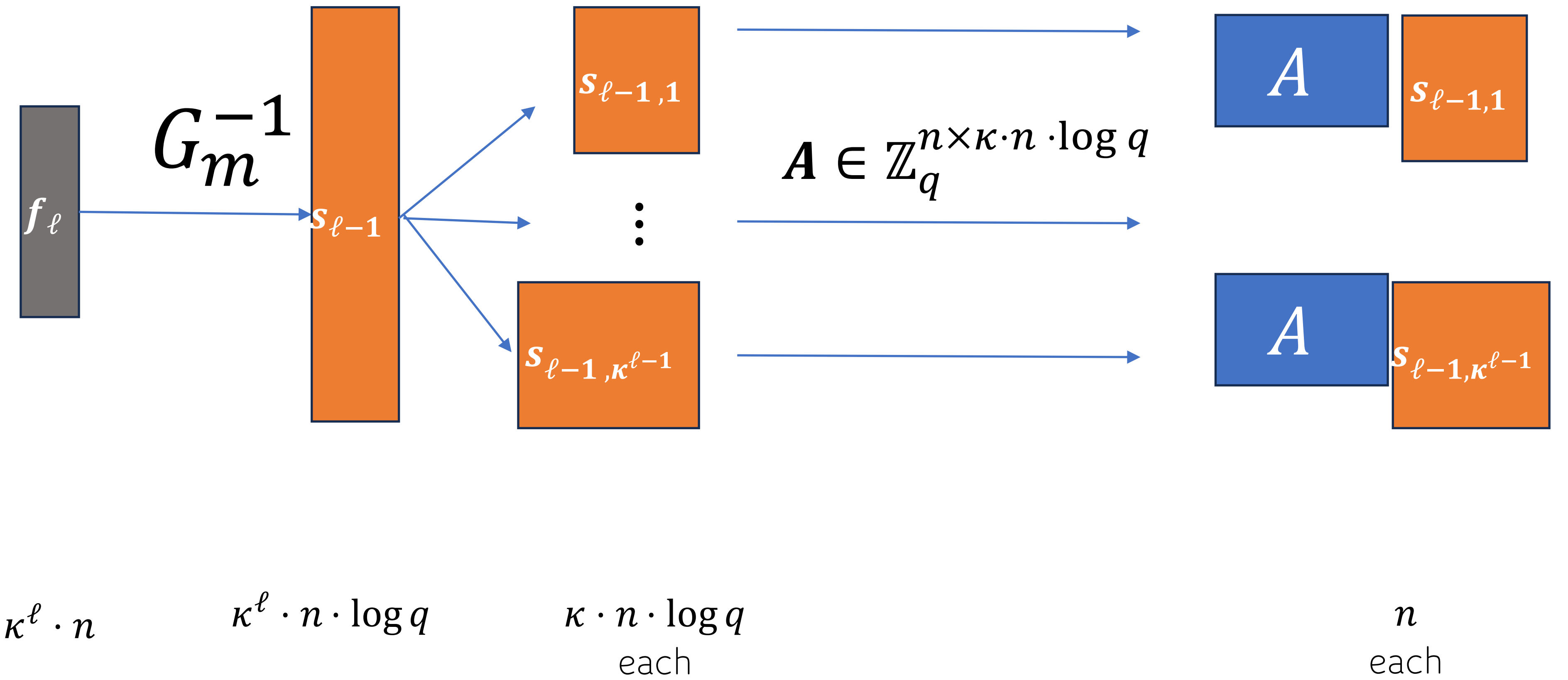
Many-to-one Ajtai commitment

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:



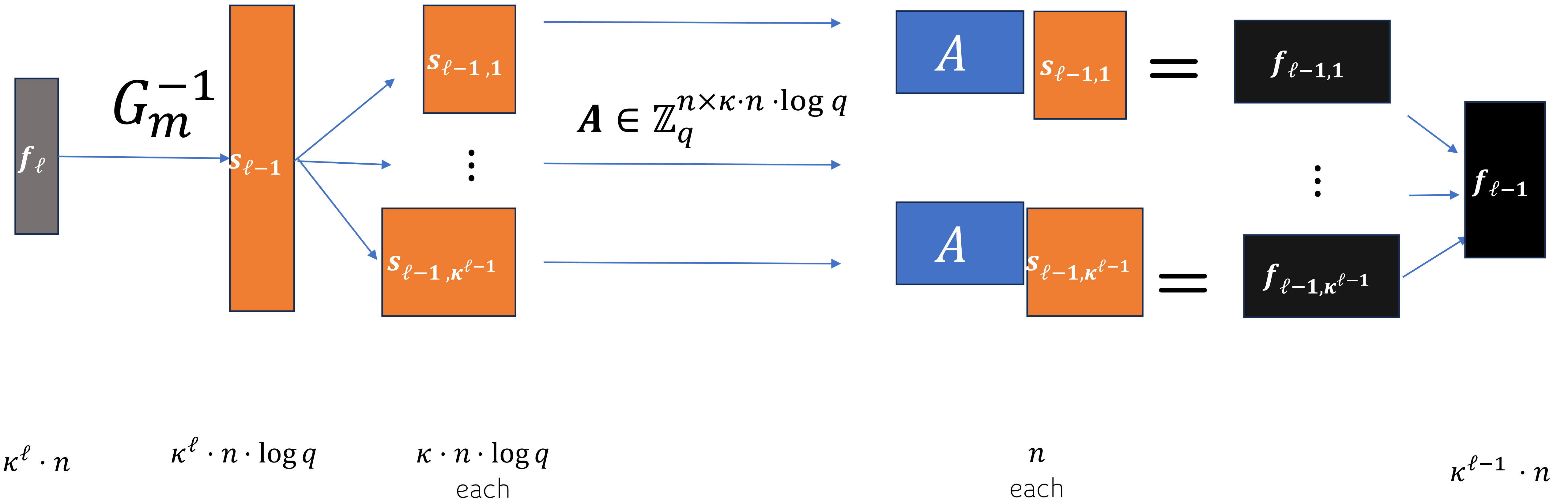
Many-to-one Ajtai commitment

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:



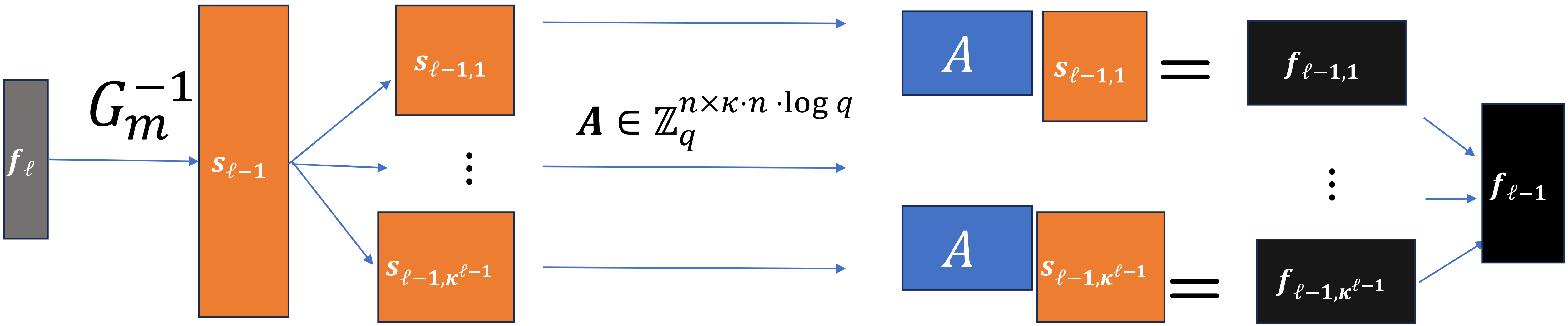
Many-to-one Ajtai commitment

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:



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

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

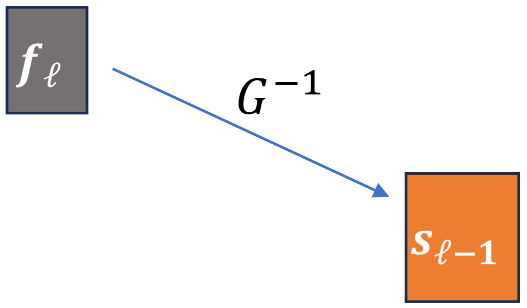
$(\boldsymbol{I}_{\kappa^{\ell-1}} \otimes \boldsymbol{A})\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_{\ell-1} = (\boldsymbol{I}_{\kappa^{\ell-1}} \otimes \boldsymbol{A})\boldsymbol{s'}_{\ell-1}$

Breaking SIS

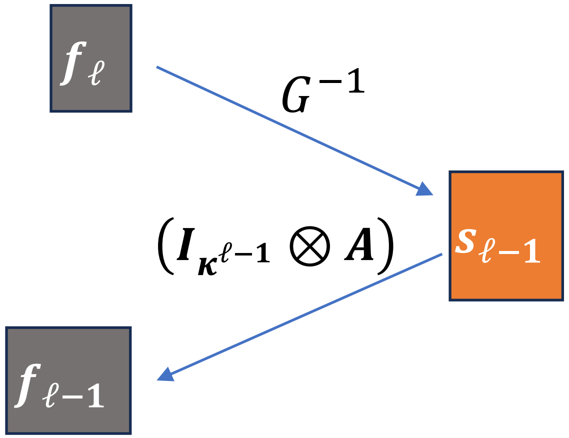
Our commitment scheme

f_ℓ

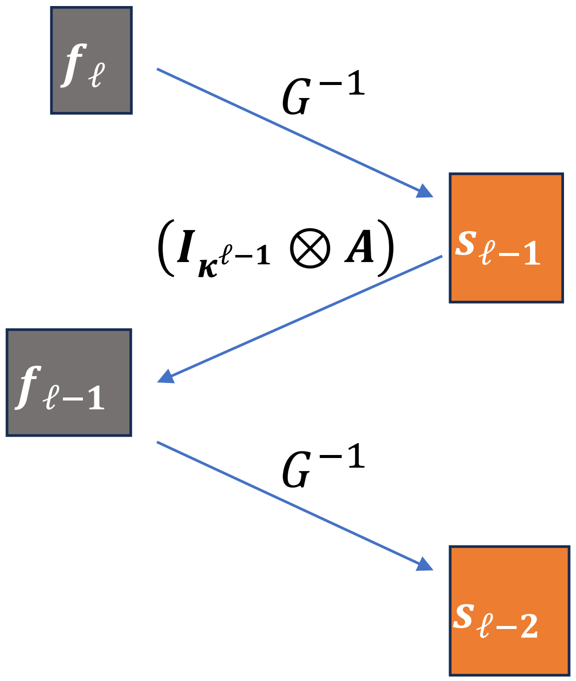
Our commitment scheme



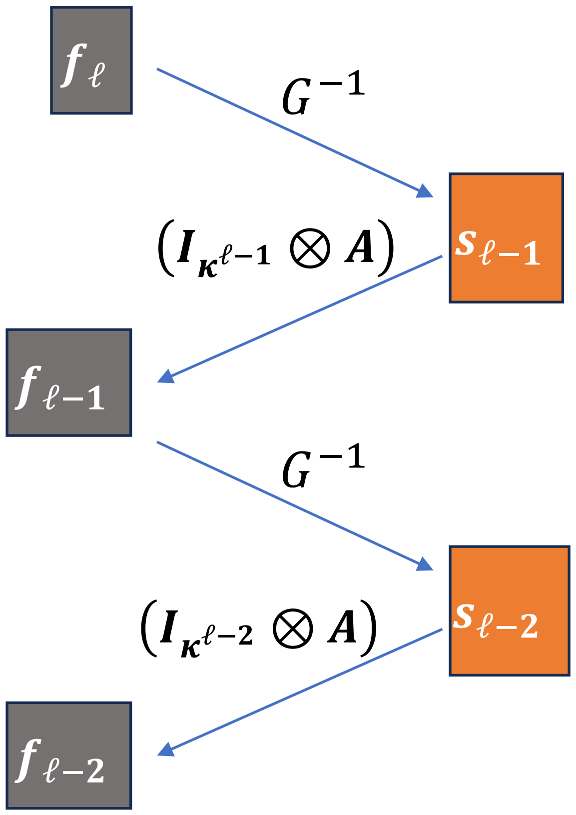
Our commitment scheme



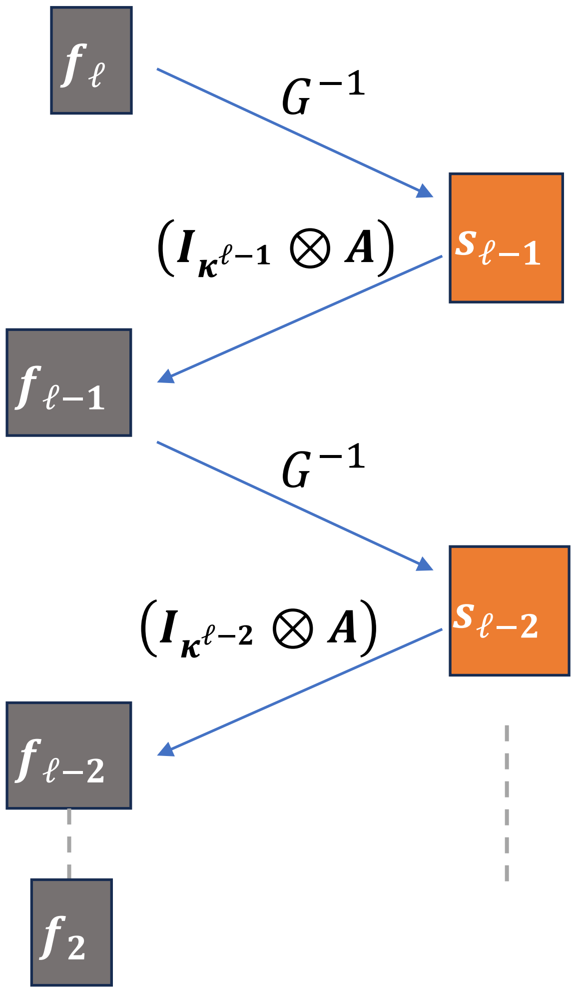
Our commitment scheme



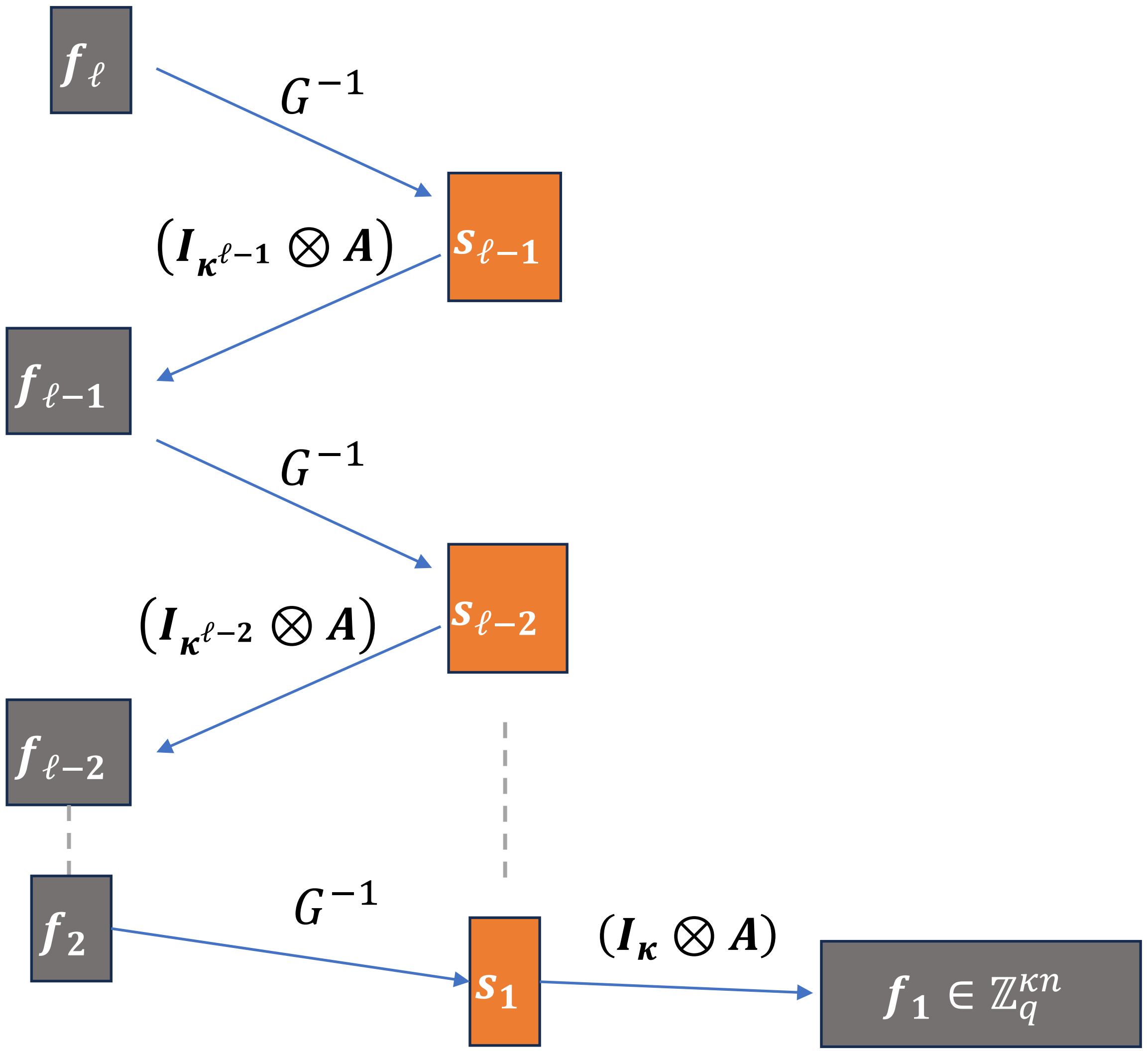
Our commitment scheme



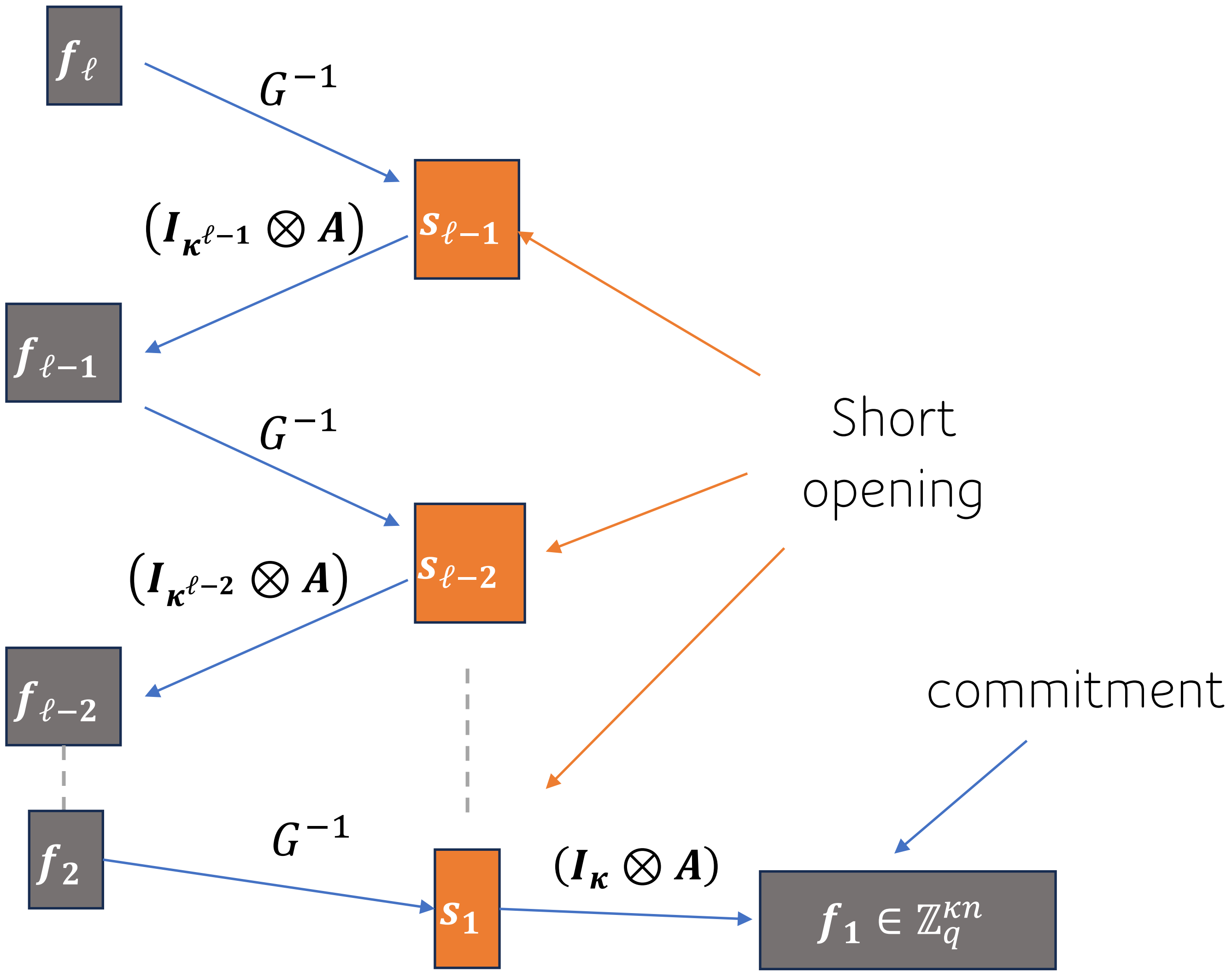
Our commitment scheme



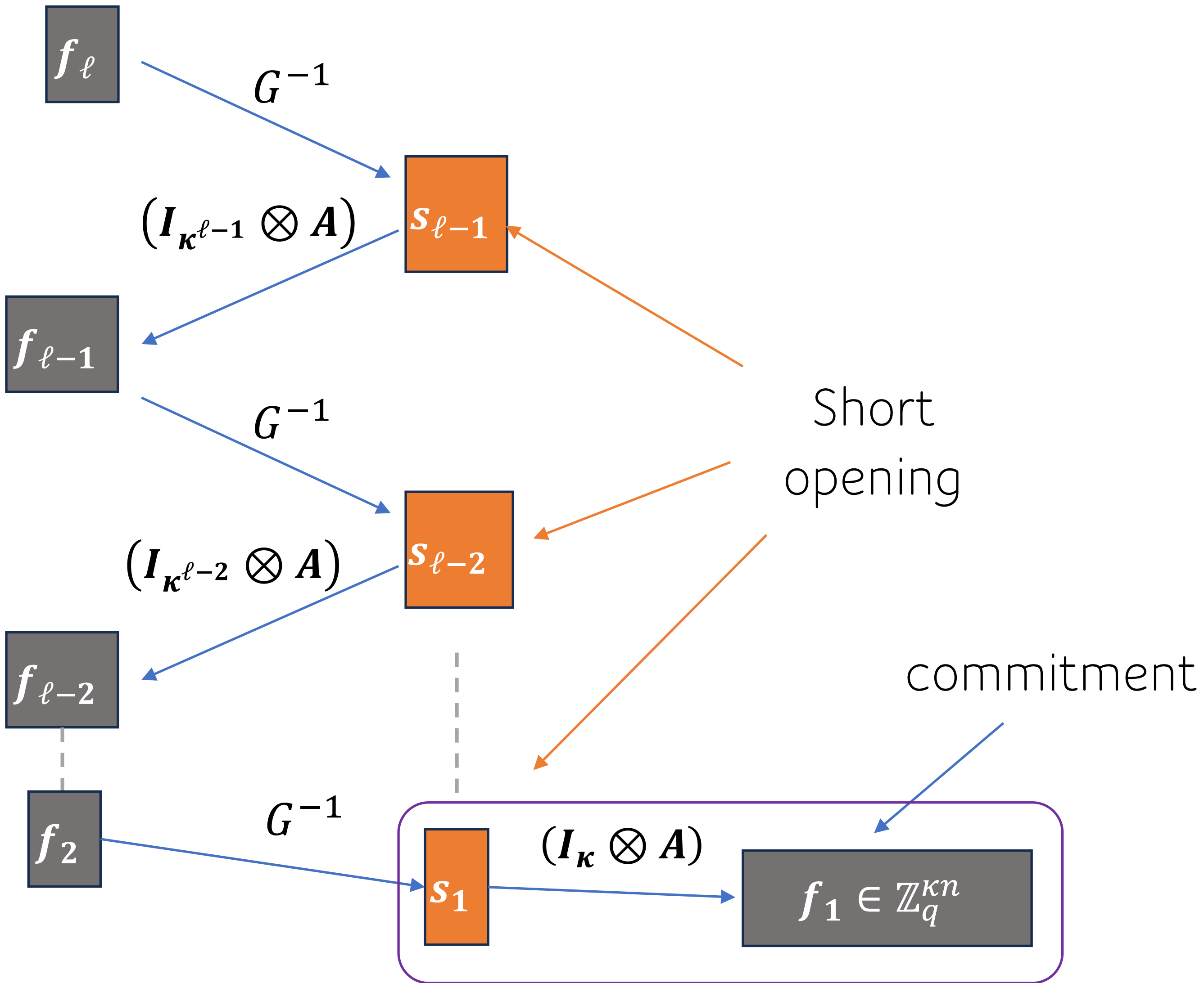
Our commitment scheme



Our commitment scheme

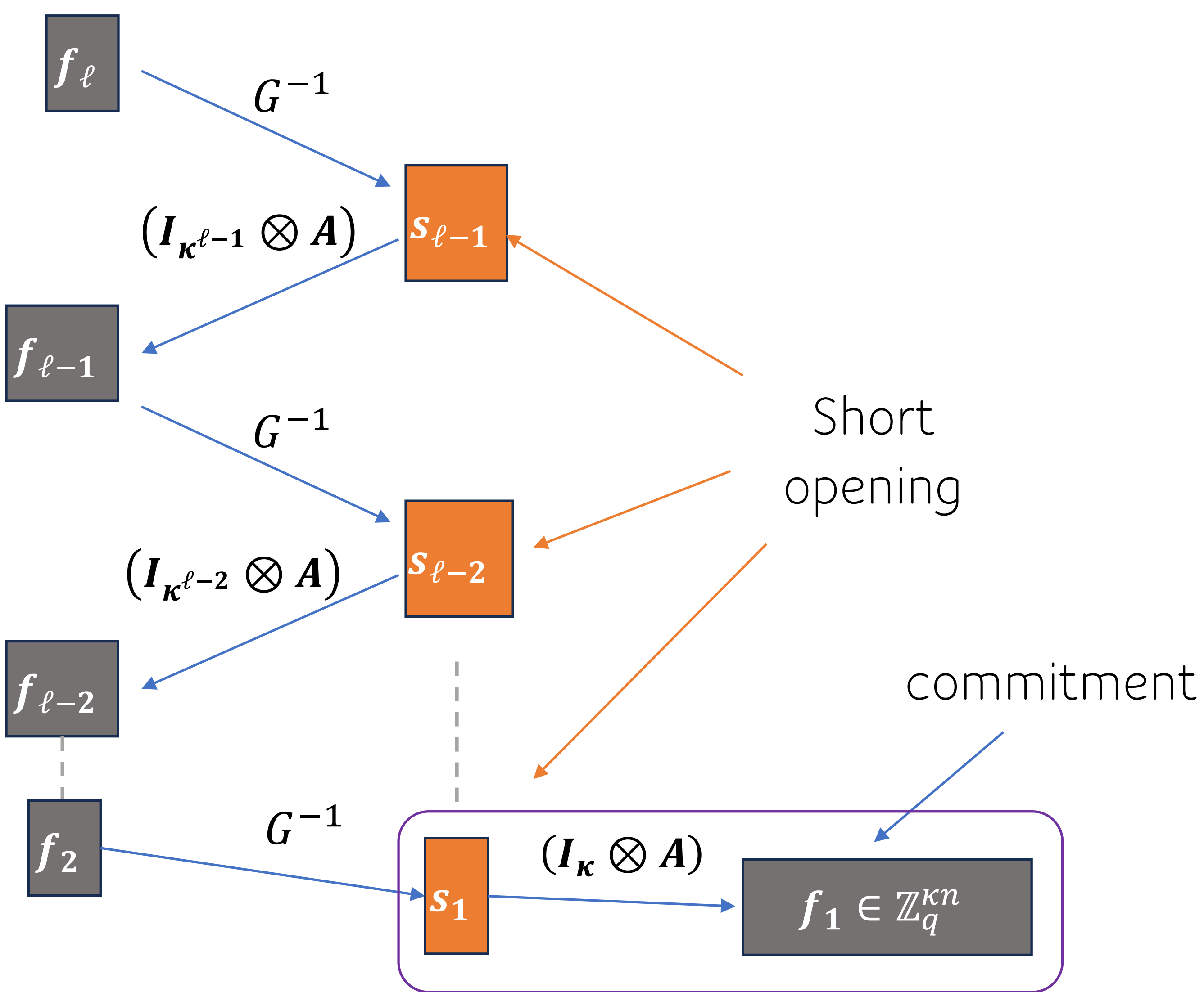


Our commitment scheme



Opening to a commitment $t = f_1$: message f_ℓ and short $s_1, \ldots, s_{\ell-1}$ s.t.

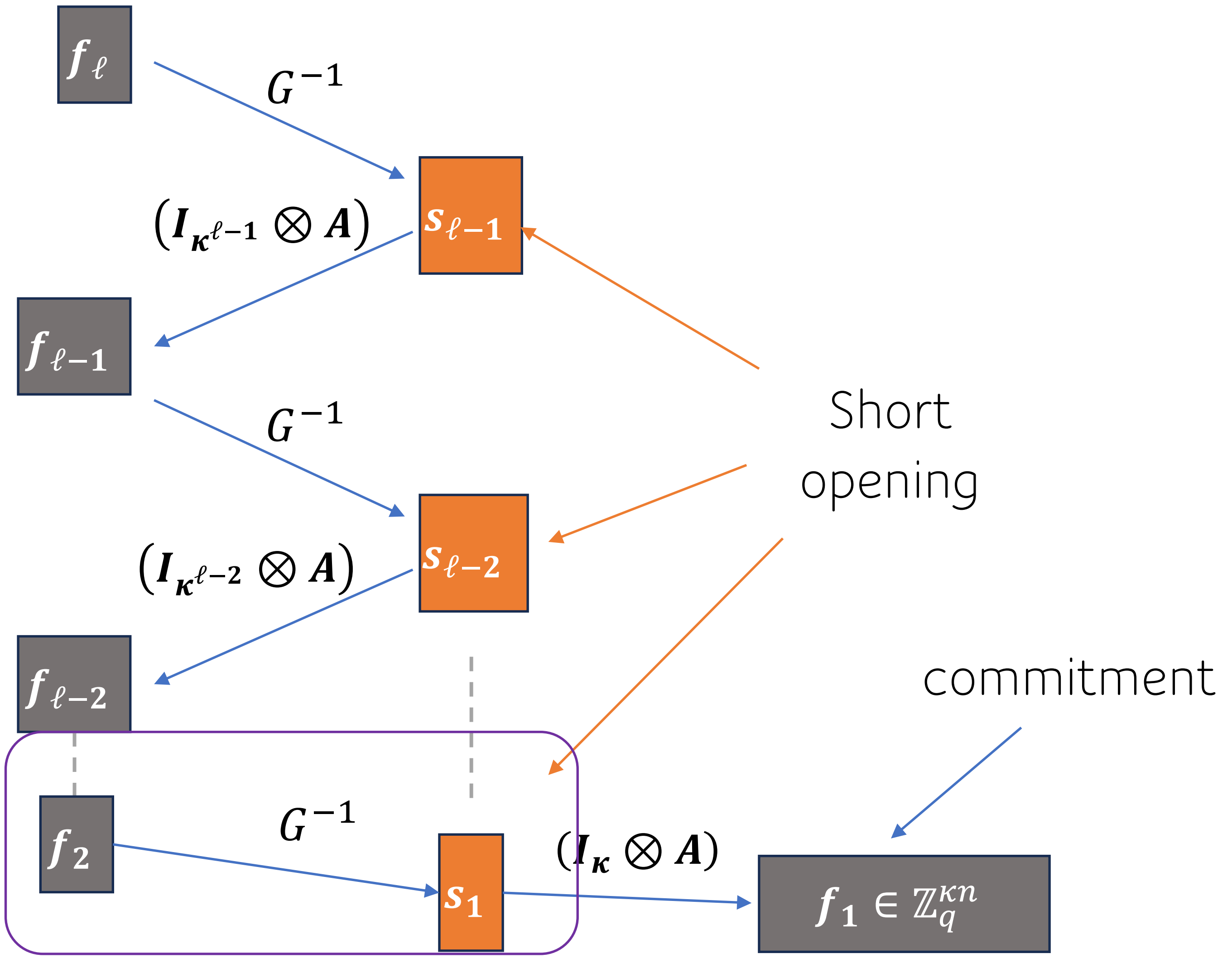
Our commitment scheme



Opening to a commitment $t = f_1$: message f_ℓ and short $s_1, \ldots, s_{\ell-1}$ s.t.

$$(I_{\kappa^1} \otimes A)s_1 = f_1$$

Our commitment scheme

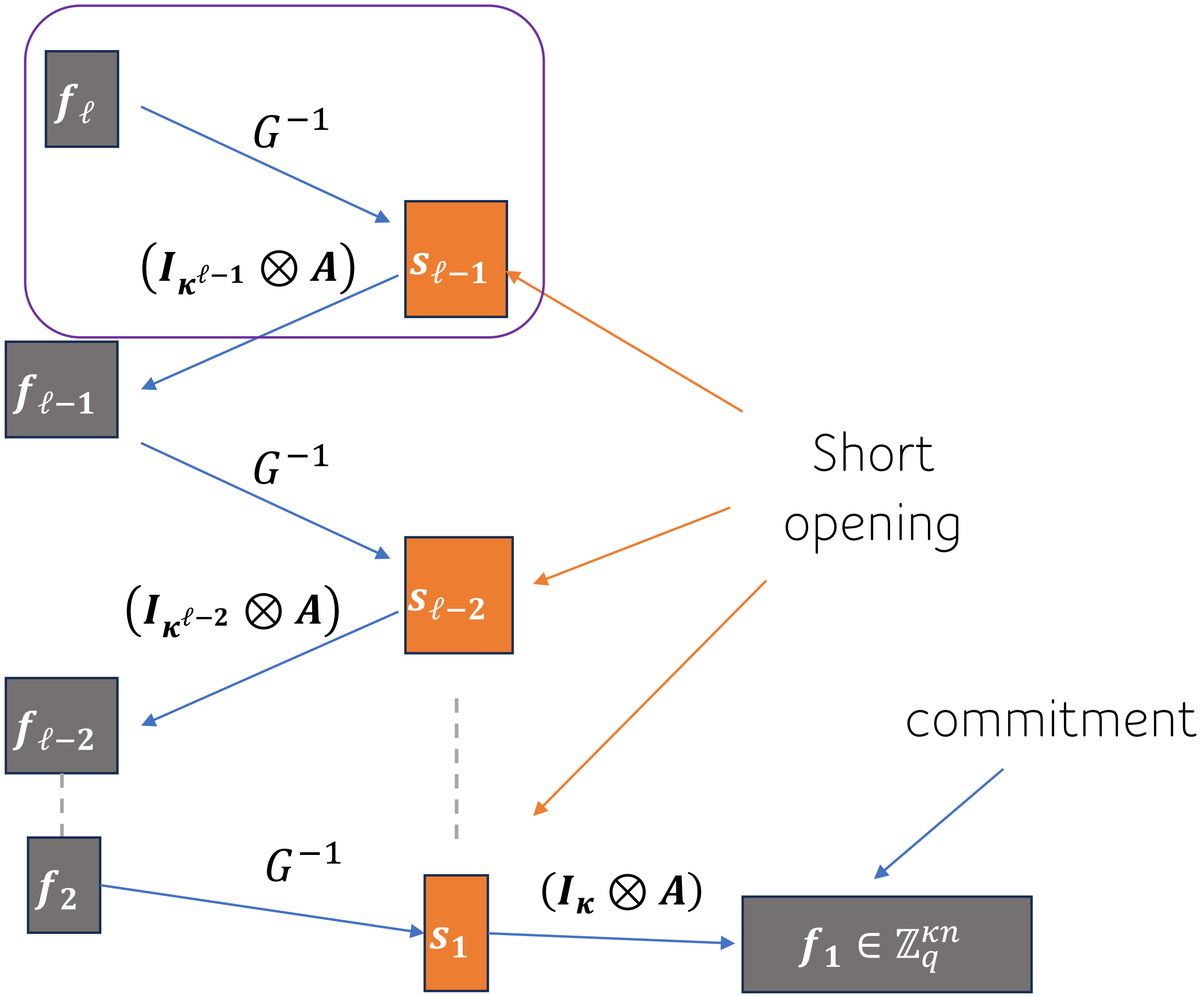


Opening to a commitment $t = f_1$: message f_ℓ and short $s_1, \ldots, s_{\ell-1}$ s.t.

$$f_2 := G s_1$$
$$(I_{\kappa^2} \otimes A) s_2 = f_2$$

$$(I_{\kappa^1} \otimes A) s_1 = f_1$$

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.

$$G s_{\ell-1} = f_\ell$$

$$f_{\ell-1} := G s_{\ell-2}$$
$$(I_{\kappa^{\ell-1}} \otimes A) s_{\ell-1} = f_{\ell-1}$$

$$f_2 := G s_1$$
$$(I_{\kappa^2} \otimes A) s_2 = f_2$$

$$(I_{\kappa^1} \otimes A) s_1 = f_1$$

Why is our scheme interesting

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 $(\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{G}\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{f}_2$

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.

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

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

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

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

Why is our scheme interesting

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

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

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

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

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

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

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.

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

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

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

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

Opening proof

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

valid opening $\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \ldots, \boldsymbol{r}_{\ell-2})$ 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: $\kappa^3 n \log q$

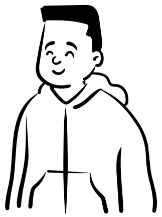
$\vdots$

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

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

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

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



$\boldsymbol{t}$

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: $\kappa^2 n \log q$

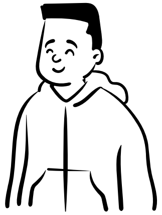
$\boldsymbol{r}_2 = (\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa^2 n \log q})\boldsymbol{s}_3$ — Length: $\kappa^3 n \log q$

⋮

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

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

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



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

$\boldsymbol{s}_1 \in \mathbb{Z}_q^{\kappa^2 n \log q}$ →

← $\boldsymbol{C}$

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

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

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

Opening proof

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

$\Downarrow$

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

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

$\boldsymbol{r}_2 = \left(\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa^2 n \log q}\right)\boldsymbol{s}_3$ 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: $\kappa^{\ell-1} n \log q$

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

Which $\boldsymbol{C}$ to choose?

Easy, pick binary coefficients.

Opening proof

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

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

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

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

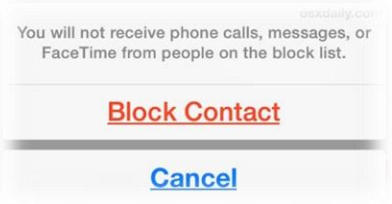
$\boldsymbol{r}_{\ell-2} = \left(\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa^{\ell-2} n \log q}\right)\boldsymbol{s}_{\ell-1}$ Length: $\kappa^{\ell-1} n \log q$

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

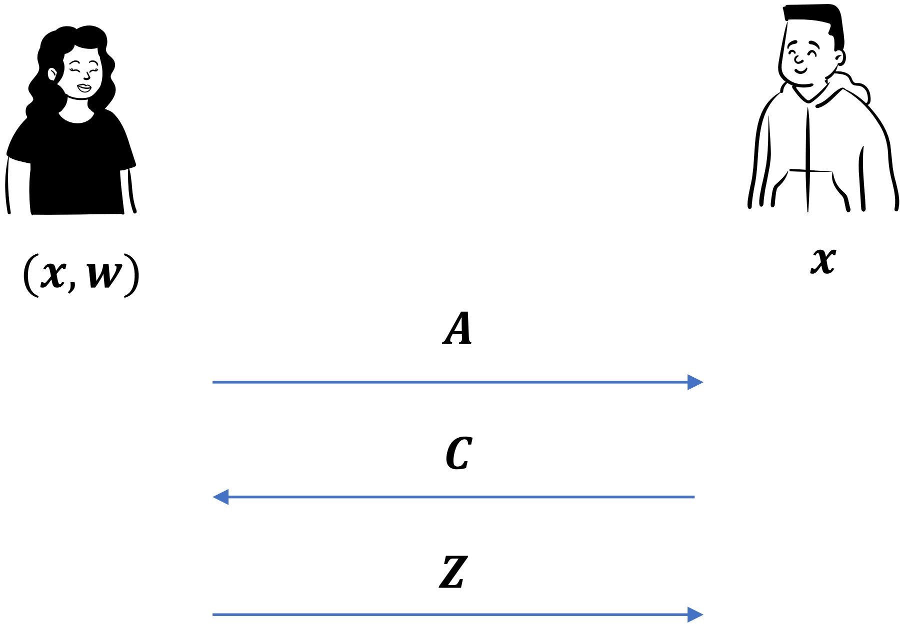
Which $\boldsymbol{C}$ to choose?

Easy, pick binary coefficients.

But what about knowledge soundness? 🤔



Coordinate-wise special soundness

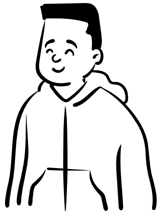


Special soundness: given two valid transcripts (A, C, Z) and (A, C', Z') with different $C \neq C'$, one can extract w.

⋮

Coordinate-wise special soundness

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



$\boldsymbol{x}$

$\boldsymbol{A}$ →

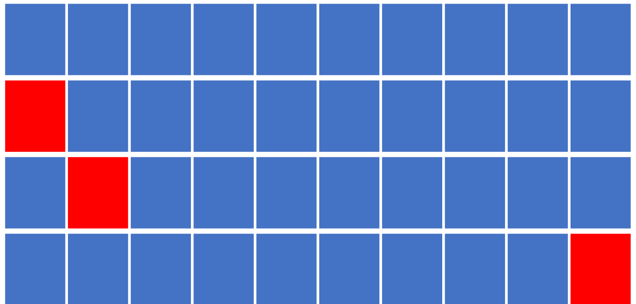
$\boldsymbol{C}$ ← $\boldsymbol{C} \leftarrow S^t$

$\boldsymbol{Z}$ →

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

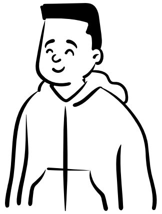
$\boldsymbol{c}_0$
$\boldsymbol{c}_1$
$\boldsymbol{c}_2$
⋮
$\boldsymbol{c}_t$



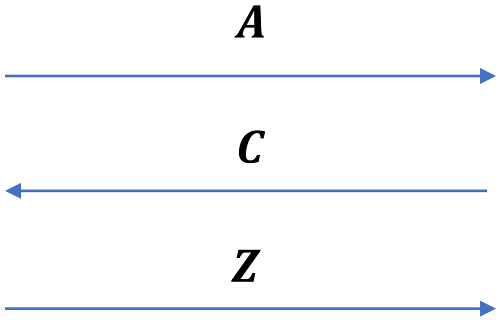
one can extract $\boldsymbol{w}$.

Coordinate-wise special soundness

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



$\boldsymbol{x}$

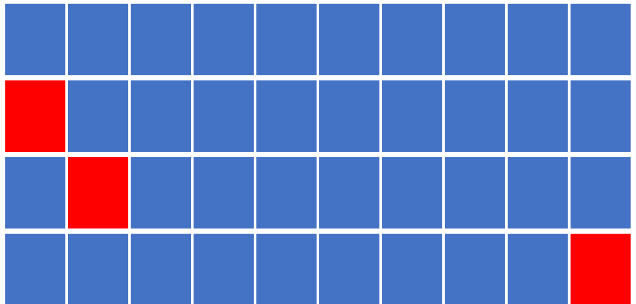


$\boldsymbol{C} \leftarrow S^t$

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

$\boldsymbol{c}_0$
$\boldsymbol{c}_1$
$\boldsymbol{c}_2$
$\vdots$
$\boldsymbol{c}_t$



one can extract $\boldsymbol{w}$.

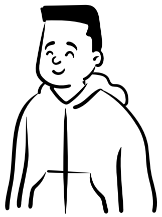
[FMN23]: CWSS implies knowledge soundness with error $t/|S|$.

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 $(\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{G}\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{f}_1$

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



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

$\boldsymbol{t}$

$\boldsymbol{s}_1 \in \mathbb{Z}_q^{\kappa^2 n \log q}$ →

$\boldsymbol{C}$ ←

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

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

$\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \dots, \boldsymbol{r}_{\ell-2})$ →

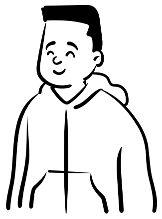
Opening proof

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

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

- 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 $\boldsymbol{t} = \boldsymbol{f}_1$



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

$\boldsymbol{s}_1 \in \mathbb{Z}_q^{\kappa^2 n \log q}$ →

$\boldsymbol{C}$ ←

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

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

$\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \ldots, \boldsymbol{r}_{\ell-2})$ →

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 $(\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{G}\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{f}_1$

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

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

$\boldsymbol{t}$

$\boldsymbol{s}_1 \in \mathbb{Z}_q^{\kappa^2 n \log q}$ →

$\boldsymbol{C}$ ←

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

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

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

Opening proof

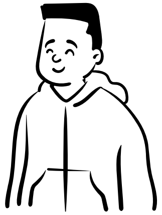
Folding property: given any matrix $\boldsymbol{C} \in \mathbb{Z}_q^{\kappa \times \kappa^2}$ and a valid opening $\boldsymbol{f}_\ell, (\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{\ell-1})$ for a commitment $\boldsymbol{t}$

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

Communication complexity:

- $\mathrm{O}(\kappa^2 n \log q)$ elements over $\mathbb{Z}_q$ per round
- there are $\mathrm{O}(\ell)$ rounds
- total proof size is $\mathrm{O}(\ell \kappa^2 n \log q)$ $\mathbb{Z}_q$-elements

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



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

$\boldsymbol{t}$

$\boldsymbol{s}_1 \in \mathbb{Z}_q^{\kappa^2 n \log q}$ →

← $\boldsymbol{C}$

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

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

Prove knowledge of an opening $\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \ldots, \boldsymbol{r}_{\ell-2})$ to the commitment $(\boldsymbol{C} \otimes \mathrm{I}_n)\boldsymbol{G}\boldsymbol{s}_1$

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:

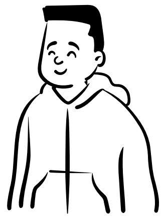
- $\mathrm{O}(\kappa^2 n \log q)$ elements over $\mathbb{Z}_q$ per round
- there are $\mathrm{O}(\ell)$ rounds
- total proof size is $\mathrm{O}(\ell \kappa^2 n \log q)$ $\mathbb{Z}_q$-elements

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

Take $n, \kappa \in O(\lambda)$. Then $\ell = O\left(\frac{\log L}{\log \lambda}\right) = O(1)$ …

Polylogarithmic proof size!

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



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

$\boldsymbol{s}_1 \in \mathbb{Z}_q^{\kappa^2 n \log q}$ →

$\boldsymbol{C}$ ←

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

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

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

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
  - Quantum security

Future work:
- Space efficiency – streaming polynomial commitments?
- Concrete efficiency for the integer construction?
- Tighter quantum reduction?

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

Thank you!

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