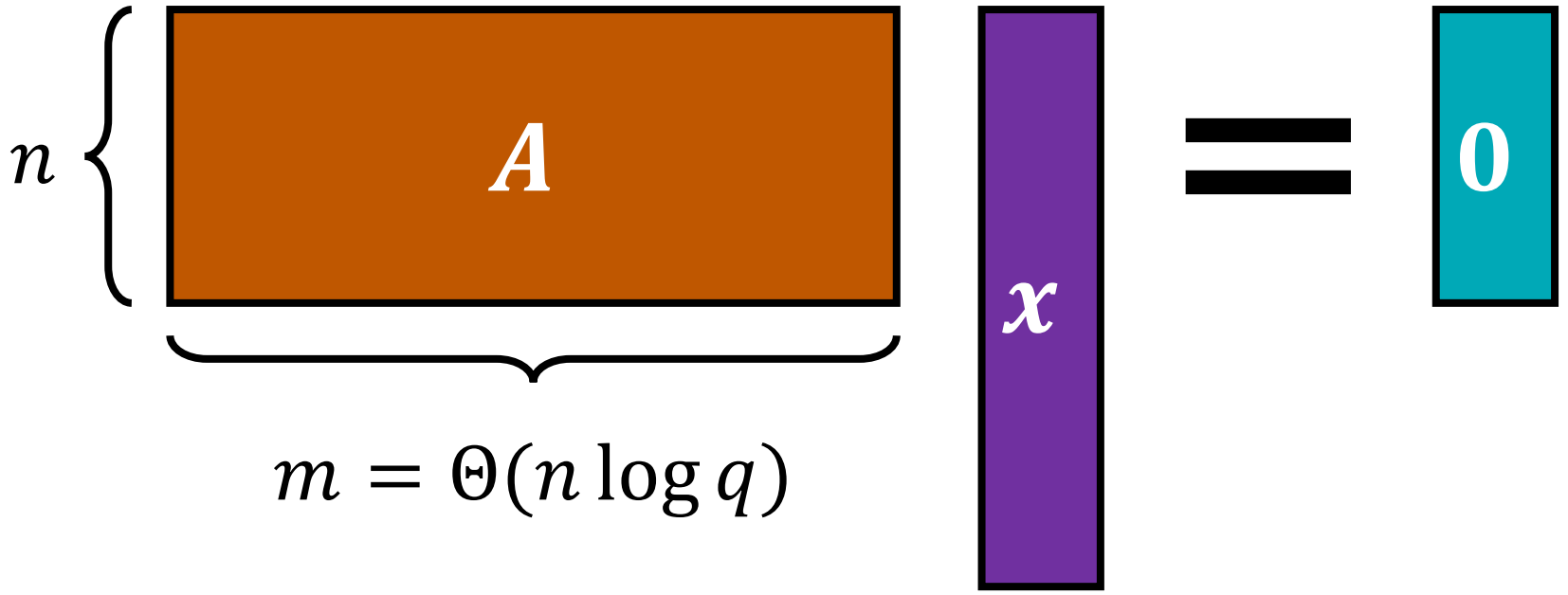
Lattice Assumptions with Hints: Succinct LWE and Decomposed LWE

David Wu

July 2026

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 $\boldsymbol{Ax} = \boldsymbol{0}$ [Ajt96]

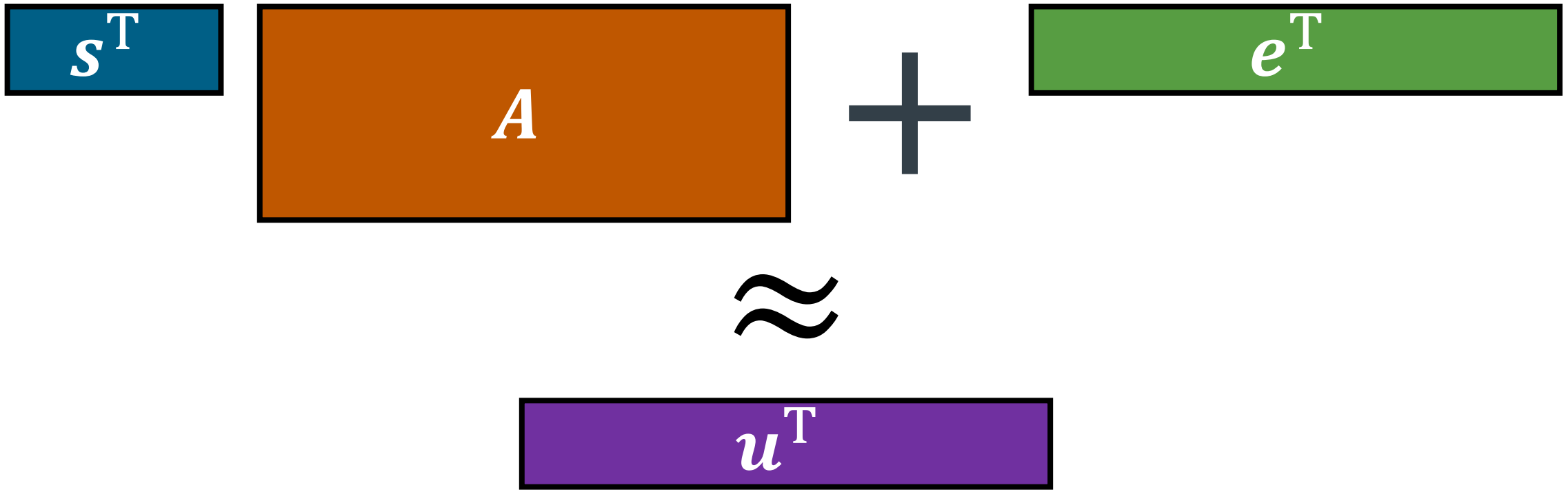


Yields one-way functions, collision-resistant hash functions, digital signatures

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 $\boldsymbol{Ax} = \boldsymbol{0}$ [Ajt96]

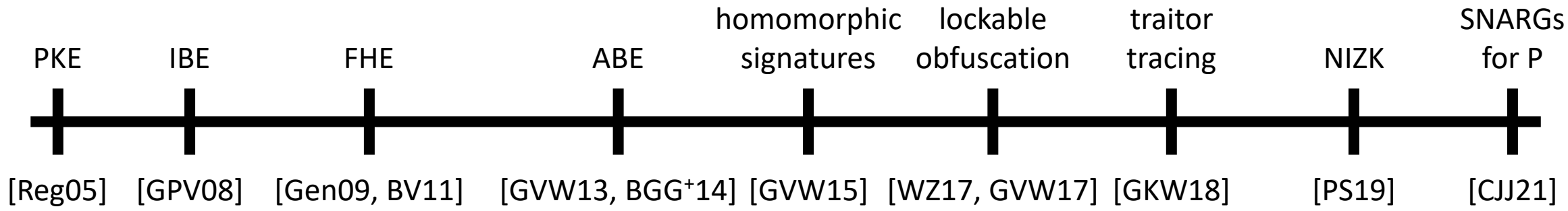
Learning with errors (LWE): Distinguish $\left(\boldsymbol{A}, \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}\right)$ from $\left(\boldsymbol{A}, \boldsymbol{u}^{\mathrm{T}}\right)$ [Reg05]



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 $\boldsymbol{Ax} = \boldsymbol{0}$ [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]



But… *not* everything

However, many **lattice-inspired** approaches

Broadcast encryption [BV22]

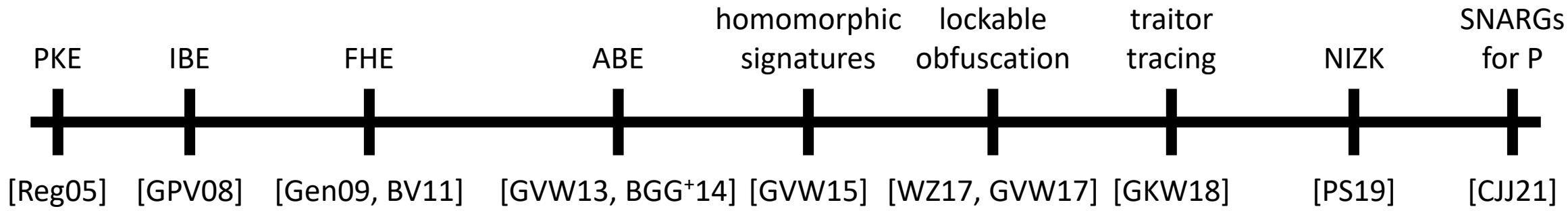
Witness encryption [GGH15, CVW18]

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 $\boldsymbol{Ax} = \boldsymbol{0}$ [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]



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

Recent years: 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

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)

Succinct and Decomposed LWE

This talk: conjecture hardness of LWE (or SIS) for a specific distribution $\boldsymbol{P}$

Two possibilities (mirroring the preconditions and postconditions of evasive LWE):

Option A: $\left(\boldsymbol{P}, \boldsymbol{s}^{\mathrm{T}}\boldsymbol{P} + \boldsymbol{e}^{\mathrm{T}}\right)$ is pseudorandom — decomposed LWE [AMR25]

Option B: $\left(\boldsymbol{A}, \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}\right)$ pseudorandom given $\left(\boldsymbol{P}, \boldsymbol{A}^{-1}(\boldsymbol{P})\right)$ — succinct LWE [Wee24]

$\boldsymbol{A}^{-1}(\boldsymbol{P}) \in \mathbb{Z}^{m \times k}$: low-norm preimage where $\boldsymbol{A} \cdot \boldsymbol{A}^{-1}(\boldsymbol{P}) = \boldsymbol{P}$

Can also define the SIS variants:

Option A: SIS is hard with respect to $\boldsymbol{P}$ — decomposed SIS [AMR26]

Option B: SIS is hard with respect to $\boldsymbol{A}$ given $\boldsymbol{A}^{-1}(\boldsymbol{P})$ — succinct SIS [Wee24]

BASIS [WW23]

Succinct and Decomposed LWE

"degree-2 correlations"

$$\boldsymbol{P} = \left[\cdots \mid \boldsymbol{W}_i \boldsymbol{R}_j - \delta_{ij} \boldsymbol{G} \mid \cdots \right] \in \mathbb{Z}_q^{n \times \ell^2 m}$$

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

$$\boldsymbol{R}_1, \ldots, \boldsymbol{R}_\ell \leftarrow D_{\mathbb{Z},\sigma}^{m \times m}$$

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Decomposed LWE [AMR25]: $\boldsymbol{s}^{\mathrm{T}} \boldsymbol{P} + \boldsymbol{e}^{\mathrm{T}}$ is pseudorandom given $\boldsymbol{W}_1, \ldots, \boldsymbol{W}_\ell, \boldsymbol{R}_1, \ldots, \boldsymbol{R}_\ell$

Succinct LWE [Wee24]: $\boldsymbol{s}^{\mathrm{T}} \boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}$ is pseudorandom given $\boldsymbol{A}^{-1}(\boldsymbol{P})$

Without $\delta_{ij} \boldsymbol{G}$, the assumption holds under LWE via [BLMR15]

$$\begin{aligned} \boldsymbol{s}^{\mathrm{T}} \boldsymbol{W}_i [\, \boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_\ell \,] + \boldsymbol{e}_i^{\mathrm{T}} &\approx \left(\boldsymbol{s}^{\mathrm{T}} \boldsymbol{W}_i + \tilde{\boldsymbol{e}}_i^{\mathrm{T}} \right) [\, \boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_\ell \,] + \boldsymbol{e}_i^{\mathrm{T}} && \textit{smudging} \\ &\approx \boldsymbol{u}_i^{\mathrm{T}} [\, \boldsymbol{R}_1 \mid \cdots \mid \boldsymbol{R}_\ell \,] + \boldsymbol{e}_i^{\mathrm{T}} && \textit{LWE} \\ &\approx \tilde{\boldsymbol{u}}_i^{\mathrm{T}} && \textit{LWE [BLMR15]} \end{aligned}$$

Succinct and Decomposed LWE

"degree-2 correlations"

$$\boldsymbol{P} = \left[\cdots \mid \boldsymbol{W}_i \boldsymbol{R}_j - \delta_{ij} \boldsymbol{G} \mid \cdots \right] \in \mathbb{Z}_q^{n \times \ell^2 m}$$

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

$$\boldsymbol{R}_1, \ldots, \boldsymbol{R}_\ell \leftarrow D_{\mathbb{Z},\sigma}^{m \times m}$$

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Decomposed LWE [AMR25]: $\boldsymbol{s}^{\mathrm{T}} \boldsymbol{P} + \boldsymbol{e}^{\mathrm{T}}$ is pseudorandom given $\boldsymbol{W}_1, \ldots, \boldsymbol{W}_\ell, \boldsymbol{R}_1, \ldots, \boldsymbol{R}_\ell$

Succinct LWE [Wee24]: $\boldsymbol{s}^{\mathrm{T}} \boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}$ is pseudorandom given $\boldsymbol{A}^{-1}(\boldsymbol{P})$

$\boldsymbol{T}_{i,j}$ are blocks of $\boldsymbol{A}^{-1}(\boldsymbol{P})$

Can also view $\boldsymbol{A}^{-1}(\boldsymbol{P})$ as trapdoor for a related matrix:

$$\boldsymbol{A}\boldsymbol{T}_{i,j} = \boldsymbol{W}_i \boldsymbol{R}_j - \delta_{ij} \boldsymbol{G}$$

$$\left[\begin{array}{ccc:c} \boldsymbol{A} & & & \boldsymbol{W}_1 \\ & \ddots & & \vdots \\ & & \boldsymbol{A} & \boldsymbol{W}_\ell \end{array}\right] \times \left[\begin{array}{ccc} -\boldsymbol{T}_{1,1} & \cdots & -\boldsymbol{T}_{1,\ell} \\ \vdots & \ddots & \vdots \\ -\boldsymbol{T}_{\ell,1} & \cdots & -\boldsymbol{T}_{\ell,\ell} \\ \hdashline \boldsymbol{R}_1 & \cdots & \boldsymbol{R}_\ell \end{array}\right] = \left[\begin{array}{ccc} \boldsymbol{G} & & \\ & \ddots & \\ & & \boldsymbol{G} \end{array}\right]$$

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:

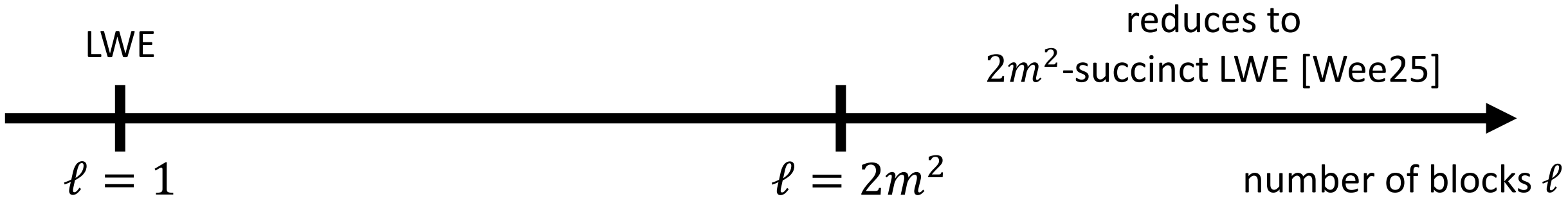
ℓ-Succinct LWE

[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:



Open Problems

$$\boldsymbol{P} = \left[\cdots \mid \boldsymbol{W}_i \boldsymbol{R}_j - \delta_{ij} \boldsymbol{G} \mid \cdots \right] \in \mathbb{Z}_q^{n \times \ell^2 m}$$

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

$$\boldsymbol{R}_1, \ldots, \boldsymbol{R}_\ell \leftarrow D_{\mathbb{Z},\sigma}^{m \times m}$$

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

Is SIS/LWE hard with respect to $\boldsymbol{P}$?

Baby step: $\mathrm{poly}(\ell)$ *improvement over a generic SIS/LWE algorithm?*

Hardness of SIS/LWE with respect to $\boldsymbol{P}$ from some worst-case lattice problem?

Applications of Succinct and Decomposed LWE

Functional commitments for all circuits (and SNARGs for P/poly)	[WW23, WW23b, Wee24, Wee25]
Optimal broadcast encryption	[Wee25, AMR26a, GY26b]
Distributed broadcast encryption	[CW24, CHW25, WW25, AMR26a, GY26a, GY26b]
Silent threshold encryption (constant thresholds)	[CW26, AGY26]
Nearly-optimal KP-ABE and CP-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]
Correlation intractability for all batch relations	[AMR26b]

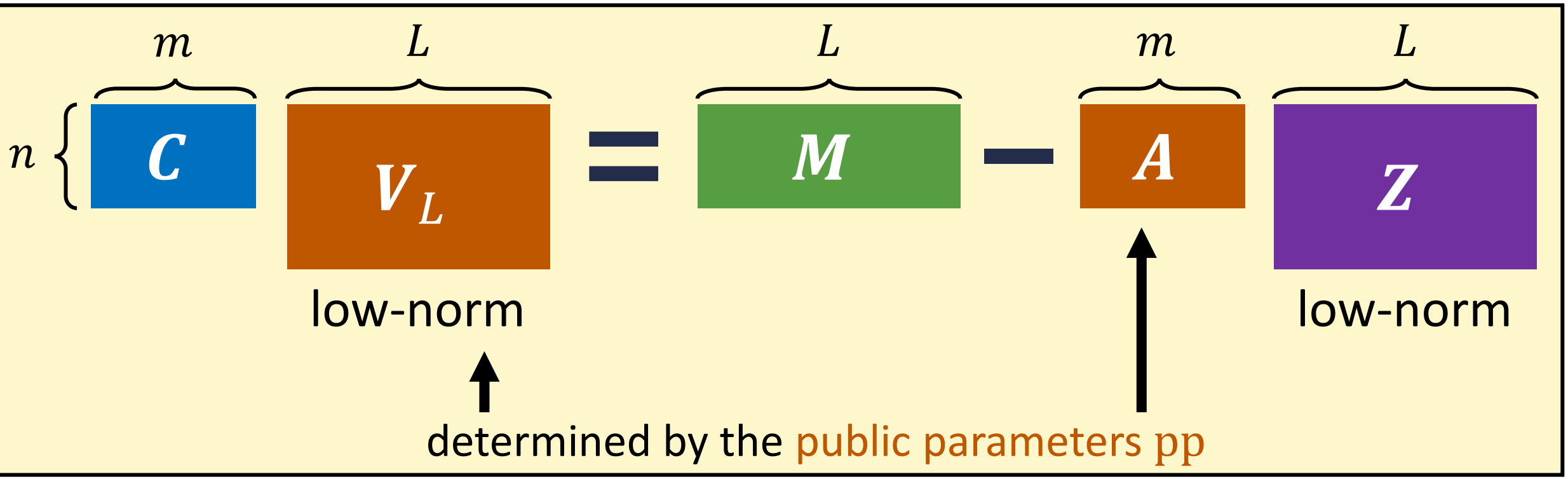
A Useful Abstraction: Matrix Commitments

[Wee24, Wee25]

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

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

deterministic algorithms



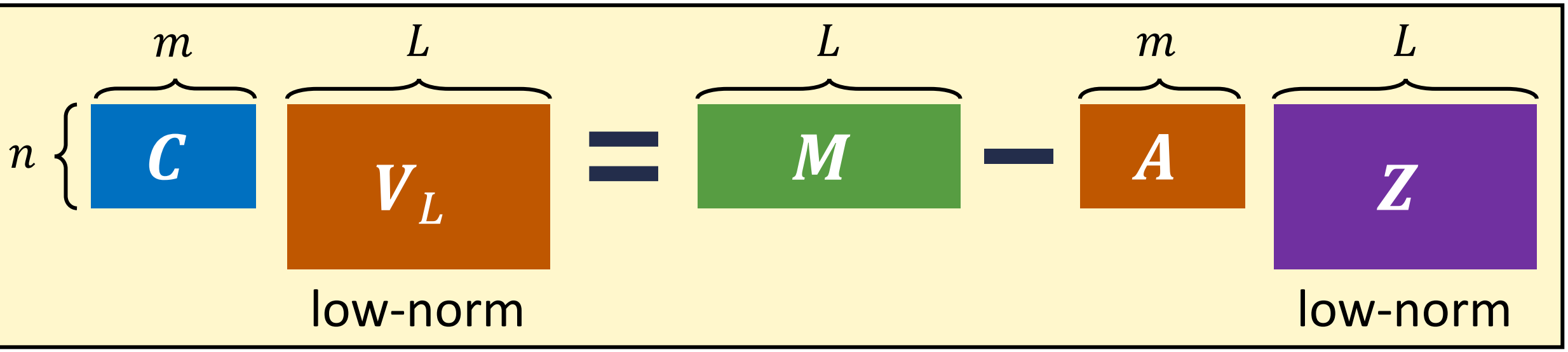
A Useful Abstraction: Matrix Commitments

[Wee24, 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



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

Compressing [BGG+] Encodings

[WW23, Wee24, Wee25, AMR25]

[BGG+] encoding of $\boldsymbol{x} \in \{0,1\}^{\ell}$: $\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$

$\boldsymbol{B}_1 - x_1\boldsymbol{G}$	$\boldsymbol{B}_2 - x_1\boldsymbol{G}$	$\cdots$	$\boldsymbol{B}_k - x_k\boldsymbol{G}$

Useful property: supports homomorphic operations

In lattice-based ABE: ciphertext contains LWE encoding $\mathbf{s}^{\mathrm{T}}\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right)$

Ciphertext size scales with $|\boldsymbol{x}|$

Compressing [BGG+] encoding

$$\boldsymbol{C} \cdot \boldsymbol{V}_L = \left(\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right) - \boldsymbol{A} \cdot \boldsymbol{Z}$$

Replace $\boldsymbol{s}^{\mathrm{T}}\left(\boldsymbol{B} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right)$ with $\left(\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}, \boldsymbol{s}^{\mathrm{T}}(\boldsymbol{B}_0 - \boldsymbol{C})\right)$ where $\boldsymbol{C}$ is a commitment to $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$

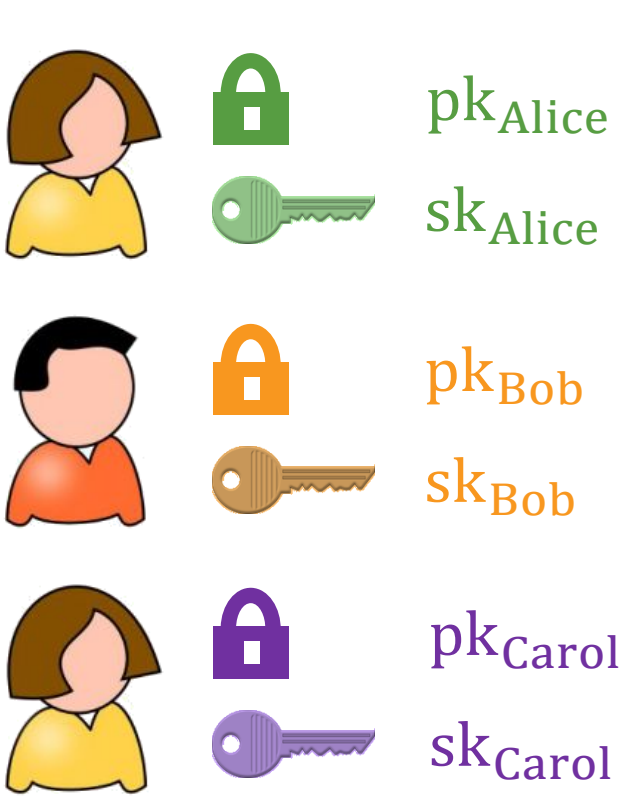
Can **expand** by computing

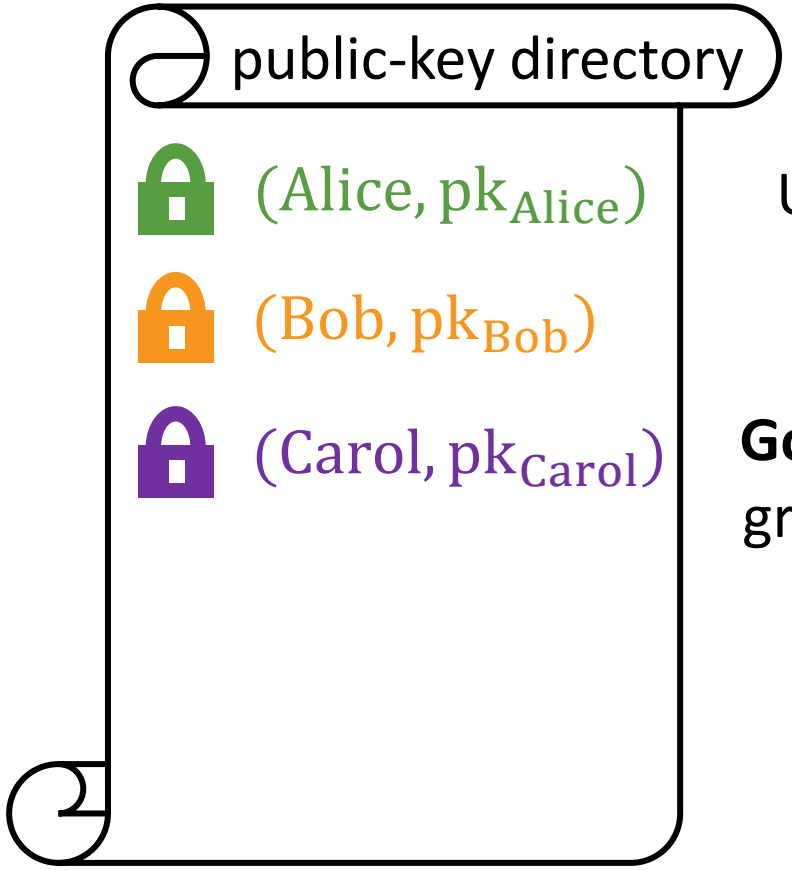
$$\left(\boldsymbol{s}^{\mathrm{T}}(\boldsymbol{B}_0 - \boldsymbol{C})\right) \cdot \boldsymbol{V}_L - \left(\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}\right) \cdot \boldsymbol{Z} = \boldsymbol{s}^{\mathrm{T}}\left(\overbrace{\boldsymbol{B}_0\boldsymbol{V}_L}^{\boldsymbol{B}} - \boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}\right)$$

dropping noise terms

An Application to Group Messaging

[WW25, BBDGW26]





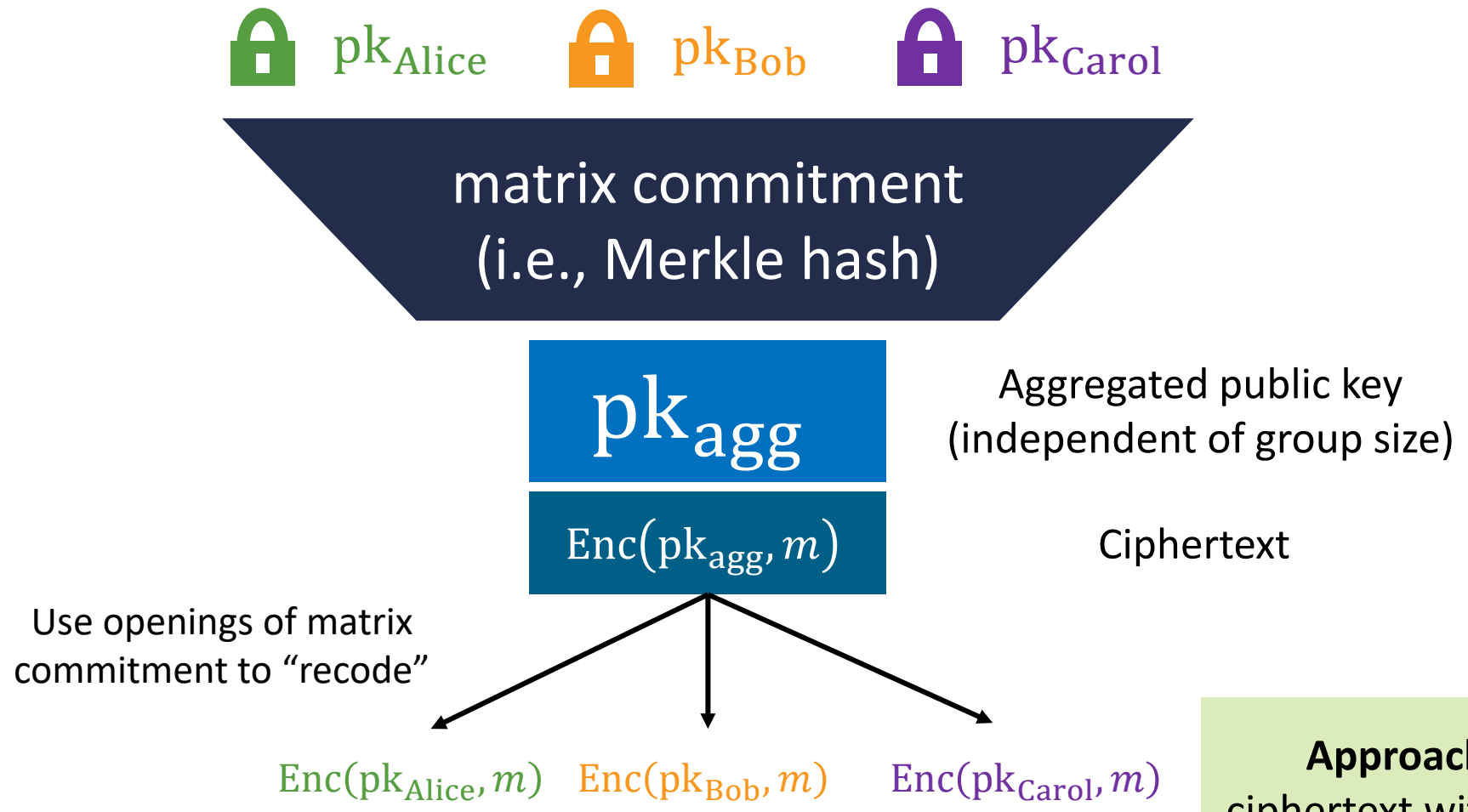
Users generate public/private keys independently

Goal: non-interactively derive a short group key from the users' public keys

Distributed broadcast encryption [WQZD14, BZ14]**:** encrypt to an **arbitrary** set of public keys with a **short** ciphertext

An Application to Group Messaging

[WW25, BBDGW26]



Approach: "recode" an LWE ciphertext with respect to $\mathrm{pk}_{\mathrm{agg}}$ to a ciphertext with respect to $\mathrm{pk}_{\mathrm{user}}$

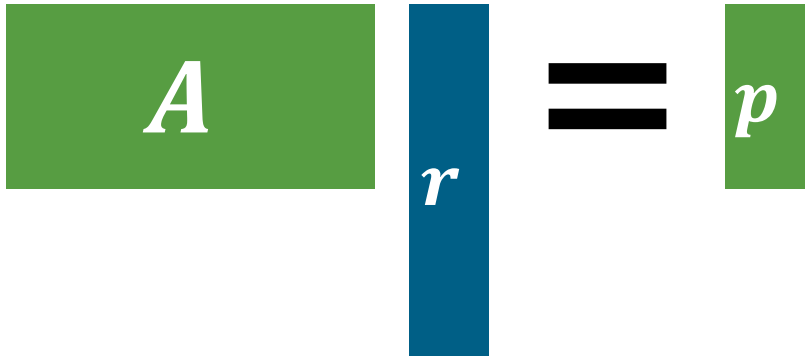
An Application to Group Messaging

[WW25, BBDGW26]

Recall: dual Regev encryption

pk: $\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$, $\boldsymbol{p} \in \mathbb{Z}_q^n$

sk: $\boldsymbol{r} \leftarrow \boldsymbol{A}^{-1}(\boldsymbol{p})$



Ciphertext:

$\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$ $\qquad$ $\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_1^{\mathrm{T}}$, $\boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + e_2 + \mu \cdot \lfloor q/2 \rfloor$

Multiply by $\boldsymbol{r}$

$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{r}$ $\qquad$ $\mu \cdot \lfloor q/2 \rfloor + (e_2 - \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{r})$

An Application to Group Messaging

[WW25, BBDGW26]

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

$\mathrm{pk}_1 = \boldsymbol{t}_1 = \boldsymbol{A}\boldsymbol{r}_1 + \boldsymbol{p} \in \mathbb{Z}_q^n$

$\mathrm{sk}_1 = \boldsymbol{r}_1 \leftarrow \{0,1\}^m$

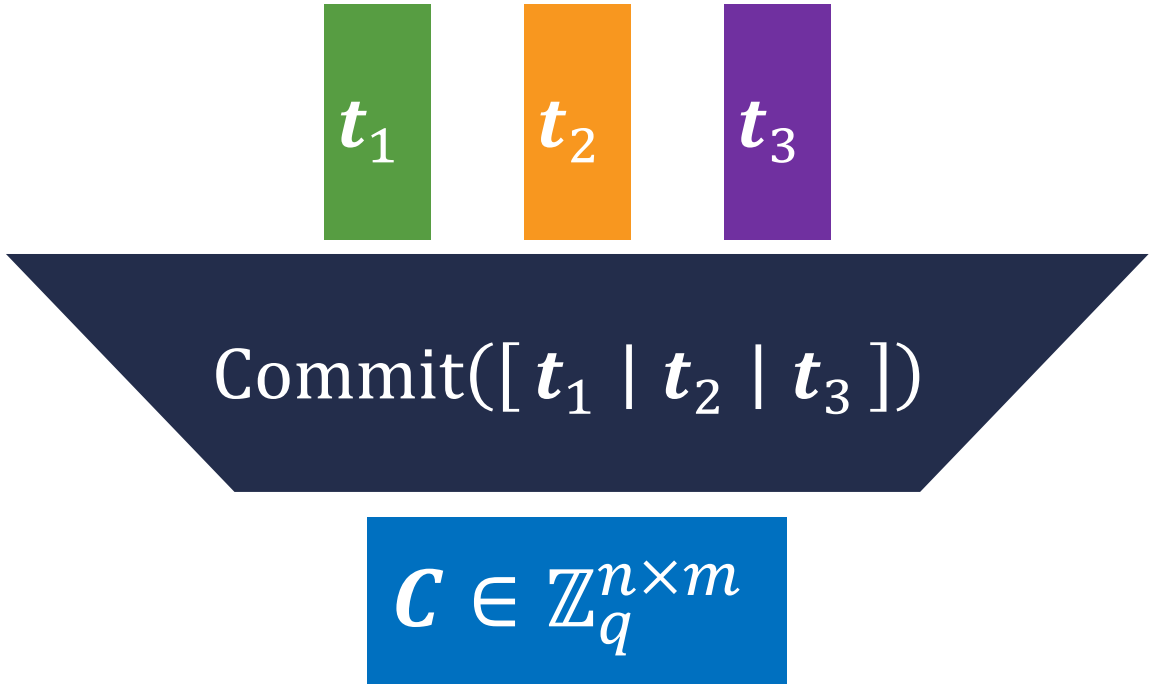
$\mathrm{pk}_2 = \boldsymbol{t}_2 = \boldsymbol{A}\boldsymbol{r}_2 + \boldsymbol{p} \in \mathbb{Z}_q^n$

$\mathrm{sk}_2 = \boldsymbol{r}_2 \leftarrow \{0,1\}^m$

$\mathrm{pk}_3 = \boldsymbol{t}_3 = \boldsymbol{A}\boldsymbol{r}_3 + \boldsymbol{p} \in \mathbb{Z}_q^n$

$\mathrm{sk}_3 = \boldsymbol{r}_3 \leftarrow \{0,1\}^m$

Aggregated group key:

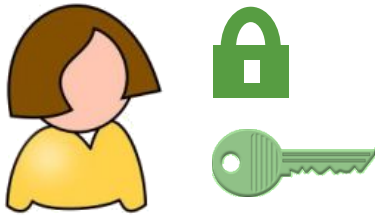


Invariant: $\boldsymbol{C}\boldsymbol{v}_i = \boldsymbol{t}_i - \boldsymbol{A}\boldsymbol{z}_i$ where $\boldsymbol{v}_i, \boldsymbol{z}_i$ are low-norm

An Application to Group Messaging

[WW25, BBDGW26]

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



$$\mathrm{pk}_1 = \boldsymbol{t}_1 = \boldsymbol{A}\boldsymbol{r}_1 + \boldsymbol{p} \in \mathbb{Z}_q^n$$

$$\mathrm{sk}_1 = \boldsymbol{r}_1 \leftarrow \{0,1\}^m$$

Ciphertext: *(suppressing error terms)*

$\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$ $\qquad$ $\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}$, $\boldsymbol{s}^{\mathrm{T}}\boldsymbol{p} + \mu \cdot \lfloor q/2 \rfloor$, $\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C}$

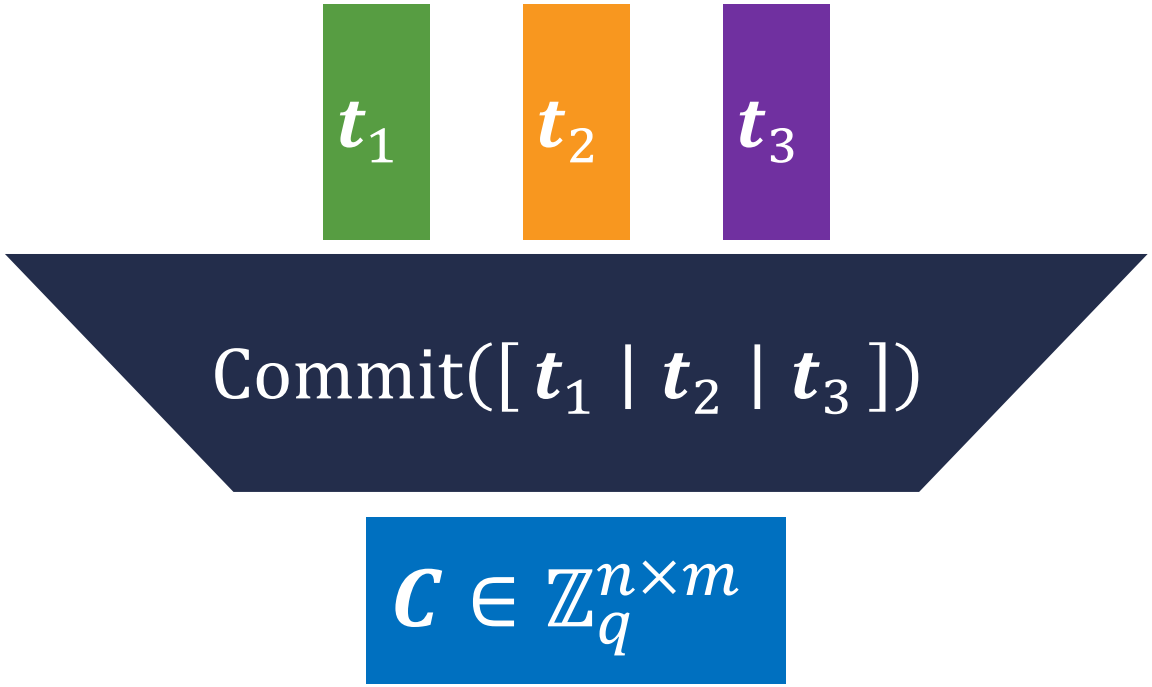
Use $\boldsymbol{v}_i, \boldsymbol{z}_i$ to recode to encryption under $\boldsymbol{t}_i$:

$$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C} \cdot \boldsymbol{v}_i + \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} \cdot \boldsymbol{z}_i \approx \boldsymbol{s}^{\mathrm{T}}\boldsymbol{t}_i - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{z}_i + \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{z}_i$$

$$= \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{s}^{\mathrm{T}}\boldsymbol{p}$$

$$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C} \cdot \boldsymbol{v}_i + \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} \cdot \boldsymbol{z}_i - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} \cdot \boldsymbol{r}_i \approx \boldsymbol{s}^{\mathrm{T}}\boldsymbol{p}$$

Aggregated group key:

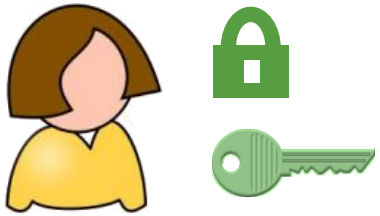


Invariant: $\boldsymbol{C}\boldsymbol{v}_i = \boldsymbol{t}_i - \boldsymbol{A}\boldsymbol{z}_i$ where $\boldsymbol{v}_i, \boldsymbol{z}_i$ are low-norm

An Application to Group Messaging

[WW25, BBDGW26]

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



$$\mathrm{pk}_1 = \boldsymbol{t}_1 = \boldsymbol{A}\boldsymbol{r}_1 + \boldsymbol{p} \in \mathbb{Z}_q^n$$

$$\mathrm{sk}_1 = \boldsymbol{r}_1 \leftarrow \{0,1\}^m$$

Ciphertext:

(suppressing error terms)

$\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$

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

To prove security, need to introduce an additional offset (i.e., so the reduction can simulate $\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C}$)

Aggregated group key:

$\boldsymbol{t}_1$ $\boldsymbol{t}_2$ $\boldsymbol{t}_3$

$$\mathrm{Commit}([\,\boldsymbol{t}_1 \mid \boldsymbol{t}_2 \mid \boldsymbol{t}_3\,])$$

$$\boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$$

Invariant: $\boldsymbol{C}\boldsymbol{v}_i = \boldsymbol{t}_i - \boldsymbol{A}\boldsymbol{z}_i$ where $\boldsymbol{v}_i, \boldsymbol{z}_i$ are low-norm

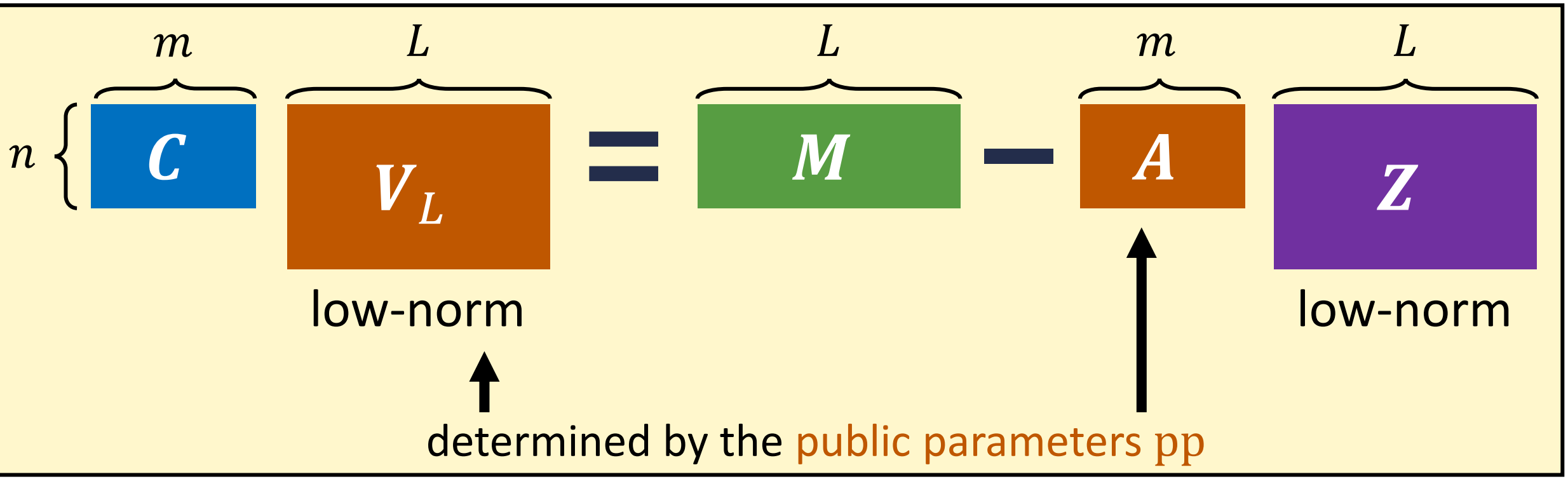
A Useful Abstraction: Matrix Commitments

[Wee24, Wee25]

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

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

deterministic algorithms



Open Problems

Is SIS/LWE hard with respect to $\boldsymbol{P} = \left[\cdots \mid \boldsymbol{W}_i \boldsymbol{R}_j - \delta_{ij} \boldsymbol{G} \mid \cdots \right] \in \mathbb{Z}_q^{n \times \ell^2 m}$

$\boldsymbol{W}_1, \ldots, \boldsymbol{W}_\ell \leftarrow \mathbb{Z}_q^{n \times m}$
$\boldsymbol{R}_1, \ldots, \boldsymbol{R}_\ell \leftarrow D_{\mathbb{Z},\sigma}^{m \times m}$
$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$

LWE variants:

Option A: $\left(\boldsymbol{P}, \boldsymbol{s}^{\mathrm{T}} \boldsymbol{P} + \boldsymbol{e}^{\mathrm{T}}\right)$ is pseudorandom — decomposed LWE [AMR25]

Option B: $\left(\boldsymbol{A}, \boldsymbol{s}^{\mathrm{T}} \boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}\right)$ pseudorandom given $\left(\boldsymbol{P}, \boldsymbol{A}^{-1}(\boldsymbol{P})\right)$ — succinct LWE [Wee24]

SIS variants:

Option A: SIS is hard with respect to $\boldsymbol{P}$ — decomposed SIS [AMR26]

Option B: SIS is hard with respect to $\boldsymbol{A}$ given $\boldsymbol{A}^{-1}(\boldsymbol{P})$ — succinct SIS [Wee24]

Open Problems

Potential new applications of succinct LWE / decomposed LWE

Adaptively-secure optimal distributed broadcast encryption in the plain model

Known: scheme with $O(N)$ size public parameters [AMR26, GY26] or unbounded scheme with ciphertext size $O\left(|S|^{1/2}\right)$ [CW26b] for N users and broadcasting to S

Succinct computational secret sharing for monotone circuits

Known: succinct computational secret sharing for DNF policies [CW26b]

Thank you!