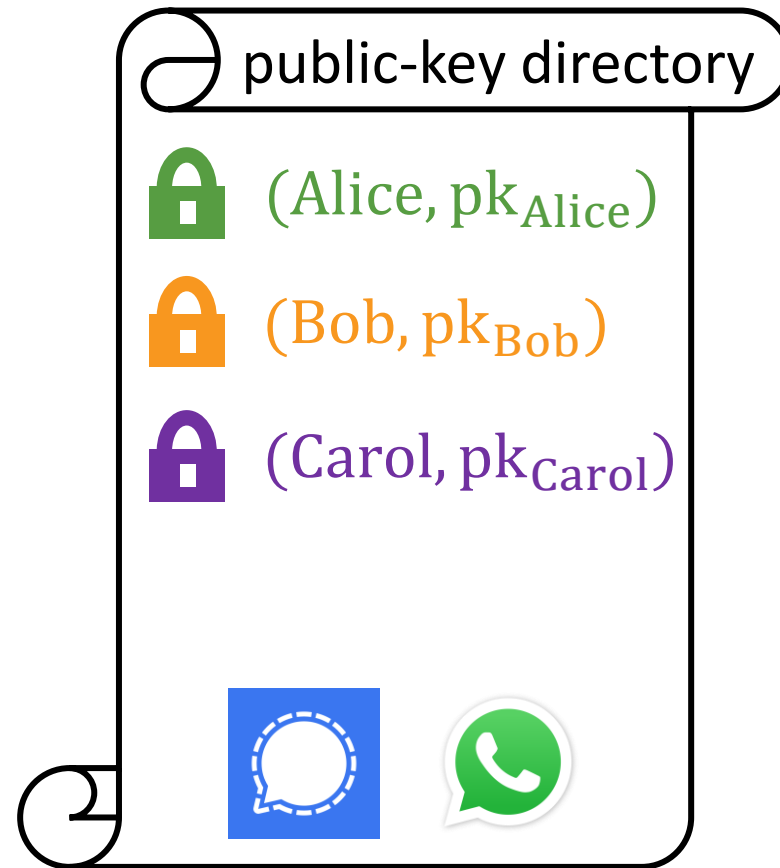
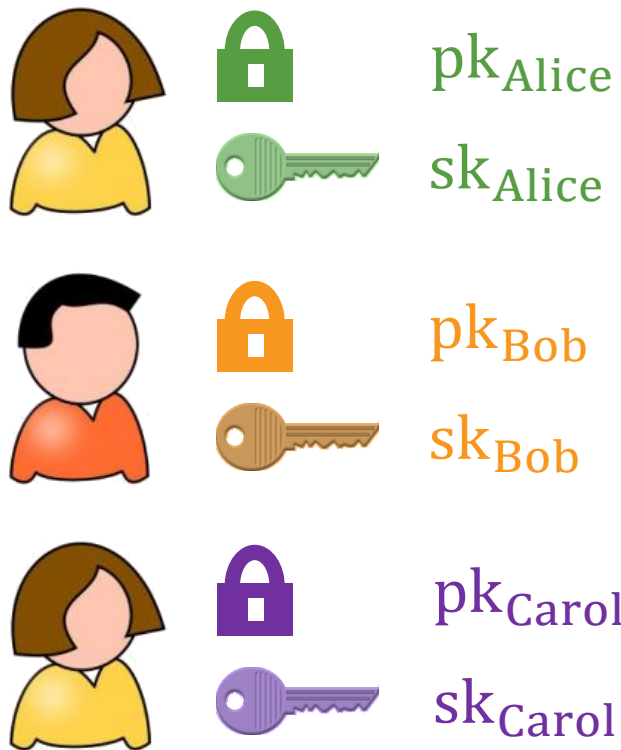


Succinct Matrix Commitments and Their Applications

David Wu

*based on joint works with James Bartusek, Nir Bitansky, Jeff Champion,
Yevgeniy Dodis, Rachit Garg, and Hoeteck Wee*

Group Messaging and Broadcast Encryption

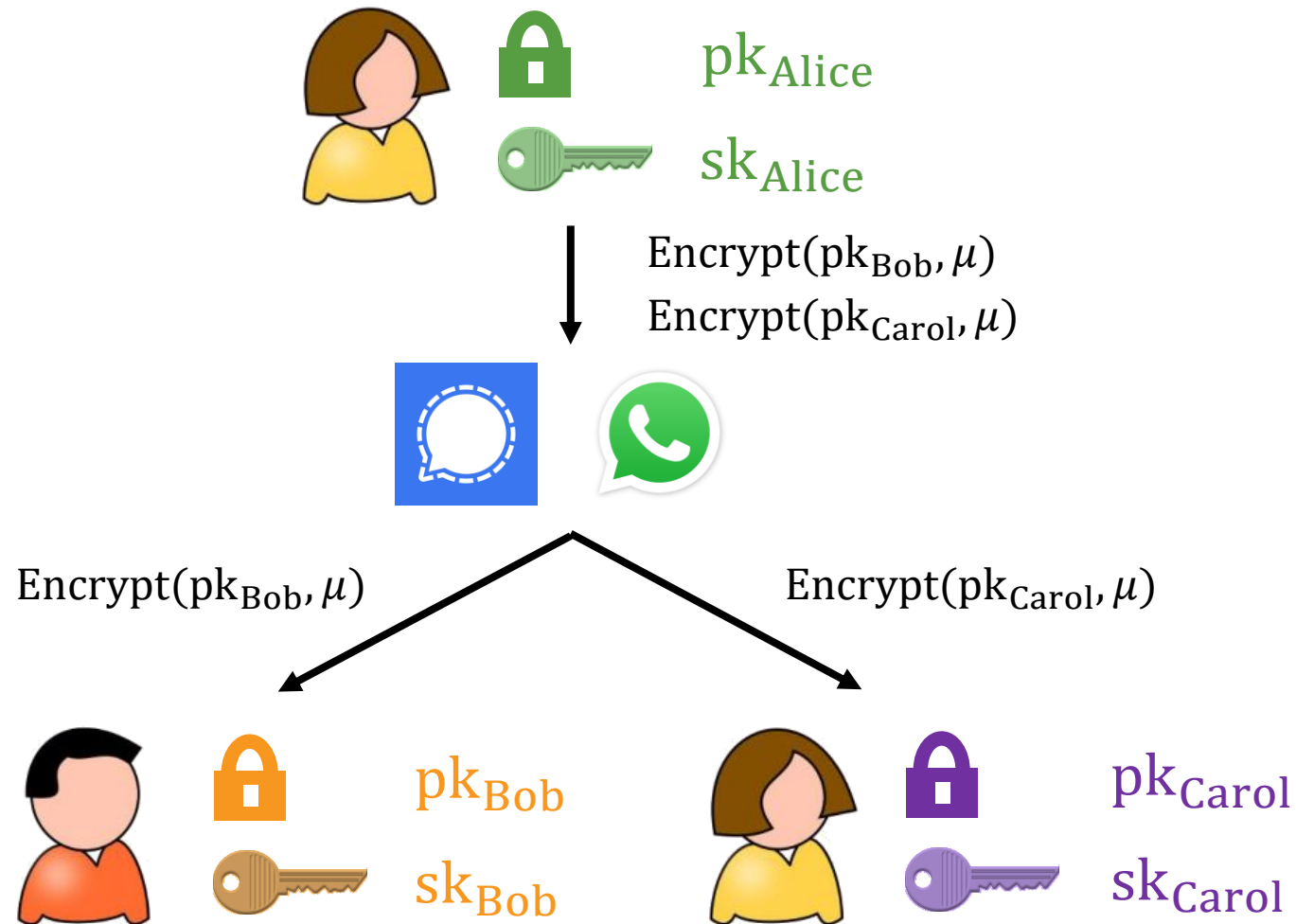


Users generate public/private keys independently

Goal: Group of users want to initiate an encrypted group chat

Group Messaging and Broadcast Encryption

Naïve solution: to send a message, user encrypts the message to each group member



Alice's communication is **linear** in the size of the group

Question: can we compress the ciphertext?

Can we encrypt a message to N public keys $pk_1, \dots, pk_N$ with ciphertext size $o(N)$?

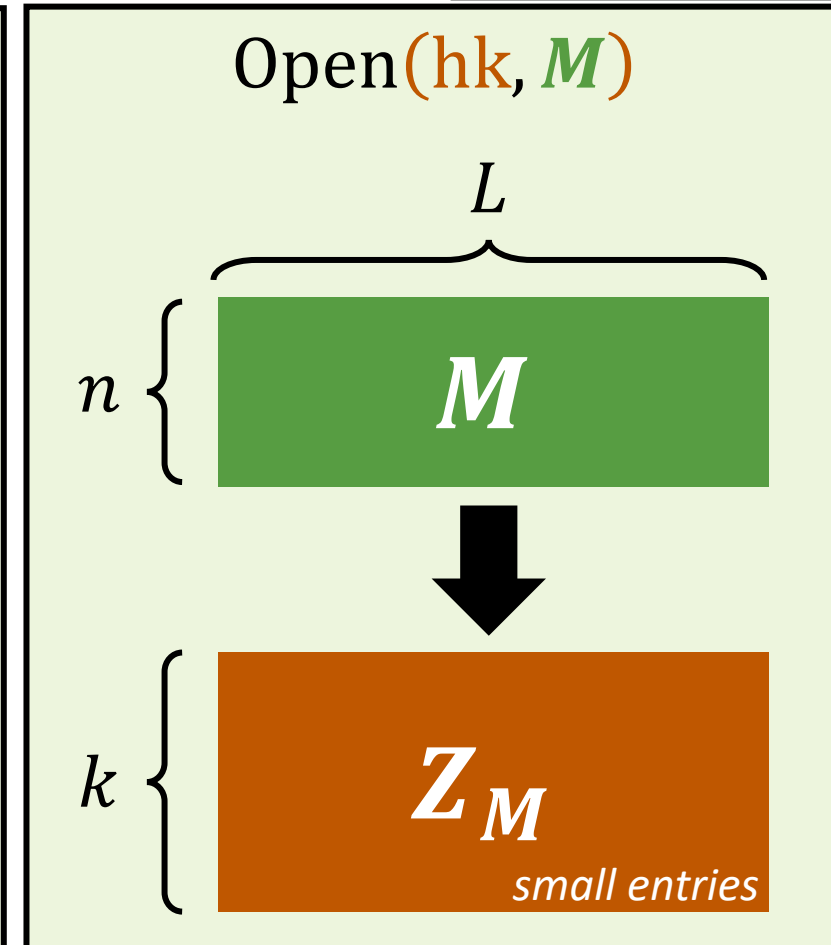
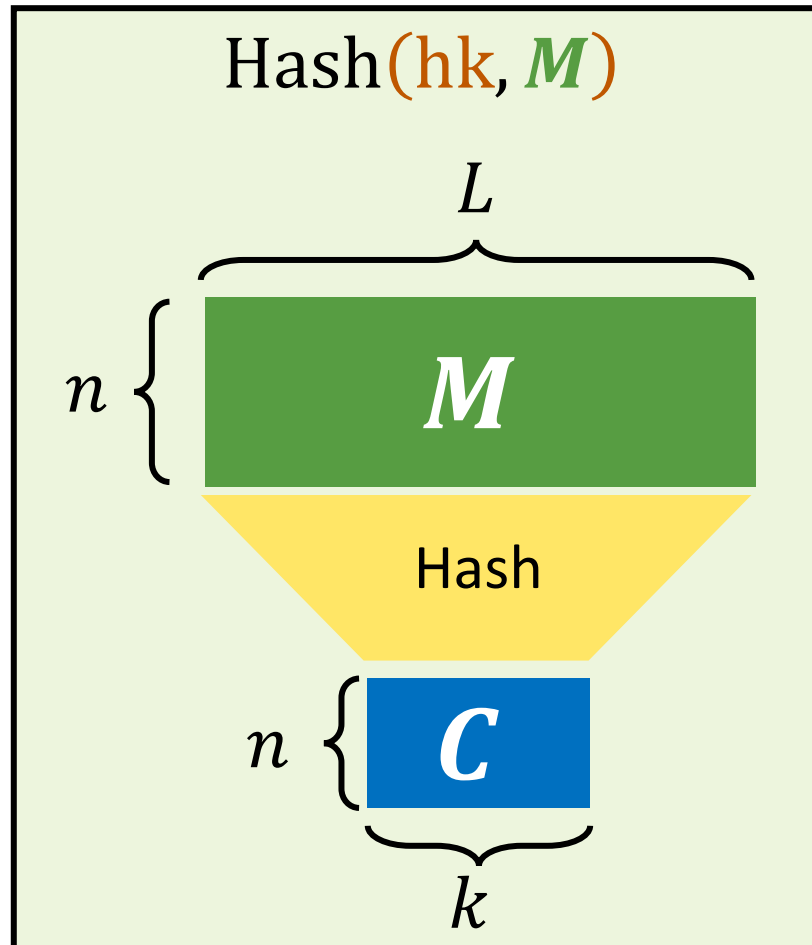
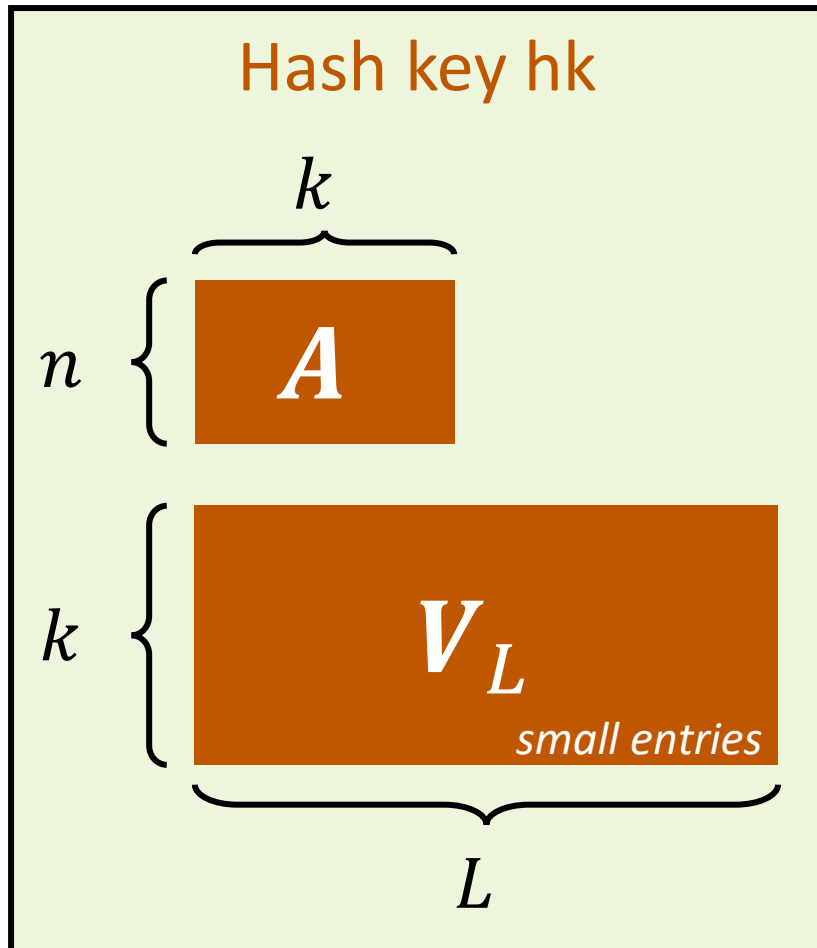
All the public keys are sampled **independently**

Matrix Hash (or Matrix Commitment)

[Wee24, Wee25]

Succinct hash of a matrix $M \in \mathbb{Z}_q^{n \times L}$

$$k = \text{poly}(n, \log q) \\ L \gg n$$



compress the matrix M into a digest C

Matrix Hash

[Wee24, Wee25]

Succinct hash of a matrix $M \in \mathbb{Z}_q^{n \times L}$

$$k = \text{poly}(n, \log q)$$

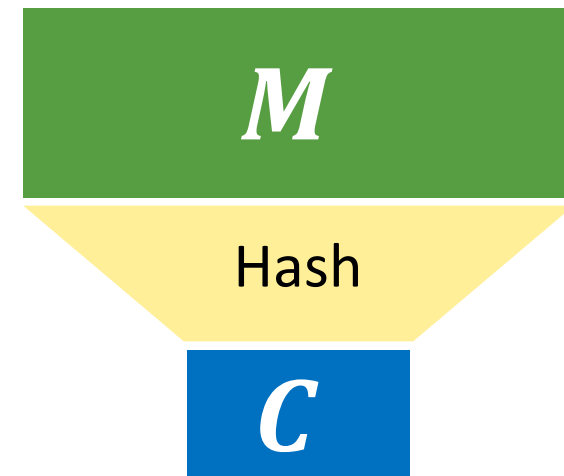
$$\text{Hash}(\text{hk}, M) \rightarrow C \in \mathbb{Z}_q^{n \times k}$$

$$\text{Open}(\text{hk}, M) \rightarrow Z_M \in \mathbb{Z}^{k \times L} \text{ low-norm}$$

Hash key $\text{hk} = (A, V_L)$

$$A \in \mathbb{Z}_q^{n \times k}$$

$$V_L \in \mathbb{Z}^{k \times L} \text{ low-norm}$$



Key opening relation:

$$C \cdot V_L = M - A \cdot Z_M$$

C is a compressed representation of M (width of C independent of M)

Can expand C to translation of M by multiplying by a fixed low-norm matrix V_L

Z_M must be “taller” since its elements are small (will be taller than M by $> \log q$ factor)

Matrix Hash

[Wee24, Wee25]

Succinct hash of a matrix $M \in \mathbb{Z}_q^{n \times L}$

$$k = \text{poly}(n, \log q)$$

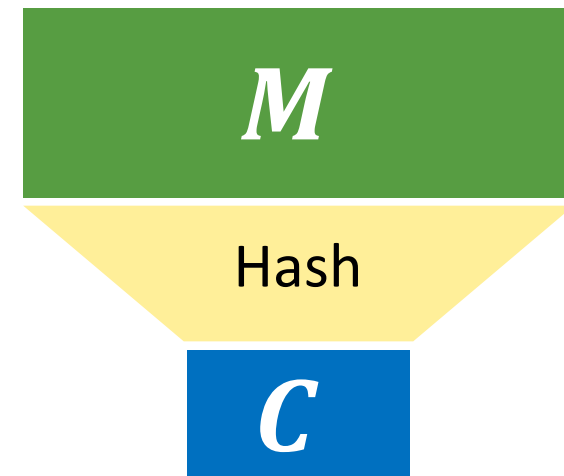
$$\text{Hash}(\text{hk}, M) \rightarrow C \in \mathbb{Z}_q^{n \times k}$$

$$\text{Open}(\text{hk}, M) \rightarrow Z_M \in \mathbb{Z}^{k \times L} \text{ low-norm}$$

Hash key $\text{hk} = (A, V_L)$

$$A \in \mathbb{Z}_q^{n \times k}$$

$$V_L \in \mathbb{Z}^{k \times L} \text{ low-norm}$$



Key opening relation:

$$C \cdot V_L = M - A \cdot Z_M$$

Security assumption: LWE problem is hard with respect to A given hk

LWE problem: distinguish $s^T A + e^T$ from random when $s \leftarrow \mathbb{Z}_q^n$ and $e \in \mathbb{Z}^k$ is low-norm
noisy linear combination of rows of A are pseudorandom

Matrix Hash

[Wee24, Wee25]

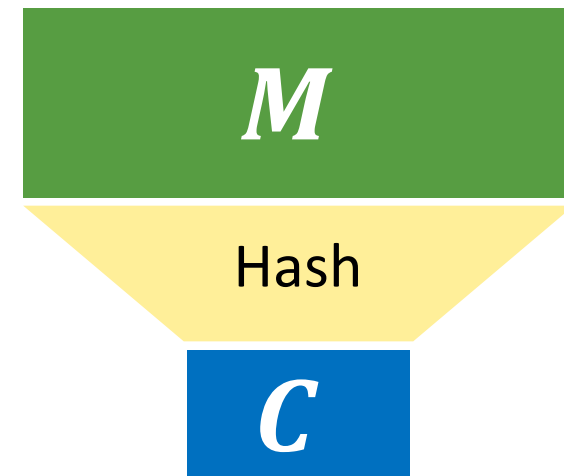
Succinct hash of a matrix $M \in \mathbb{Z}_q^{n \times L}$

$$k = \text{poly}(n, \log q)$$

$$\text{Hash}(\text{hk}, M) \rightarrow C \in \mathbb{Z}_q^{n \times k}$$

$$\text{Open}(\text{hk}, M) \rightarrow Z_M \in \mathbb{Z}^{k \times L} \text{ low-norm}$$

Hardness of LWE with respect to A
given hk holds under the
decomposed LWE assumption



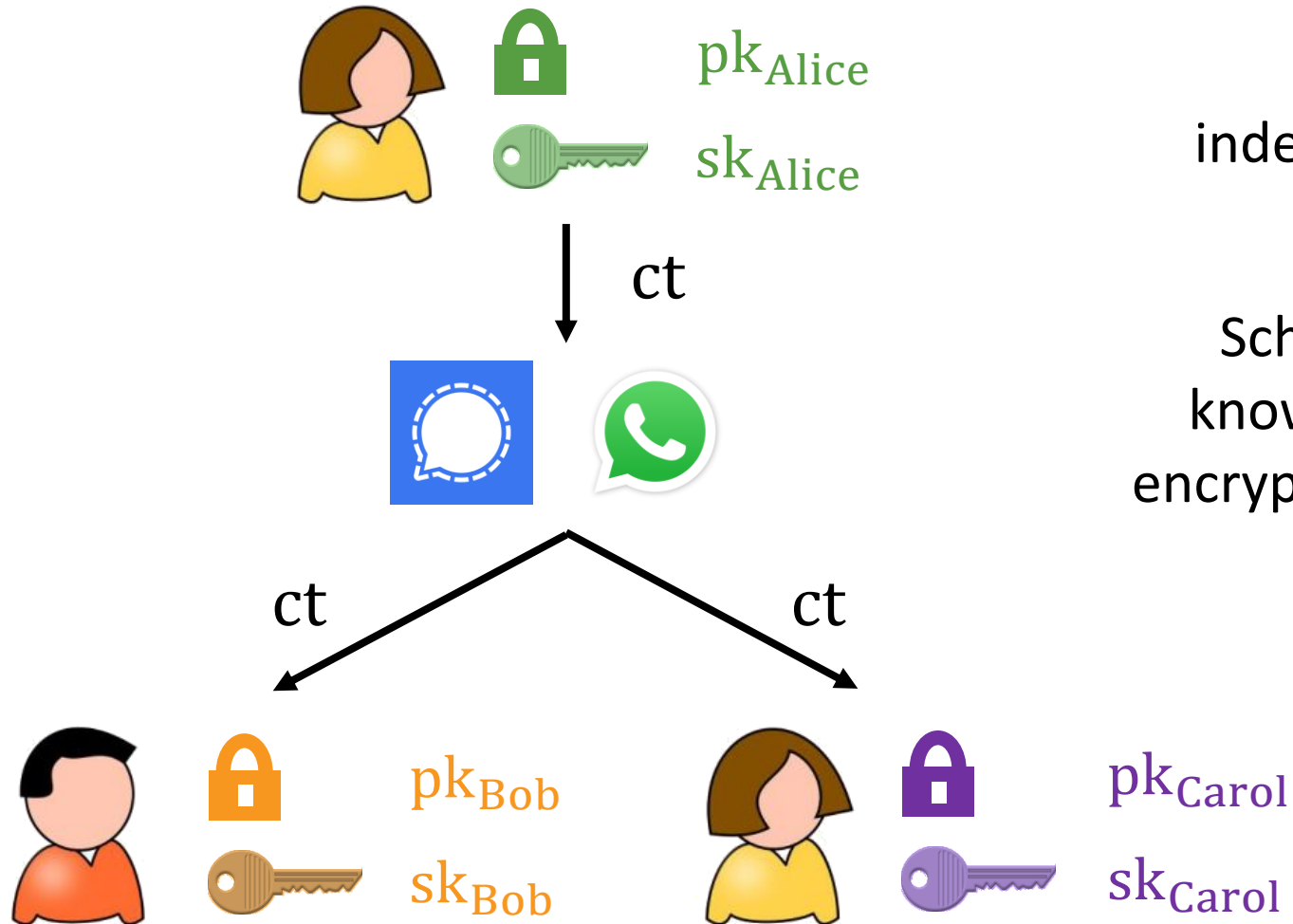
Key opening relation:

$$C \cdot V_L = M - A \cdot Z_M$$

Security assumption: LWE problem is hard with respect to A given hk

LWE problem: distinguish $s^T A + e^T$ from random when $s \leftarrow \mathbb{Z}_q^n$ and $e \in \mathbb{Z}^k$ is low-norm
noisy linear combination of rows of A are pseudorandom

Group Messaging and Broadcast Encryption

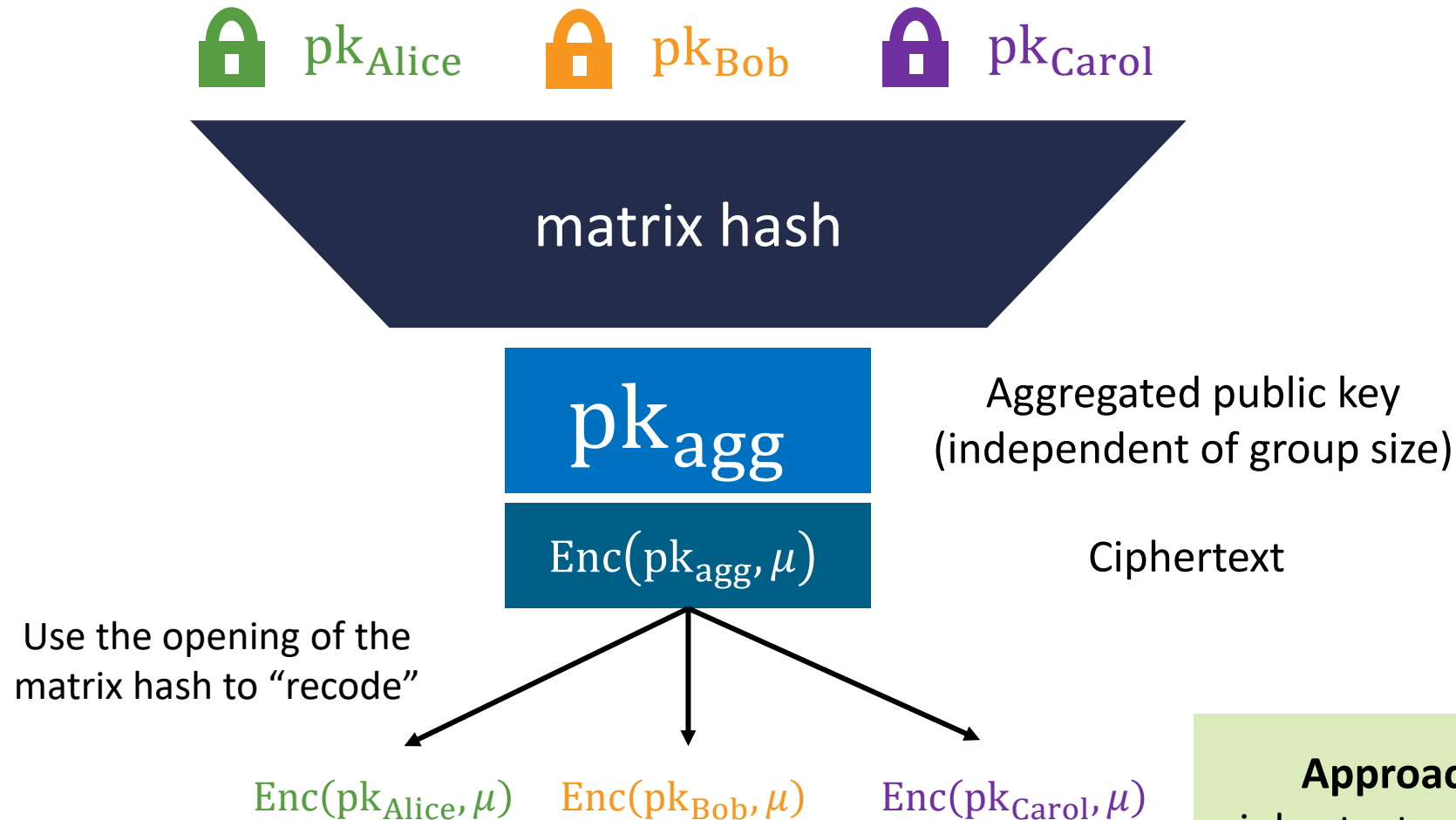


Goal: size of the ciphertext ct is independent of the number of receivers

Scheme with optimal parameters only known from strong tools such as witness encryption or indistinguishability obfuscation

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]



Approach: "recode" an LWE ciphertext with respect to pk_{agg} to a ciphertext with respect to pk_{user}

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]

Starting point: dual Regev encryption

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

sk: low-norm r where $Ar = p$

$$A r = p$$

Ciphertext (encrypting $\mu \in \{0, 1\}$):

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

$s^T A + e_1^T$, $s^T p + e_2 + \mu \cdot \lfloor q/2 \rfloor$

Multiply by r

Decryption:

$s^T p + e_1^T r$

$\mu \cdot \lfloor q/2 \rfloor + (e_2 - e_1^T r)$

$$\|r\|, \|e_1\|, |e_2| \ll q \Rightarrow |e_2 - e_1^T r| \ll q$$

Learning with errors (LWE)

$$[A \mid p], s^T [A \mid p] + [e_1^T \mid e_2]$$

is pseudorandom

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]

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



$$pk_1 = t_1 = Ar_1 + p \in \mathbb{Z}_q^n$$



$$sk_1 = r_1 \leftarrow \{0,1\}^k$$



$$pk_2 = t_2 = Ar_2 + p \in \mathbb{Z}_q^n$$



$$sk_2 = r_2 \leftarrow \{0,1\}^k$$



$$pk_3 = t_3 = Ar_3 + p \in \mathbb{Z}_q^n$$



$$sk_3 = r_3 \leftarrow \{0,1\}^k$$

Aggregated group key:



Hash($[t_1 \mid t_2 \mid t_3]$)

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

Invariant: $Cv_i = t_i - Az_i$ where v_i, z_i are low-norm

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]

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



$$pk_1 = t_1 = Ar_1 + p \in \mathbb{Z}_q^n$$

$$sk_1 = r_1 \leftarrow \{0,1\}^k$$

Ciphertext:

(suppressing error terms)

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

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

Use v_i, z_i to recode to encryption under t_i :

Aggregated group key:

$$t_1$$

$$t_2$$

$$t_3$$

$$\text{Hash}([t_1 \mid t_2 \mid t_3])$$

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

Invariant: $Cv_i = t_i - Az_i$ where v_i, z_i are low-norm

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]

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



$$pk_1 = t_1 = Ar_1 + p \in \mathbb{Z}_q^n$$

$$sk_1 = r_1 \leftarrow \{0,1\}^k$$

Ciphertext:

(suppressing error terms)

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

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

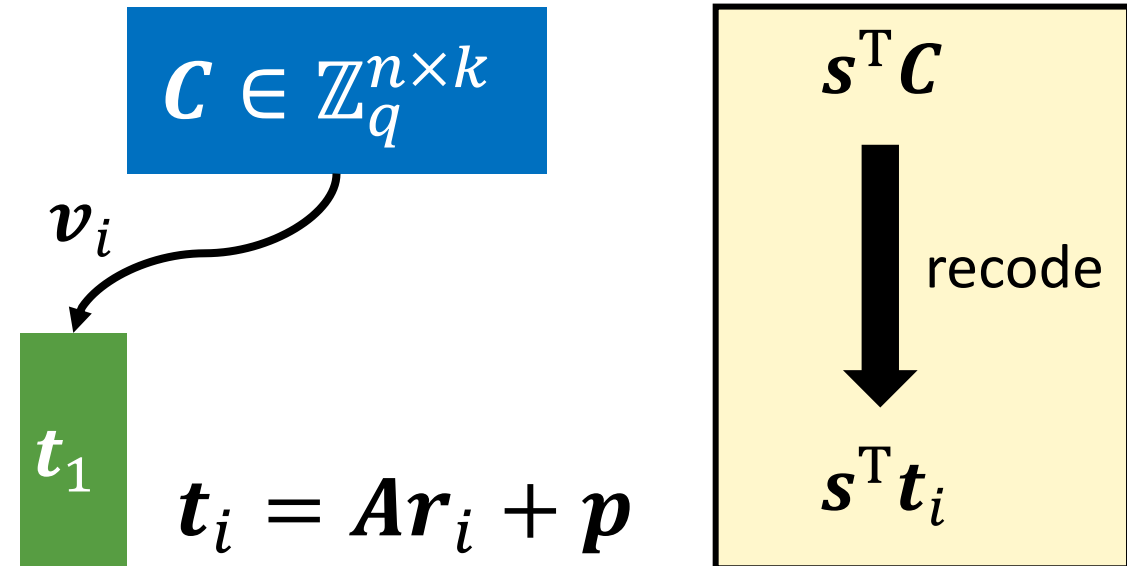
Use v_i, z_i to recode to encryption under t_i :

$$s^T C \cdot v_i + s^T A \cdot z_i \approx s^T t_i - s^T A z_i + s^T A z_i$$

$$= s^T t_i = s^T A r_i + s^T p$$

$$s^T C \cdot v_i + s^T A \cdot z_i - s^T A \cdot r_i \approx s^T p$$

Aggregated group key:



Invariant: $Cv_i = t_i - Az_i$ where v_i, z_i are low-norm

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]

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



$$\text{pk}_1 = t_1 = Ar_1 + p \in \mathbb{Z}_q^n$$

$$\text{sk}_1 = r_1 \leftarrow \{0,1\}^k$$

Ciphertext:

(suppressing error terms)

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

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

Overall ciphertext size:
 $|\text{ct}| = \text{poly}(n, \log q)$

(independent of group size)

Aggregated group key:

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

v_i

$$t_1$$

$$t_i = Ar_i + p$$

$$s^T C$$

decode

$$s^T t_i$$

Invariant: $Cv_i = t_i - Az_i$ where v_i, z_i are low-norm

Group Messaging and Broadcast Encryption

[WW25, BBDGW26]

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



$$pk_1 = t_1 = Ar_1 + p \in \mathbb{Z}_q^n$$

$$sk_1 = r_1 \leftarrow \{0,1\}^k$$

Ciphertext:

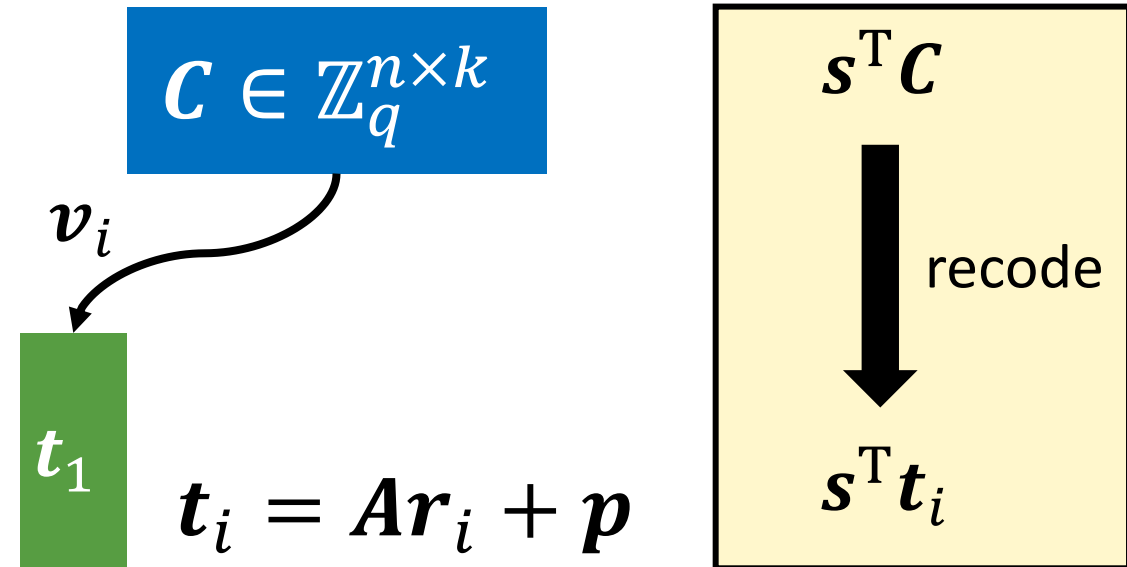
(suppressing error terms)

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

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

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

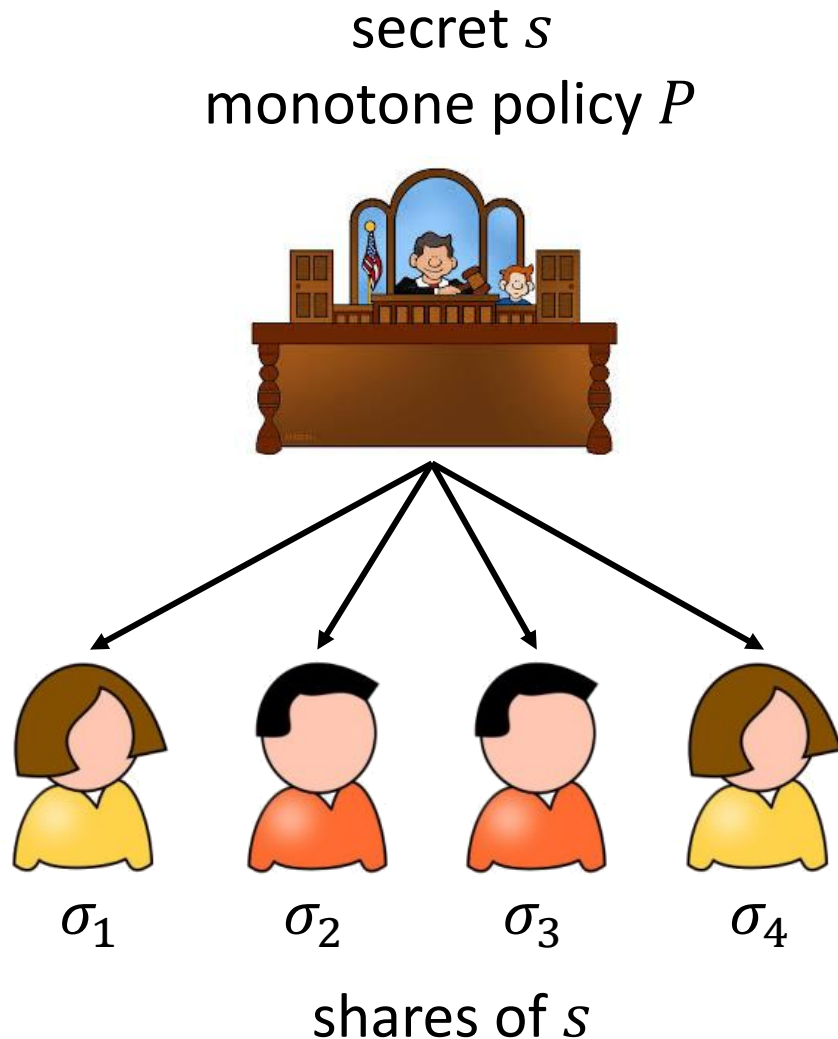
Aggregated group key:



Invariant: $Cv_i = t_i - Az_i$ where v_i, z_i are low-norm

Succinct Computational Secret Sharing

[ABIKLV25]



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

For general monotone policies on n -bits (e.g., truth table of size 2^n), best information-theoretic construction has share size $\approx 2^{0.585n}$

Best information-theoretic lower bound: $\Omega(n^2 / \log n)$

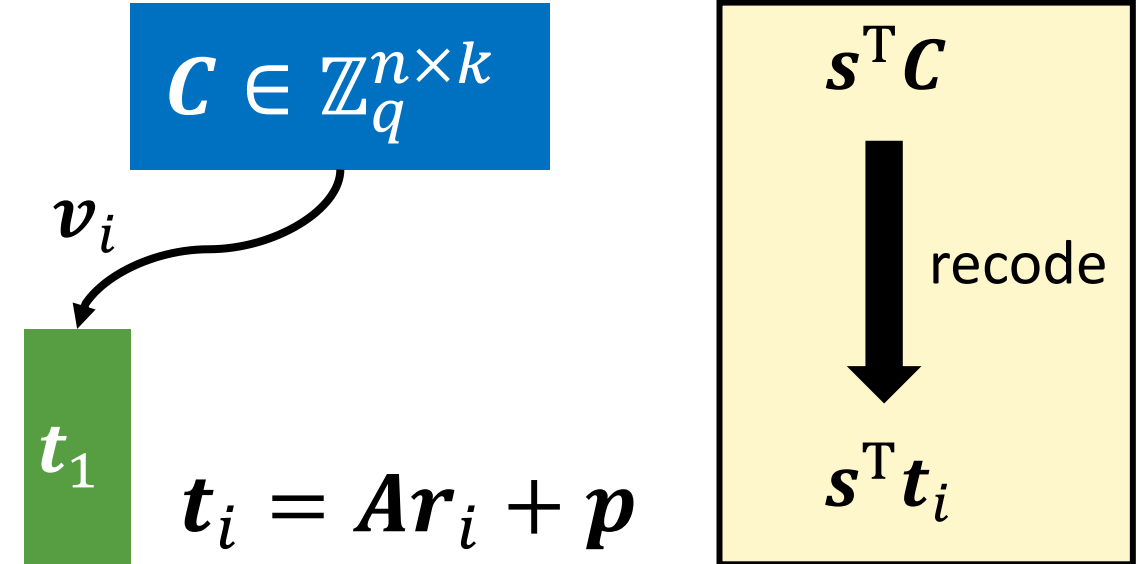
With computational assumptions: $\text{poly}(n) = \text{poly}(\log |P|)$

Succinct Computational Secret Sharing

[CW26]

Recall approach to group messaging:

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



r_i is user i 's secret key

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

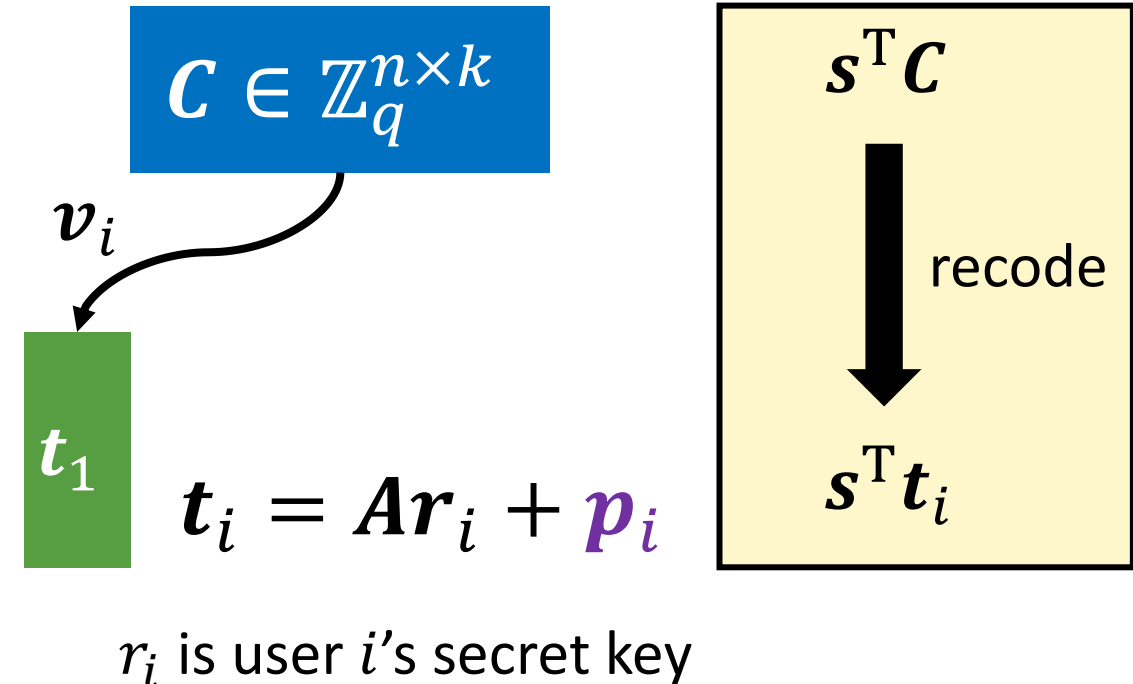
Succinct Computational Secret Sharing

[CW26]

Recall approach to group messaging:

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

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



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

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

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

Technicality: can only prove security for DNFs with constant-size shares

[some details omitted]

Matrix Hash

[Wee24, Wee25]

Succinct hash of a matrix $M \in \mathbb{Z}_q^{n \times L}$

$$k = \text{poly}(n, \log q)$$

$$\text{Hash}(\text{hk}, M) \rightarrow C \in \mathbb{Z}_q^{n \times k}$$

$$\text{Open}(\text{hk}, M) \rightarrow Z_M \in \mathbb{Z}^{k \times L} \text{ low-norm}$$

Key opening relation: $C \cdot V_L = M - A \cdot Z_M$

Very versatile tool for realizing applications that require succinctness

Verifiable computation for arithmetic circuits

[WW23a, WW23b, Wee24, Wee25]

Broadcast encryption and group messaging

[CW24, Wee25, CHW25, WW25, AMR26, CW26, BBDGW26, GY26a, GY26b]

Nearly optimal attribute-based encryption

[Wee24, Wee25]

Succinct computational secret sharing for DNFs

[CW26, GY26c]

Thank you!