Lattice Assumptions with Hints: Succinct LWE and its Applications

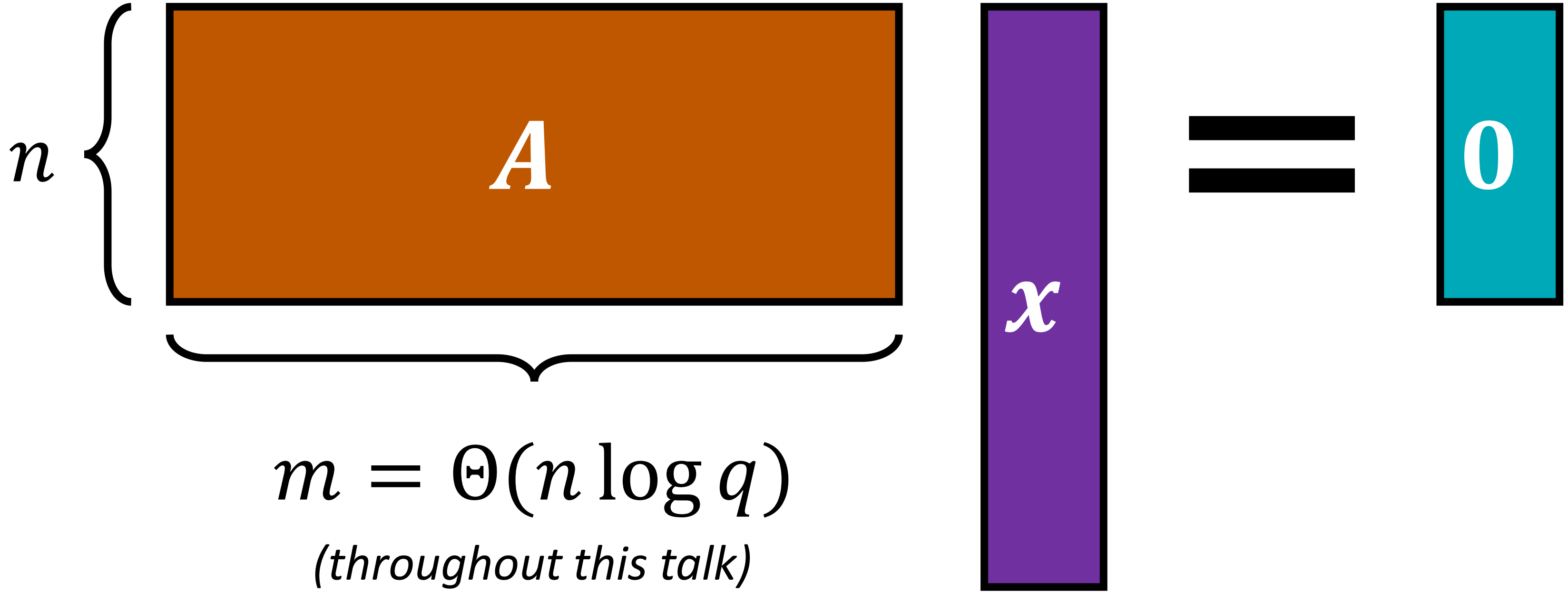
David Wu

June 2025

Special thanks to Hoeteck Wee for many insightful discussions and collaborations

Lattice Problems in Cryptography

Short integer solutions (SIS): Given $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$, find low-norm $\boldsymbol{x} \neq \boldsymbol{0}$ such that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$ [Ajt96]



$$m = \Theta(n \log q)$$

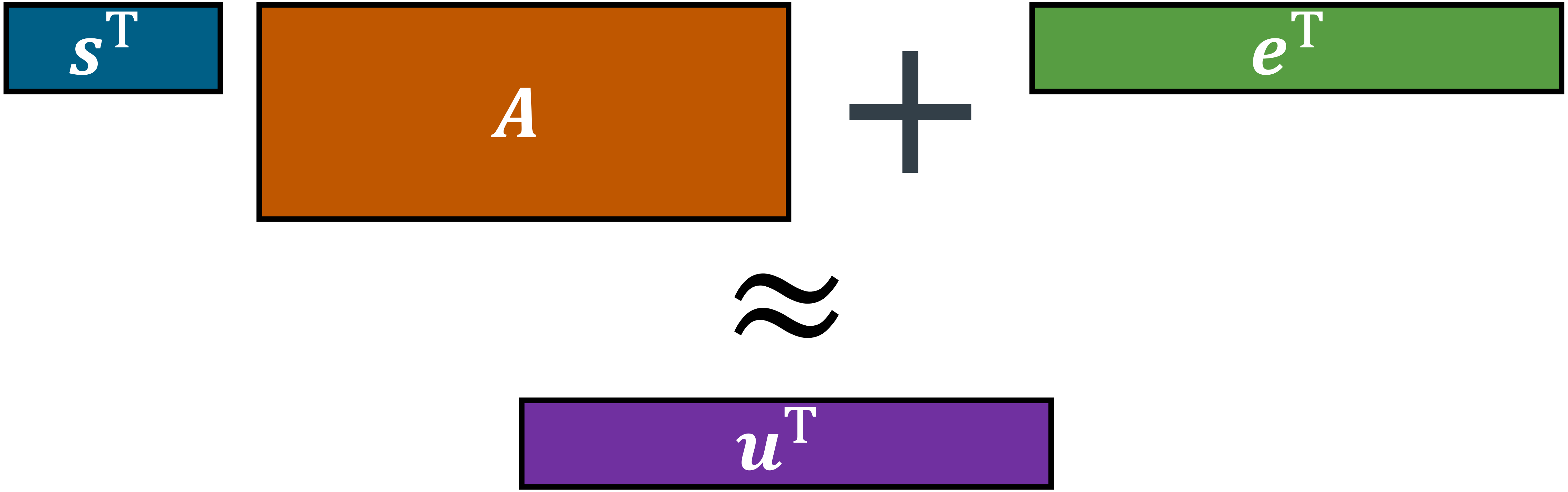
(throughout this talk)

Yields one-way functions, collision-resistant hash functions, digital signatures

Lattice Problems in Cryptography

Short integer solutions (SIS): Given $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$, find low-norm $\boldsymbol{x} \neq \boldsymbol{0}$ such that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$ [Ajt96]

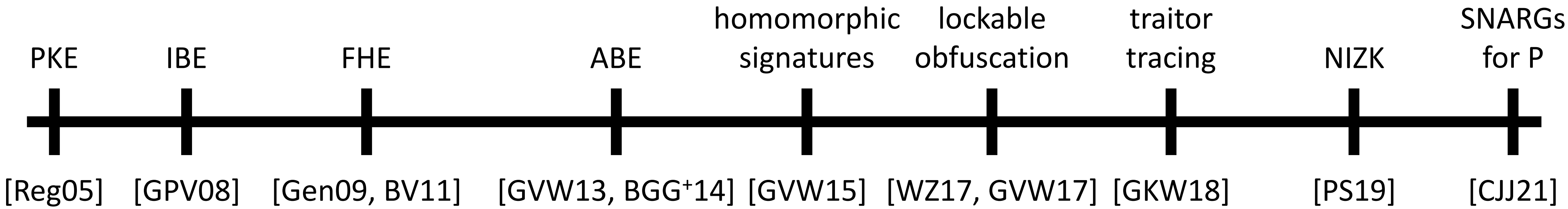
Learning with errors (LWE): Distinguish $(\boldsymbol{A}, \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}})$ from $(\boldsymbol{A}, \boldsymbol{u}^{\mathrm{T}})$ [Reg05]



Lattice Problems in Cryptography

Short integer solutions (SIS): Given $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$, find low-norm $\boldsymbol{x} \neq \mathbf{0}$ such that $\boldsymbol{A}\boldsymbol{x} = \mathbf{0}$ [Ajt96]

Learning with errors (LWE): Distinguish $(\boldsymbol{A}, \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}})$ from $(\boldsymbol{A}, \boldsymbol{u}^{\mathrm{T}})$ [Reg05]



PKE	IBE	FHE	ABE	homomorphic signatures	lockable obfuscation	traitor tracing	NIZK	SNARGs for P
[Reg05]	[GPV08]	[Gen09, BV11]	[GVW13, BGG+14]	[GVW15]	[WZ17, GVW17]	[GKW18]	[PS19]	[CJJ21]

But… *not* everything

However, many **lattice-inspired** approaches

Broadcast encryption [BV22]

Witness encryption [GGH15, CVW18]

Indistinguishability obfuscation

[GGH15, Agr19, CHVW19, AP20, BDGM20a, WW21, GP21, BDGM20b, DQVWW21]

Lattice Problems in Cryptography

Short integer solutions (SIS): Given $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$, find low-norm $\boldsymbol{x} \neq \boldsymbol{0}$ such that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$ [Ajt96]

Learning with errors (LWE): Distinguish $\left(\boldsymbol{A}, \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}\right)$ from $\left(\boldsymbol{A}, \boldsymbol{u}^{\mathrm{T}}\right)$ [Reg05]

PKE	IBE	FHE	ABE	homomorphic signatures	lockable obfuscation	traitor tracing	NIZK	SNARGs for P
[Reg05]	[GPV08]	[Gen09, BV11]	[GVW13, BGG$^+$14]	[GVW15]	[WZ17, GVW17]	[GKW18]	[PS19]	[CJJ21]

But… *not* everything

Broadcast encryption [BV22]

Witness encryption [GGH15, CVW18]

Indistinguishability obfuscation

[GGH15, Agr19, CHVW19, AP20, BDGM20a, WW21, GP21, BDGM20b, DQVWW21]

However, many **lattice-inspired** approaches

Most schemes did not have a concrete hardness assumption or were based on a hardness assumption that was subsequently broken (in the most general setting)

Lattice Problems in Cryptography

Short integer solutions (SIS): Given $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$, find low-norm $\boldsymbol{x} \neq \boldsymbol{0}$ such that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$ [Ajt96]

Learning with errors (LWE): Distinguish $\left(\boldsymbol{A}, \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}\right)$ from $\left(\boldsymbol{A}, \boldsymbol{u}^{\mathrm{T}}\right)$ [Reg05]

PKE	IBE	FHE	ABE	homomorphic signatures	lockable obfuscation	traitor tracing	NIZK	SNARGs for P
[Reg05]	[GPV08]	[Gen09, BV11]	[GVW13, BGG$^+$14]	[GVW15]	[WZ17, GVW17]	[GKW18]	[PS19]	[CJJ21]

Recent developments:

- Broadcast encryption from public-coin evasive LWE [Wee22]
- Witness encryption based on private-coin evasive LWE [Tsa22, VWW22]
- New indistinguishability obfuscation candidates: [BDJMMPV25, HJL25, AMYY25, CLW25, SBP25]

Lattice Problems in Cryptography

Short integer solutions (SIS): Given $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$, find low-norm $\boldsymbol{x} \neq \boldsymbol{0}$ such that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$ [Ajt96]

Learning with errors (LWE): Distinguish $\left(\boldsymbol{A}, \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}\right)$ from $\left(\boldsymbol{A}, \boldsymbol{u}^{\mathrm{T}}\right)$ [Reg05]

PKE	IBE	FHE	ABE	homomorphic signatures	lockable obfuscation	traitor tracing	NIZK	SNARGs for P
[Reg05]	[GPV08]	[Gen09, BV11]	[GVW13, BGG+14]	[GVW15]	[WZ17, GVW17]	[GKW18]	[PS19]	[CJJ21]

Recent developments:

- Broadcast encryption from public-coin evasive LWE [Wee22]
- Witness encryption based on private-coin evasive LWE [Tsa22, VWW22]
- New indistinguishability obfuscation candidates: [BDJMMPV25, HJL25, AMYY25, CLW25, SBP25]

later this afternoon!

Lattice Problems in Cryptography

This talk: explore lattice assumptions with **minimum additional structure** that allow us to reason about security of **simple** (and natural) constructions of new cryptographic primitives

Hope: over time, will be able to reduce to the standard lattice problems

Very successful in the area of bilinear maps: many new assumptions (e.g., composite-order, q-type, etc.), but can now do most things from k-Lin

Recent developments:

- Broadcast encryption from public-coin evasive LWE [Wee22]
- Witness encryption based on private-coin evasive LWE [Tsa22, VWW22]
- New indistinguishability obfuscation candidates: [BDJMMPV25, HJL25, AMYY25, CLW25, SBP25]

later this afternoon!

The Succinct LWE Family of Assumptions

General template: SIS/LWE assumptions hold with respect to $\boldsymbol{A}$ even given some “hint”

Hint is a matrix $\boldsymbol{D}_\ell$ related to $\boldsymbol{A}$ and a (gadget) trapdoor $\boldsymbol{T}$ for $\boldsymbol{D}_\ell$

Alternatively: low-norm vectors in ***correlated*** *cosets of* $\mathcal{L}^\perp(\boldsymbol{A})$

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\begin{bmatrix} \text{—} \; \boldsymbol{T}_1 \; \text{—} \\ \vdots \\ \text{—} \; \boldsymbol{T}_\ell \; \text{—} \\ \text{—} \; \underline{\boldsymbol{T}} \; \text{—} \end{bmatrix}}_{\boldsymbol{T}} = \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}$$

$\boldsymbol{A}, \boldsymbol{W}_i \in \mathbb{Z}_q^{n \times m}$

$\boldsymbol{T}_i, \underline{\boldsymbol{T}} \in \mathbb{Z}_q^{m \times \ell m}$

$$\boxed{\boldsymbol{G} = \boldsymbol{I}_n \otimes [1,2,\ldots,2^{\lceil \log q \rceil - 1}]}$$

Typically: $\boldsymbol{T}$ is **random** gadget trapdoor (a discrete Gaussian conditioned on $\boldsymbol{D}_\ell \boldsymbol{T} = \boldsymbol{I}_\ell \otimes \boldsymbol{G}$)

The Succinct LWE Family of Assumptions

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\begin{bmatrix} — & \boldsymbol{T}_1 & — \\ — & \vdots & — \\ — & \boldsymbol{T}_\ell & — \\ — & \underline{\boldsymbol{T}} & — \end{bmatrix}}_{\boldsymbol{T}} = \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}$$

$\boldsymbol{A}, \boldsymbol{W}_i \in \mathbb{Z}_q^{n\times m}$

$\boldsymbol{T}_i, \underline{\boldsymbol{T}} \in \mathbb{Z}_q^{m\times \ell m}$

SIS/LWE holds with respect to $\boldsymbol{A}$ given $\boldsymbol{D}_\ell, \boldsymbol{T}$

Concrete instances:

Basis-augmented SIS (BASIS) [WW23]

$$\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times m}, \boldsymbol{W}_i = \boldsymbol{W}_i'\boldsymbol{G} \text{ where } \boldsymbol{W}_i' \leftarrow \mathbb{Z}_q^{n\times n}$$

ℓ-succinct LWE [Wee24]

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

BASIS ⇒ ℓ-succinct SIS (similarly for LWE variant)

The Succinct LWE Family of Assumptions

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\begin{bmatrix} — & \boldsymbol{T}_1 & — \\ — & \vdots & — \\ — & \boldsymbol{T}_\ell & — \\ — & \underline{\boldsymbol{T}} & — \end{bmatrix}}_{\boldsymbol{T}} = \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}$$

$\boldsymbol{A}, \boldsymbol{W}_i \in \mathbb{Z}_q^{n \times m}$

$\boldsymbol{T}_i, \underline{\boldsymbol{T}} \in \mathbb{Z}_q^{m \times \ell m}$

SIS/LWE holds with respect to $\boldsymbol{A}$ given $\boldsymbol{D}_\ell, \boldsymbol{T}$

Can also consider **structured** $\boldsymbol{A}$

The Succinct LWE Family of Assumptions

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\begin{bmatrix} — & \boldsymbol{T}_1 & — \\ — & \vdots & — \\ — & \boldsymbol{T}_\ell & — \\ — & \underline{\boldsymbol{T}} & — \end{bmatrix}}_{\boldsymbol{T}} = \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}$$

$\boldsymbol{A}, \boldsymbol{W}_i \in \mathbb{Z}_q^{n \times m}$

$\boldsymbol{T}_i, \underline{\boldsymbol{T}} \in \mathbb{Z}_q^{m \times \ell m}$

SIS/LWE holds with respect to $\boldsymbol{A}$ given $\boldsymbol{D}_\ell, \boldsymbol{T}$

Can also consider **structured** $\boldsymbol{A}$: sample $\boldsymbol{W}_1, \dots, \boldsymbol{W}_\ell \leftarrow \mathbb{Z}_q^{n \times m}$ and $\boldsymbol{R}_1, \dots, \boldsymbol{R}_\ell \leftarrow D_{\mathbb{Z},\sigma}^{m \times m}$

Define $\boldsymbol{A} = [\, \cdots \mid \boldsymbol{W}_i \boldsymbol{R}_j + \delta_{ij} \boldsymbol{G} \mid \cdots \,] \in \mathbb{Z}_q^{n \times \ell^2 m}$ where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise

The matrix $\boldsymbol{D}_\ell$ has a **public** trapdoor $\boldsymbol{T} = \begin{bmatrix} \mathrm{vec}(\boldsymbol{I}_\ell) \otimes \boldsymbol{I}_{\ell m} \\ -\boldsymbol{R} \end{bmatrix}$ where $\boldsymbol{R} = [\boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_\ell]$

LWE assumption with respect to $\boldsymbol{A}$ given $\boldsymbol{D}_\ell, \boldsymbol{T}$ asks that

decomposed LWE [AMR25]

$\boldsymbol{s}^{\mathrm{T}}(\boldsymbol{W}_i \boldsymbol{R}_j + \delta_{ij} \boldsymbol{G}) + \boldsymbol{e}_{ij}^T$ is pseudorandom for all $i, j \in [\ell]$ given $\boldsymbol{W}_i, \boldsymbol{R}_i$

The Succinct LWE Family of Assumptions

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\begin{bmatrix} - & \boldsymbol{T}_1 & - \\ - & \vdots & - \\ - & \boldsymbol{T}_\ell & - \\ - & \underline{\boldsymbol{T}} & - \end{bmatrix}}_{\boldsymbol{T}} = \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}$$

$\boldsymbol{A}, \boldsymbol{W}_i \in \mathbb{Z}_q^{n\times m}$

$\boldsymbol{T}_i, \underline{\boldsymbol{T}} \in \mathbb{Z}_q^{m\times \ell m}$

The decomposed LWE assumption does not refer to any trapdoors!

Assumption similar in spirit to a "circular security" assumption (note: without the $\delta_{ij}\boldsymbol{G}$ term, assumption is implied by plain LWE)

Open problem: show hardness of decomposed LWE from plain LWE (or some *worst-case* lattice problem)

decomposed LWE [AMR25]

$\boldsymbol{s}^{\mathrm{T}}\left(\boldsymbol{W}_i\boldsymbol{R}_j + \delta_{ij}\boldsymbol{G}\right) + \boldsymbol{e}_{ij}^T$ is pseudorandom for all $i, j \in [\ell]$ given $\boldsymbol{W}_i, \boldsymbol{R}_i$

The Succinct LWE Family of Assumptions

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\begin{bmatrix} — & \boldsymbol{T}_1 & — \\ — & \vdots & — \\ — & \boldsymbol{T}_\ell & — \\ — & \underline{\boldsymbol{T}} & — \end{bmatrix}}_{\boldsymbol{T}} = \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}$$

$\boldsymbol{A}, \boldsymbol{W}_i \in \mathbb{Z}_q^{n \times m}$

$\boldsymbol{T}_i, \underline{\boldsymbol{T}} \in \mathbb{Z}_q^{m \times \ell m}$

SIS/LWE holds with respect to $\boldsymbol{A}$ given $\boldsymbol{D}_\ell, \boldsymbol{T}$

Concrete instances:

Basis-augmented SIS (BASIS) [WW23]

$$\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}, \boldsymbol{W}_i = \boldsymbol{W}_i'\boldsymbol{G} \text{ where } \boldsymbol{W}_i' \leftarrow \mathbb{Z}_q^{n \times n}$$

BASIS ⇒ ℓ-succinct SIS (similarly for LWE variant)

ℓ-succinct LWE [Wee24]

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

succinct LWE ⇒ decomposed LWE (with super-polynomial modulus)

decomposed LWE [AMR25]

$$\boldsymbol{W}_i \leftarrow \mathbb{Z}_q^{n \times m}, \boldsymbol{R}_i \leftarrow D_{\mathbb{Z},\sigma}^{m \times m}, \ \boldsymbol{A} = [\cdots \mid \boldsymbol{W}_i \boldsymbol{R}_j + \delta_{ij}\boldsymbol{G} \mid \cdots]$$

trapdoor is **public**

The Succinct LWE Family of Assumptions

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\begin{bmatrix} — & \boldsymbol{T}_1 & — \\ — & \vdots & — \\ — & \boldsymbol{T}_\ell & — \\ — & \underline{\boldsymbol{T}} & — \end{bmatrix}}_{\boldsymbol{T}} = \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}$$

$\boldsymbol{A}, \boldsymbol{W}_i \in \mathbb{Z}_q^{n \times m}$

$\boldsymbol{T}_i, \underline{\boldsymbol{T}} \in \mathbb{Z}_q^{m \times \ell m}$

SIS/LWE holds with respect to $\boldsymbol{A}$ given $\boldsymbol{D}_\ell, \boldsymbol{T}$

Concrete instances:

Basis-augmented SIS (BASIS) [WW23]

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

ℓ-succinct LWE [Wee24]

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

decomposed LWE [AMR25]

$\boldsymbol{W}_i \leftarrow \mathbb{Z}_q^{n \times m}, \boldsymbol{R}_i \leftarrow D_{\mathbb{Z},\sigma}^{m \times m}, \ \boldsymbol{A} = [\cdots \mid \boldsymbol{W}_i \boldsymbol{R}_j + \delta_{ij} \boldsymbol{G} \mid \cdots]$

2026: LWE?

ℓ-Succinct LWE

[Wee24]

LWE is hard with respect to $\boldsymbol{A}$ given a trapdoor $\boldsymbol{T}$ for a related matrix $\boldsymbol{D}_\ell$

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

Two axis for hardness:

Applications need the width to be $o(\ell) \cdot \mathrm{poly}(n, \log q)$

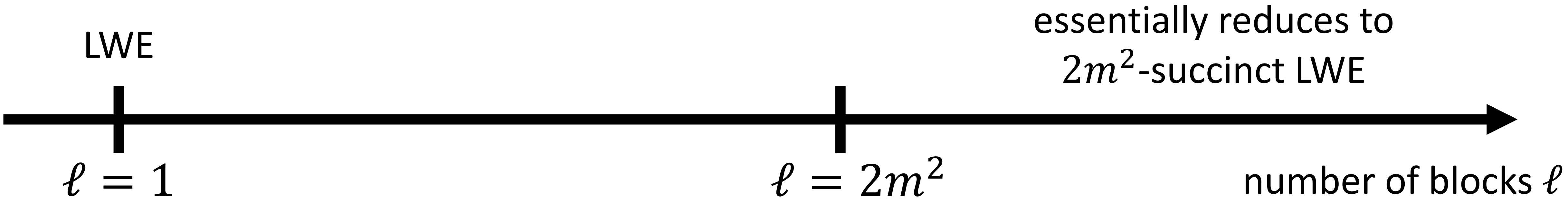
ℓ-Succinct LWE

[Wee24]

LWE is hard with respect to $\boldsymbol{A}$ *given a trapdoor* $\boldsymbol{T}$ *for a related matrix* $\boldsymbol{D}_\ell$

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

Two axis for hardness:



LWE

essentially reduces to $2m^2$-succinct LWE

$\ell = 1$

$\ell = 2m^2$

number of blocks ℓ

Applications of Succinct and Decomposed LWE

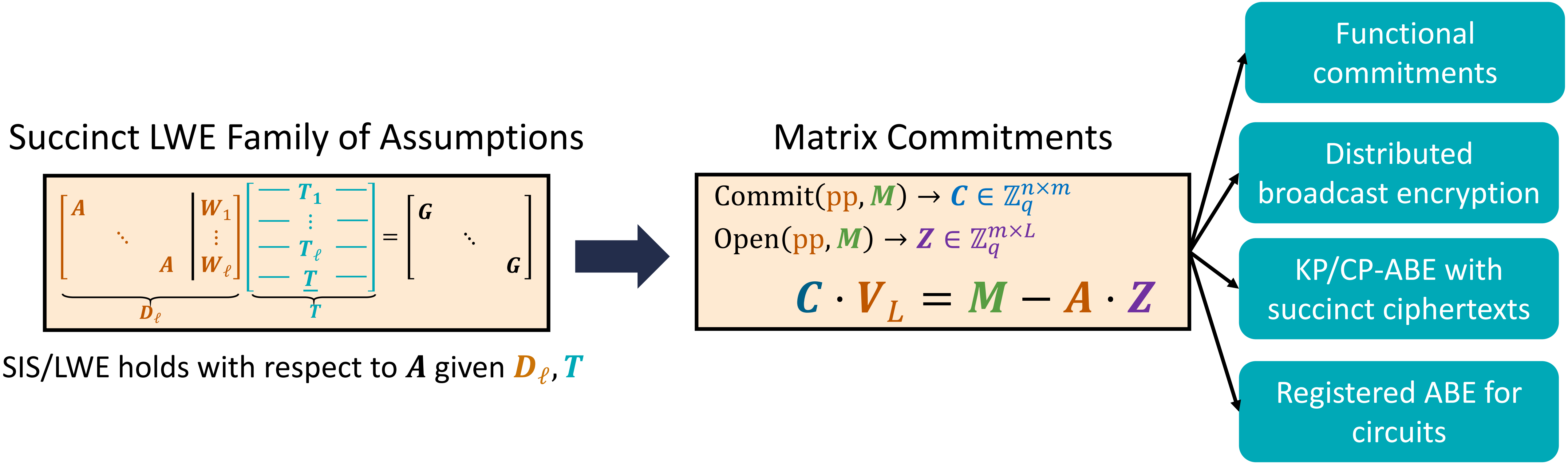
Functional commitments for all circuits (and SNARGs for P/poly)	[WW23, WW23b, Wee24, Wee25]
Optimal broadcast encryption	[Wee25]
Distributed broadcast encryption	[CW24, CHW25, WW25]
Nearly-optimal key-policy (and ciphertext-policy) ABE for circuits	[Wee24, Wee25]
Registered ABE for circuits	[CHW25, WW25]
Fully succinct randomized encodings	[AMR25]
Laconic function evaluation (and ABE) for RAM programs	[AMR25]

Applications of Succinct and Decomposed LWE

Functional commitments for all circuits (and SNARGs for P/poly)	[WW23, WW23b, Wee24, Wee25]
Optimal broadcast encryption	
Distributed broadcast encryption	
Nearly-optimal key-policy (and ciphertext-policy) ABE for circuits	[Wee24, Wee25]
Registered ABE for circuits	[CHW25, WW25]
Fully succinct randomized encodings	[AMR25]
Laconic function evaluation (and ABE) for RAM programs	[AMR25]

[Wee25b]: Functional commitments from circuits and SNARGs for P/poly from **standard SIS**!

Roadmap



Succinct LWE Family of Assumptions

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\begin{bmatrix} — & \boldsymbol{T}_1 & — \\ — & \vdots & — \\ — & \boldsymbol{T}_\ell & — \\ — & \underline{\boldsymbol{T}} & — \end{bmatrix}}_{\boldsymbol{T}} = \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}$$

SIS/LWE holds with respect to $\boldsymbol{A}$ given $\boldsymbol{D}_\ell, \boldsymbol{T}$

Matrix Commitments

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \boldsymbol{V}_L = \boldsymbol{M} - \boldsymbol{A} \cdot \boldsymbol{Z}$$

Functional commitments

Distributed broadcast encryption

KP/CP-ABE with succinct ciphertexts

Registered ABE for circuits

Roadmap

Succinct LWE Family of Assumptions

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\left[\begin{array}{ccc} \text{---} & \boldsymbol{T}_1 & \text{---} \\ \text{---} & \vdots & \text{---} \\ \text{---} & \boldsymbol{T}_\ell & \text{---} \\ \text{---} & \underline{\boldsymbol{T}} & \text{---} \end{array}\right]}_{\boldsymbol{T}} = \left[\begin{array}{ccc} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{array}\right]$$

SIS/LWE holds with respect to $\boldsymbol{A}$ given $\boldsymbol{D}_\ell, \boldsymbol{T}$

Matrix Commitments

$$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$$

$$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$$

$$\boldsymbol{C} \cdot \boldsymbol{V}_L = \boldsymbol{M} - \boldsymbol{A} \cdot \boldsymbol{Z}$$

- Functional commitments
- Distributed broadcast encryption
- KP/CP-ABE with succinct ciphertexts
- Registered ABE for circuits

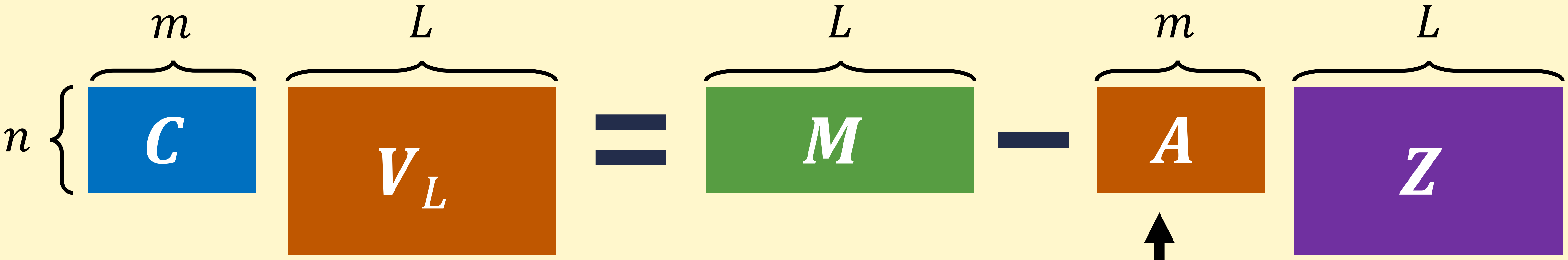
A Useful Abstraction: Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$ $\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

deterministic algorithms



$$n\left\{\overbrace{\boldsymbol{C}}^{m}\right.\overbrace{\boldsymbol{V}_L}^{L} = \overbrace{\boldsymbol{M}}^{L} - \overbrace{\boldsymbol{A}}^{m}\,\overbrace{\boldsymbol{Z}}^{L}$$

low-norm

low-norm

determined by the public parameters pp

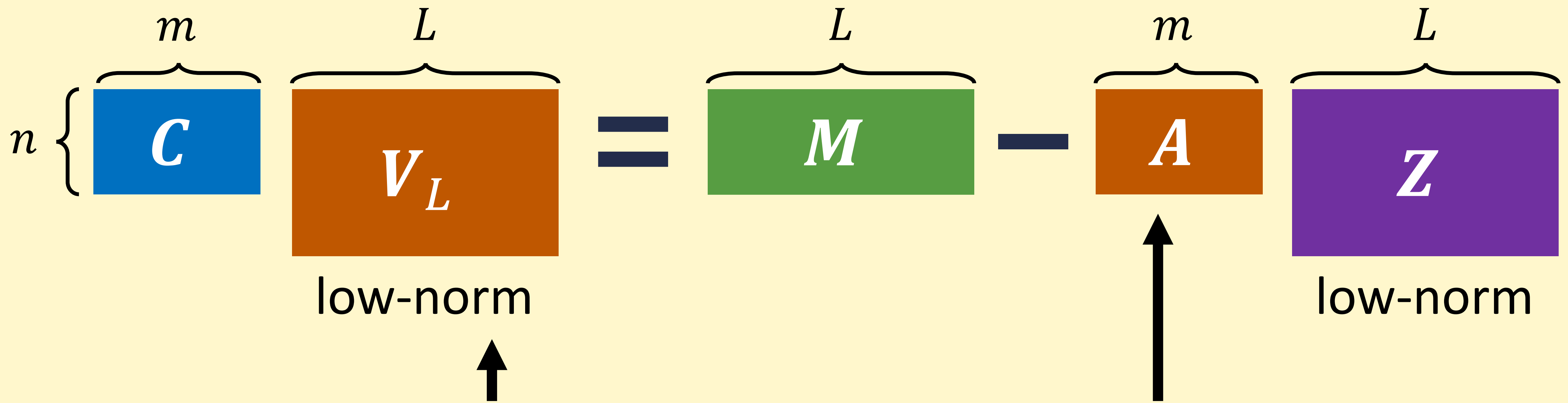
A Useful Abstraction: Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$ $\qquad$ $\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

deterministic algorithms



Instantiation: pp is uniform random string of length $\mathrm{poly}(m, \log L)$

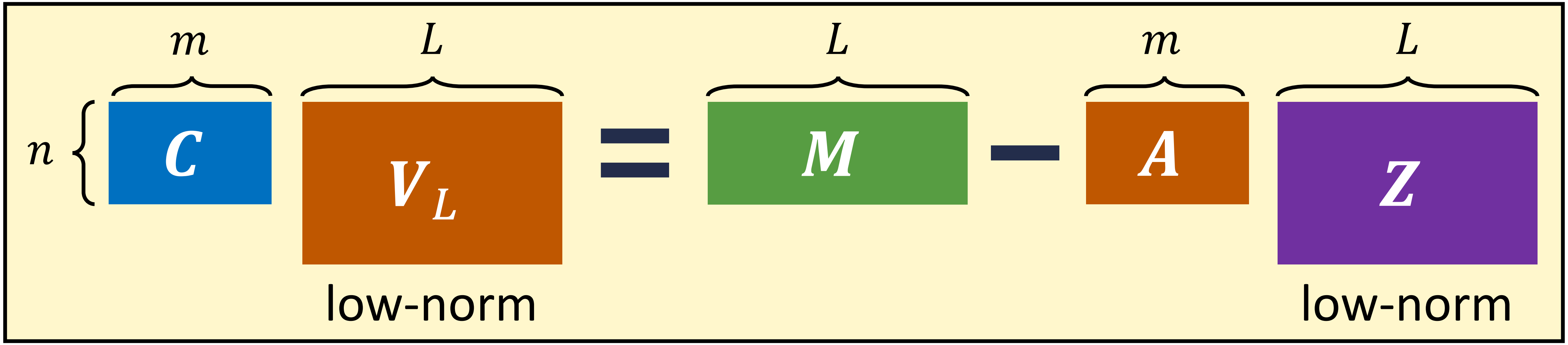
A Useful Abstraction: Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$ $\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

deterministic algorithms



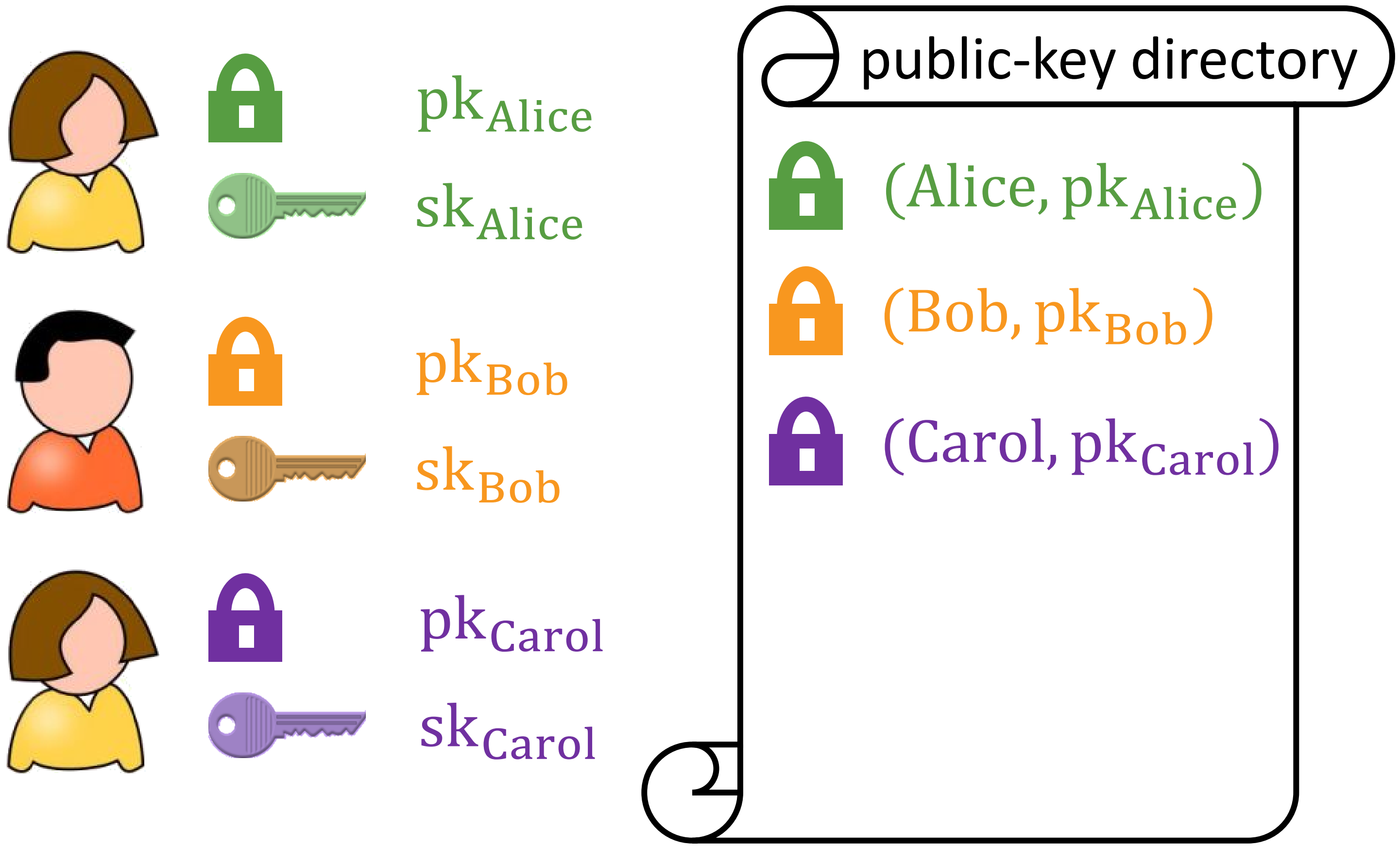
$$n\left\{\overbrace{\boldsymbol{C}}^{m}\right.\underset{\text{low-norm}}{\overbrace{\boldsymbol{V}_L}^{L}} = \overbrace{\boldsymbol{M}}^{L} - \overbrace{\boldsymbol{A}}^{m}\underset{\text{low-norm}}{\overbrace{\boldsymbol{Z}}^{L}}$$

Security property: $(\mathrm{pp}, \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}) \approx (\mathrm{pp}, \boldsymbol{u}^{\mathrm{T}})$

LWE holds with respect to $\boldsymbol{A}$ *given* pp

Distributed Broadcast Encryption

[WQZD14, BZ14]



$\mathrm{pk}_{\mathrm{Alice}}$

$\mathrm{sk}_{\mathrm{Alice}}$

$\mathrm{pk}_{\mathrm{Bob}}$

$\mathrm{sk}_{\mathrm{Bob}}$

$\mathrm{pk}_{\mathrm{Carol}}$

$\mathrm{sk}_{\mathrm{Carol}}$

public-key directory

$(\mathrm{Alice}, \mathrm{pk}_{\mathrm{Alice}})$

$(\mathrm{Bob}, \mathrm{pk}_{\mathrm{Bob}})$

$(\mathrm{Carol}, \mathrm{pk}_{\mathrm{Carol}})$

Users generate public/private keys independently

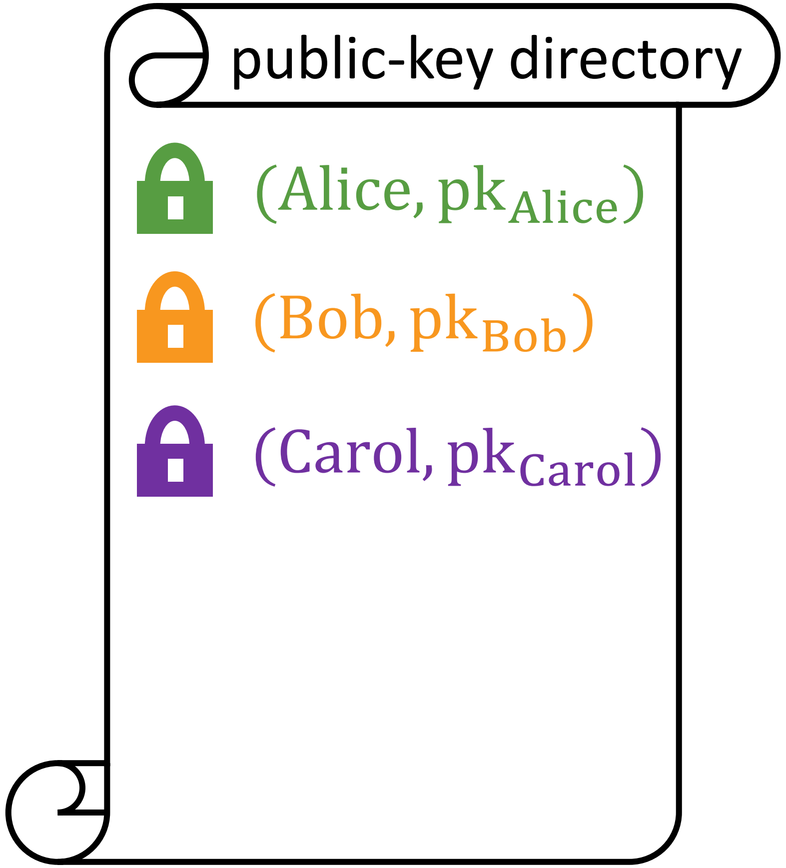
Suppose we want to send a message to an arbitrary set of N users

Trivial solution: encrypt individual to each user; ciphertext size scales linearly with N

Distributed broadcast encryption: encrypt to an **arbitrary** set of public keys with a **short** ciphertext

Distributed Broadcast Encryption

[WQZD14, BZ14]



public-key directory

$(\text{Alice}, \text{pk}_{\text{Alice}})$

$(\text{Bob}, \text{pk}_{\text{Bob}})$

$(\text{Carol}, \text{pk}_{\text{Carol}})$

$\text{Setup}(1^\lambda) \to \text{pp}$

Generates a set of public parameters

$\text{KeyGen}(\text{pp}, \text{id}) \to (\text{pk}_{\text{id}}, \text{sk}_{\text{id}})$

Samples a key-pair for a user

$\text{Encrypt}(\text{pp}, \{\text{pk}_{\text{id}}\}_{\text{id} \in S}, m) \to \text{ct}$

Can encrypt a message m to any set of user public keys

Efficiency: $|\text{ct}| = |m| + \text{poly}(\lambda, \log|S|)$

$\text{Decrypt}(\text{pp}, \{\text{pk}_{\text{id}}\}_{\text{id} \in S}, \text{sk}_{\text{id}}, \text{ct}) \to m$

Correctness: Any secret key sk_{id} associated with $\text{id} \in S$ can decrypt

Security: ct computationally hides m if adversary does not have a key for an identity $\text{id} \in S$

Distributed Broadcast Encryption

[WQZD14, BZ14]

- *Trustless* version of broadcast encryption [FN93] without a central authority (or master secret key)
- Implies broadcast encryption with a long master public key
- Can also consider "registered" variant where encryption and decryption only needs to know identities and not public keys

$\mathsf{Setup}(1^\lambda) \to \mathrm{pp}$

Generates a set of public parameters

$\mathsf{KeyGen}(\mathrm{pp}, \mathrm{id}) \to (\mathrm{pk}_{\mathrm{id}}, \mathrm{sk}_{\mathrm{id}})$

Samples a key-pair for a user

$\mathsf{Encrypt}(\mathrm{pp}, \{\mathrm{pk}_{\mathrm{id}}\}_{\mathrm{id} \in S}, m) \to \mathrm{ct}$

Can encrypt a message m to any set of user public keys

Efficiency: $|\mathrm{ct}| = |m| + \mathrm{poly}(\lambda, \log|S|)$

$\mathsf{Decrypt}(\mathrm{pp}, \{\mathrm{pk}_{\mathrm{id}}\}_{\mathrm{id} \in S}, \mathrm{sk}_{\mathrm{id}}, \mathrm{ct}) \to m$

Correctness: Any secret key $\mathrm{sk}_{\mathrm{id}}$ associated with $\mathrm{id} \in S$ can decrypt

Security: ct computationally hides m if adversary does not have a key for an identity $\mathrm{id} \in S$

Distributed Broadcast Encryption via Matrix Commitments

[WW25]

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Public parameters: pp , $\boldsymbol{A}_0 \leftarrow \mathbb{Z}_q^{n \times m}$, $\boldsymbol{p} \leftarrow \mathbb{Z}_q^n$

$\boldsymbol{V} = [\, \boldsymbol{v}_1 \mid \cdots \mid \boldsymbol{v}_L \,]$

Key generation (for identity $i \leq L$): $\boldsymbol{r}_i \leftarrow \{0,1\}^m$

Set $L = 2^\lambda$ and assume identities are λ-bits

$$\mathrm{pk}_i = \boldsymbol{t}_i = \boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p} - \boldsymbol{A}_0 \boldsymbol{v}_i \in \mathbb{Z}_q^n \qquad \mathrm{sk}_i = \boldsymbol{r}_i$$

Encryption (of message μ to public keys $\{\mathrm{pk}_i\}_{i \in S}$):

Construct **sparse** public-key matrix $\boldsymbol{M} \in \mathbb{Z}_q^L$

i^{th} column of $\boldsymbol{M}$ is $\mathrm{pk}_i = \boldsymbol{t}_i$ if $i \in S$ and $\boldsymbol{0}$ otherwise

$\boldsymbol{C} = \mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \qquad \boldsymbol{s} \leftarrow \mathbb{Z}_q^n$

$\boldsymbol{s}^{\mathrm{T}} \boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}}$

$\boldsymbol{s}^{\mathrm{T}} (\boldsymbol{A}_0 + \boldsymbol{C}) + \boldsymbol{e}_2^{\mathrm{T}}$

$\boldsymbol{s}^{\mathrm{T}} \boldsymbol{p} + e_3 + \mu \cdot \lfloor q/2 \rceil$

Ciphertext

Distributed Broadcast Encryption via Matrix Commitments

[WW25]

$\text{Commit}(\text{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\text{Open}(\text{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

$\text{pk}_i = \boldsymbol{t}_i = \boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p} - \boldsymbol{A}_0\boldsymbol{v}_i \in \mathbb{Z}_q^n$

$\text{sk}_i = \boldsymbol{r}_i$

Public key

$\boldsymbol{C} = \text{Commit}(\text{pp}, \boldsymbol{M})$ $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$

$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}}$

(dual-Regev style)

$\boldsymbol{s}^{\mathrm{T}}(\boldsymbol{A}_0 + \boldsymbol{C}) + \boldsymbol{e}_2^{\mathrm{T}}$

$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + e_3 + \mu \cdot \lfloor q/2 \rceil$

Ciphertext

i^{th} column of $\boldsymbol{M}$ is $\text{pk}_i = \boldsymbol{t}_i$ if $i \in S$ and $\boldsymbol{0}$ otherwise

Suppose $i \in S$:

$$\begin{aligned} \boldsymbol{C} \cdot \boldsymbol{v}_i &= \boldsymbol{t}_i - \boldsymbol{A} \cdot \boldsymbol{z}_i \\ &= \boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p} - \boldsymbol{A}_0\boldsymbol{v}_i - \boldsymbol{A}\boldsymbol{z}_i \end{aligned}$$

Decryption:

$$\left(\boldsymbol{s}^{\mathrm{T}}(\boldsymbol{A}_0 + \boldsymbol{C}) + \boldsymbol{e}_2^{\mathrm{T}}\right) \cdot \boldsymbol{v}_i$$

$$\approx \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}_0\boldsymbol{v}_i + \boldsymbol{s}^{\mathrm{T}}(\boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p} - \boldsymbol{A}_0\boldsymbol{v}_i - \boldsymbol{A}\boldsymbol{z}_i)$$

Distributed Broadcast Encryption via Matrix Commitments

[WW25]

$\mathsf{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\mathsf{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

$\mathrm{pk}_i = \boldsymbol{t}_i = \boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p} - \boldsymbol{A}_0\boldsymbol{v}_i \in \mathbb{Z}_q^n$

$\mathrm{sk}_i = \boldsymbol{r}_i$

Public key

$\boldsymbol{C} = \mathsf{Commit}(\mathrm{pp}, \boldsymbol{M})$ $\quad$ $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$

$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}}$

(dual-Regev style)

$\boldsymbol{s}^{\mathrm{T}}(\boldsymbol{A}_0 + \boldsymbol{C}) + \boldsymbol{e}_2^{\mathrm{T}}$

$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + e_3 + \mu \cdot \lfloor q/2 \rceil$

Ciphertext

i^{th} column of $\boldsymbol{M}$ is $\mathrm{pk}_i = \boldsymbol{t}_i$ if $i \in S$ and $\boldsymbol{0}$ otherwise

Suppose $i \in S$:

$$\begin{aligned}\boldsymbol{C} \cdot \boldsymbol{v}_i &= \boldsymbol{t}_i - \boldsymbol{A} \cdot \boldsymbol{z}_i \\ &= \boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p} - \boldsymbol{A}_0\boldsymbol{v}_i - \boldsymbol{A}\boldsymbol{z}_i\end{aligned}$$

Decryption:

$$\left.\begin{aligned}&\left(\boldsymbol{s}^{\mathrm{T}}(\boldsymbol{A}_0 + \boldsymbol{C}) + \boldsymbol{e}_2^{\mathrm{T}}\right) \cdot \boldsymbol{v}_i \\ &\quad \approx \cancel{\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}_0}\boldsymbol{v}_i + \boldsymbol{s}^{\mathrm{T}}(\boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p} - \cancel{\boldsymbol{A}_0\boldsymbol{v}_i} - \boldsymbol{A}\boldsymbol{z}_i) \\ &\quad = \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}(\boldsymbol{r}_i - \boldsymbol{z}_i) + \boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} \\ &\left(\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}}\right) \cdot (\boldsymbol{r}_i - \boldsymbol{z}_i) \approx \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}(\boldsymbol{r}_i - \boldsymbol{z}_i)\end{aligned}\right\} \text{Recover } \boldsymbol{s}^{\mathrm{T}}\boldsymbol{p}$$

Distributed Broadcast Encryption via Matrix Commitments

[WW25]

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n\times m}$

$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m\times L}$

$$\boldsymbol{C} \cdot \underset{\text{low-norm}}{\boldsymbol{V}_L} = \boldsymbol{M} - \boldsymbol{A} \cdot \underset{\text{low-norm}}{\boldsymbol{Z}}$$

$$\mathrm{pk}_i = \boldsymbol{t}_i = \boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p} - \boldsymbol{A}_0\boldsymbol{v}_i \in \mathbb{Z}_q^n$$

$$\mathrm{sk}_i = \boldsymbol{r}_i$$

Public key

$\boldsymbol{C} = \mathrm{Commit}(\mathrm{pp}, \boldsymbol{M})$ $\quad$ $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$

$$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}}$$

(dual-Regev style)

$$\boldsymbol{s}^{\mathrm{T}}(\boldsymbol{A}_0 + \boldsymbol{C}) + \boldsymbol{e}_2^{\mathrm{T}}$$

$$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + e_3 + \mu \cdot \lfloor q/2 \rceil$$

Ciphertext

i^{th} column of $\boldsymbol{M}$ is $\mathrm{pk}_i = \boldsymbol{t}_i$ if $i \in S$ and $\boldsymbol{0}$ otherwise

Gives a selectively-secure distributed broadcast encryption scheme (for arbitrary number of users) and a transparent setup

Previously: only known from witness encryption or indistinguishability obfuscation

Generalizations:

- Adaptive security in the random oracle model
- Registered attribute-based encryption for unbounded number of users and succinct ciphertexts (in random oracle model)

Not known from witness encryption!

Succinct Attribute-Based Encryption

[Wee25]

$$\mathrm{Setup}(1^\lambda) \to (\mathrm{mpk}, \mathrm{msk})$$

$$\mathrm{KeyGen}(\mathrm{msk}, f) \to \mathrm{sk}_f$$

$$\mathrm{Encrypt}(\mathrm{mpk}, x, m) \to \mathrm{ct}_{x,m}$$

$$\mathrm{Decrypt}(x, f, \mathrm{sk}_f, \mathrm{ct}_{x,m}) \to \begin{cases} m & f(x) = 0 \\ \bot & f(x) = 1 \end{cases}$$

Key-policy ABE: Secret keys associated with functions $f: \{0,1\}^\ell \to \{0,1\}$

Ciphertexts associated with attributes $x \in \{0,1\}^\ell$

Correctness: Can decryption when $f(x) = 0$

Security: Message hidden when $f(x) = 1$

Succinctness: $|\mathrm{ct}_{x,m}| = |m| + \mathrm{poly}(\lambda, \log|x|)$

In the following, we will allow for a depth dependence as well:

$|\mathrm{ct}_{x,m}| = |m| + \mathrm{poly}(\lambda, d, \log|x|)$, where d is the depth of the Boolean circuit computing f

Homomorphic Computation using Lattices

[GSW13, BGGHNSVV14]

Encodes a vector $\boldsymbol{x} \in \{0,1\}^{\ell}$ with respect to matrix $\boldsymbol{B} = [\boldsymbol{B}_1 \mid \cdots \mid \boldsymbol{B}_{\ell}] \in \mathbb{Z}_q^{n \times \ell m}$

$$\boxed{\boldsymbol{B}_1 - x_1 \boldsymbol{G}} \boxed{\boldsymbol{B}_2 - x_2 \boldsymbol{G}} \boxed{\cdots} \boxed{\boldsymbol{B}_{\ell} - x_{\ell} \boldsymbol{G}} \qquad \boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$$

Given any function $f: \{0,1\}^{\ell} \rightarrow \{0,1\}$, there exists a low-norm matrix $\boldsymbol{H}_{\boldsymbol{B},f,\boldsymbol{x}}$ where

$$\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \boldsymbol{H}_{\boldsymbol{B},f,\boldsymbol{x}} = \boldsymbol{B}_f - f(x) \cdot \boldsymbol{G}$$

encoding of $\boldsymbol{x}$ with respect to $\boldsymbol{B}$

encoding of $f(\boldsymbol{x})$ with respect to $\boldsymbol{B}_f$

Given $\boldsymbol{B}$ and f, can efficiently compute the matrix $\boldsymbol{B}_f$

Attribute-Based Encryption

[BGGHNSVV14]

"dual Regev public key" attribute-encoding matrix

Public key: $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}, \quad \boldsymbol{p} \in \mathbb{Z}_q^n, \quad \boldsymbol{B} \in \mathbb{Z}_q^{n \times \ell m}$

Secret key for f: low-norm vector $\boldsymbol{v}_f \in \mathbb{Z}^{2m}$ where $[\, \boldsymbol{A} \mid \boldsymbol{B}_f \,]\boldsymbol{v}_f = \boldsymbol{p}$

Ciphertext with attribute x: $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$

$$\boxed{\begin{array}{l} \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}} \\ \boldsymbol{s}^{\mathrm{T}}(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}) + \boldsymbol{e}_2^{\mathrm{T}} \\ \boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + e_3 + \mu \cdot \lfloor q/2 \rfloor \end{array}}$$

$$\longrightarrow \approx [\, \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} \mid \boldsymbol{s}^{\mathrm{T}}\boldsymbol{B}_f \,]\boldsymbol{v}_f$$

$$\xrightarrow{\text{multiply by } \boldsymbol{H}_{\boldsymbol{B},f,\boldsymbol{x}}} \approx \boldsymbol{s}^{\mathrm{T}}\boldsymbol{B}_f \nearrow$$

$$\approx \boldsymbol{s}^{\mathrm{T}}[\, \boldsymbol{A} \mid \boldsymbol{B}_f \,]\boldsymbol{v}_f$$

$$\approx \boldsymbol{s}^{\mathrm{T}}\boldsymbol{p}$$

$$\boxed{(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}) \cdot \boldsymbol{H}_{\boldsymbol{B},f,\boldsymbol{x}} = \boldsymbol{B}_f - f(\boldsymbol{x}) \cdot \boldsymbol{G}}$$

Attribute-Based Encryption

[BGGHNSVV14]

“dual Regev public key” attribute-encoding matrix

Public key: $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}, \quad \boldsymbol{p} \in \mathbb{Z}_q^n,$ $\boldsymbol{B} \in \mathbb{Z}_q^{n \times \ell m}$

Secret key for f: low-norm vector $\boldsymbol{v}_f \in \mathbb{Z}^{2m}$ where $[\, \boldsymbol{A} \mid \boldsymbol{B}_f \,]\boldsymbol{v}_f = \boldsymbol{p}$

Ciphertext with attribute x:

$$\boxed{\begin{array}{l} \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}} \\ \boldsymbol{s}^{\mathrm{T}}\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) + \boldsymbol{e}_2^{\mathrm{T}} \\ \boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + e_3 + \mu \cdot \lfloor q/2 \rceil \end{array}}$$

Not succinct because $|\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}| = \ell \cdot nm \log q$

Need to encode attribute to compute on it

$$\boxed{\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \boldsymbol{H}_{\boldsymbol{B},f,\boldsymbol{x}} = \boldsymbol{B}_f - f(\boldsymbol{x}) \cdot \boldsymbol{G}}$$

Succinct Attribute-Based Encryption

[Wee24, Wee25]

“dual Regev public key” attribute-encoding matrix

Public key: $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}, \quad \boldsymbol{p} \in \mathbb{Z}_q^n,$ $\boldsymbol{B} \in \mathbb{Z}_q^{n\times \ell m}$

Secret key for f: low-norm vector $\boldsymbol{v}_f \in \mathbb{Z}^{2m}$ where $[\,\boldsymbol{A} \mid \boldsymbol{B}_f\,]\boldsymbol{v}_f = \boldsymbol{p}$

Ciphertext with attribute x:

$$\boxed{\begin{array}{l} \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}} \\ \boldsymbol{s}^{\mathrm{T}}\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) + \boldsymbol{e}_2^{\mathrm{T}} \\ \boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + e_3 + \mu \cdot \lfloor q/2 \rfloor \end{array}}$$

[Wee24, Wee25] approach: compress $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$

- Let $\boldsymbol{C}_{\boldsymbol{x}} \in \mathbb{Z}_q^{n\times m}$ be a commitment to $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$
- Then $\boldsymbol{C}_{\boldsymbol{x}}\boldsymbol{V} = \left(\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) - \boldsymbol{A}\boldsymbol{Z}$
- Sample $\widetilde{\boldsymbol{B}} \leftarrow \mathbb{Z}_q^{n\times m}$ and take $\boldsymbol{B} = \widetilde{\boldsymbol{B}}\boldsymbol{V} \in \mathbb{Z}_q^{n\times \ell m}$
- Then $\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G} = \widetilde{\boldsymbol{B}}\boldsymbol{V} - \boldsymbol{C}_{\boldsymbol{x}}\boldsymbol{V} - \boldsymbol{A}\boldsymbol{Z}$

$$\boxed{\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \boldsymbol{H}_{\boldsymbol{B},f,\boldsymbol{x}} = \boldsymbol{B}_f - f(\boldsymbol{x}) \cdot \boldsymbol{G}}$$

Succinct Attribute-Based Encryption

[Wee24, Wee25]

“dual Regev public key” attribute-encoding matrix

Public key: $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}, \quad \boldsymbol{p} \in \mathbb{Z}_q^{n},$ $\cancel{\boldsymbol{B} \in \mathbb{Z}_q^{n\times \ell m}} \longrightarrow \widetilde{\boldsymbol{B}} \in \mathbb{Z}_q^{n\times m}$

public parameters independent of attribute length!

Secret key for f: low-norm vector $\boldsymbol{v}_f \in \mathbb{Z}^{2m}$ where $[\,\boldsymbol{A} \mid \boldsymbol{B}_f\,]\boldsymbol{v}_f = \boldsymbol{p}$

Ciphertext with attribute x:

$$\boxed{\begin{array}{l} \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}} \\ \boldsymbol{s}^{\mathrm{T}}\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) + \boldsymbol{e}_2^{\mathrm{T}} \\ \boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + e_3 + \mu \cdot \lfloor q/2 \rfloor \end{array}}$$

[Wee24, Wee25] approach: compress $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$

- Let $\boldsymbol{C}_{\boldsymbol{x}} \in \mathbb{Z}_q^{n\times m}$ be a commitment to $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$
- Then $\boldsymbol{C}_{\boldsymbol{x}}\boldsymbol{V} = \left(\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) - \boldsymbol{A}\boldsymbol{Z}$
- Sample $\widetilde{\boldsymbol{B}} \leftarrow \mathbb{Z}_q^{n\times m}$ and take $\boldsymbol{B} = \widetilde{\boldsymbol{B}}\boldsymbol{V} \in \mathbb{Z}_q^{n\times \ell m}$
- Then $\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G} = \widetilde{\boldsymbol{B}}\boldsymbol{V} - \boldsymbol{C}_{\boldsymbol{x}}\boldsymbol{V} - \boldsymbol{A}\boldsymbol{Z}$

$$\boxed{\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \boldsymbol{H}_{\boldsymbol{B},f,\boldsymbol{x}} = \boldsymbol{B}_f - f(\boldsymbol{x}) \cdot \boldsymbol{G}}$$

Succinct Attribute-Based Encryption

[Wee24, Wee25]

"dual Regev public key" attribute-encoding matrix

Public key: $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}, \quad \boldsymbol{p} \in \mathbb{Z}_q^{n},$ $\boldsymbol{B} \in \mathbb{Z}_q^{n\times \ell m}$ $\longrightarrow$ $\widetilde{\boldsymbol{B}} \in \mathbb{Z}_q^{n\times m}$

public parameters independent of attribute length!

Secret key for f: low-norm vector $\boldsymbol{v}_f \in \mathbb{Z}^{2m}$ where $[\,\boldsymbol{A} \mid \boldsymbol{B}_f\,]\boldsymbol{v}_f = \boldsymbol{p}$

Ciphertext with attribute x:

$$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}}$$

$$\cancel{\boldsymbol{s}^{\mathrm{T}}\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) + \boldsymbol{e}_2^{\mathrm{T}}}$$

$$\boldsymbol{s}^{\mathrm{T}}\left(\widetilde{\boldsymbol{B}} - \boldsymbol{C}_x\right) + \boldsymbol{e}_2^{\mathrm{T}}$$

$$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + e_3 + \mu \cdot \lfloor q/2 \rfloor$$

Everything else unchanged!

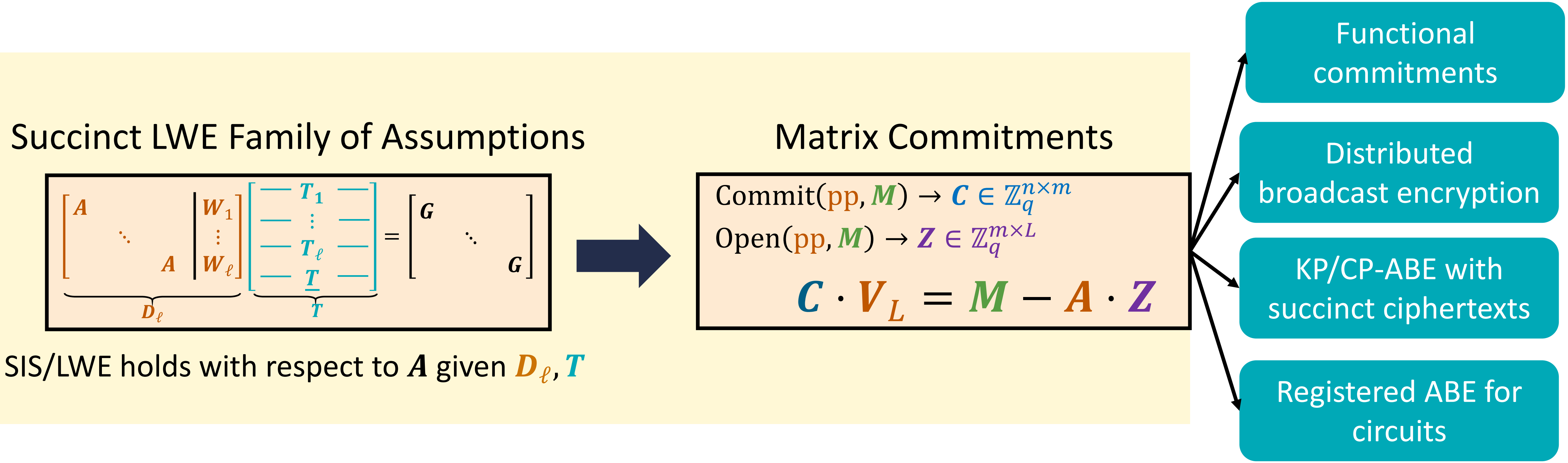
[Wee24, Wee25] approach: compress $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$

- Let $\boldsymbol{C}_x \in \mathbb{Z}_q^{n\times m}$ be a commitment to $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$
- Then $\boldsymbol{C}_x\boldsymbol{V} = \left(\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) - \boldsymbol{A}\boldsymbol{Z}$
- Sample $\widetilde{\boldsymbol{B}} \leftarrow \mathbb{Z}_q^{n\times m}$ and take $\boldsymbol{B} = \widetilde{\boldsymbol{B}}\boldsymbol{V} \in \mathbb{Z}_q^{n\times \ell m}$
- Then $\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G} = \widetilde{\boldsymbol{B}}\boldsymbol{V} - \boldsymbol{C}_x\boldsymbol{V} - \boldsymbol{A}\boldsymbol{Z}$

Correctness:

$$\left(\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}\right)(-\boldsymbol{Z}) + \boldsymbol{s}^{\mathrm{T}}\left(\widetilde{\boldsymbol{B}} - \boldsymbol{C}_x\right)\boldsymbol{V} = \boldsymbol{s}^{\mathrm{T}}\left(\widetilde{\boldsymbol{B}}\boldsymbol{V} - \boldsymbol{C}_x\boldsymbol{V} - \boldsymbol{A}\boldsymbol{Z}\right) = \boldsymbol{s}^{\mathrm{T}}\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right)$$

Roadmap



Succinct LWE Family of Assumptions

$$\underbrace{\left[\begin{array}{ccc|c} A & & & W_1 \\ & \ddots & & \vdots \\ & & A & W_\ell \end{array}\right]}_{D_\ell}\underbrace{\begin{bmatrix} — & T_1 & — \\ — & \vdots & — \\ — & T_\ell & — \\ — & \underline{T} & — \end{bmatrix}}_{T} = \begin{bmatrix} G & & \\ & \ddots & \\ & & G \end{bmatrix}$$

SIS/LWE holds with respect to $\boldsymbol{A}$ given $\boldsymbol{D}_\ell, \boldsymbol{T}$

Matrix Commitments

$\text{Commit}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\text{Open}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \boldsymbol{V}_L = \boldsymbol{M} - \boldsymbol{A} \cdot \boldsymbol{Z}$$

Functional commitments

Distributed broadcast encryption

KP/CP-ABE with succinct ciphertexts

Registered ABE for circuits

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$$

$$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$$

$$\underbrace{\boldsymbol{C} \cdot \boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \underbrace{\boldsymbol{A} \cdot \boldsymbol{Z}}_{\text{low-norm}}$$

Basic building block: the trapdoor from a succinct LWE instance

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\begin{bmatrix} - & \boldsymbol{T}_1 & - \\ - & \vdots & - \\ - & \boldsymbol{T}_\ell & - \\ - & \underline{\boldsymbol{T}} & - \end{bmatrix}}_{\boldsymbol{T}} = \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}$$

$\boldsymbol{A}, \boldsymbol{W}_i \in \mathbb{Z}_q^{n \times m}$

$\boldsymbol{T}_i, \underline{\boldsymbol{T}} \in \mathbb{Z}_q^{m \times \ell m}$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n\times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n\times m}$

$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m\times L}$

$$\boldsymbol{C} \cdot \underset{\text{low-norm}}{\boldsymbol{V}_L} = \boldsymbol{M} - \boldsymbol{A} \cdot \underset{\text{low-norm}}{\boldsymbol{Z}}$$

Starting point: commitment to $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G} = [x_1 \boldsymbol{G} \mid x_2 \boldsymbol{G} \mid \cdots \mid x_\ell \boldsymbol{G}]$ where $\boldsymbol{x} \in \{0,1\}^\ell$

$$\underbrace{[x_1 \boldsymbol{I} \mid \cdots \mid x_\ell \boldsymbol{I}] \left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{[x_1 \boldsymbol{A} \mid \cdots \mid x_\ell \boldsymbol{A} \mid \Sigma_{i\in[\ell]} x_i \boldsymbol{W}_i]} \begin{bmatrix} \boldsymbol{T}_1 \\ \vdots \\ \boldsymbol{T}_\ell \\ \underline{\boldsymbol{T}} \end{bmatrix} = \underbrace{[x_1 \boldsymbol{I} \mid \cdots \mid x_\ell \boldsymbol{I}] \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}}_{[x_1 \boldsymbol{G} \mid \cdots \mid x_\ell \boldsymbol{G}] = \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}}$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$$\text{Commit}(\text{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$$

$$\text{Open}(\text{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Starting point: commitment to $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G} = [x_1 \boldsymbol{G} \mid x_2 \boldsymbol{G} \mid \cdots \mid x_\ell \boldsymbol{G}]$ where $\boldsymbol{x} \in \{0,1\}^\ell$

$$\left[x_1 \boldsymbol{A} \mid \cdots \mid x_\ell \boldsymbol{A} \mid \Sigma_{i \in [\ell]} x_i \boldsymbol{W}_i\right] \begin{bmatrix} \boldsymbol{T}_1 \\ \vdots \\ \boldsymbol{T}_\ell \\ \underline{\boldsymbol{T}} \end{bmatrix} = [x_1 \boldsymbol{G} \mid \cdots \mid x_\ell \boldsymbol{G}] = \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underset{\text{low-norm}}{\boldsymbol{V}_L} = \boldsymbol{M} - \boldsymbol{A} \cdot \underset{\text{low-norm}}{\boldsymbol{Z}}$$

Starting point: commitment to $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G} = [x_1 \boldsymbol{G} \mid x_2 \boldsymbol{G} \mid \cdots \mid x_\ell \boldsymbol{G}]$ where $\boldsymbol{x} \in \{0,1\}^\ell$

$$\underbrace{\left[x_1 \boldsymbol{A} \mid \cdots \mid x_\ell \boldsymbol{A} \mid \Sigma_{i \in [\ell]} x_i \boldsymbol{W}_i\right] \begin{bmatrix} \boldsymbol{T}_1 \\ \vdots \\ \boldsymbol{T}_\ell \\ \underline{\boldsymbol{T}} \end{bmatrix}}_{\boldsymbol{A} \cdot \left(\Sigma_{i \in [\ell]} x_i \boldsymbol{T}_i\right) + \left(\Sigma_{i \in [\ell]} x_i \boldsymbol{W}_i\right) \underline{\boldsymbol{T}}} = [x_1 \boldsymbol{G} \mid \cdots \mid x_\ell \boldsymbol{G}] = \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Starting point: commitment to $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G} = [x_1 \boldsymbol{G} \mid x_2 \boldsymbol{G} \mid \cdots \mid x_\ell \boldsymbol{G}]$ where $\boldsymbol{x} \in \{0,1\}^\ell$

$$\boldsymbol{A} \cdot \left(\Sigma_{i \in [\ell]} x_i \boldsymbol{T}_i\right) + \left(\Sigma_{i \in [\ell]} x_i \boldsymbol{W}_i\right) \underline{\boldsymbol{T}} \quad = \quad [x_1 \boldsymbol{G} \mid \cdots \mid x_\ell \boldsymbol{G}] = \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$$

Rearranging:

$$\underbrace{\left(\Sigma_{i \in [\ell]} x_i \boldsymbol{W}_i\right)}_{\textbf{commitment}} \cdot \underline{\boldsymbol{T}} = \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G} - \boldsymbol{A} \cdot \underbrace{\left(\Sigma_{i \in [\ell]} x_i \boldsymbol{T}_i\right)}_{\textbf{opening}}$$

Note: $\underline{\boldsymbol{T}}, \boldsymbol{T}_i$ are blocks of the succinct LWE trapdoor, so they have low norm

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Committing to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times m}$:

Compactification [BTVW17]: $\left(\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right) = \boldsymbol{M}$

$\mathrm{bits}(\boldsymbol{M}) = \mathrm{vec}\left(\boldsymbol{G}^{-1}(\boldsymbol{M})\right)$: vectorization of bit decomposition of $\boldsymbol{M}$

$\mathrm{vec}(\boldsymbol{M})$: concatenation of the columns of $\boldsymbol{M}$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\text{Commit}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\text{Open}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underset{\text{low-norm}}{\boldsymbol{V}_L} = \boldsymbol{M} - \boldsymbol{A} \cdot \underset{\text{low-norm}}{\boldsymbol{Z}}$$

Committing to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times m}$:

Compactification [BTVW17]: $$\left(\text{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \overbrace{\left(\boldsymbol{I}_L \otimes \text{vec}(\boldsymbol{I}_m)\right)}^{\text{has small norm, only depends on dimension } L \text{, not } \boldsymbol{M}} = \boldsymbol{M}$$

Commit to $\text{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}$:

$$\boldsymbol{C} \cdot \underline{\boldsymbol{T}} = \text{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G} - \boldsymbol{A} \cdot \boldsymbol{Z}'$$

Multiply by $\boldsymbol{I}_L \otimes \text{vec}(\boldsymbol{I}_m)$:

$$\boldsymbol{C} \cdot \underline{\boldsymbol{T}} \cdot \left(\boldsymbol{I}_L \otimes \text{vec}(\boldsymbol{I}_m)\right) = \left(\text{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}\right)\left(\boldsymbol{I}_L \otimes \text{vec}(\boldsymbol{I}_m)\right) - \boldsymbol{A} \cdot \boldsymbol{Z}' \cdot \left(\boldsymbol{I}_L \otimes \text{vec}(\boldsymbol{I}_m)\right)$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n\times L}$

$$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{C} \in \mathbb{Z}_q^{n\times m}$$

$$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{Z} \in \mathbb{Z}_q^{m\times L}$$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Committing to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n\times m}$:

Compactification [BTVW17]: $\left(\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \overbrace{\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)}^{\text{has small norm, only depends on dimension } L, \text{ not } \boldsymbol{M}} = \boldsymbol{M}$

Commit to $\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}$:

$$\boldsymbol{C} \cdot \underline{\boldsymbol{T}} = \mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G} - \boldsymbol{A} \cdot \boldsymbol{Z}'$$

$$\boxed{\boldsymbol{V}_L \quad = \quad \underline{\boldsymbol{T}}\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)}$$

Multiply by $\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)$:

$$\boldsymbol{C} \cdot \underline{\boldsymbol{T}} \cdot \left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right) = \left(\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}\right)\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right) - \boldsymbol{A} \cdot \boldsymbol{Z}' \cdot \left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underset{\text{low-norm}}{\boldsymbol{V}_L} = \boldsymbol{M} - \boldsymbol{A} \cdot \underset{\text{low-norm}}{\boldsymbol{Z}}$$

Committing to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times m}$:

$$\textbf{Compactification } \text{[BTVW17]}\textbf{:} \; \left(\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \overbrace{\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)}^{\text{has small norm, only depends on dimension } L\text{, not } \boldsymbol{M}} = \boldsymbol{M}$$

Commit to $\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}$:

$$\boldsymbol{C} \cdot \underline{\boldsymbol{T}} = \mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G} - \boldsymbol{A} \cdot \boldsymbol{Z}'$$

$$\boxed{\boldsymbol{V}_L \quad = \quad \underline{\boldsymbol{T}}\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)}$$

Multiply by $\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)$:

$$\boldsymbol{C} \cdot \boldsymbol{V}_L = \left(\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}\right)\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right) - \boldsymbol{A} \cdot \boldsymbol{Z}' \cdot \left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\text{Commit}(\text{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\text{Open}(\text{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Committing to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times m}$:

Compactification [BTVW17]: $$\left(\text{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \overbrace{\left(\boldsymbol{I}_L \otimes \text{vec}(\boldsymbol{I}_m)\right)}^{\text{has small norm, only depends on dimension } L, \text{ not } \boldsymbol{M}} = \boldsymbol{M}$$

Commit to $\text{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}$:

$$\boldsymbol{C} \cdot \underline{\boldsymbol{T}} = \text{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G} - \boldsymbol{A} \cdot \boldsymbol{Z}'$$

$$\boxed{\boldsymbol{V}_L = \underline{\boldsymbol{T}}\left(\boldsymbol{I}_L \otimes \text{vec}(\boldsymbol{I}_m)\right)}$$

Multiply by $\boldsymbol{I}_L \otimes \text{vec}(\boldsymbol{I}_m)$:

$$\boldsymbol{C} \cdot \boldsymbol{V}_L = \boldsymbol{M} - \boldsymbol{A} \cdot \boldsymbol{Z}' \cdot \left(\boldsymbol{I}_L \otimes \text{vec}(\boldsymbol{I}_m)\right)$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n\times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n\times m}$

$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m\times L}$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Committing to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n\times m}$:

Compactification [BTVW17]: $$\left(\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \overbrace{\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)}^{\text{has small norm, only depends on dimension } L\text{, not } \boldsymbol{M}} = \boldsymbol{M}$$

Commit to $\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}$:

$$\boldsymbol{C} \cdot \underline{\boldsymbol{T}} = \mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G} - \boldsymbol{A} \cdot \boldsymbol{Z}'$$

$$\boxed{\begin{aligned} \boldsymbol{V}_L &= \underline{\boldsymbol{T}}\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right) \\ \boldsymbol{Z} &= \boldsymbol{Z}'\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right) \end{aligned}}$$

Multiply by $\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)$:

$$\boldsymbol{C} \cdot \boldsymbol{V}_L = \boldsymbol{M} - \boldsymbol{A} \cdot \boldsymbol{Z}' \cdot \left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$$

$$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \rightarrow \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Committing to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times m}$:

$$\textbf{Compactification [BTVW17]: } \left(\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}\right) \cdot \overbrace{\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)}^{\text{has small norm, only depends on dimension } L, \text{ not } \boldsymbol{M}} = \boldsymbol{M}$$

Commit to $\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G}$:

$$\boldsymbol{C} \cdot \underline{\boldsymbol{T}} = \mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{G} - \boldsymbol{A} \cdot \boldsymbol{Z}'$$

$$\boxed{\begin{aligned} \boldsymbol{V}_L &= \underline{\boldsymbol{T}}\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right) \\ \boldsymbol{Z} &= \boldsymbol{Z}'\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right) \end{aligned}}$$

Multiply by $\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)$:

$$\boldsymbol{C} \cdot \boldsymbol{V}_L \qquad = \quad \boldsymbol{M} \qquad - \boldsymbol{A} \cdot \boldsymbol{Z}$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n\times L}$

$$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n\times m}$$

$$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m\times L}$$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Recap:

succinct LWE trapdoor ($\ell = Lm$)

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

More compactly:

$$[\, \boldsymbol{I}_\ell \otimes \boldsymbol{A} \mid \boldsymbol{W} \,] \begin{bmatrix} \overline{\boldsymbol{T}} \\ \underline{\boldsymbol{T}} \end{bmatrix} = \boldsymbol{I}_\ell \otimes \boldsymbol{G}$$

$$\mathrm{pp} = \left(\boldsymbol{A}, \boldsymbol{W}, \overline{\boldsymbol{T}}, \underline{\boldsymbol{T}}\right)$$

$$\boldsymbol{V}_L = \underline{\boldsymbol{T}}\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)$$

$$\boldsymbol{C} = \left(\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{I}_n\right)\boldsymbol{W}$$

$$\boldsymbol{Z} = \left(\mathrm{bits}(\boldsymbol{M})^{\mathrm{T}} \otimes \boldsymbol{I}_n\right)\overline{\boldsymbol{T}}\left(\boldsymbol{I}_L \otimes \mathrm{vec}(\boldsymbol{I}_m)\right)$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

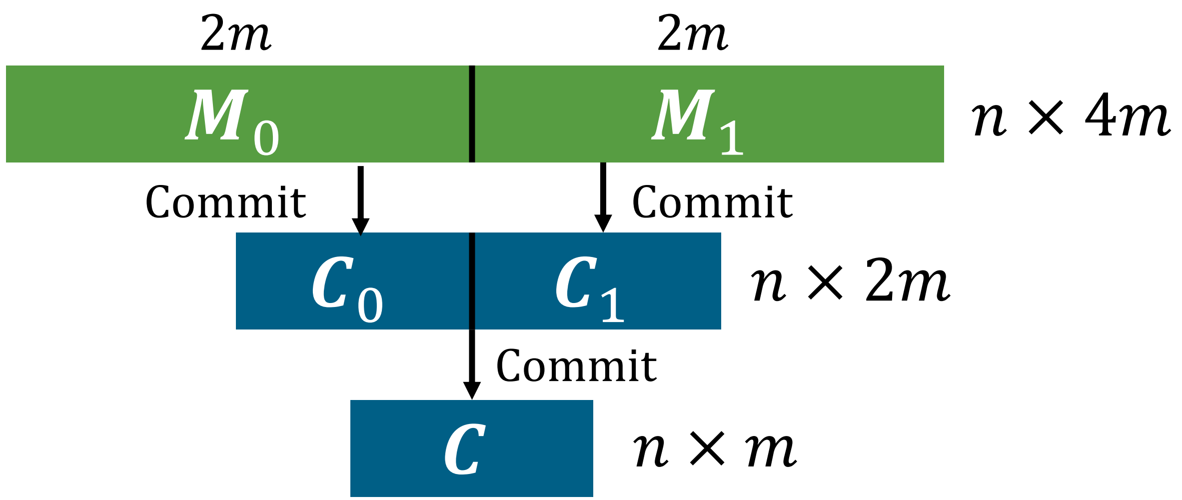
$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Currently, to commit to $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$, need trapdoor of dimension $\ell = Lm$

Sufficient to use trapdoor where $\ell = 2m^2$ (***independent*** of L) by using Merkel-style recursion

Approach ($L = 4m$):



Constructing Matrix Commitments

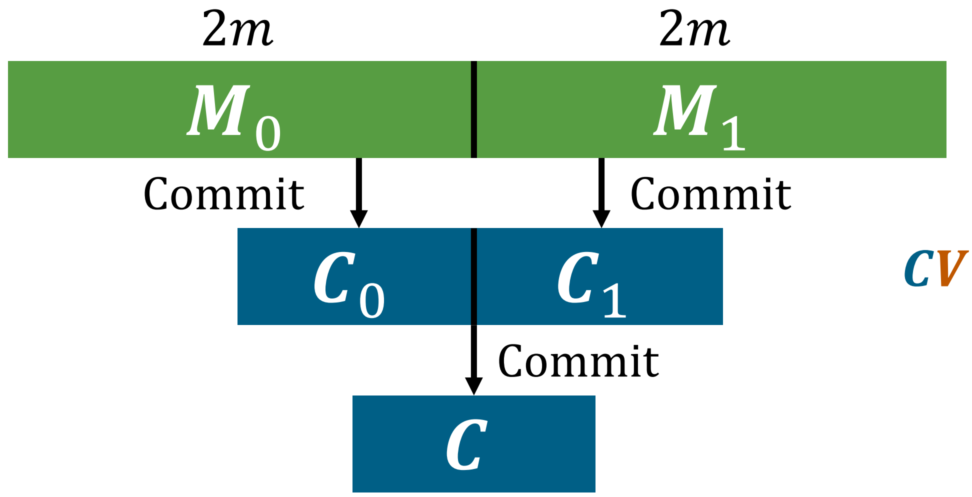
[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n\times L}$

$\text{Commit}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n\times m}$

$\text{Open}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m\times L}$

$$\boldsymbol{C} \cdot \underset{\text{low-norm}}{\boldsymbol{V}_L} = \boldsymbol{M} - \boldsymbol{A} \cdot \underset{\text{low-norm}}{\boldsymbol{Z}}$$



Generalizes to arbitrary $L \geq 2m$

$$\boldsymbol{C}_0\boldsymbol{V}_{2m} = \boldsymbol{M}_0 - \boldsymbol{A}\boldsymbol{Z}_0 \qquad \boldsymbol{C}_1\boldsymbol{V}_{2m} = \boldsymbol{M}_1 - \boldsymbol{A}\boldsymbol{Z}_1$$

$$\boldsymbol{C}\boldsymbol{V}_{2m} = [\,\boldsymbol{C}_0 \mid \boldsymbol{C}_1\,] - \boldsymbol{A}\boldsymbol{Z}_{01}$$

multiply by $\boldsymbol{I}_2 \otimes \boldsymbol{V}_{2m}$

$$\boldsymbol{C}\underbrace{\boldsymbol{V}_{2m}\begin{bmatrix} \boldsymbol{V}_{2m} & \\ & \boldsymbol{V}_{2m} \end{bmatrix}}_{\boldsymbol{V}_{4m}} = [\,\boldsymbol{C}_0 \mid \boldsymbol{C}_1\,]\begin{bmatrix} \boldsymbol{V}_{2m} & \\ & \boldsymbol{V}_{2m} \end{bmatrix} - \boldsymbol{A}\boldsymbol{Z}_{01}\begin{bmatrix} \boldsymbol{V}_{2m} & \\ & \boldsymbol{V}_{2m} \end{bmatrix}$$

$$= [\,\boldsymbol{M}_0 \mid \boldsymbol{M}_1\,] - \underbrace{\boldsymbol{A}[\,\boldsymbol{Z}_0 \mid \boldsymbol{Z}_1\,] - \boldsymbol{A}\boldsymbol{Z}_{01}\begin{bmatrix} \boldsymbol{V}_{2m} & \\ & \boldsymbol{V}_{2m} \end{bmatrix}}_{\boldsymbol{A}\boldsymbol{Z}}$$

Constructing Matrix Commitments

[Wee25]

Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$\mathrm{Commit}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$

$\mathrm{Open}(\mathrm{pp}, \boldsymbol{M}) \to \boldsymbol{Z} \in \mathbb{Z}_q^{m \times L}$

$$\boldsymbol{C} \cdot \underbrace{\boldsymbol{V}_L}_{\text{low-norm}} = \boldsymbol{M} - \boldsymbol{A} \cdot \underbrace{\boldsymbol{Z}}_{\text{low-norm}}$$

Merkle-style commitment

Public parameter size is **independent** of L

Can commit to sparse matrices of **exponential** width (e.g., $L = 2^\lambda$, but $\boldsymbol{M}$ contains $K = \mathrm{poly}(\lambda)$ non-zero columns; running time of Commit and Open is $\mathrm{poly}(K)$)

Can realize from any assumption in the succinct LWE family

Constructing Matrix Commitments

[Wee25]

$$\underbrace{\left[\begin{array}{ccc|c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right]}_{\boldsymbol{D}_\ell} \underbrace{\begin{bmatrix} \text{—} & \boldsymbol{T}_1 & \text{—} \\ \text{—} & \vdots & \text{—} \\ \text{—} & \boldsymbol{T}_\ell & \text{—} \\ \text{—} & \underline{\boldsymbol{T}} & \text{—} \end{bmatrix}}_{\boldsymbol{T}} = \begin{bmatrix} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{bmatrix}$$

$\boldsymbol{A}, \boldsymbol{W}_i \in \mathbb{Z}_q^{n \times m}$

$\boldsymbol{T}_i, \underline{\boldsymbol{T}} \in \mathbb{Z}_q^{m \times \ell m}$

SIS/LWE holds with respect to $\boldsymbol{A}$ given $\boldsymbol{D}_\ell, \boldsymbol{T}$

Public parameters pp is the matrix $\boldsymbol{D}_\ell$ and the trapdoor $\boldsymbol{T}$ (for $\ell = 2m^2$)

With decomposed LWE, both $\boldsymbol{D}_\ell, \boldsymbol{T}$ can be described by a uniform random string; this means the public parameters pp can be sampled **transparently**

$$\left(\mathrm{pp}, \boldsymbol{s}^{\mathrm{T}} \boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}\right) \approx \left(\mathrm{pp}, \boldsymbol{u}^{\mathrm{T}}\right)$$

Succinct LWE and Matrix Commitments

Succinct LWE assumption family:

$$\underbrace{\left[\begin{array}{ccc|c} A & & & W_1 \\ & \ddots & & \vdots \\ & & A & W_\ell \end{array}\right]}_{D_\ell} \underbrace{\begin{bmatrix} — & T_1 & — \\ — & \vdots & — \\ — & T_\ell & — \\ — & \underline{T} & — \end{bmatrix}}_{T} = \begin{bmatrix} G & & \\ & \ddots & \\ & & G \end{bmatrix}$$

$A, W_i \in \mathbb{Z}_q^{n\times m}$

$T_i, \underline{T} \in \mathbb{Z}_q^{m\times \ell m}$

SIS/LWE holds with respect to A given D_ℓ, T

Concrete instantiations (strongest to weakest)**:** BASIS, succinct LWE, decomposed LWE

Matrix commitments provide a useful intermediary tool for building primitives

$$\mathrm{Commit}(\mathrm{pp}, M) \rightarrow C \in \mathbb{Z}_q^{n\times m}$$

$$\mathrm{Open}(\mathrm{pp}, M) \rightarrow Z \in \mathbb{Z}_q^{m\times L}$$

$$C \cdot \underbrace{V_L}_{\text{low-norm}} = M - A \cdot \underbrace{Z}_{\text{low-norm}}$$

Succinct LWE and Matrix Commitments

Succinct LWE assumption family:

$$\underbrace{\left[\begin{array}{ccc|c} A & & & W_1 \\ & \ddots & & \vdots \\ & & A & W_\ell \end{array}\right]}_{D_\ell} \underbrace{\begin{bmatrix} — & T_1 & — \\ — & \vdots & — \\ — & T_\ell & — \\ — & \underline{T} & — \end{bmatrix}}_{T} = \begin{bmatrix} G & & \\ & \ddots & \\ & & G \end{bmatrix}$$

$A, W_i \in \mathbb{Z}_q^{n \times m}$

$T_i, \underline{T} \in \mathbb{Z}_q^{m \times \ell m}$

SIS/LWE holds with respect to A given D_ℓ, T

Concrete instantiations (strongest to weakest)**:** BASIS, succinct LWE, decomposed LWE

Matrix commitments provide a useful intermediary tool for building primitives

Implications:

- Nearly-optimal KP/CP-ABE (including optimal broadcast encryption)
- Unbounded distributed broadcast encryption, succinct registered ABE for circuits

$$C \cdot \underset{\text{low-norm}}{V_L} = M - A \cdot \underset{\text{low-norm}}{Z}$$

Open Problems

Show hardness of decomposed LWE (or another instance of succinct LWE) from

- Worst-case lattice problem
- Plain LWE assumption

Cryptanalysis of succinct LWE instances

Other primitives from succinct LWE:

- Succinct computational secret sharing
- Witness encryption
- Indistinguishability obfuscation

Thank you!