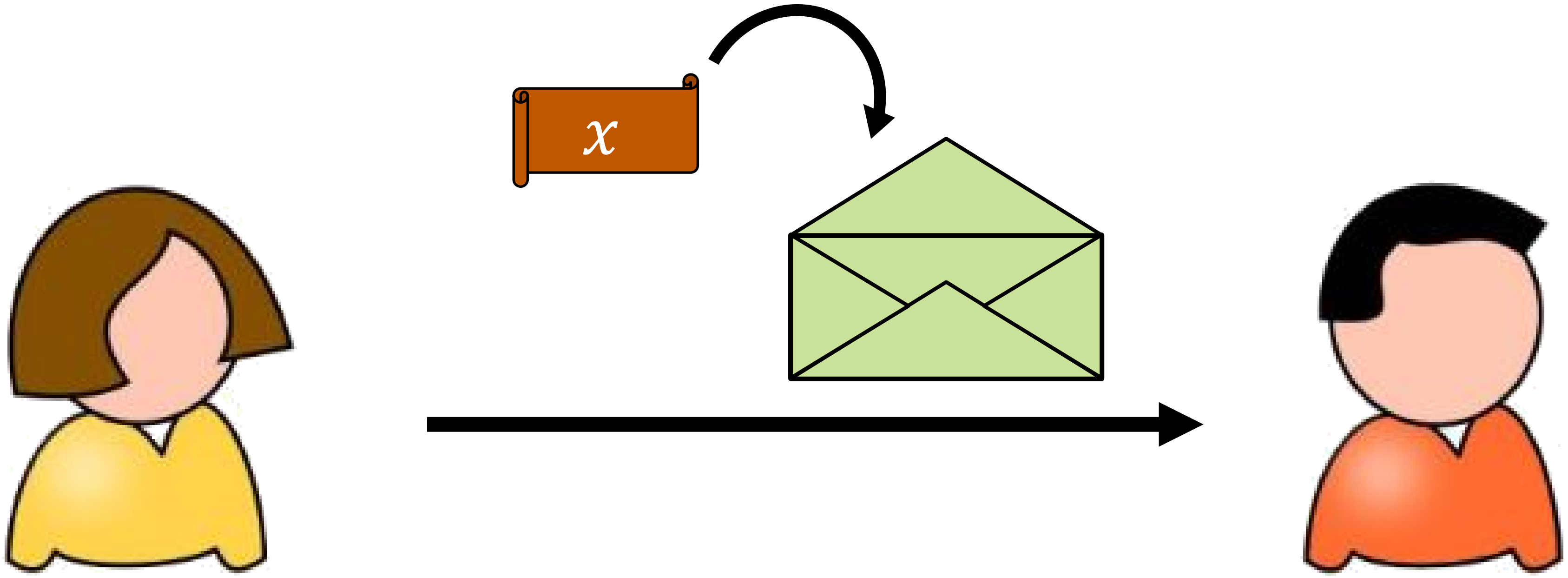
Succinct Vector, Polynomial, and Functional Commitments from Lattices

Hoeteck Wee and David Wu

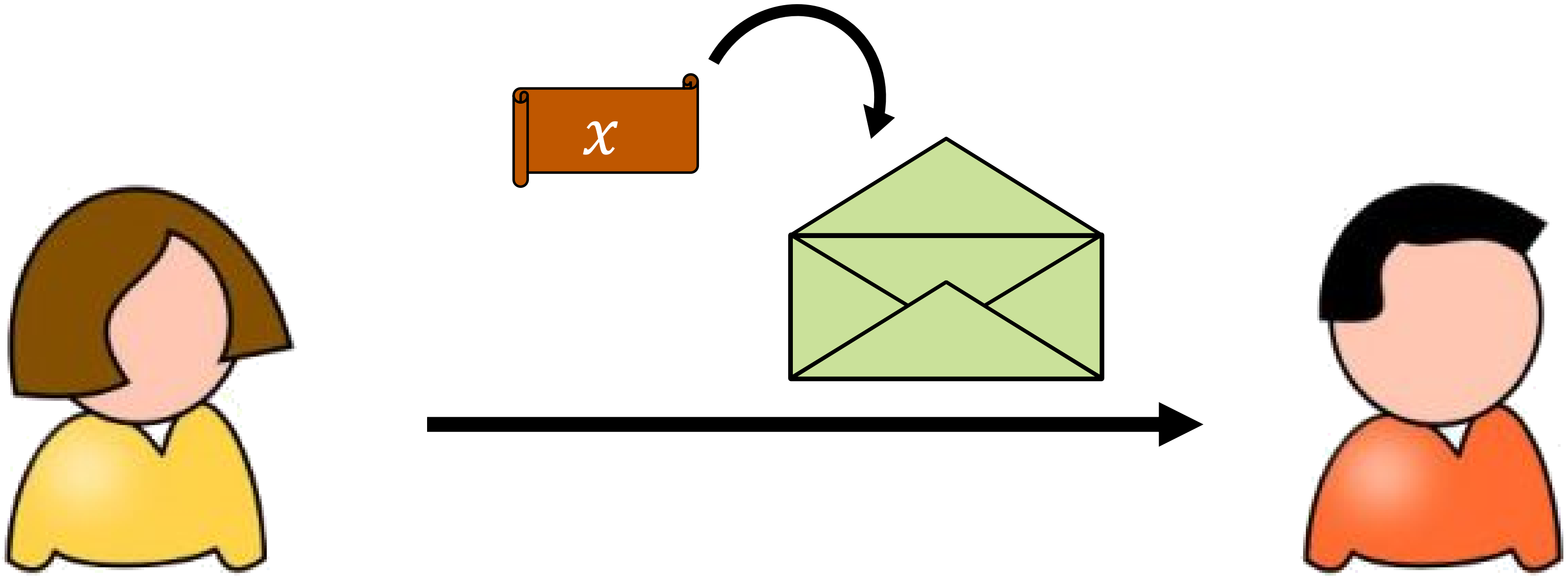
April 2023

Commitment Schemes



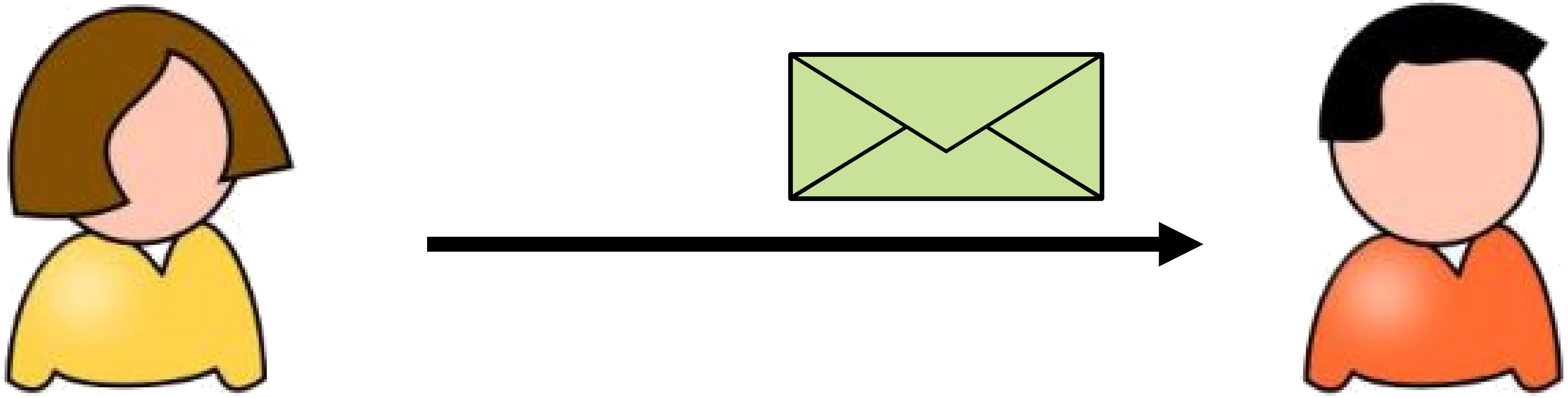
cryptographic analog of a sealed envelope

Commitment Schemes



cryptographic analog of a sealed envelope

Commitment Schemes



cryptographic analog of a sealed envelope

Commitment Schemes

$$\mathrm{Commit}(\mathrm{crs}, x) \to (\sigma, \mathrm{st})$$

Takes a common reference string and commits to a message

Outputs commitment σ and commitment state st

Commitment Schemes

$\mathrm{Commit}(\mathrm{crs}, x) \to (\sigma, \mathrm{st})$

$\mathrm{Open}(\mathrm{st}) \to \pi$

Takes the commitment state and outputs an opening π

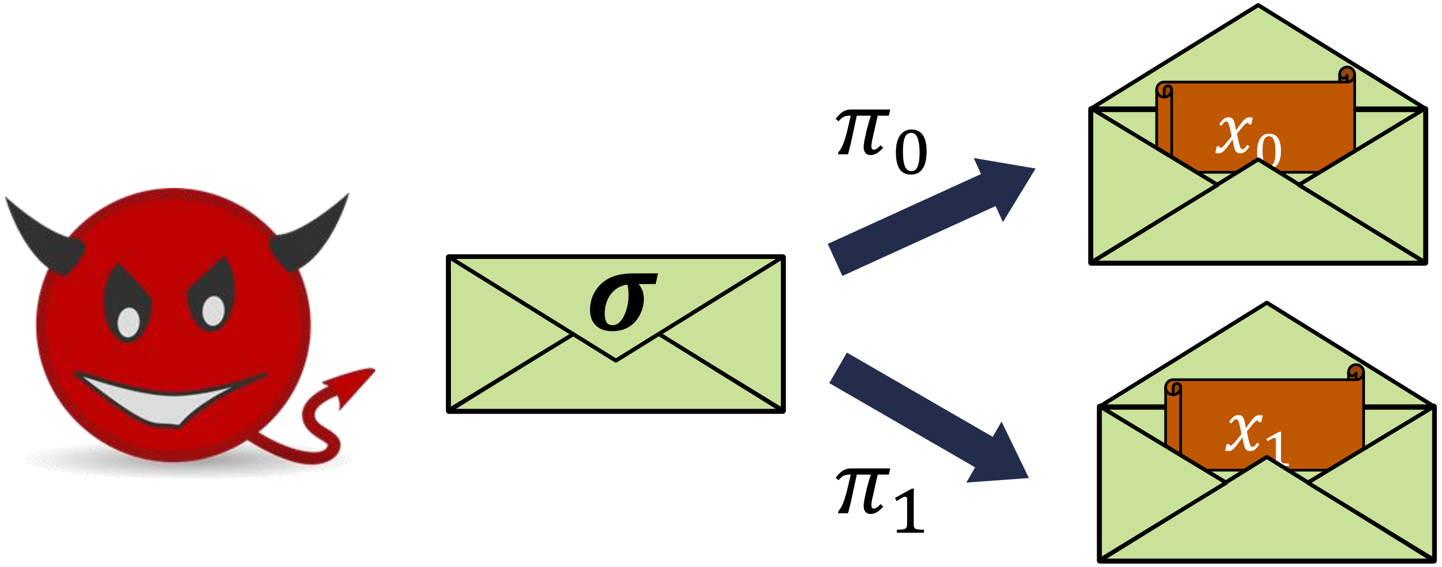
$\mathrm{Verify}(\mathrm{crs}, \sigma, x, \pi) \to 0/1$

Checks whether π is valid opening of σ to x

Alternatively: *Could define* Commit *to output* (σ, π) *and remove* Open

Commitment Schemes

Binding: efficient adversary cannot open σ to two different values

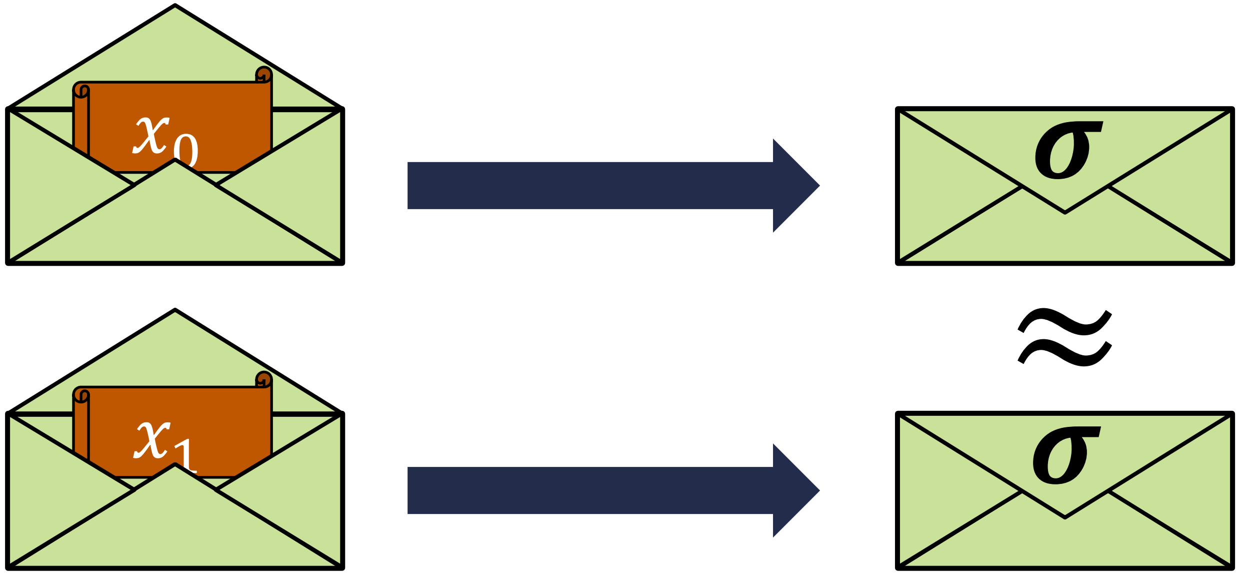


$$\mathrm{Verify}(\mathrm{crs}, \sigma, x_0, \pi_0) = 1$$

$$\mathrm{Verify}(\mathrm{crs}, \sigma, x_1, \pi_1) = 1$$

Commitment Schemes

Hiding: the commitment σ hides the input x



$$\mathrm{Commit}(\mathrm{crs}, x_0) \approx \mathrm{Commit}(\mathrm{crs}, x_1)$$

This Talk: Succinct Functional Commitments

$\mathrm{Commit}(\mathrm{crs}, x) \to (\sigma, \mathrm{st})$

$\mathrm{Open}(\mathrm{st}, f) \to \pi$

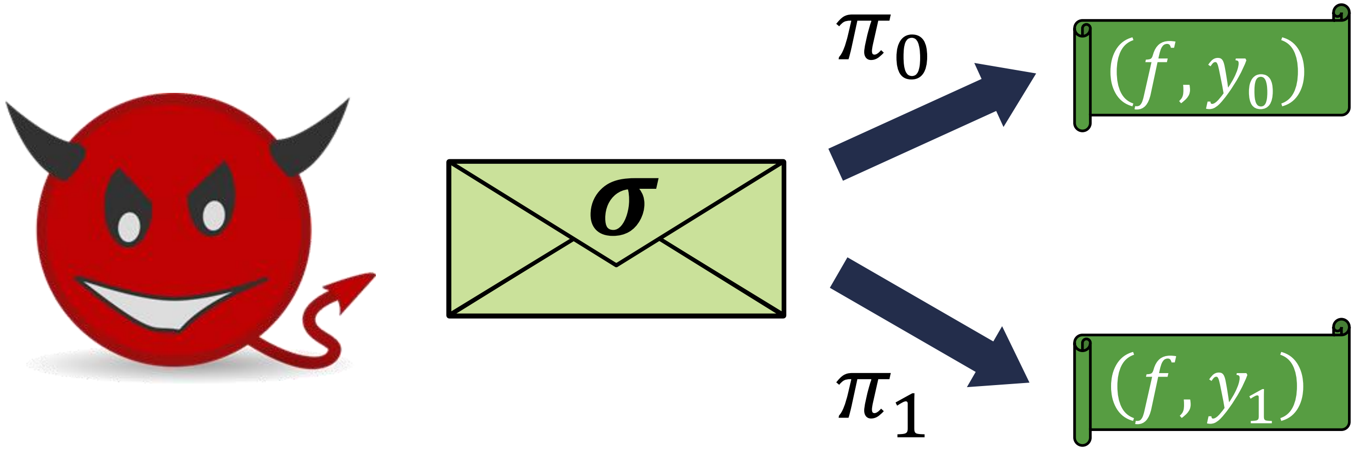
Takes the commitment state and a function f and outputs an opening π

$\mathrm{Verify}(\mathrm{crs}, \sigma, (f, y), \pi) \to 0/1$

Checks whether π is valid opening of σ to value y with respect to f

This Talk: Succinct Functional Commitments

Binding: efficient adversary cannot open σ to two different values with respect to the **same** f



$\text{Verify}(\text{crs}, \sigma, (f, y_0), \pi_0) = 1$

$\text{Verify}(\text{crs}, \sigma, (f, y_1), \pi_1) = 1$

This Talk: Succinct Functional Commitments

Hiding: commitment σ and opening π only reveal $f(x)$

Succinctness: commitments and openings should be short

- **Short commitment:** $|\sigma| = \text{poly}(\lambda, \log|x|)$
- **Short opening:** $|\pi| = \text{poly}(\lambda, \log|x|, |f(x)|)$

Special Cases of Functional Commitments

Vector commitments:

$$[x_1, x_2, \dots, x_n] \xrightarrow{\mathrm{ind}_i(x_1, \dots, x_n) \coloneqq x_i} x_i$$

commit to a vector, open at an index

Polynomial commitments:

$$[\alpha_0, \alpha_1, \dots, \alpha_d] \xrightarrow{f_x(\alpha_0, \dots, \alpha_d) \coloneqq \alpha_0 + \alpha_1 x + \cdots + \alpha_d x^d} y$$

commit to a polynomial, open to the evaluation at x

Succinct Functional Commitments

(not an exhaustive list!)

Scheme	Function Class	Assumption
[Mer87]	vector commitment	collision-resistant hash functions
[LY10, CF13, LM19, GRWZ20]	vector commitment	q-type pairing assumptions
[CF13, LM19, BBF19]	vector commitment	groups of unknown order
[PPS21]	vector commitment	short integer solutions (SIS)
[KZG10, Lee20]	polynomial commitment	q-type pairing assumptions
[BFS19, BHRRS21, BF23]	polynomial commitment	groups of unknown order
[LRY16]	Boolean circuits	collision-resistant hash functions + SNARKs
[LRY16]	linear functions	q-type pairing assumptions
[ACLMT22]	constant-degree polynomials	k-R-ISIS assumption (falsifiable)
This work	**vector commitment**	**short integer solutions (SIS)**

supports private openings, commitments to large values, linearly-homomorphic

Succinct Functional Commitments

(not an exhaustive list!)

Scheme	Function Class	Assumption
[Mer87]	vector commitment	collision-resistant hash functions
[LY10, CF13, LM19, GRWZ20]	vector commitment	q-type pairing assumptions
[CF13, LM19, BBF19]	vector commitment	groups of unknown order
[PPS21]	vector commitment	short integer solutions (SIS)
[KZG10, Lee20]	polynomial commitment	q-type pairing assumptions
[BFS19, BHRRS21, BF23]	polynomial commitment	groups of unknown order
[LRY16]	Boolean circuits	collision-resistant hash functions + SNARKs
[LRY16]	linear functions	q-type pairing assumptions
[ACLMT22]	constant-degree polynomials	k-R-ISIS assumption (falsifiable)
This work	**vector commitment**	**short integer solutions (SIS)**
This work	**Boolean circuits**	$\mathbf{BASIS_{struct}}$ **assumption (falsifiable)**

Concurrent works [BCFL22, dCP23]: lattice-based constructions of functional commitments for Boolean circuits

Framework for Lattice Commitments

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Common reference string (for inputs of length ℓ):

matrices $\boldsymbol{A}_1, \dots, \boldsymbol{A}_\ell \in \mathbb{Z}_q^{n \times m}$

target vectors $\boldsymbol{t}_1, \dots, \boldsymbol{t}_\ell \in \mathbb{Z}_q^n$

auxiliary data: cross-terms $\boldsymbol{u}_{ij} \leftarrow \boldsymbol{A}_i^{-1}(\boldsymbol{t}_j) \in \mathbb{Z}_q^m$ where $i \neq j$

short (i.e., low-norm) vector satisfying $\boldsymbol{A}_i \boldsymbol{u}_{ij} = \boldsymbol{t}_j$

Framework for Lattice Commitments

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Common reference string (for inputs of length ℓ):

matrices $\boldsymbol{A}_1, \dots, \boldsymbol{A}_\ell \in \mathbb{Z}_q^{n \times m}$

target vectors $\boldsymbol{t}_1, \dots, \boldsymbol{t}_\ell \in \mathbb{Z}_q^n$

auxiliary data: cross-terms $\boldsymbol{u}_{ij} \leftarrow \boldsymbol{A}_i^{-1}(\boldsymbol{t}_j) \in \mathbb{Z}_q^m$ where $i \neq j$

Commitment to $\boldsymbol{x} \in \mathbb{Z}_q^\ell$:

$$\boldsymbol{c} = \sum_{i \in [\ell]} x_i \boldsymbol{t}_i$$

linear combination of target vectors

Opening to value y at index i:

short $\boldsymbol{v}_i$ such that $\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + y \cdot \boldsymbol{t}_i$

Honest opening:

$$\boldsymbol{v}_i = \sum_{j \neq i} x_j \boldsymbol{u}_{ij}$$

*Correct as long as $\boldsymbol{x}$ is **short***

$$\boxed{\boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i = \sum_{j \neq i} x_j \boldsymbol{A}_i \boldsymbol{u}_{ij} + x_i \boldsymbol{t}_i = \sum_{j \in [\ell]} x_j \boldsymbol{t}_j = \boldsymbol{c}}$$

Framework for Lattice Commitments

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Common reference string (for inputs of length ℓ):

matrices $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_\ell \in \mathbb{Z}_q^{n \times m}$

target vectors $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_\ell \in \mathbb{Z}_q^n$

auxiliary data: cross-terms $\boldsymbol{u}_{ij} \leftarrow \boldsymbol{A}_i^{-1}(\boldsymbol{t}_j) \in \mathbb{Z}_q^m$ where $i \neq j$

[PPS21]: $\boldsymbol{A}_i \leftarrow \mathbb{Z}_q^{n \times m}$ and $\boldsymbol{t}_i \leftarrow \mathbb{Z}_q^n$ are independent and uniform

suffices for vector commitments (from SIS)

[ACLMT21]: $\boldsymbol{A}_i = \boldsymbol{W}_i \boldsymbol{A}$ and $\boldsymbol{t}_i = \boldsymbol{W}_i \boldsymbol{u}_i$ where $\boldsymbol{W}_i \leftarrow \mathbb{Z}_q^{n \times n}, \boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}, \boldsymbol{u}_i \leftarrow \mathbb{Z}_q^n$

(one candidate adaptation to the integer case)

<u>generalizes</u> to functional commitments for constant-degree polynomials (from k-R-ISIS)

Our Approach

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Verification invariant: $\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i \qquad \forall i \in [\ell]$

for a short $\boldsymbol{v}_i$

Our approach: rewrite ℓ relations as a single linear system

$$\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{I}_n \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{I}_n \end{array}\right] \cdot \begin{bmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_\ell \\ \boldsymbol{c} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{t}_1 \\ \vdots \\ -x_\ell \boldsymbol{t}_\ell \end{bmatrix}$$

$\boldsymbol{I}_n$ denotes the identity matrix

Our Approach

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Verification invariant: $\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i \qquad \forall i \in [\ell]$

for a short $\boldsymbol{v}_i$

Our approach: rewrite ℓ relations as a single linear system

$$\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right] \cdot \begin{bmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_\ell \\ \hat{\boldsymbol{c}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{t}_1 \\ \vdots \\ -x_\ell \boldsymbol{t}_\ell \end{bmatrix}$$

"powers of two matrix"

$$\boldsymbol{G} = \begin{bmatrix} 1 & 2 & \cdots & 2^{\lfloor \log q \rfloor} & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & 2 & \cdots & 2^{\lfloor \log q \rfloor} \end{bmatrix}$$

For security and functionality, it will be useful to write $\boldsymbol{c} = \boldsymbol{G}\hat{\boldsymbol{c}}$

Our Approach

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Verification invariant: $\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i \qquad \forall i \in [\ell]$

for a short $\boldsymbol{v}_i$

Our approach: rewrite ℓ relations as a single linear system

$$\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right] \cdot \begin{bmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_\ell \\ \hat{\boldsymbol{c}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{t}_1 \\ \vdots \\ -x_\ell \boldsymbol{t}_\ell \end{bmatrix}$$

Common reference string:

matrices $\boldsymbol{A}_1, \dots, \boldsymbol{A}_\ell \in \mathbb{Z}_q^{n \times m}$

target vectors $\boldsymbol{t}_1, \dots, \boldsymbol{t}_\ell \in \mathbb{Z}_q^n$

auxiliary data: cross-terms $\boldsymbol{u}_{ij} \leftarrow \boldsymbol{A}_i^{-1}(\boldsymbol{t}_j)$

Our Approach

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Verification invariant: $\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i \qquad \forall i \in [\ell]$

for a short $\boldsymbol{v}_i$

Our approach: rewrite ℓ relations as a single linear system

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right]}_{\boldsymbol{B}_\ell} \cdot \begin{bmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_\ell \\ \hat{\boldsymbol{c}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{t}_1 \\ \vdots \\ -x_\ell \boldsymbol{t}_\ell \end{bmatrix}$$

Common reference string:

- matrices $\boldsymbol{A}_1, \dots, \boldsymbol{A}_\ell \in \mathbb{Z}_q^{n \times m}$
- target vectors $\boldsymbol{t}_1, \dots, \boldsymbol{t}_\ell \in \mathbb{Z}_q^n$
- *auxiliary data:* ~~cross-terms $\boldsymbol{u}_{ij} \leftarrow \boldsymbol{A}_i^{-1}(\boldsymbol{t}_j)$~~
  trapdoor for $\boldsymbol{B}_\ell$

Trapdoor for $\boldsymbol{B}_\ell$ can be used to sample short solutions $\boldsymbol{x}$ to the linear system $\boldsymbol{B}_\ell \boldsymbol{x} = \boldsymbol{y}$ (for arbitrary $\boldsymbol{y}$)

Our Approach

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Verification invariant: $\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i \qquad \forall i \in [\ell]$

for a short $\boldsymbol{v}_i$

Our approach: rewrite ℓ relations as a single linear system

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right]}_{\boldsymbol{B}_\ell} \cdot \begin{bmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_\ell \\ \hat{\boldsymbol{c}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{t}_1 \\ \vdots \\ -x_\ell \boldsymbol{t}_\ell \end{bmatrix}$$

Committing to an input $\boldsymbol{x}$:

Use trapdoor for $\boldsymbol{B}_\ell$ to **jointly** sample a solution $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell, \hat{\boldsymbol{c}}$

$\boldsymbol{c} = \boldsymbol{G}\hat{\boldsymbol{c}}$ is the commitment and $\boldsymbol{v}_1, \ldots \boldsymbol{v}_\ell$ are the openings

Supports commitments to arbitrary (i.e., large) values over $\mathbb{Z}_q$

Our Approach

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Verification invariant: $\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i \qquad \forall i \in [\ell]$

for a short $\boldsymbol{v}_i$

Our approach: rewrite ℓ relations as a single linear system

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right]}_{\boldsymbol{B}_\ell} \cdot \begin{bmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_\ell \\ \hat{\boldsymbol{c}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{t}_1 \\ \vdots \\ -x_\ell \boldsymbol{t}_\ell \end{bmatrix}$$

Committing to an input $\boldsymbol{x}$:

Use trapdoor for $\boldsymbol{B}_\ell$ to **jointly** sample a solution $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell, \hat{\boldsymbol{c}}$

$\boldsymbol{c} = \boldsymbol{G}\hat{\boldsymbol{c}}$ is the commitment and $\boldsymbol{v}_1, \ldots \boldsymbol{v}_\ell$ are the openings

Supports statistically private openings
(commitment + opening *hides* unopened positions)

Proving Security

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Verification invariant: $\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i \qquad \forall i \in [\ell]$

for a short $\boldsymbol{v}_i$

Suppose adversary can break binding

outputs $\boldsymbol{c}, (\boldsymbol{v}_i, x_i), (\boldsymbol{v}_i', x_i')$ such that

$$\begin{aligned} \boldsymbol{c} &= \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i \\ &= \boldsymbol{A}_i \boldsymbol{v}_i' + x_i' \boldsymbol{t}_i \end{aligned}$$

given matrices $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_\ell$ — set $\boldsymbol{A}_i \leftarrow \mathbb{Z}_q^{n \times m}$

target vectors $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_\ell$ — set $\boldsymbol{t}_i = \boldsymbol{e}_1 = [1,0,\ldots,0]^{\mathrm{T}}$

trapdoor for $\boldsymbol{B}_\ell$

$\Rightarrow$

Short integer solutions (SIS)

given $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$, hard to find short $\boldsymbol{x} \neq 0$ such that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$

$$\boldsymbol{A}_i(\boldsymbol{v}_i - \boldsymbol{v}_i') = (x_i - x_i')\boldsymbol{e}_1$$

$\boldsymbol{v}_i - \boldsymbol{v}_i'$ is a SIS solution for $\boldsymbol{A}_i$ without the first row

Basis-Augmented SIS (BASIS) Assumption

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Verification invariant: $\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i \qquad \forall i \in [\ell]$

for a short $\boldsymbol{v}_i$

Adversary that breaks binding can solve SIS with respect to $\boldsymbol{A}_i$

(technically $\boldsymbol{A}_i$ without the first row – which is equivalent to SIS with dimension $n - 1$)

Basis-Augmented SIS (BASIS) Assumption

Captures and generalizes previous lattice-based functional commitments [PPS21, ACLMT22]

Verification invariant: $\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i \qquad \forall i \in [\ell]$

for a short $\boldsymbol{v}_i$

Adversary that breaks binding can solve SIS with respect to $\boldsymbol{A}_i$

Basis-augmented SIS (BASIS) assumption:

SIS is hard with respect to $\boldsymbol{A}_i$

given a trapdoor (a basis) for the matrix

$$\boldsymbol{B}_\ell = \left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right]$$

Can simulate CRS from BASIS challenge:

matrices $\boldsymbol{A}_1, \ldots, \boldsymbol{A}_\ell \leftarrow \mathbb{Z}_q^{n \times m}$

trapdoor for $\boldsymbol{B}_\ell$

Basis-Augmented SIS (BASIS) Assumption

SIS is hard with respect to $\boldsymbol{A}_i$ given a trapdoor (a basis) for the matrix

$$\boldsymbol{B}_\ell = \left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right]$$

When $\boldsymbol{A}_1, \dots, \boldsymbol{A}_\ell \leftarrow \mathbb{Z}_q^{n \times m}$ are uniform and independent:

hardness of SIS implies hardness of BASIS

(follows from standard lattice trapdoor extension techniques)

Vector Commitments from SIS

Common reference string (for inputs of length ℓ):

matrices $\boldsymbol{A}_1, \dots, \boldsymbol{A}_\ell \in \mathbb{Z}_q^{n \times m}$

auxiliary data: trapdoor for $\boldsymbol{B}_\ell = \left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right]$

To commit to a vector $\boldsymbol{x} \in \mathbb{Z}_q^\ell$: sample solution $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_\ell, \hat{\boldsymbol{c}})$

$$\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right] \cdot \begin{bmatrix} \boldsymbol{v}_1 \\ \vdots \\ \boldsymbol{v}_\ell \\ \hat{\boldsymbol{c}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{e}_1 \\ \vdots \\ -x_\ell \boldsymbol{e}_\ell \end{bmatrix}$$

Commitment is $\boldsymbol{c} = \boldsymbol{G}\hat{\boldsymbol{c}}$ Openings are $\boldsymbol{v}_1, \dots, \boldsymbol{v}_\ell$

Can commit and open to **arbitrary** $\mathbb{Z}_q$ vectors

Commitments and openings statistically **hide** unopened components

Linearly homomorphic:
$\boldsymbol{c} + \boldsymbol{c}'$ is a commitment to $\boldsymbol{x} + \boldsymbol{x}'$ with openings $\boldsymbol{v}_i + \boldsymbol{v}_i'$

Functional Commitments for Circuits

Setting: commit to an input $\boldsymbol{x} \in \{0,1\}^{\ell}$, open to $f(\boldsymbol{x})$

(f can be an arbitrary Boolean circuit)

Will need some basic lattice machinery for homomorphic computation

[GSW13, BGGHNSVV14, GVW15]

Let $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ be an arbitrary matrix

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{V}_1 + x_1\boldsymbol{G}$$
$$\vdots$$
$$\boldsymbol{C}_\ell = \boldsymbol{A}\boldsymbol{V}_\ell + x_\ell\boldsymbol{G}$$

homomorphic evaluation

$$\boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{V}_f + f(\boldsymbol{x}) \cdot \boldsymbol{G}$$

$\boldsymbol{C}_i$ is an encoding of x_i with (short) randomness $\boldsymbol{V}_i$

$\boldsymbol{C}_f$ is an encoding of $f(\boldsymbol{x})$ with (short) randomness $\boldsymbol{V}_f$

Functional Commitments using Structured A_i

Instead of using random $\boldsymbol{A}_i$, consider *structured* $\boldsymbol{A}_i$ (like in [ACLMT22])

$$\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$$

$$\boldsymbol{W}_1, \ldots, \boldsymbol{W}_\ell \leftarrow \mathbb{Z}_q^{n \times n}$$ *(invertible)*

$$\boldsymbol{A_i} = \boldsymbol{W}_i \boldsymbol{A}$$

Common reference string still consists of trapdoor for $\boldsymbol{B}_\ell$ (with the structured $\boldsymbol{A}_i$)

$$\boldsymbol{B}_\ell = \left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right]$$

Functional Commitments using Structured A_i

Instead of using random $\boldsymbol{A}_i$, consider *structured* $\boldsymbol{A}_i$ (like in [ACLMT22])

$$\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$$

$$\boldsymbol{W}_1, \dots, \boldsymbol{W}_\ell \leftarrow \mathbb{Z}_q^{n \times n} \quad \textit{(invertible)}$$

$$\boldsymbol{A}_i = \boldsymbol{W}_i \boldsymbol{A}$$

$$\boldsymbol{B}_\ell = \left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right]$$

To commit to an input $\boldsymbol{x} \in \{0,1\}^\ell$:

Use trapdoor for $\boldsymbol{B}_\ell$ to **jointly** sample $\boldsymbol{V}_1, \dots, \boldsymbol{V}_\ell, \widehat{\boldsymbol{C}}$ that satisfy

$$\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right] \cdot \begin{bmatrix} \boldsymbol{V}_1 \\ \vdots \\ \boldsymbol{V}_\ell \\ \widehat{\boldsymbol{C}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{W}_1 \boldsymbol{G} \\ \vdots \\ -x_\ell \boldsymbol{W}_\ell \boldsymbol{G} \end{bmatrix}$$

Functional Commitments using Structured A_i

Commitment relation:

$$\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right] \cdot \begin{bmatrix} \boldsymbol{V}_1 \\ \vdots \\ \boldsymbol{V}_\ell \\ \widehat{\boldsymbol{C}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{W}_1 \boldsymbol{G} \\ \vdots \\ -x_\ell \boldsymbol{W}_\ell \boldsymbol{G} \end{bmatrix}$$

Homomorphic evaluation:

$$\begin{gathered} \boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{V}_1 + x_1 \boldsymbol{G} \\ \vdots \\ \boldsymbol{C}_\ell = \boldsymbol{A}\boldsymbol{V}_\ell + x_\ell \boldsymbol{G} \end{gathered} \quad \Rightarrow \quad \boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{V}_f + f(\boldsymbol{x}) \cdot \boldsymbol{G}$$

for all $i \in [\ell]$

$$\boldsymbol{A}_i \boldsymbol{V}_i - \boldsymbol{G}\widehat{\boldsymbol{C}} = -x_i \boldsymbol{W}_i \boldsymbol{G}$$

recall $\boldsymbol{A}_i = \boldsymbol{W}_i \boldsymbol{A}$

$$\boldsymbol{W}_i \boldsymbol{A} \boldsymbol{V}_i - \boldsymbol{G}\widehat{\boldsymbol{C}} = -x_i \boldsymbol{W}_i \boldsymbol{G}$$

recall $\boldsymbol{W}_i$ is invertible

$$\boldsymbol{A}\boldsymbol{V}_i - \boldsymbol{W}_i^{-1} \boldsymbol{G}\widehat{\boldsymbol{C}} = -x_i \boldsymbol{G}$$

rearranging

$$\boldsymbol{W}_i^{-1} \boldsymbol{G}\widehat{\boldsymbol{C}} = \boldsymbol{A}\boldsymbol{V}_i + x_i \boldsymbol{G}$$

Functional Commitments using Structured A_i

Commitment relation:

$$\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right] \cdot \begin{bmatrix} \boldsymbol{V}_1 \\ \vdots \\ \boldsymbol{V}_\ell \\ \widehat{\boldsymbol{C}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{W}_1 \boldsymbol{G} \\ \vdots \\ -x_\ell \boldsymbol{W}_\ell \boldsymbol{G} \end{bmatrix}$$

Homomorphic evaluation:

$$\begin{array}{c} \boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{V}_1 + x_1 \boldsymbol{G} \\ \vdots \\ \boldsymbol{C}_\ell = \boldsymbol{A}\boldsymbol{V}_\ell + x_\ell \boldsymbol{G} \end{array} \quad \Rightarrow \quad \boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{V}_f + f(\boldsymbol{x}) \cdot \boldsymbol{G}$$

function only of the commitment $\boldsymbol{C} = \boldsymbol{G}\widehat{\boldsymbol{C}}$

$$\boxed{\widetilde{\boldsymbol{C}}_i = \boldsymbol{W}_i^{-1}\boldsymbol{G}\widehat{\boldsymbol{C}}}$$

for all $i \in [\ell]$

$$\boldsymbol{A}_i \boldsymbol{V}_i - \boldsymbol{G}\widehat{\boldsymbol{C}} = -x_i \boldsymbol{W}_i \boldsymbol{G}$$

recall $\boldsymbol{A}_i = \boldsymbol{W}_i \boldsymbol{A}$

$$\boldsymbol{W}_i \boldsymbol{A} \boldsymbol{V}_i - \boldsymbol{G}\widehat{\boldsymbol{C}} = -x_i \boldsymbol{W}_i \boldsymbol{G}$$

recall $\boldsymbol{W}_i$ is invertible

$$\boldsymbol{A}\boldsymbol{V}_i - \boldsymbol{W}_i^{-1}\boldsymbol{G}\widehat{\boldsymbol{C}} = -x_i \boldsymbol{G}$$

rearranging

$$\boldsymbol{W}_i^{-1}\boldsymbol{G}\widehat{\boldsymbol{C}} = \boldsymbol{A}\boldsymbol{V}_i + x_i \boldsymbol{G}$$

$$\widetilde{\boldsymbol{C}}_i = \boldsymbol{A}\boldsymbol{V}_i + x_i \boldsymbol{G}$$

Functional Commitments using Structured A_i

Commitment relation:

$$\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right] \cdot \begin{bmatrix} \boldsymbol{V}_1 \\ \vdots \\ \boldsymbol{V}_\ell \\ \widehat{\boldsymbol{C}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{W}_1 \boldsymbol{G} \\ \vdots \\ -x_\ell \boldsymbol{W}_\ell \boldsymbol{G} \end{bmatrix}$$

Homomorphic evaluation:

$$\boldsymbol{C}_1 = \boldsymbol{A}\boldsymbol{V}_1 + x_1 \boldsymbol{G}$$
$$\vdots$$
$$\boldsymbol{C}_\ell = \boldsymbol{A}\boldsymbol{V}_\ell + x_\ell \boldsymbol{G}$$

$$\Rightarrow \quad \boldsymbol{C}_f = \boldsymbol{A}\boldsymbol{V}_f + f(\boldsymbol{x}) \cdot \boldsymbol{G}$$

function only of the commitment $\boldsymbol{C} = \boldsymbol{G}\widehat{\boldsymbol{C}}$

$$\boxed{\widetilde{\boldsymbol{C}}_i = \boldsymbol{W}_i^{-1} \boldsymbol{G} \widehat{\boldsymbol{C}}}$$

$$\widetilde{\boldsymbol{C}}_i = \boldsymbol{A}\boldsymbol{V}_i + x_i \boldsymbol{G}$$

$\widetilde{\boldsymbol{C}}_i$ is an encoding of x_i with randomness $\boldsymbol{V}_i$

compute on $\widetilde{\boldsymbol{C}}_1, \dots \widetilde{\boldsymbol{C}}_f$ | compute on $\boldsymbol{V}_1, \dots, \boldsymbol{V}_\ell$

$$\widetilde{\boldsymbol{C}}_f = \boldsymbol{A}\boldsymbol{V}_{f,f(\boldsymbol{x})} + f(\boldsymbol{x})\boldsymbol{G}$$

$\widetilde{\boldsymbol{C}}_f$ is an encoding of $f(\boldsymbol{x})$ with randomness $\boldsymbol{V}_{f,f(\boldsymbol{x})}$

[GVW15]: independent $\boldsymbol{V}_i$ is sampled for each input bit, so commitments $\boldsymbol{C}_i$ are independent

- long commitment, security from SIS

This work: publish a trapdoor that allows deriving $\boldsymbol{C}_i$ (and associated $\boldsymbol{V}_i$) from a **single** commitment $\widehat{\boldsymbol{C}}$

- short commitment, stronger assumption

Functional Commitments using Structured A_i

Commitment relation:

$$\left[\begin{array}{ccc|c} A_1 & & & -G \\ & \ddots & & \vdots \\ & & A_\ell & -G \end{array}\right] \cdot \begin{bmatrix} V_1 \\ \vdots \\ V_\ell \\ \hat{C} \end{bmatrix} = \begin{bmatrix} -x_1 W_1 G \\ \vdots \\ -x_\ell W_\ell G \end{bmatrix}$$

Homomorphic evaluation:

$$\begin{matrix} C_1 = AV_1 + x_1 G \\ \vdots \\ C_\ell = AV_\ell + x_\ell G \end{matrix} \Longrightarrow C_f = AV_f + f(x) \cdot G$$

Opening is $V_{f,f(x)}$ is
(short) linear function of $V_1, \ldots, V_\ell$

Opening to function f proceeds exactly as in [GVW15]

To verify:

1. Expand commitment

$$C \xrightarrow{\tilde{C}_i = W_i^{-1} G \hat{C}} \boxed{\begin{matrix} \tilde{C}_1 = AV_1 + x_1 G \\ \vdots \\ \tilde{C}_\ell = AV_\ell + x_\ell G \end{matrix}}$$

2. Homomorphically evaluate f

$$\tilde{C}_1, \ldots \tilde{C}_\ell \Longrightarrow \tilde{C}_f$$

3. Check verification relation

$$AV_{f,z} = \tilde{C}_f - z \cdot G$$

Functional Commitments from Lattices

Security follows from BASIS assumption with a **structured** matrix:

SIS is hard with respect to $\boldsymbol{A}$ given a trapdoor (a basis) for the matrix

$$\boldsymbol{B}_\ell = \left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right]$$

where $\boldsymbol{A}_i = \boldsymbol{W}_i \boldsymbol{A}$ where $\boldsymbol{W}_i \leftarrow \mathbb{Z}_q^{n \times n}$ and $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$

Falsifiable assumption but does not appear to reduce to standard SIS

$\ell = 1$ case does follow from plain SIS

Open problem: Understanding security or attacks when $\ell > 1$

Functional Commitments from Lattices

Common reference string (for inputs of length ℓ):

matrices $\boldsymbol{A}_1, \dots, \boldsymbol{A}_\ell \in \mathbb{Z}_q^{n \times m}$ where $\boldsymbol{A}_i = \boldsymbol{W}_i \boldsymbol{A}$

auxiliary data: trapdoor for $\boldsymbol{B}_\ell = \left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right]$

To commit to a vector $\boldsymbol{x} \in \{0,1\}^\ell$: sample $(\boldsymbol{V}_1, \dots, \boldsymbol{V}_\ell, \widehat{\boldsymbol{C}})$

$$\left[\begin{array}{ccc|c} \boldsymbol{A}_1 & & & -\boldsymbol{G} \\ & \ddots & & \vdots \\ & & \boldsymbol{A}_\ell & -\boldsymbol{G} \end{array}\right] \cdot \begin{bmatrix} \boldsymbol{V}_1 \\ \vdots \\ \boldsymbol{V}_\ell \\ \widehat{\boldsymbol{C}} \end{bmatrix} = \begin{bmatrix} -x_1 \boldsymbol{W}_1 \boldsymbol{G} \\ \vdots \\ -x_\ell \boldsymbol{W}_\ell \boldsymbol{G} \end{bmatrix}$$

Commitment is $\boldsymbol{C} = \boldsymbol{G}\widehat{\boldsymbol{C}}$

Openings for function f is $[\boldsymbol{V}_1 \mid \cdots \mid \boldsymbol{V}_\ell] \cdot \boldsymbol{H}_{\widetilde{\boldsymbol{C}}, f, \boldsymbol{x}}$

Scheme supports functions computable by Boolean circuits of (bounded) depth d

$$|\mathrm{crs}| = \ell^2 \cdot \mathrm{poly}(\lambda, d, \log \ell)$$

$$|\boldsymbol{C}| = \mathrm{poly}(\lambda, d, \log \ell)$$

$$|\boldsymbol{V}_{f, f(\boldsymbol{x})}| = \mathrm{poly}(\lambda, d, \log \ell)$$

Verification **time** scales with $|f|$ (i.e., size of circuit computing f)

Fast Verification with Preprocessing

$$\widetilde{\boldsymbol{C}}_i = \boldsymbol{W}_i^{-1}\boldsymbol{G}\widehat{\boldsymbol{C}} = \boldsymbol{W}_i^{-1}\boldsymbol{C}$$

To verify opening $\boldsymbol{V}$ to (f, z), verifier computes the following:

- Homomorphic evaluation: $\widetilde{\boldsymbol{C}}_1, \ldots, \widetilde{\boldsymbol{C}}_\ell, f \mapsto \widetilde{\boldsymbol{C}}_f$
- Verification relation: $\boldsymbol{A}\boldsymbol{V} = \widetilde{\boldsymbol{C}}_f - z \cdot \boldsymbol{G}$

Computing $\widetilde{\boldsymbol{C}}_f$ corresponds to homomorphic computation on $\widetilde{\boldsymbol{C}}_1, \ldots, \widetilde{\boldsymbol{C}}_\ell$

Suppose f is a linear function:

$$f(x_1, \ldots, x_\ell) = \sum_{i \in [\ell]} \alpha_i x_i$$

Then we can write $\widetilde{\boldsymbol{C}}_f = \boldsymbol{M}_f \cdot \boldsymbol{C}$

$\boldsymbol{M}_f$ is a fixed matrix that depends only on f and can be computed in *offline phase*

For linear functions, if f is known in advance, verification runs in time $\mathrm{poly}(\lambda, \log \ell)$

Fast Verification with Preprocessing

$$\widetilde{\boldsymbol{C}}_i = \boldsymbol{W}_i^{-1}\boldsymbol{G}\widehat{\boldsymbol{C}} = \boldsymbol{W}_i^{-1}\boldsymbol{C}$$

To verify opening $\boldsymbol{V}$ to (f, z), verifier computes the following:

- Homomorphic evaluation: $\widetilde{\boldsymbol{C}}_1, \dots, \widetilde{\boldsymbol{C}}_\ell, f \mapsto \widetilde{\boldsymbol{C}}_f$
- Verification relation: $\boldsymbol{AV} = \widetilde{\boldsymbol{C}}_f - z \cdot \boldsymbol{G}$

Computing $\widetilde{\boldsymbol{C}}_f$ corresponds to homomorphic computation on $\widetilde{\boldsymbol{C}}_1, \dots, \widetilde{\boldsymbol{C}}_\ell$

Suppose f is a linear function:

$$f(x_1, \dots, x_\ell) = \sum \alpha_i x_i$$

Captures polynomial commitments as a special case
(polynomial evaluation can be described by a linear function)

For linear functions, if f is known in advance, verification runs in time $\mathrm{poly}(\lambda, \log \ell)$

Summary

New methodology for constructing lattice-based commitments:

1. Write down the main verification relation ($\boldsymbol{c} = \boldsymbol{A}_i \boldsymbol{v}_i + x_i \boldsymbol{t}_i$)
2. Publish a trapdoor for the linear system by the verification relation

Security analysis relies on basis-augmented SIS assumptions:

SIS with respect to $\boldsymbol{A}$ is hard given a trapdoor for a ***related*** *matrix $\boldsymbol{B}$*

"Random" variant of BASIS assumption implies vector commitments and reduces to SIS

"Structured" variant of BASIS assumption implies functional commitments

- Yields linear and polynomial commitments with fast preprocessed verification
- Structure also enables **aggregating** openings

[see paper for details]

Open Questions

Analyzing BASIS family of assumptions (new reductions to SIS or attacks)

Describe and analyze knowledge variants of the assumption or the constructions

Reducing CRS size: can we obtain functional commitments with *linear*-size CRS?

Thank you!

`https://eprint.iacr.org/2022/1515`