

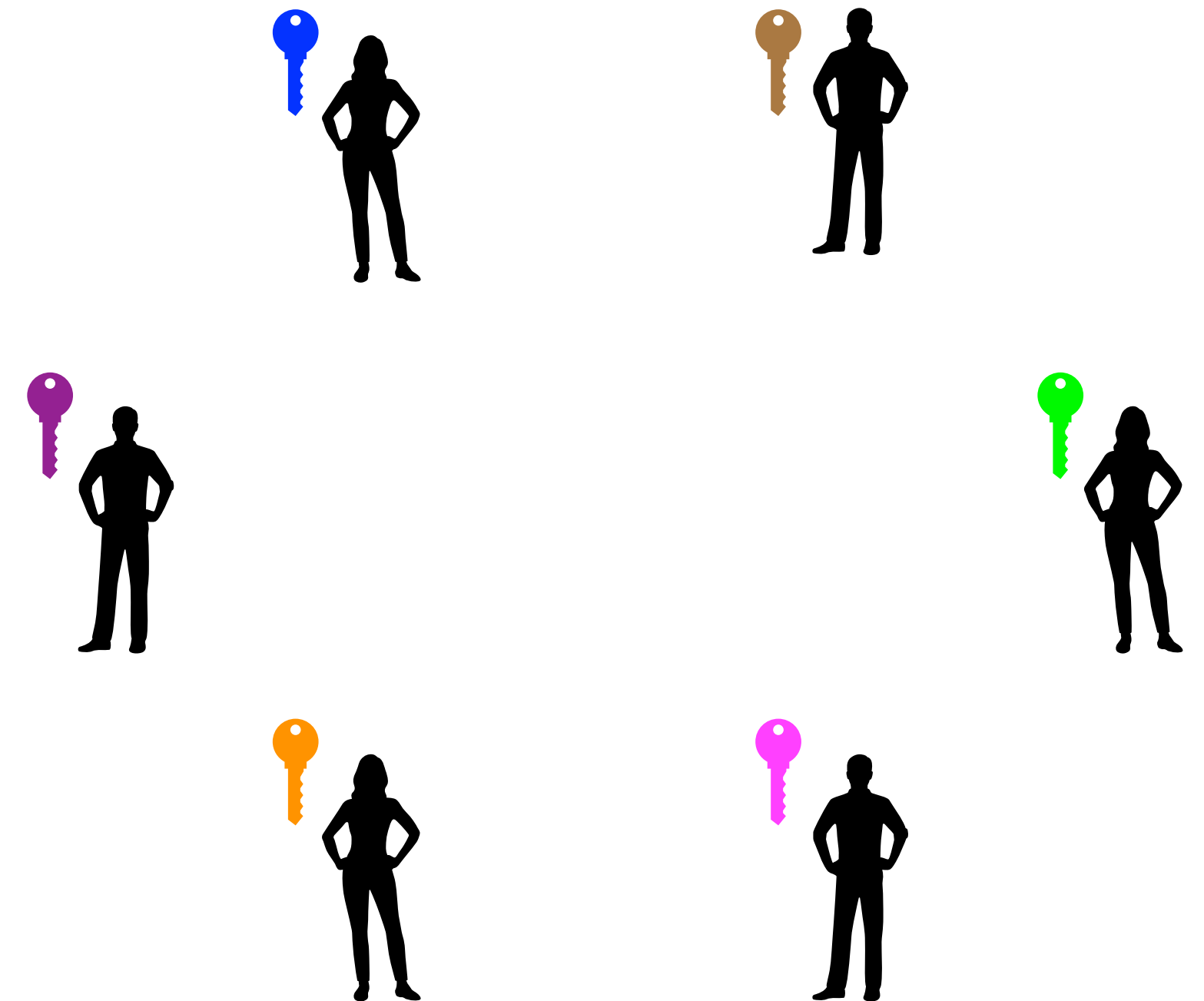
How to share lattice trapdoors

Literally

Based on the ongoing work with Martin Albrecht, Russell Lai and Ivy Woo.

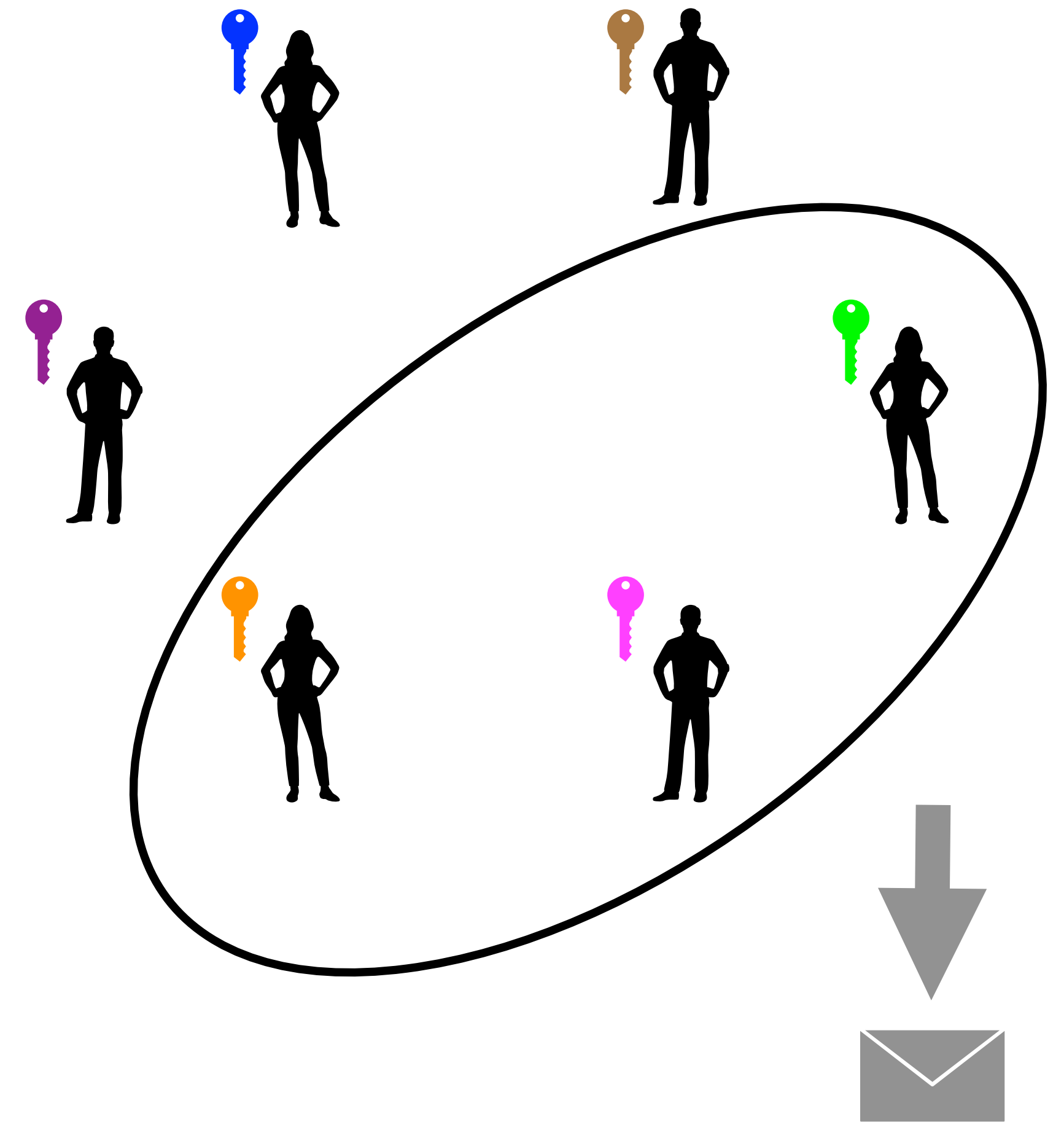
Threshold Cryptography

Goal: Distribute Trust
E.g. Threshold Signatures



Threshold Signatures

Total number of k users
Any group t can sign

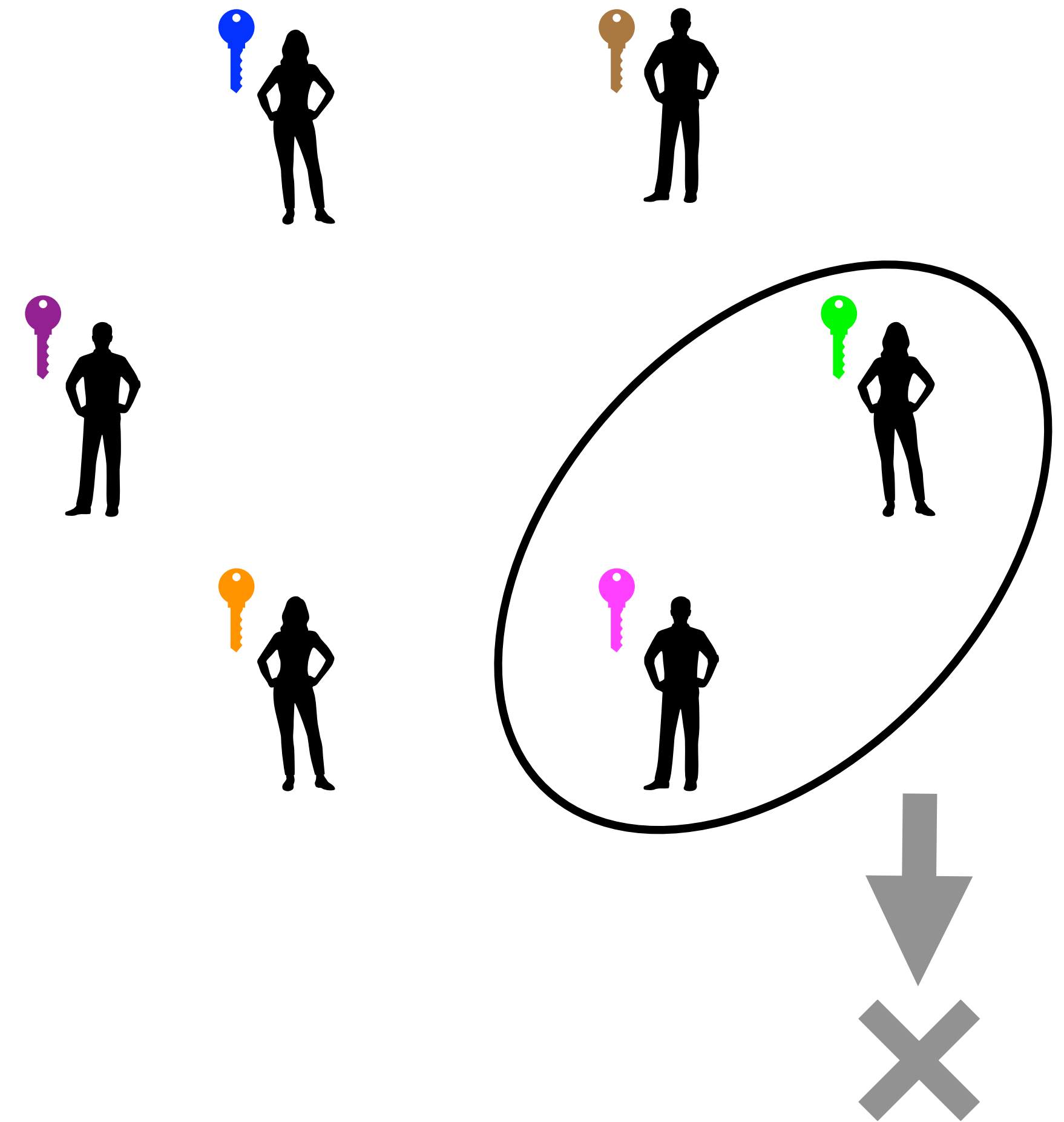


Threshold Signatures

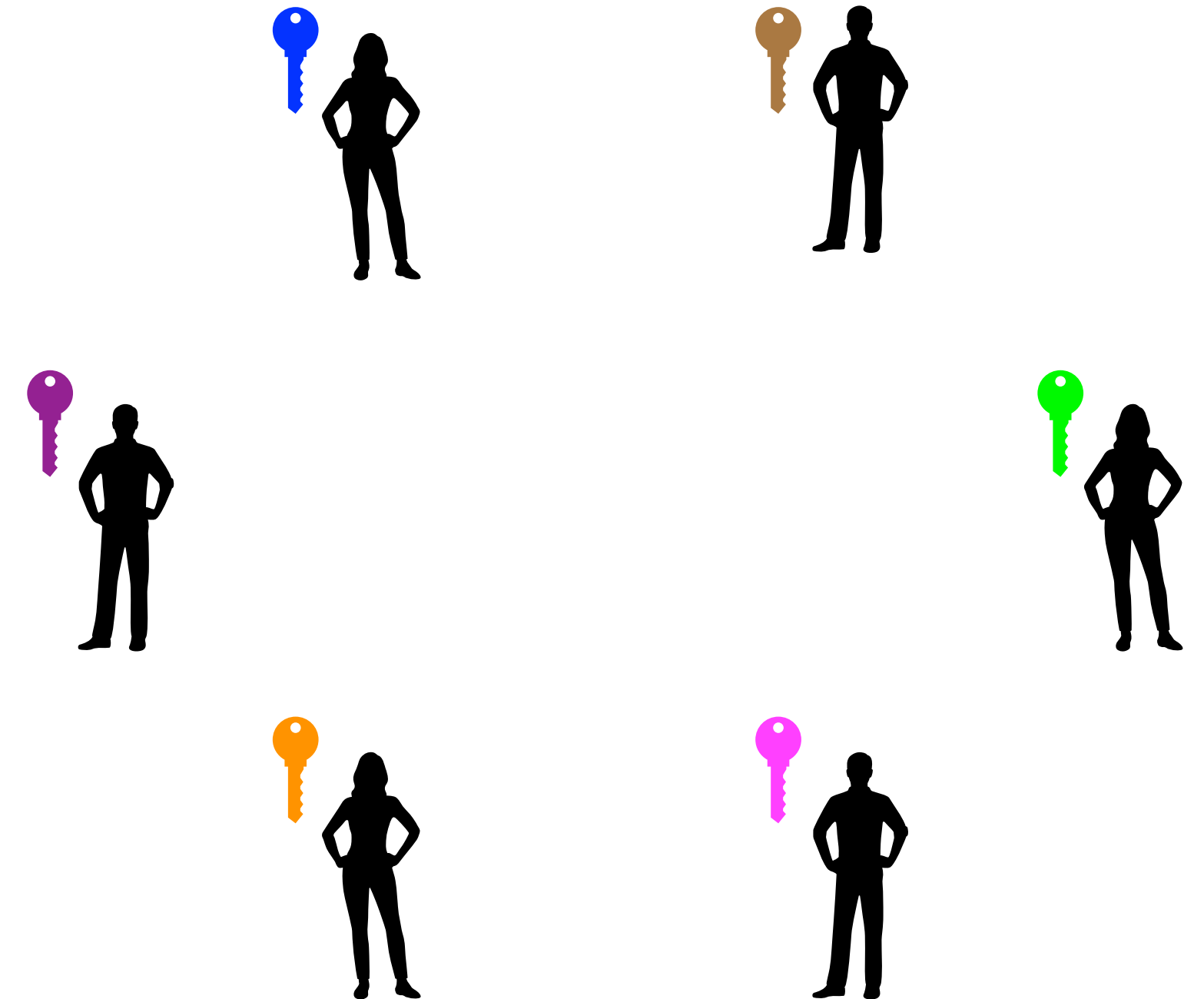
Total number of k users

Any group t can sign

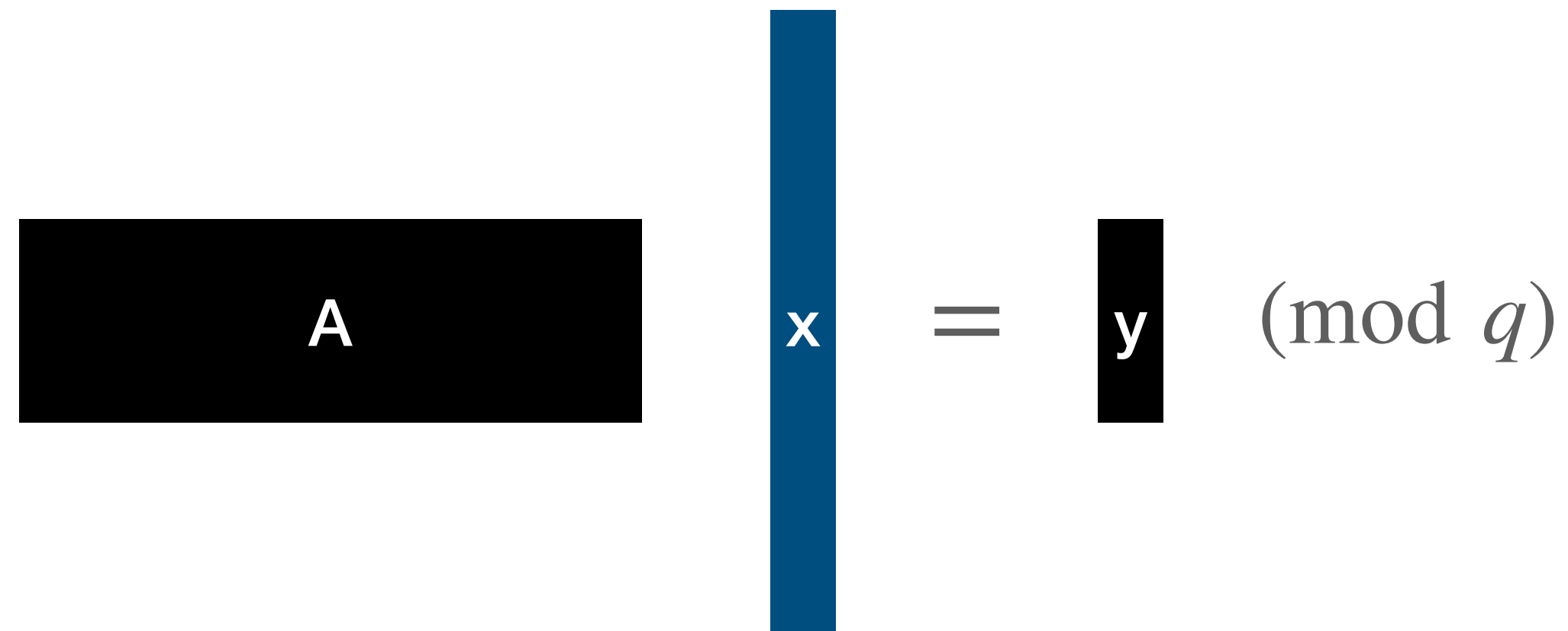
No smaller group can produce a signature



Lattice Trapdoors



Lattice Trapdoors


$$A x = y \pmod{q}$$

x - sufficiently short vector.

Lattice Trapdoors

A

x

=

y

(mod q)

x - short vector.

A

T

=

00

⋮

00

(mod q)

T - matrix of short vectors

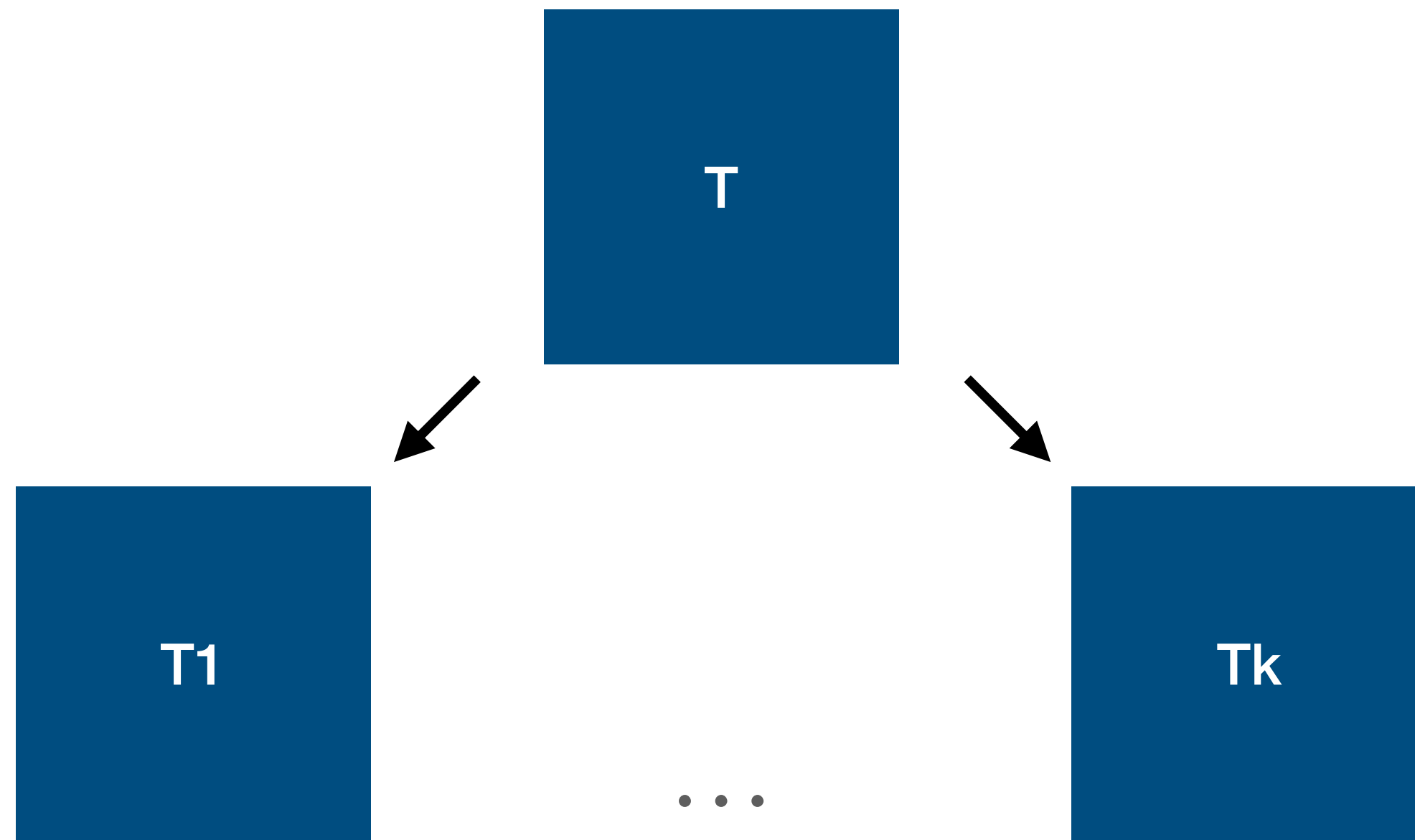
How to share T?

- **Fancy Crypto**
 - **Homomorphic encryption**
 - **Multi-party computation**
- **Natively**
 - **???????**

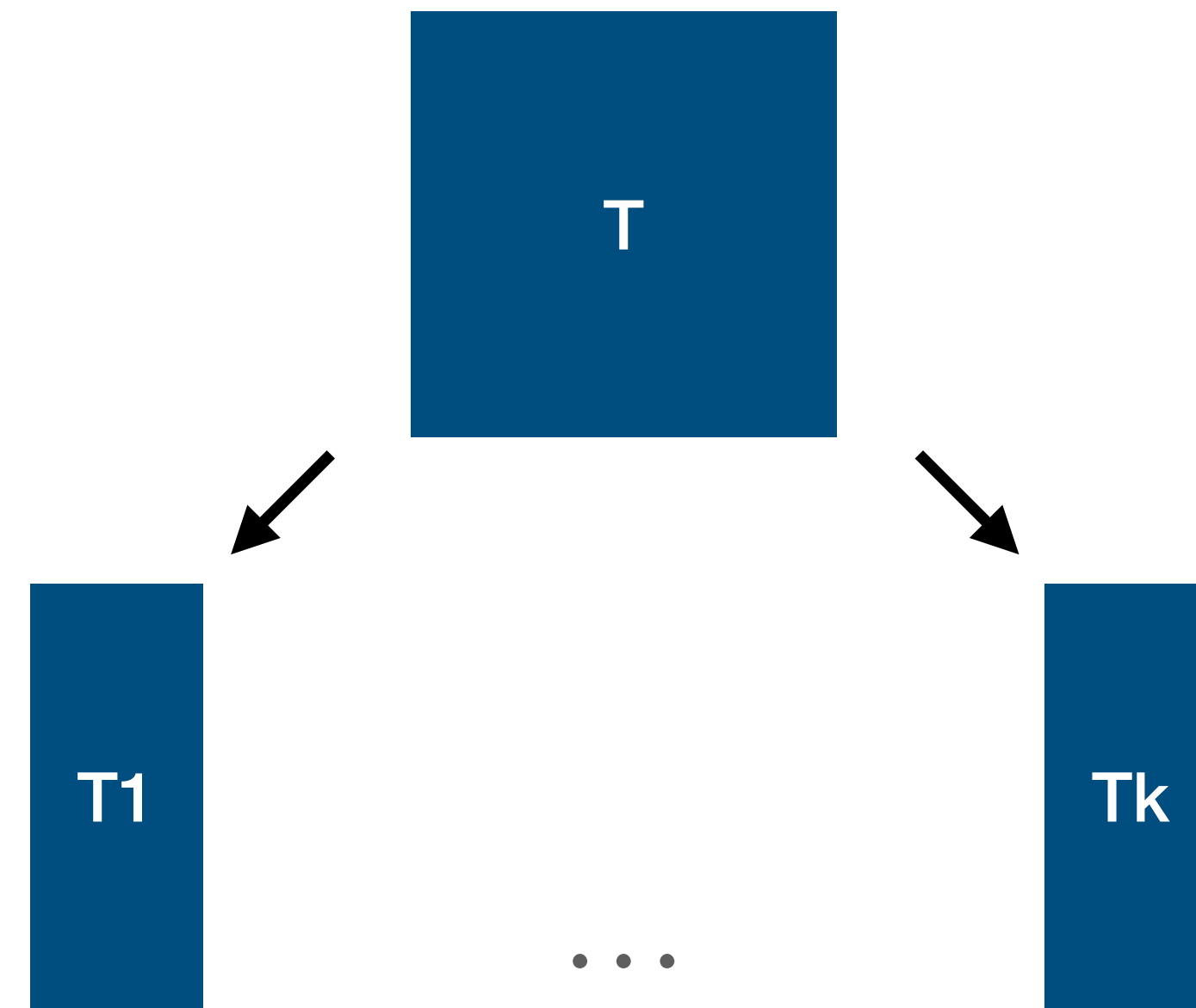
$$\boxed{A \cdot T = \begin{pmatrix} 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix} \pmod{q}}$$

Bad Ideas

Give T - insecure



Split T - incorrect



Gadget Trapdoors

A

x

=

y

(mod q)

x - short vector.

A

T

=

G

g

0

0

g

(mod q)

T - matrix of short vectors

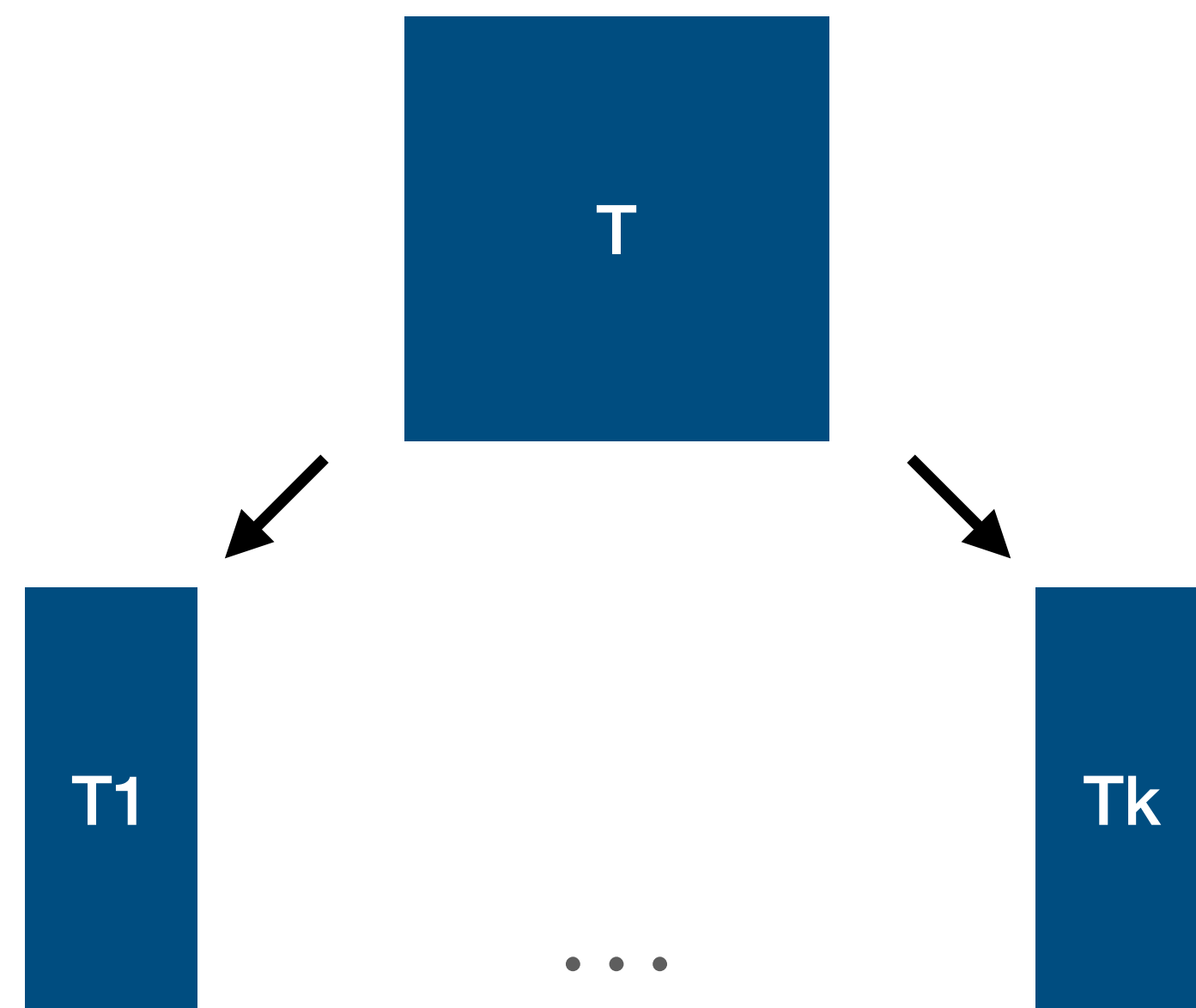
g

=

1 2 ... 2^[log q]

Our Idea

Split T + Split the image space.

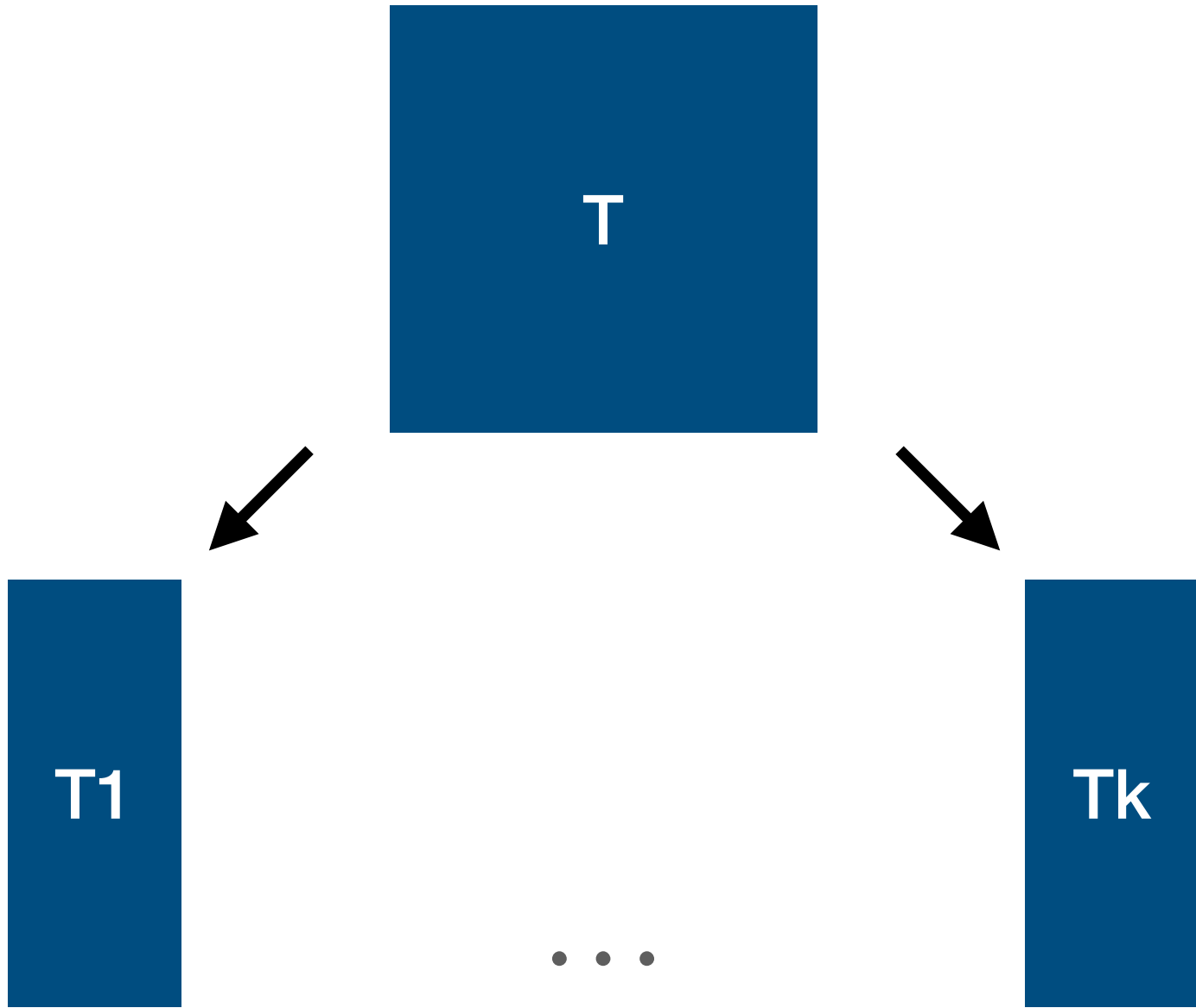


Given vectors $\mathbf{v}_1, \dots, \mathbf{v}_k$ such that any combination of t of them forms an invertible matrix.

An equation showing the product of a matrix A and a transformation T_1 modulo q . On the left, a black rectangle labeled A is followed by a blue rectangle labeled T_1 . This is followed by an equals sign and a black rectangle containing a matrix structure. The matrix has three rows and three columns. The first row contains $|$, $|$, and $\dots$. The second row contains $\mathbf{v}_1$, $2\mathbf{v}_1$, and $\dots$. The third row contains $|$, $|$, and $\dots$. To the right of the matrix is the expression $(\text{mod } q)$.

Our Idea

Split T + Split the image space.



Given vectors $v_1, \dots, v_k$ such that any combination of t of them forms an invertible matrix.

The equation shows a black rectangle labeled A multiplied by a blue rectangle labeled T_1 , followed by an equals sign and a matrix representation of the result modulo q . The matrix is shown as a grid with three rows and two columns of elements, with ellipses indicating continuation. Below the equation, a box contains the text "In the full version:" followed by the equation $v_1 \otimes g \rightarrow v_1 \otimes G$.

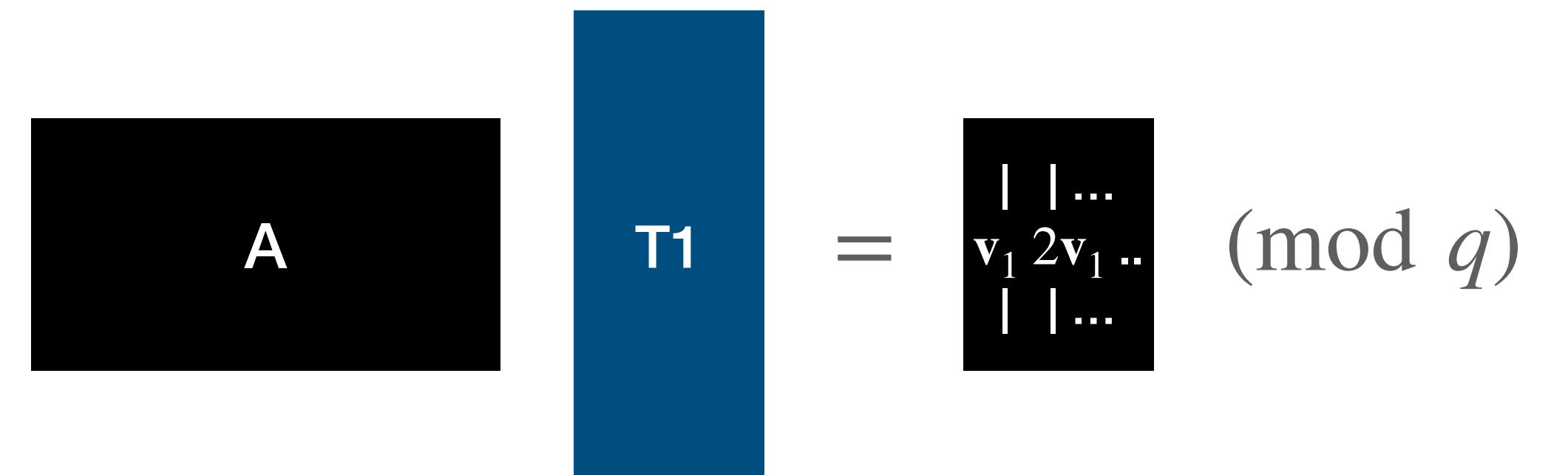
$$A \cdot T_1 = \begin{bmatrix} | & | & \dots \\ v_1 & 2v_1 & \dots \\ | & | & \dots \end{bmatrix} \pmod{q}$$

In the full version:
 $v_1 \otimes g \rightarrow v_1 \otimes G$

Our Idea

To compute a preimage of y with parties $1, \dots, t$

1. Set $V = (\mathbf{v}_1 \mid \dots \mid \mathbf{v}_t)$.



The diagram illustrates the computation of a preimage. It shows a black rectangular box labeled 'A' multiplied by a blue rectangular box labeled 'T1'. The result is an equals sign followed by a black box containing a vector representation: the first row has three entries (a vertical bar, a vertical bar, and an ellipsis), the second row has three entries ($\mathbf{v}_1$, $2\mathbf{v}_1$, and an ellipsis), and the third row has three entries (a vertical bar, a vertical bar, and an ellipsis). This is followed by the text $(\text{mod } q)$.

$$A \cdot T1 = \begin{bmatrix} | & | & \dots \\ \mathbf{v}_1 & 2\mathbf{v}_1 & \dots \\ | & | & \dots \end{bmatrix} \pmod{q}$$

Our Idea

To compute a preimage of y with parties $1, \dots, t$

1. Set $V = (v_1 \mid \dots \mid v_t)$.

2. Compute $z = V^{-1}y$ then we have: $Vz = y$.

The diagram illustrates the computation of a preimage. It shows a black rectangular box labeled 'A' multiplied by a blue rectangular box labeled 'T1'. The result is shown as a black square box containing a matrix structure, followed by an equals sign and the text '(mod q)'. The matrix structure inside the black box is:

$$\begin{bmatrix} | & | & \dots \\ v_1 & 2v_1 & \dots \\ | & | & \dots \end{bmatrix}$$

Our Idea

To compute a preimage of y with parties $1, \dots, t$

1. Set $V = (\mathbf{v}_1 \mid \dots \mid \mathbf{v}_t)$.
2. Compute $\mathbf{z} = V^{-1}y$ then we have: $V\mathbf{z} = y$.
3. Party i computes $\mathbf{x}_i : A\mathbf{x}_i = z_i\mathbf{v}_i$

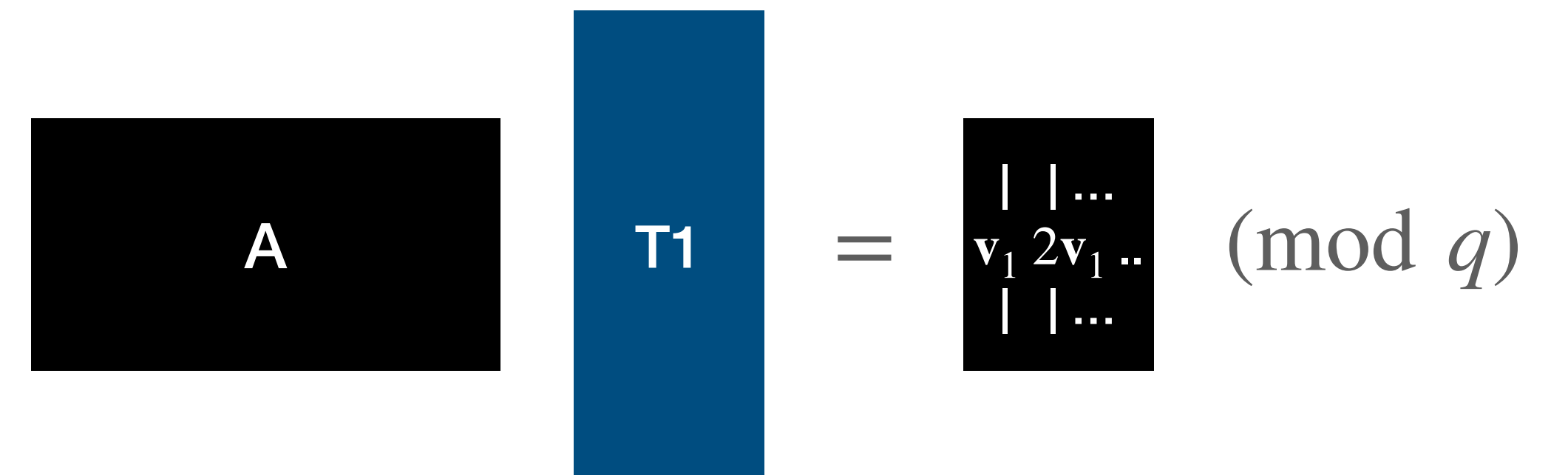
$$\begin{array}{|c|} \hline A \\ \hline \end{array} \begin{array}{|c|} \hline T1 \\ \hline \end{array} = \begin{array}{|c|} \hline \begin{array}{c} | \quad | \dots \\ \mathbf{v}_1 \quad 2\mathbf{v}_1 \dots \\ | \quad | \dots \end{array} \\ \hline \end{array} \pmod{q}$$

Our Idea

To compute a preimage of y with parties $1, \dots, t$

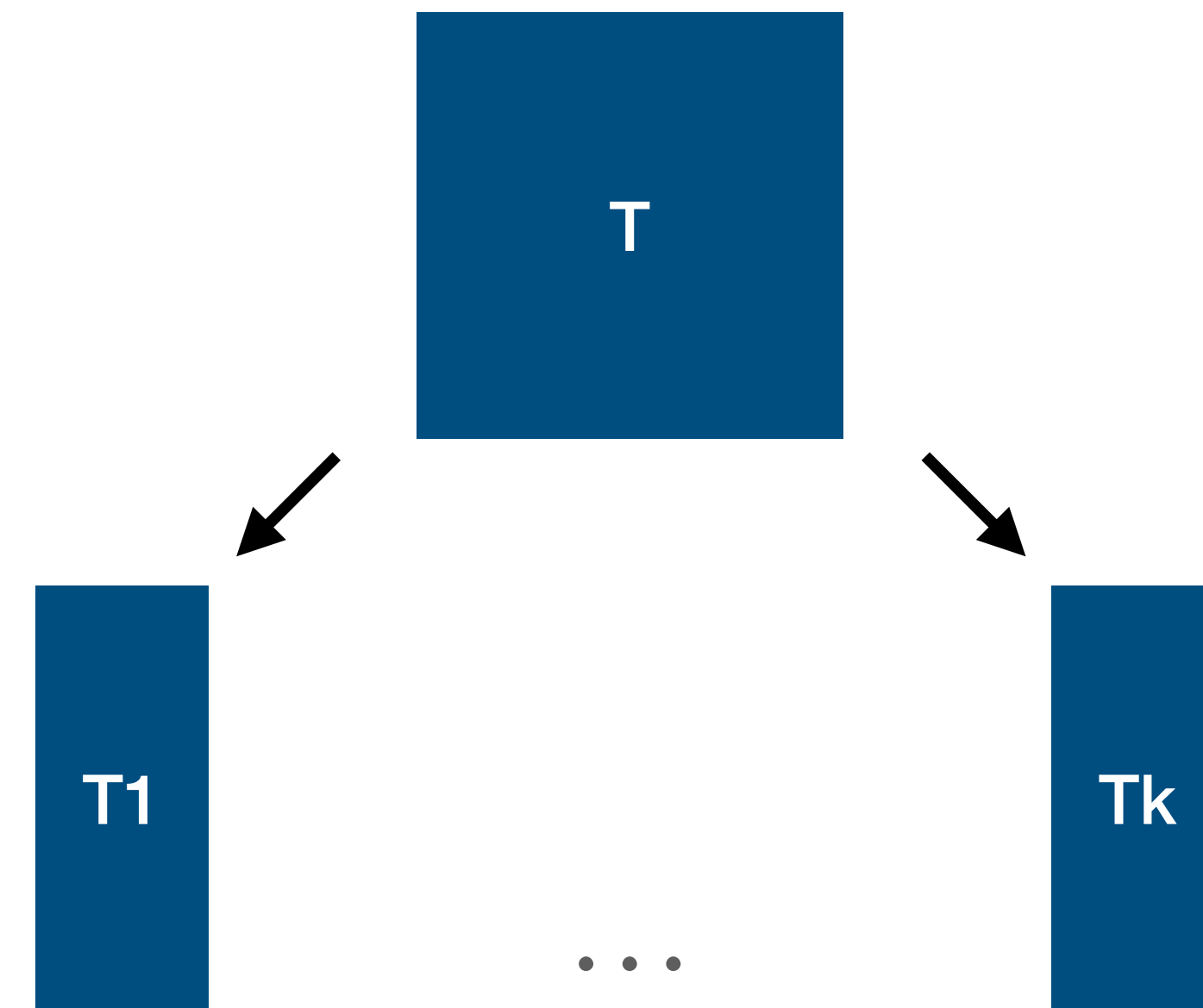
1. Set $V = (\mathbf{v}_1 \mid \dots \mid \mathbf{v}_t)$.
2. Compute $\mathbf{z} = V^{-1}y$ then we have: $V\mathbf{z} = y$.
3. Party i computes $\mathbf{x}_i : A\mathbf{x}_i = z_i\mathbf{v}_i$
4. The signature is the sum:

$$A\Sigma\mathbf{x}_i = \Sigma z_i\mathbf{v}_i = V\mathbf{z} = y$$

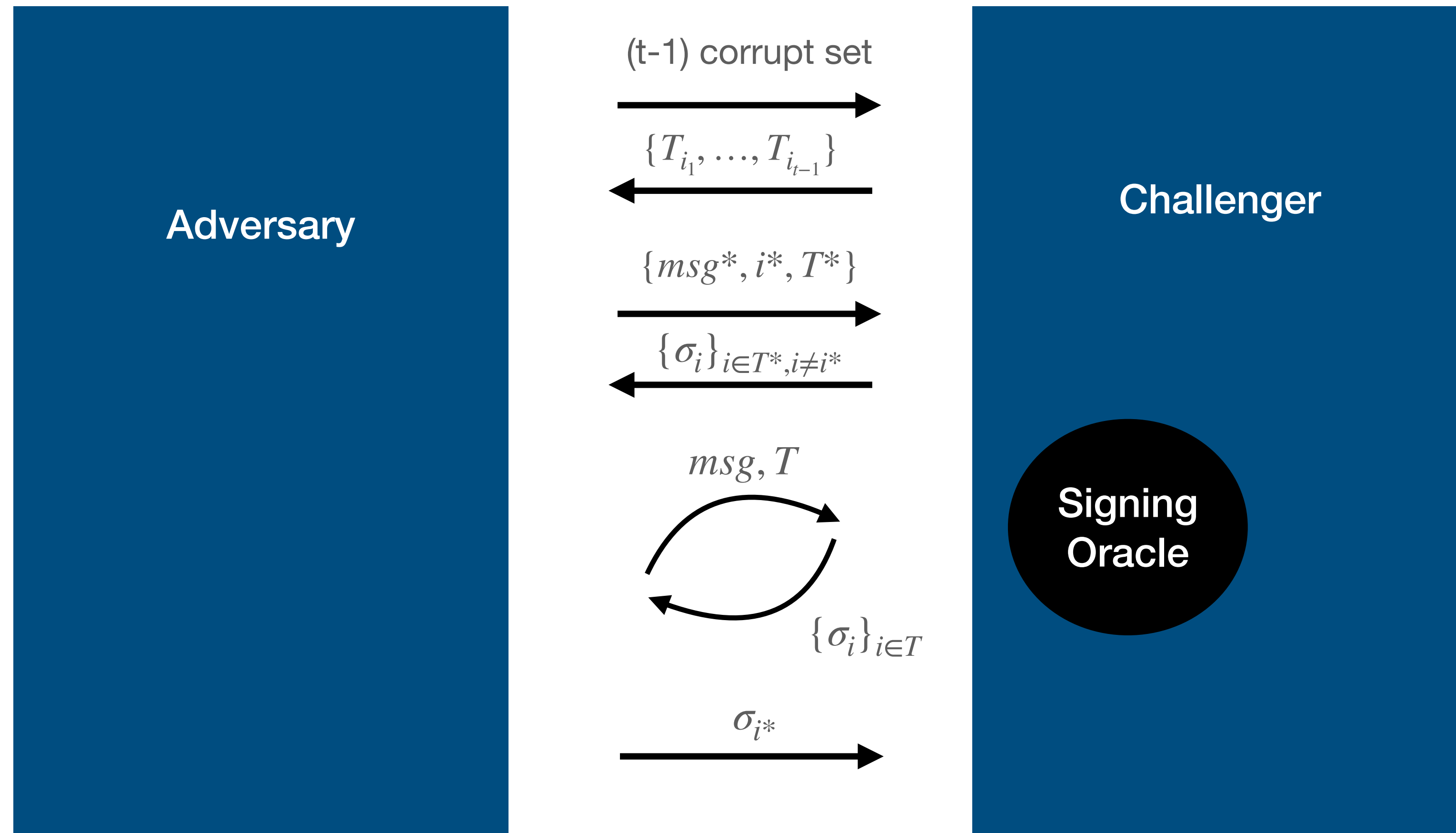

$$A \cdot T1 = \begin{bmatrix} | & | & \dots \\ \mathbf{v}_1 & 2\mathbf{v}_1 & \dots \\ | & | & \dots \end{bmatrix} \pmod{q}$$

Challenges

Partial Trapdoor Definitions
New Signature Distributions
Distributions of Lattices



Selective Security



k-SIS Assumption

Given:

$$\begin{array}{c} n \\ \mathbf{A} \end{array} \begin{array}{c} mt \\ \mathbf{T} \end{array} \begin{array}{c} m(t-1) \end{array} = \begin{array}{c} 0 \quad \dots \quad 0 \\ 0 \quad \ddots \quad 0 \end{array} \pmod{q}$$

Find: short $\mathbf{x} \in \mathcal{R}^{mt}$ such that

- $\mathbf{A} \cdot \mathbf{x} = \mathbf{0} \pmod{q}$
- $\mathbf{x}$ not in field span of T .

Reduces to $(n \times m)$ MSIS.

GPV08

The key pair: $(pk, sk) = (\mathbf{A}, \mathbf{T}_A)$

To sign msg :

- **Compute** $\mathbf{y} := H(msg)$
- **Using $\mathbf{T}_A$ sample small $\mathbf{x}$:** $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \pmod{q}$
- **Return $\mathbf{x}$.**

To verify: Check $\mathbf{A} \cdot \mathbf{x} = H(msg) \pmod{q}$

GPV08

Signature distribution:

$$\mathbf{x} \leftarrow \mathcal{D}_{\Lambda_q^y(\mathbf{A}), \sigma}$$

The key pair: $(pk, sk) = (\mathbf{A}, \mathbf{T}_A)$

To sign msg :

- **Compute** $\mathbf{y} := H(msg)$
- **Using $\mathbf{T}_A$ sample small $\mathbf{x}$:** $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \pmod{q}$
- **Return $\mathbf{x}$.**

To verify: Check $\mathbf{A} \cdot \mathbf{x} = H(msg) \pmod{q}$

Simulating oracles

On hash query msg :

- Sample random small element $\mathbf{x} \leftarrow \mathcal{D}_{\mathcal{R}^m, \sigma}$
- Compute $\mathbf{y} := \mathbf{A} \cdot \mathbf{x} \pmod{q}$
- Program RO $H(msg) := \mathbf{y}$

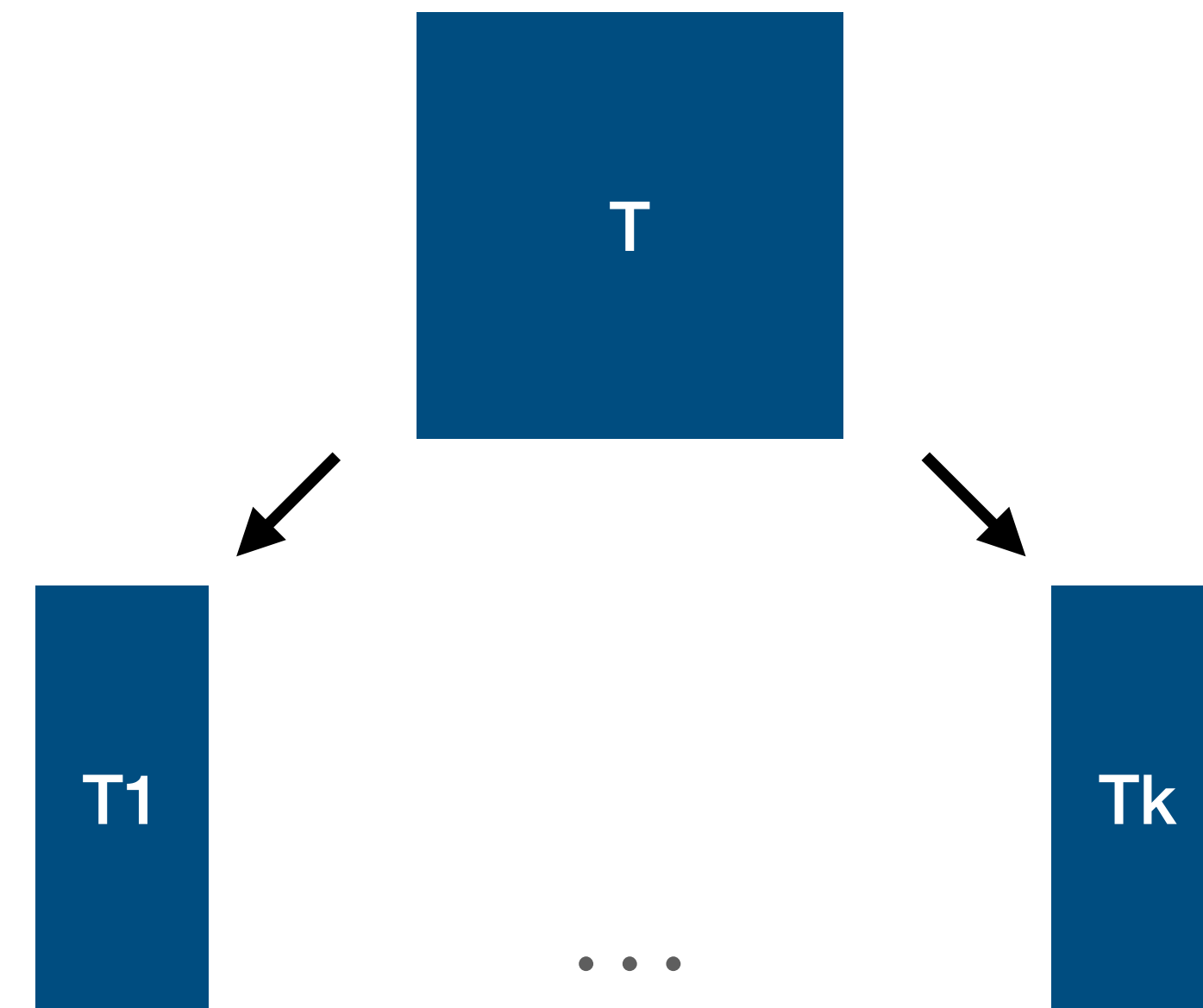
On signature query msg :

- Return $\mathbf{x}$

Partial Trapdoor Distributions

$$\mathbf{T}_i \leftarrow PTrapGen(\mathbf{A}, \mathbf{T}_A, \sigma)$$

$$\mathbf{x}_i \leftarrow \mathcal{D}_{\Lambda(\mathbf{T}_i) \cap \Lambda_q^{\mathbf{v}_i \otimes \mathbf{y}}(\mathbf{A}), \sigma'}$$



The Corrupt Trapdoors

Given a k-SIS instance: $\tilde{\mathbf{A}}_0 \cdot \mathbf{T} = \mathbf{0} \pmod{q}$

Compute $\tilde{\mathbf{A}}_{\neq 0}$ s.t.

$$\begin{array}{c} n \\ \hline \tilde{\mathbf{A}}_0 \\ \hline n(t-1) \end{array} \begin{array}{c} mt \\ \tilde{\mathbf{A}}_{\neq 0} \end{array} \begin{array}{c} m(t-1) \\ \mathbf{T} \end{array} = \begin{array}{c} \begin{array}{ccc} 0 & & 0 \\ 0 & \ddots & 0 \end{array} \\ \hline \begin{array}{ccc} G & & 0 \\ 0 & \ddots & G \end{array} \end{array} \pmod{q}$$

The Corrupt Trapdoors

Then set $\mathbf{A} = (\mathbf{V}' \otimes \mathbf{I}_n) \cdot \tilde{\mathbf{A}}$ for $\mathbf{V}' = \begin{bmatrix} | & | & & | \\ \mathbf{v}_0 & \mathbf{v}_1 & \cdots & \mathbf{v}_{t-1} \\ | & | & & | \end{bmatrix}$ a $(t \times t)$ matrix.

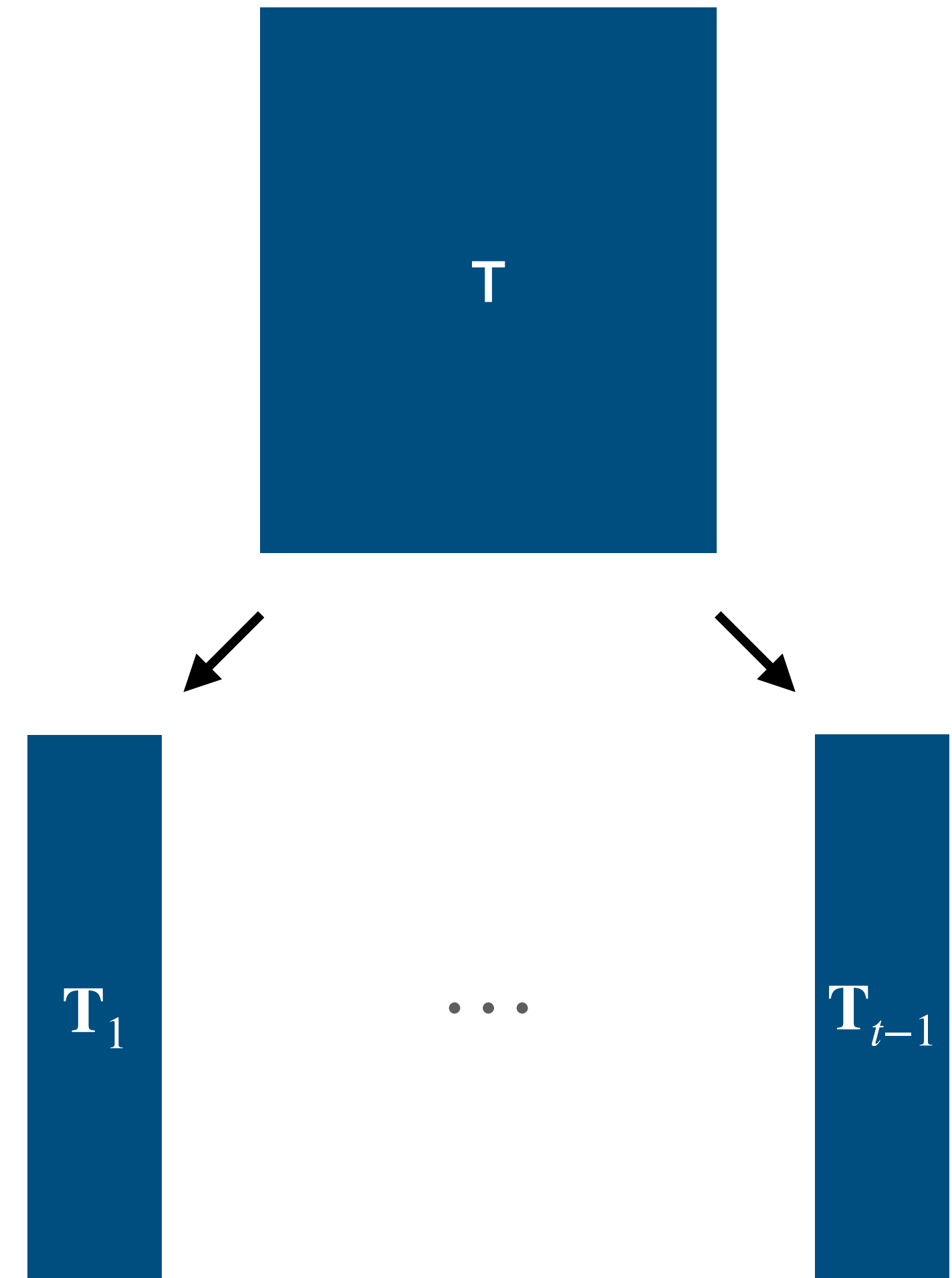
Since

$$\begin{bmatrix} | & | & & | \\ \mathbf{v}_0 \otimes \mathbf{I}_n & \mathbf{v}_1 \otimes \mathbf{I}_n & \cdots & \mathbf{v}_{t-1} \otimes \mathbf{I}_n \\ | & | & & | \end{bmatrix} \otimes \begin{bmatrix} 0 & & 0 \\ & \ddots & \\ 0 & & 0 \\ \hline \mathbf{G} & & 0 \\ & \ddots & \\ 0 & & \mathbf{G} \end{bmatrix} = \begin{bmatrix} & & & \\ \mathbf{v}_1 \otimes \mathbf{G} & & & 0 \\ & \ddots & & \\ 0 & & \mathbf{v}_{t-1} \otimes \mathbf{G} & \end{bmatrix} \pmod{q}$$

The Corrupt Trapdoors

$$\mathbf{A} \cdot \mathbf{T} = \begin{bmatrix} \mathbf{v}_1 \otimes \mathbf{G} & & 0 \\ & \ddots & \\ 0 & & \mathbf{v}_{t-1} \otimes \mathbf{G} \end{bmatrix} \pmod{q}$$

And $\mathbf{A} \cdot \mathbf{T}_i = \mathbf{v}_i \otimes \mathbf{G} \pmod{q}$



Signing Oracle

Idea: Use $\mathbf{T}$ again to get preimages of other $\mathbf{v}_i \otimes \mathbf{y}$.

$$\mathbf{B}_i = \begin{array}{c|c} v_{i,0}^{-1} \mathbf{A}_0 & -\mathbf{G} \\ v_{i,1}^{-1} \mathbf{A}_1 & -\mathbf{G} \\ \vdots & \vdots \\ v_{i,t-1}^{-1} \mathbf{A}_{t-1} & -\mathbf{G} \end{array}$$

Signing Oracle

Idea: Use $\mathbf{T}$ again to get preimages of other $\mathbf{v}_i \otimes \mathbf{y}$.

$$\mathbf{B}_i = \left[\begin{array}{c|c} v_{i,0}^{-1} \mathbf{A}_0 & -\mathbf{G} \\ v_{i,1}^{-1} \mathbf{A}_1 & -\mathbf{G} \\ \vdots & \vdots \\ v_{i,t-1}^{-1} \mathbf{A}_{t-1} & -\mathbf{G} \end{array} \right]$$

Remember:

$$\left(\begin{bmatrix} v_{i,0}^{-1} & & 0 \\ & \ddots & \\ 0 & & v_{i,t-1}^{-1} \end{bmatrix} \otimes \mathbf{I}_n \right) \cdot (\mathbf{V}' \otimes \mathbf{I}_n) \cdot \tilde{\mathbf{A}}$$

Signing Oracle

Idea: Use $\mathbf{T}$ again to get preimages of other $\mathbf{v}_i \otimes \mathbf{y}$.

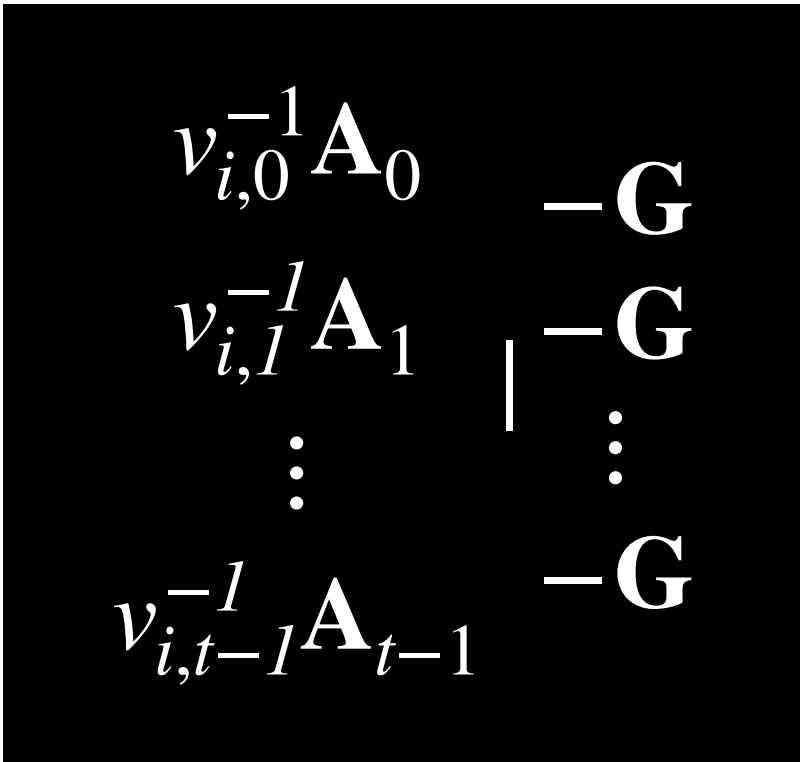
$$\mathbf{B}_i = \left[\begin{array}{c|c} v_{i,0}^{-1} \mathbf{A}_0 & -\mathbf{G} \\ v_{i,1}^{-1} \mathbf{A}_1 & -\mathbf{G} \\ \vdots & \vdots \\ v_{i,t-1}^{-1} \mathbf{A}_{t-1} & -\mathbf{G} \end{array} \right]$$

Remember:

$$\left(\begin{bmatrix} v_{i,0}^{-1} & & 0 \\ & \ddots & \\ 0 & & v_{i,t-1}^{-1} \end{bmatrix} \otimes \mathbf{I}_n \right) \cdot (\mathbf{V}' \otimes \mathbf{I}_n) \cdot \tilde{\mathbf{A}} := \mathbf{H}_i \cdot \tilde{\mathbf{A}}$$

Signing Oracle

Idea: Use $\mathbf{T}$ again to get preimages of other $v_i \otimes y$.

$\mathbf{B}_i =$ 

Remember:

$$\begin{pmatrix} v_{i,0}^{-1} & 0 \\ & \ddots \\ 0 & v_{i,t-1}^{-1} \end{pmatrix} \otimes \mathbf{I}_n \cdot (\mathbf{V}' \otimes \mathbf{I}_n) \cdot \tilde{\mathbf{A}} := \mathbf{H}_i \cdot \tilde{\mathbf{A}}$$

and $\tilde{\mathbf{A}} \cdot \mathbf{T} = \begin{pmatrix} \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{G} & \dots & \mathbf{0} \\ 0 & \dots & \mathbf{G} \end{pmatrix} \pmod{q}$

Signing Oracle

Then

$$\begin{bmatrix} v_{i,0}^{-1} \mathbf{A}_0 & -\mathbf{G} \\ v_{i,1}^{-1} \mathbf{A}_1 & -\mathbf{G} \\ \vdots & \vdots \\ v_{i,t-1}^{-1} \mathbf{A}_{t-1} & -\mathbf{G} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{0}_{mt \times m} & \mathbf{T} \\ -\mathbf{I}_m & \mathbf{0}_{m \times m(t-1)} \end{bmatrix} = \begin{bmatrix} \mathbf{G} \\ \vdots \\ \mathbf{G} \end{bmatrix} | \mathbf{H}_i \cdot \begin{pmatrix} \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{G} & \dots & \mathbf{0} \\ & \ddots & \\ 0 & \dots & \mathbf{G} \end{pmatrix}$$

Signing Oracle

Then

$$\begin{array}{c|c} v_{i,0}^{-1} \mathbf{A}_0 & -\mathbf{G} \\ v_{i,l}^{-1} \mathbf{A}_1 & -\mathbf{G} \\ \vdots & \vdots \\ v_{i,t-1}^{-1} \mathbf{A}_{t-1} & -\mathbf{G} \end{array} \cdot \begin{array}{c|c} \mathbf{0}_{mt \times m} & \mathbf{T} \\ -\mathbf{I}_m & \mathbf{0}_{m \times m(t-1)} \end{array} = \begin{array}{c|c} \mathbf{G} & \begin{pmatrix} \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{G} & \ddots & \mathbf{0} \\ \mathbf{0} & \dots & \mathbf{G} \end{pmatrix} \\ \vdots & \vdots \\ \mathbf{G} & \mathbf{H}_i \end{array} = \begin{array}{c|c} \mathbf{I}_m & \mathbf{G} & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{I}_m & \mathbf{0} & \dots & \mathbf{G} \end{array} \cdot \begin{array}{c|c} \mathbf{I}_m & \mathbf{H}_i \end{array}$$

Signing Oracle

Sample $\mathbf{U}_i, \mathbf{W}_i$ such that

$$\left[\begin{array}{c|c} v_{i,0}^{-1} \mathbf{A}_0 & -\mathbf{G} \\ v_{i,1}^{-1} \mathbf{A}_1 & -\mathbf{G} \\ \vdots & \vdots \\ v_{i,t-1}^{-1} \mathbf{A}_{t-1} & -\mathbf{G} \end{array} \right] \begin{bmatrix} \mathbf{U}_i \\ \mathbf{W}_i \end{bmatrix} = \mathbf{0} \pmod{q}$$

Then for each $j = 0, \dots, t - 1$ we have $\mathbf{A}_j \cdot \mathbf{U}_i = v_{i,j} \cdot \mathbf{G} \cdot \mathbf{W}_i \pmod{q}$

Signing Oracle

Sample $\mathbf{U}_i, \mathbf{W}_i$ such that

$$\begin{bmatrix} v_{i,0}^{-1} \mathbf{A}_0 & -\mathbf{G} \\ v_{i,1}^{-1} \mathbf{A}_1 & -\mathbf{G} \\ \vdots & \vdots \\ v_{i,t-1}^{-1} \mathbf{A}_{t-1} & -\mathbf{G} \end{bmatrix} \begin{bmatrix} \mathbf{U}_i \\ \mathbf{W}_i \end{bmatrix} = \mathbf{0} \pmod{q}$$

Then for each $j = 0, \dots, t - 1$ we have $\mathbf{A}_j \cdot \mathbf{U}_i = v_{i,j} \cdot \mathbf{G} \cdot \mathbf{W}_i \pmod{q}$

So $\mathbf{A} \cdot \mathbf{U}_i = \mathbf{v}_i \otimes \mathbf{G} \cdot \mathbf{W}_i \pmod{q}$

Signing Oracle

Sample $\mathbf{U}_i, \mathbf{W}_i$ such that

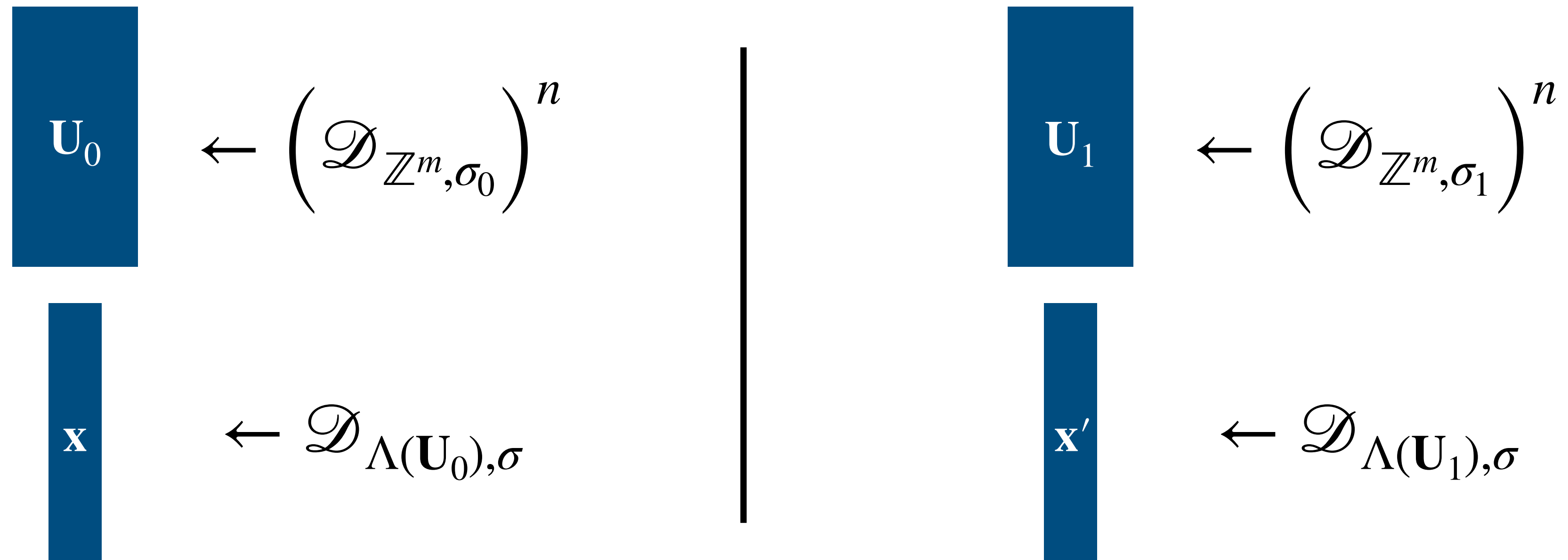
$$\begin{bmatrix} v_{i,0}^{-1} \mathbf{A}_0 & -\mathbf{G} \\ v_{i,1}^{-1} \mathbf{A}_1 & -\mathbf{G} \\ \vdots & \vdots \\ v_{i,t-1}^{-1} \mathbf{A}_{t-1} & -\mathbf{G} \end{bmatrix} \begin{bmatrix} \mathbf{U}_i \\ \mathbf{W}_i \end{bmatrix} = \mathbf{0} \pmod{q}$$

Then for each $j = 0, \dots, t - 1$ we have $\mathbf{A}_j \cdot \mathbf{U}_i = v_{i,j} \cdot \mathbf{G} \cdot \mathbf{W}_i \pmod{q}$

So $\mathbf{A} \cdot \mathbf{U}_i = \mathbf{v}_i \otimes \mathbf{G} \cdot \mathbf{W}_i = \mathbf{v}_i \otimes \mathbf{R}_i \pmod{q}$

The Distribution Conjecture

Let $m > n$, and $\sigma/m > \sigma_1 > \sigma_0$.



Then $x \approx x'$.

Open directions

Conjecture

Stronger Security

Set of Collaborators

Anonymity



Other projects



Image by rawpixel.com on Freepik

Thank you!