Succinct Matrix Commitments and Their Applications

David Wu

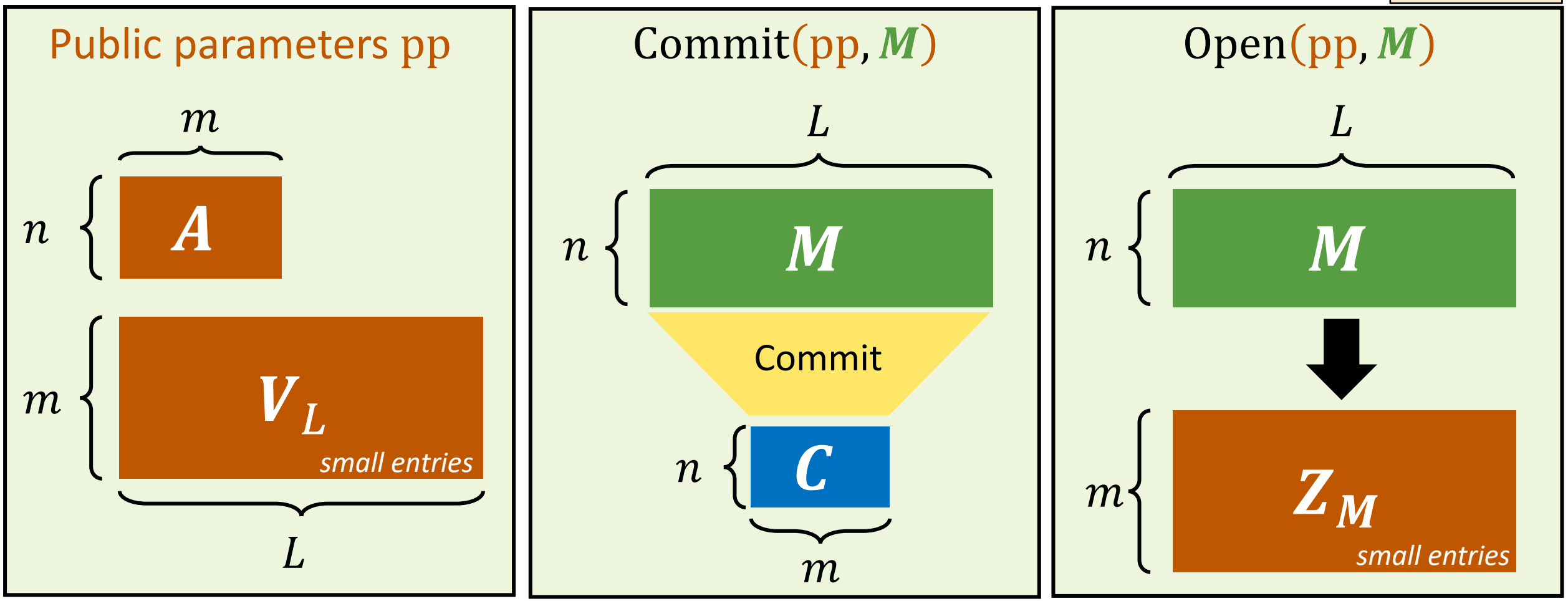
Full disclosure: this talk is primarily about computational objects…

Matrix Commitments

[Wee24, Wee25]

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

$m > n \log q$
$L \gg n$



compress the matrix $\boldsymbol{M}$

Matrix Commitments

[Wee24, Wee25]

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

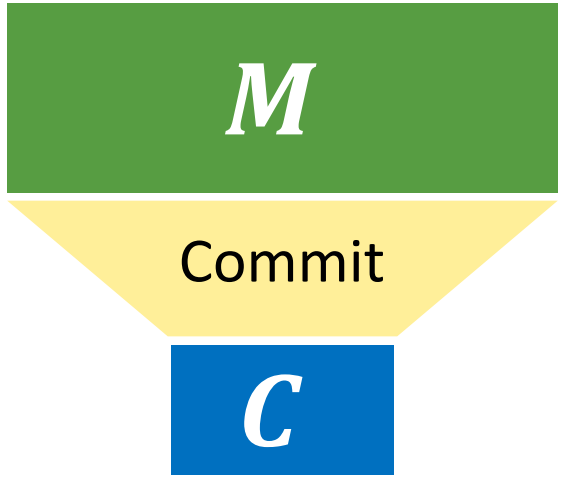
$m > n \log q$

$\text{Commit}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$ $\quad$ $\text{Open}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{Z_M} \in \mathbb{Z}^{m \times L}$ *low-norm*

---

public parameters $\text{pp} = (\boldsymbol{A}, \boldsymbol{V}_L)$

$\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ $\quad$ $\boldsymbol{V}_L \in \mathbb{Z}^{m \times L}$ *low-norm*



Key opening relation: $\boldsymbol{C} \cdot \boldsymbol{V}_L = \boldsymbol{M} - \boldsymbol{A} \cdot \boldsymbol{Z_M}$

$\boldsymbol{C}$ is a compressed representation of $\boldsymbol{M}$

Can expand $\boldsymbol{C}$ to translation of $\boldsymbol{M}$ by multiplying by a fixed low-norm matrix $\boldsymbol{V_L}$

So far… this object is information-theoretic…

Matrix Commitments

[Wee24, Wee25]

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

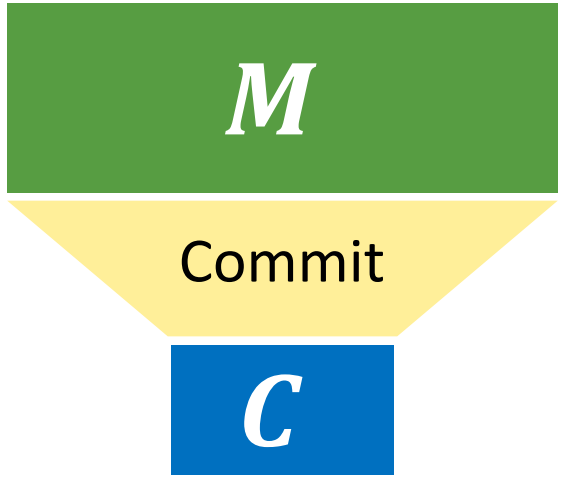
$m > n \log q$

$\text{Commit}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{C} \in \mathbb{Z}_q^{n \times m}$ $\quad$ $\text{Open}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{Z_M} \in \mathbb{Z}^{m \times L}$ *low-norm*

---

public parameters $\text{pp} = (\boldsymbol{A}, \boldsymbol{V}_L)$

$\boldsymbol{A} \in \mathbb{Z}_q^{n \times m}$ $\quad$ $\boldsymbol{V}_L \in \mathbb{Z}^{m \times L}$ *low-norm*



Key opening relation: $\boldsymbol{C} \cdot \boldsymbol{V}_L = \boldsymbol{M} - \boldsymbol{A} \cdot \boldsymbol{Z_M}$

Security assumption: SIS or LWE problem is hard with respect to $\boldsymbol{A}$ given pp

SIS problem: given $\boldsymbol{A}$, find low-norm $\boldsymbol{0} \neq \boldsymbol{x} \in \mathbb{Z}^m$ where $\boldsymbol{Ax} = 0$

LWE problem: distinguish $\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}$ from random when $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$ and $\boldsymbol{e} \in \mathbb{Z}^m$ is low-norm

Matrix Commitments

[Wee24, Wee25]

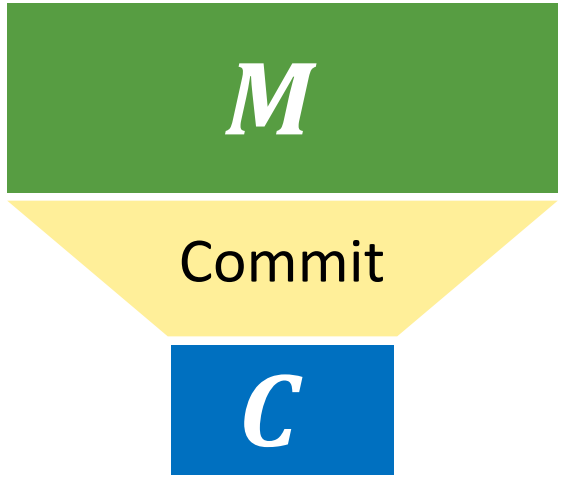
Succinct commitment to a matrix $\boldsymbol{M} \in \mathbb{Z}_q^{n \times L}$

$m > n \log q$

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

$\text{Open}(\text{pp}, \boldsymbol{M}) \to \boldsymbol{Z_M} \in \mathbb{Z}^{m \times L}$ *low-norm*

Security assumptions hold under the succinct/decomposed SIS/LWE assumptions



Key opening relation: $\boldsymbol{C} \cdot \boldsymbol{V}_L = \boldsymbol{M} - \boldsymbol{A} \cdot \boldsymbol{Z_M}$

Security assumption: SIS or LWE problem is hard with respect to $\boldsymbol{A}$ given pp

SIS problem: given $\boldsymbol{A}$, find low-norm $\boldsymbol{0} \neq \boldsymbol{x} \in \mathbb{Z}^m$ where $\boldsymbol{Ax} = 0$

LWE problem: distinguish $\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}^{\mathrm{T}}$ from random when $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$ and $\boldsymbol{e} \in \mathbb{Z}^m$ is low-norm

So What is it Good For?

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

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

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

$\mathrm{pp} = \left(\boldsymbol{A} \in \mathbb{Z}^{n \times m}, \boldsymbol{V}_L \in \mathbb{Z}^{m \times L}\right)$

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

Functional commitments for all circuits + SNARGs for P/poly	[WW23a, WW23b, Wee24, Wee25]
Optimal broadcast encryption	[Wee25, AMR26, GY26a]
Distributed broadcast encryption	[CW24, CHW25, WW25, AMR26, CW26, GY26a, GY26b]
Nearly optimal continuous group key agreement	[BBDGW26]
Silent threshold encryption	[GY26b, GY26c, CWY26]
Nearly-optimal KP-ABE and CP-ABE for circuits	[Wee24, Wee25]
Registered ABE for circuits	[CHW25, AMR25, WW25]
Succinct computational secret sharing for DNFs	[CW26, GY26c]

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

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

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 $\boldsymbol{x}^{\mathrm{T}} \otimes \boldsymbol{G}$

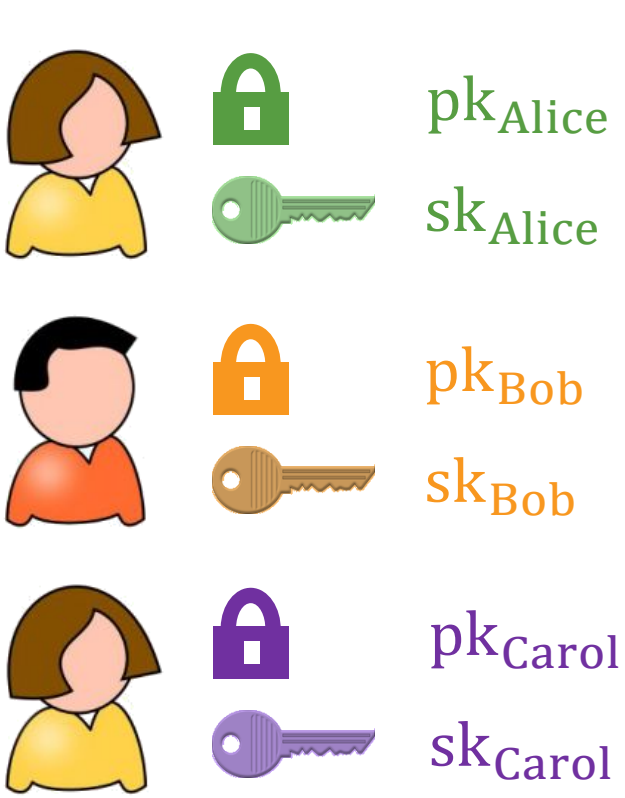
Can **expand** by computing

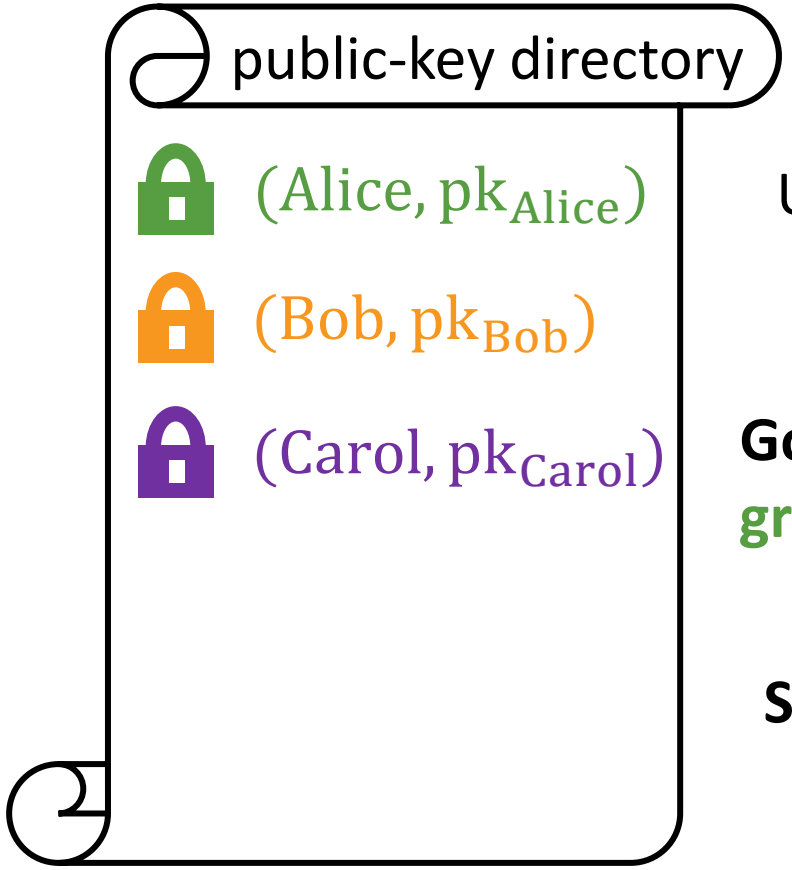
$$\left(\boldsymbol{s}^{\mathrm{T}}(\boldsymbol{B}_0 - \boldsymbol{C})\right) \cdot \boldsymbol{V}_L - \left(\boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}\right) \cdot \boldsymbol{Z}_{\boldsymbol{x}} = \boldsymbol{s}^{\mathrm{T}}\left(\overbrace{\boldsymbol{B}_0\boldsymbol{V}_L}^{\boldsymbol{B}} - \boldsymbol{x}^{\mathrm{T}}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

dropping noise terms

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]





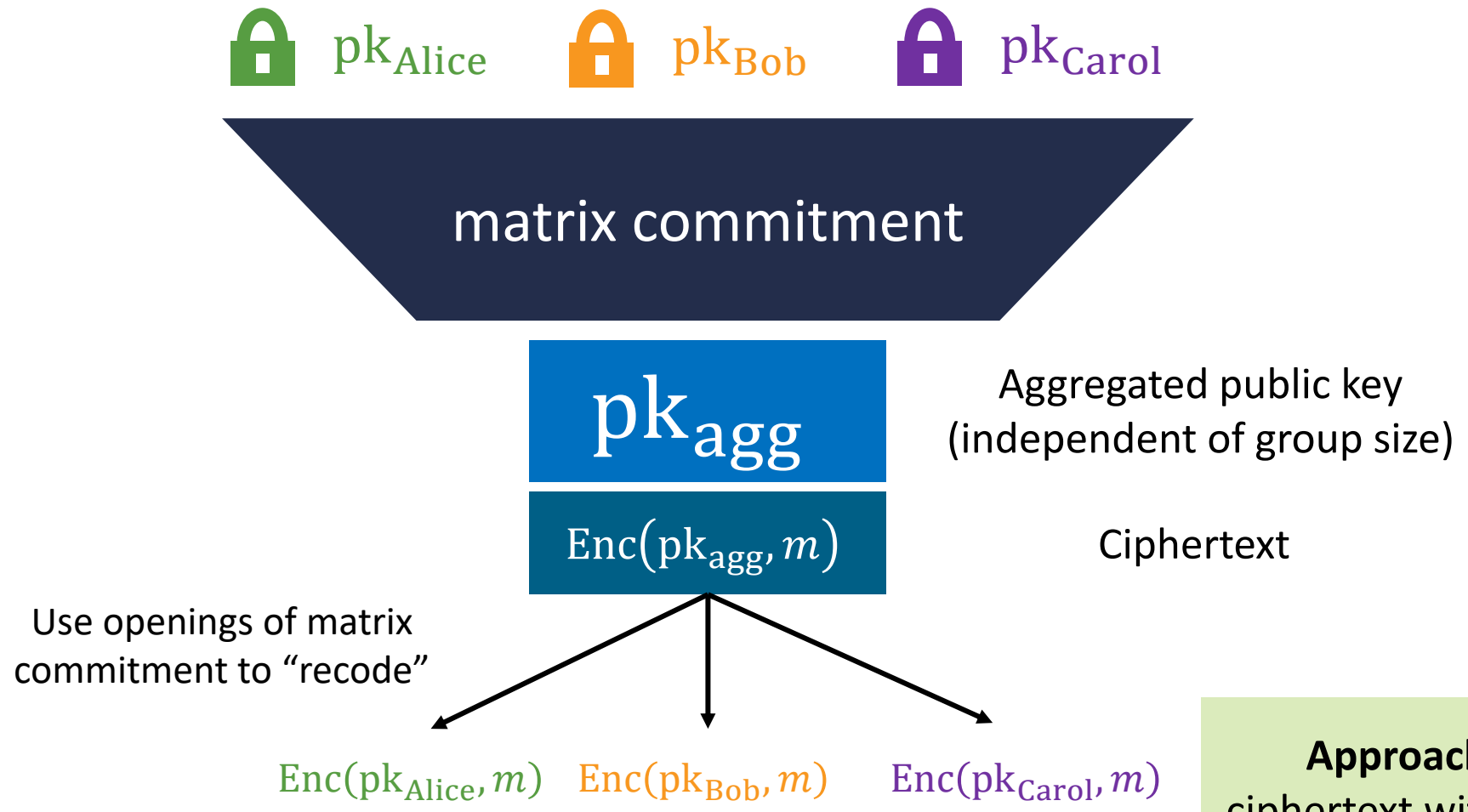
Users generate public/private keys independently

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

Succinctness: encryption under the group key should be short (independent of group size)

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]



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

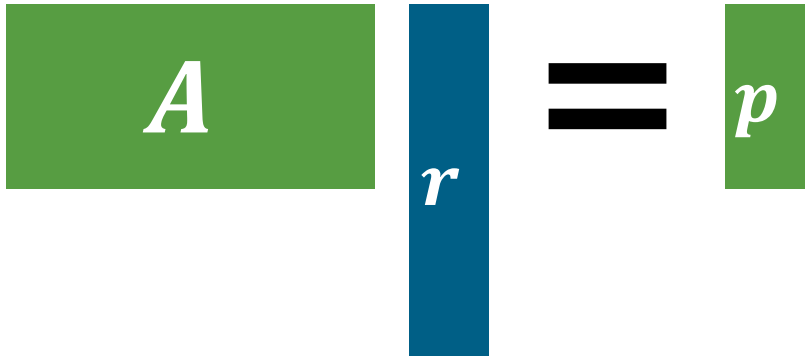
Group Messaging and Broadcast Encryption

[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 $\boldsymbol{r}$ ↓

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

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]

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

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

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

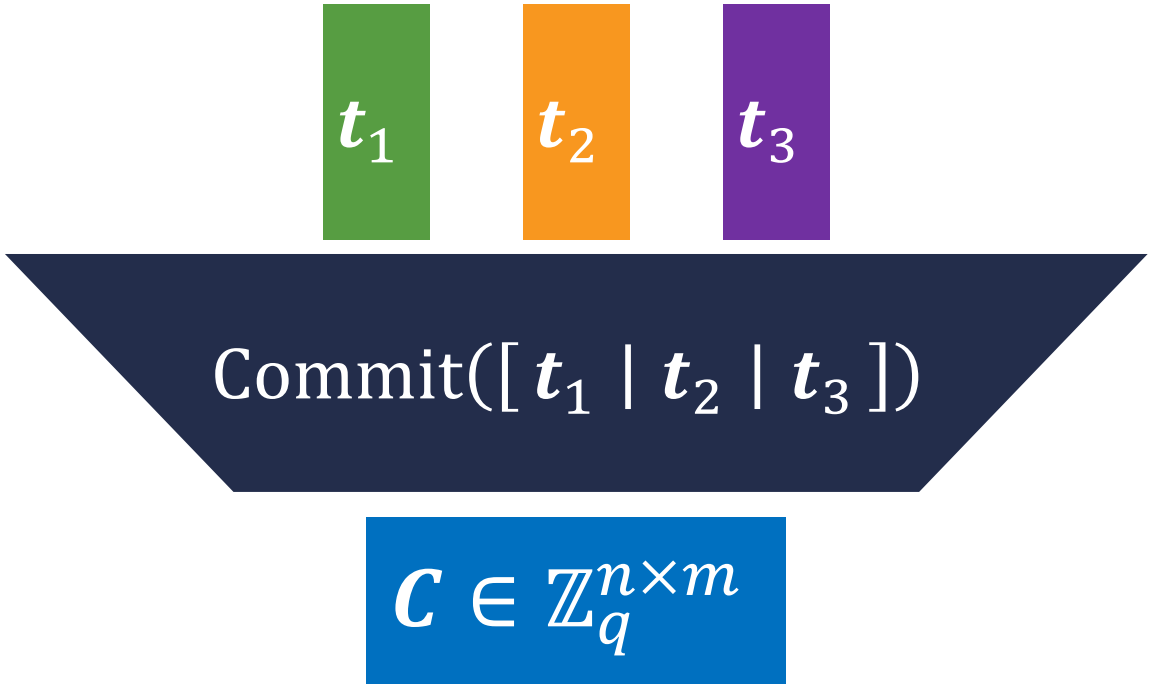
$$\mathrm{pk}_2 = \boldsymbol{t}_2 = \boldsymbol{A}\boldsymbol{r}_2 + \boldsymbol{p} \in \mathbb{Z}_q^n$$

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

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

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

Aggregated group key:

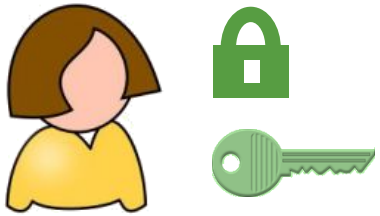


Invariant: $\boldsymbol{C}\boldsymbol{v}_i = \boldsymbol{t}_i - \boldsymbol{A}\boldsymbol{z}_i$ where $\boldsymbol{v}_i, \boldsymbol{z}_i$ are low-norm

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]

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



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

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

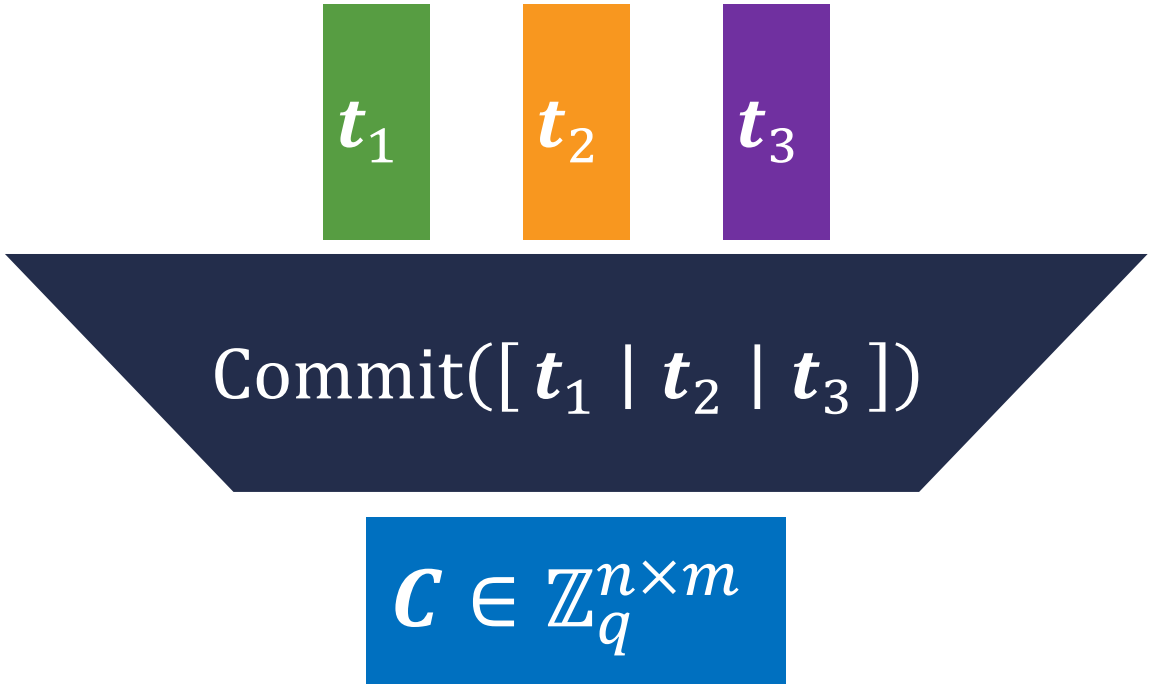
Ciphertext:

(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 $\boldsymbol{t}_i$:

Aggregated group key:

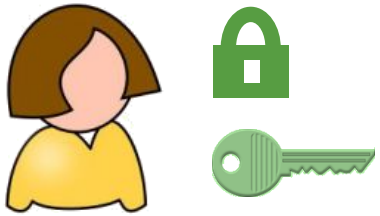


Invariant: $\boldsymbol{C}\boldsymbol{v}_i = \boldsymbol{t}_i - \boldsymbol{A}\boldsymbol{z}_i$ where $\boldsymbol{v}_i, \boldsymbol{z}_i$ are low-norm

Group Messaging and Broadcast Encryption

[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)*

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

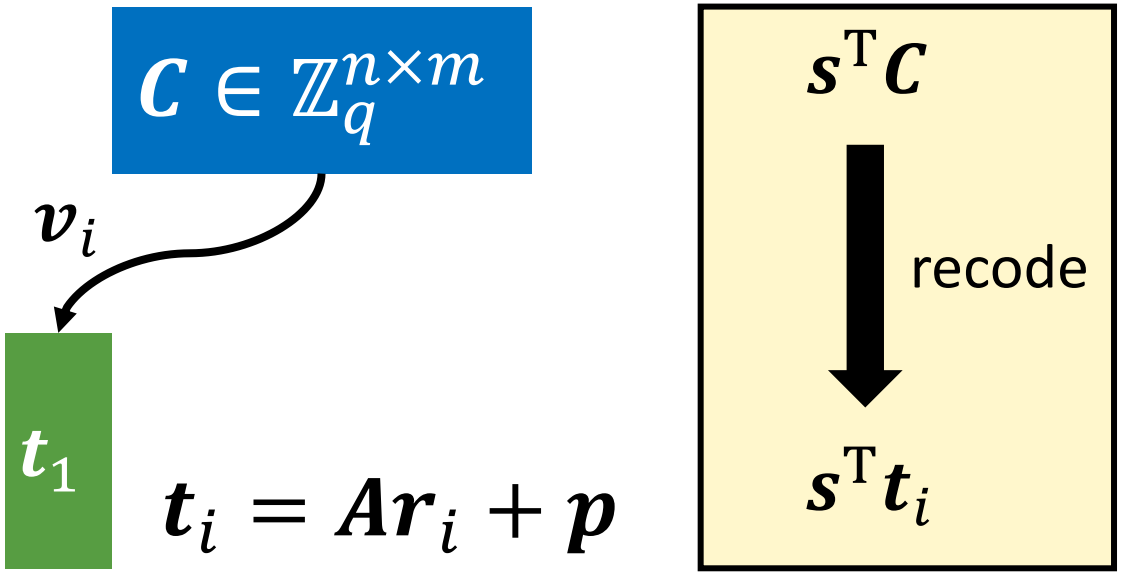
Use $\boldsymbol{v}_i, \boldsymbol{z}_i$ to recode to encryption under $\boldsymbol{t}_i$:

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

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

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

Aggregated group key:

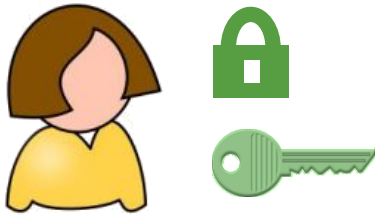


Invariant: $\boldsymbol{C}\boldsymbol{v}_i = \boldsymbol{t}_i - \boldsymbol{A}\boldsymbol{z}_i$ where $\boldsymbol{v}_i, \boldsymbol{z}_i$ are low-norm

Group Messaging and Broadcast Encryption

[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)

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

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:

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

$\boldsymbol{v}_i$

$\boldsymbol{t}_1$

$$\boldsymbol{t}_i = \boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p}$$

$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C}$

recode

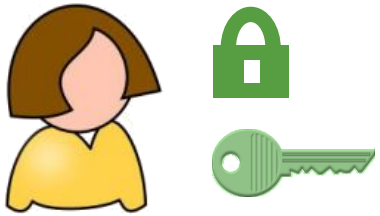
$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{t}_i$

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

Group Messaging and Broadcast Encryption

[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)

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

Overall ciphertext size:

$$|\mathrm{ct}| = \mathrm{poly}(\lambda)$$

(independent of group size)

Aggregated group key:

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

$\boldsymbol{v}_i$

$\boldsymbol{t}_1$

$$\boldsymbol{t}_i = \boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p}$$

$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C}$

recode

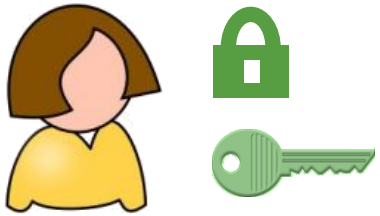
$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{t}_i$

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

Group Messaging and Broadcast Encryption

[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)

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

Can augment scheme to support incremental updates and key refreshes ⇒ continuous group key-agreement and secure group messaging

Aggregated group key:

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

$\boldsymbol{v}_i$

$\boldsymbol{t}_1$

$$\boldsymbol{t}_i = \boldsymbol{A}\boldsymbol{r}_i + \boldsymbol{p}$$

$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{C}$

recode

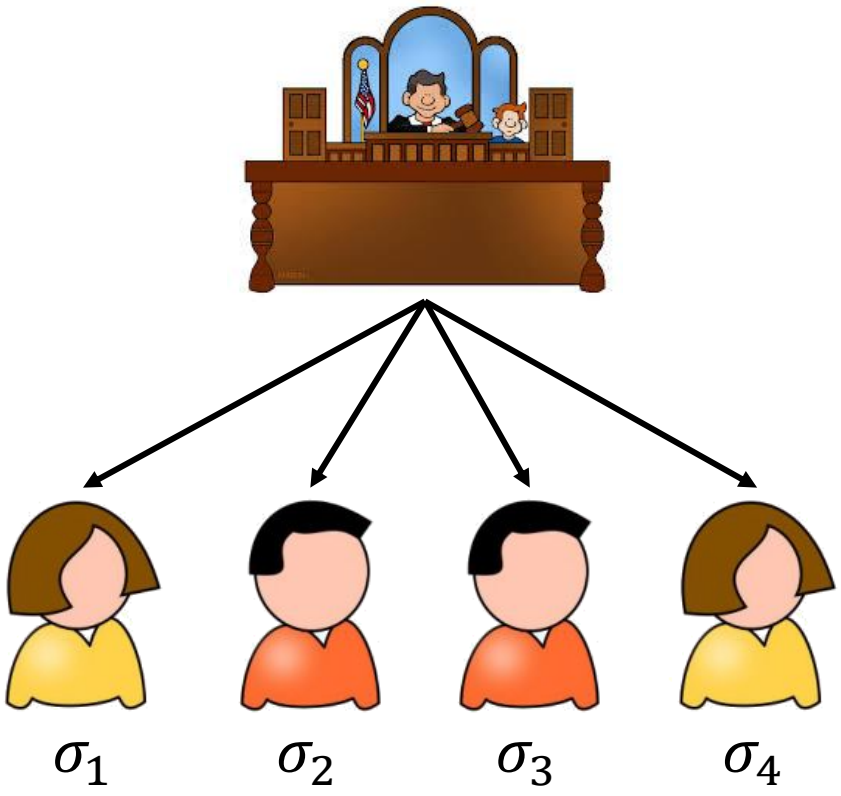
$\boldsymbol{s}^{\mathrm{T}}\boldsymbol{t}_i$

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

Succinct Computational Secret Sharing

[ABIKLV25]

secret s
monotone policy P



shares of s

Correctness: any set of users T where $P(T) = 1$ can reconstruct s

Security: shares for users T where $P(T) = 0$ should hide s

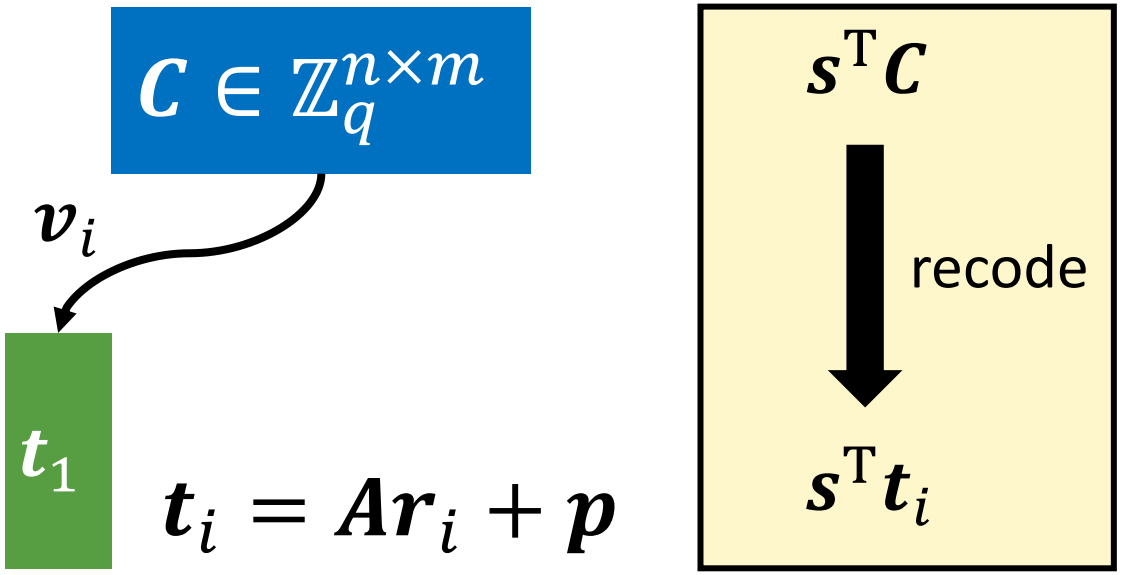
Succinctness: share size σ_i should be polylogarithmic in size of P

Succinct Computational Secret Sharing for DNFs

[CW26]

Recall approach to group messaging:

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



r_i is user i's secret key

Invariant: if party i knows $\boldsymbol{r}_i$, can recover $\boldsymbol{s}^{\mathrm{T}}\boldsymbol{p}$ and decrypt

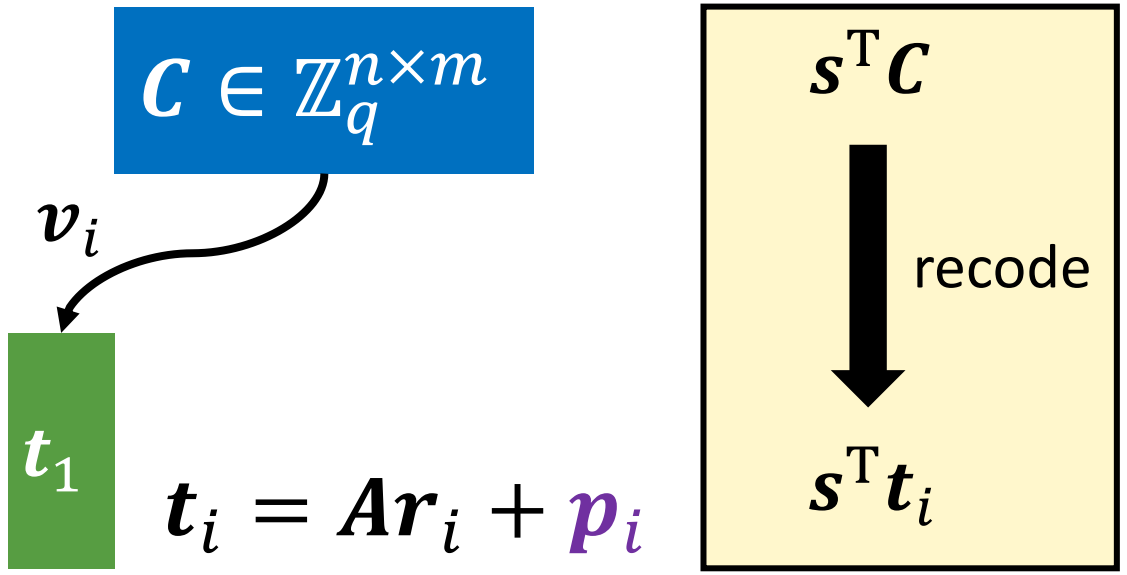
Succinct Computational Secret Sharing for DNFs

[CW26]

Recall approach to group messaging:

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

In more detail: secret share p according to a **non-succinct** linear secret sharing scheme, attach a public key to each share, and commit to the public keys



r_i is user i's secret key

Invariant: if party i knows r_i, can recover $s^{\mathrm{T}}p$ and decrypt

Secret sharing: if party i knows r_i, can recover $s^{\mathrm{T}}p_i$ where p_i is a share of p

Approach: commit to t_i that now recodes to p_i for each user (each party can have multiple t_i)

Conclusion: succinct CSS for DNFs with $\mathrm{poly}(\lambda)$-size shares

[some details omitted]

Matrix Commitments

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

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

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

$\text{pp} = \left(\boldsymbol{A} \in \mathbb{Z}^{n \times m}, \boldsymbol{V}_L \in \mathbb{Z}^{m \times L}\right)$

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

Functional commitments for all circuits + SNARGs for P/poly	[WW23a, WW23b, Wee24, Wee25]
Optimal broadcast encryption	[Wee25, AMR26, GY26a]
Distributed broadcast encryption	[CW24, CHW25, WW25, AMR26, CW26, GY26a, GY26b]
Nearly optimal continuous group key agreement	[BBDGW26]
Silent threshold encryption	[GY26b, GY26c, CWY26]
Nearly-optimal KP-ABE and CP-ABE for circuits	[Wee24, Wee25]
Registered ABE for circuits	[CHW25, AMR25, WW25]
Succinct computational secret sharing for DNFs	[CW26, GY26c]
Your favorite application here	