

# Lova: Lattice-Based Folding Scheme from Unstructured Lattices

**Duc Tu Pham**

**Joint work with Giacomo Fenzi, Christian Knabenhans, and Ngoc Khanh Nguyen**

**[eprint.iacr.org/2024/1964](https://eprint.iacr.org/2024/1964)**

THX for the slides

**EPFL**



**KING'S**  
*College*  
**LONDON**

# Folding Scheme

# Incrementally Verifiable Computation [Val08]



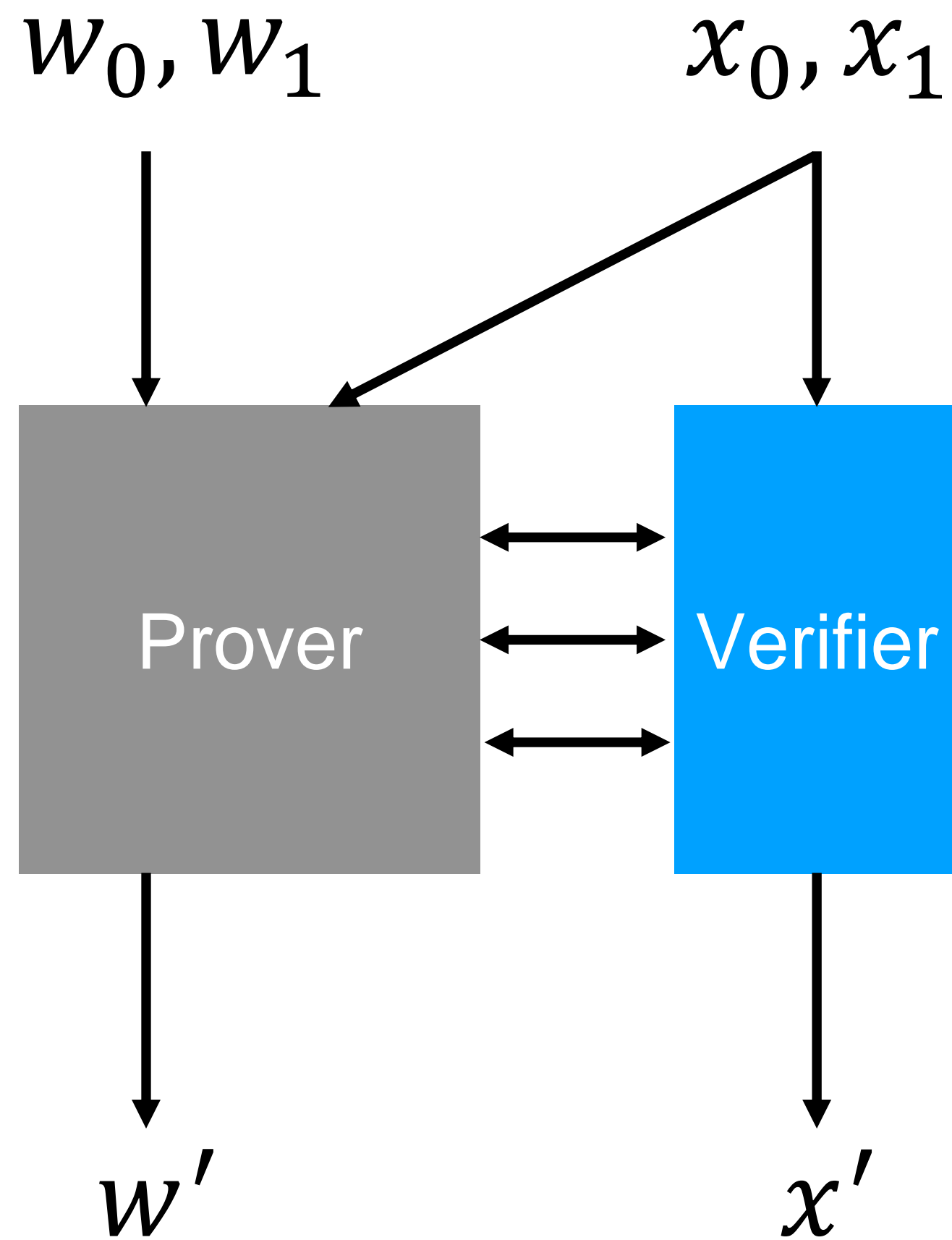
# Incrementally Verifiable Computation [Val08]



## Applications:

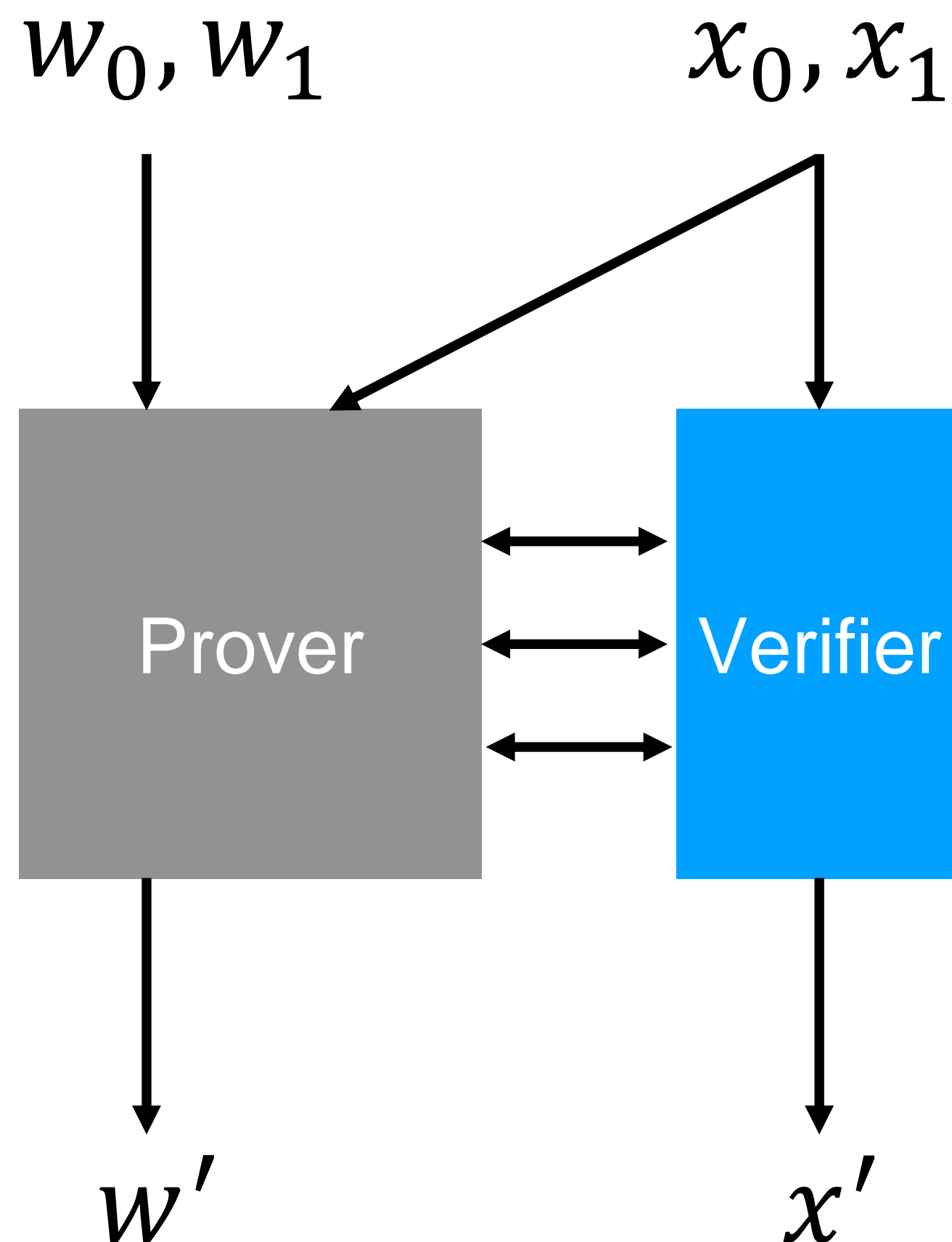
- Verifiable Delay Functions
- ZK-Virtual Machine
- zkRollups

# Folding scheme [KST22]



# Folding scheme [KST22]

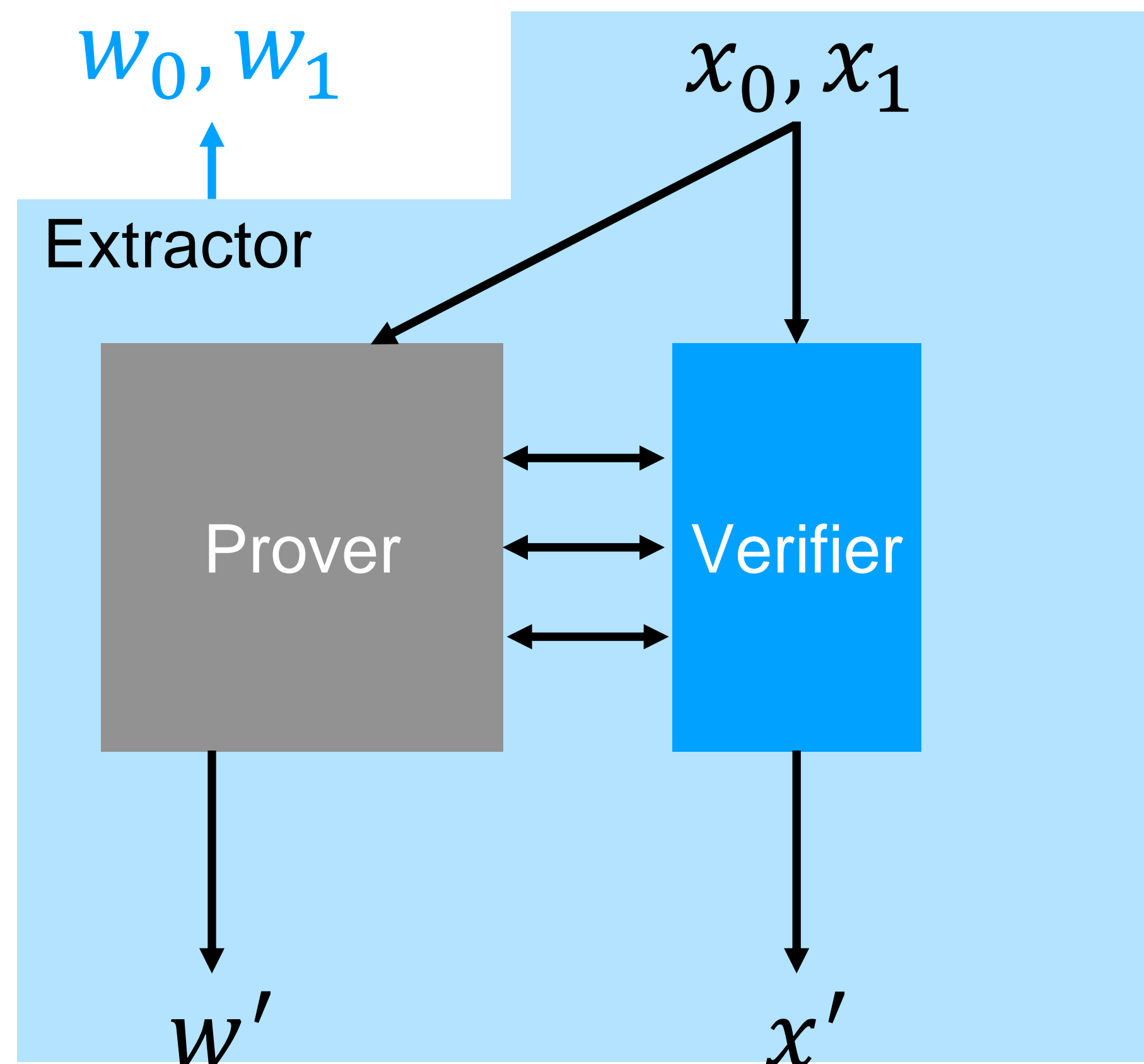
## Completeness



W.h.p.,  
 $(x_0, w_0) \in R$  and  $(x_1, w_1) \in R$   
 $\implies (x', w') \in R$

# Folding scheme [KST22]

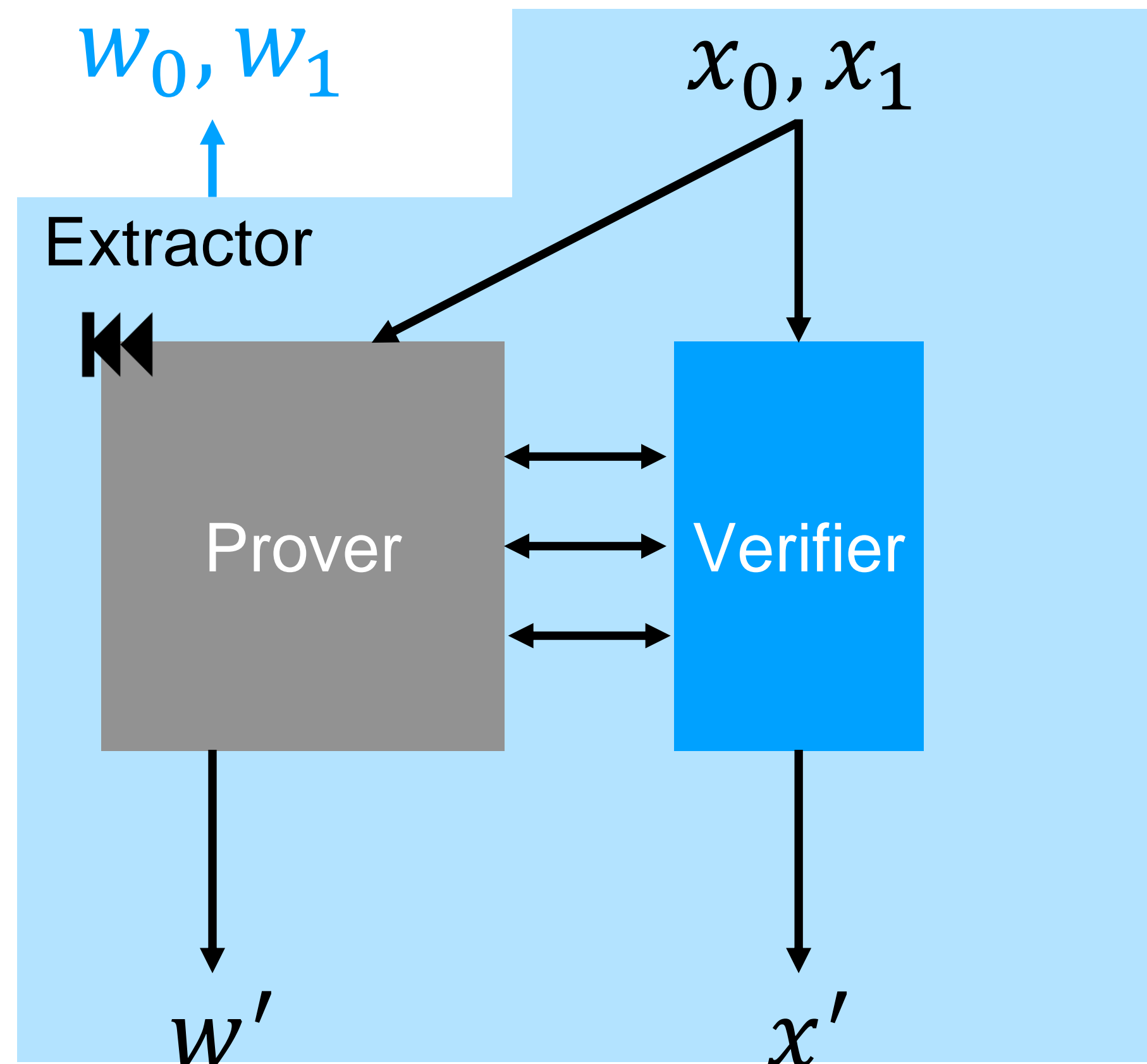
## Knowledge Soundness



W.h.p.,  
 $(x', w') \in R \implies$  The prover must have known valid  $w_0, w_1$  for  $x_0, x_1$

# Folding scheme [KST22]

## Knowledge Soundness

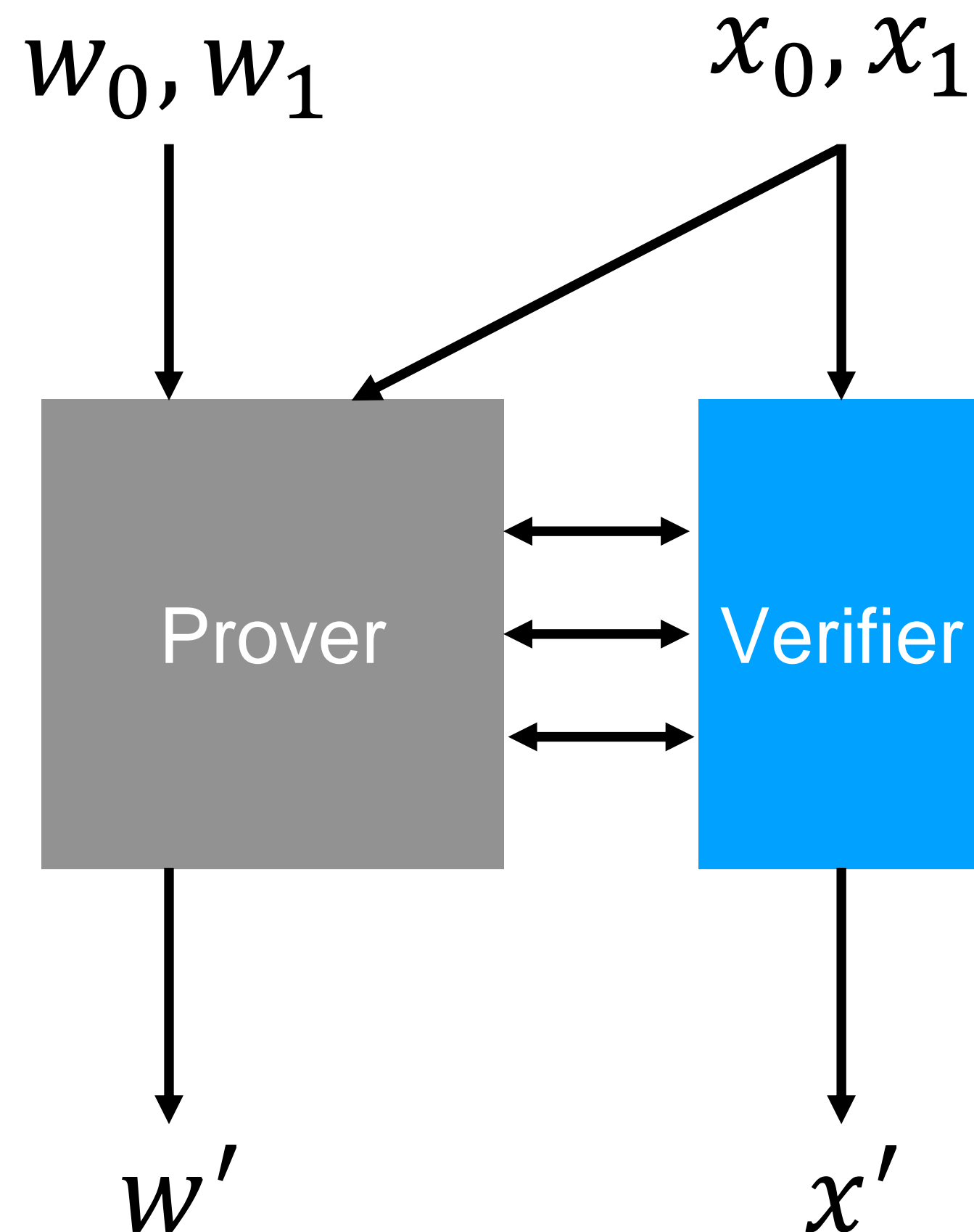


W.h.p.,  
 $(x', w') \in R \implies$  The prover must  
have known valid  
 $w_0, w_1$  for  $x_0, x_1$



# Folding scheme [KST22]

## Succinctness



Verifier:  $o(|w_0|, |w_1|)$

# Nova folding scheme [KST22]

- First folding scheme for a *Committed Relaxed R1CS* under DL assumption
- The construction only needs a **compressing, additively homomorphic commitment scheme** (e.g., Pedersen commitment)
- Generic way to obtain IVC from folding schemes in ROM

Lova  - Nova from lattices

# Our contribution

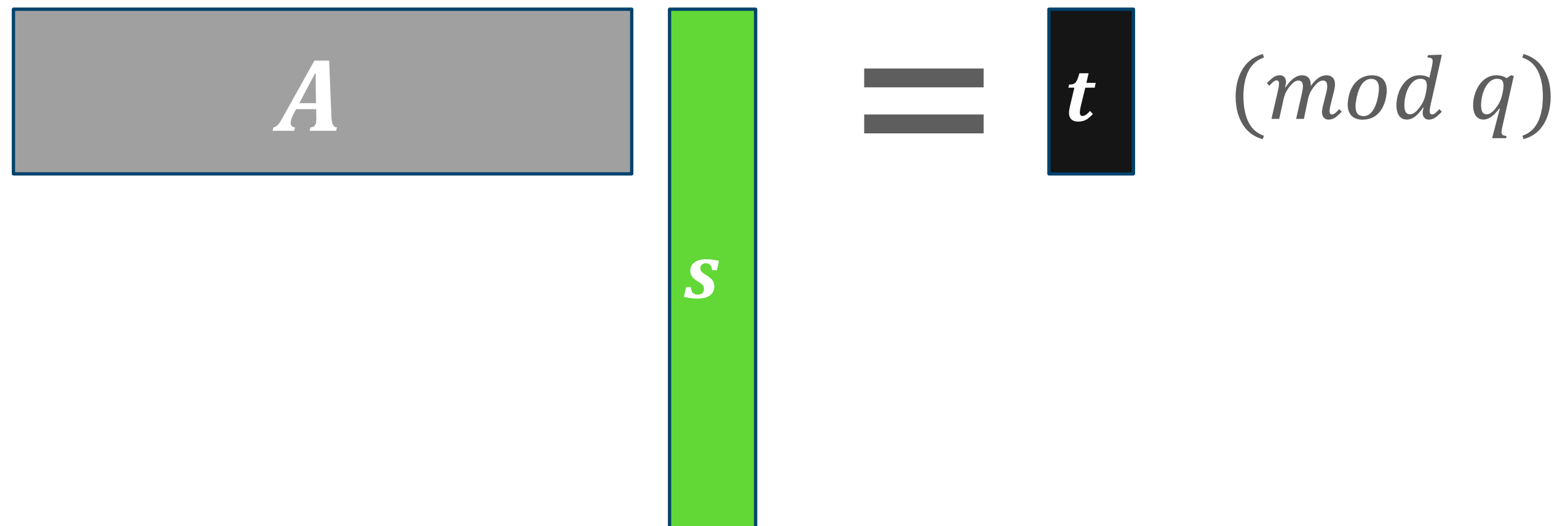
- First lattice-based folding scheme
- Based on the (**unstructured**) SIS assumption
- **Exact** Euclidean norm proof

# Ajtai commitment [Ajt96]

- Let  $\mathbb{Z}_q$  be a ring of integers modulo  $q$ .
- To commit to a **short** message vector  $s$ , we compute:

# Ajtai commitment [Ajt96]

- Let  $\mathbb{Z}_q$  be a ring of integers modulo  $q$ .
- To commit to a **short** message vector  $s$ , we compute:


$$A \cdot s = t \pmod{q}$$

# Ajtai commitment [Ajt96]

- Let  $\mathbb{Z}_q$  be a ring of integers modulo  $q$ .
- To commit to a **short** message vector  $s$ , we compute:

The diagram illustrates the commitment process. On the left, a gray rectangular box labeled  $A$  is positioned above a vertical green bar labeled  $s$ . To the right of  $s$  is an equals sign, followed by a black rectangular box labeled  $t$ . To the right of  $t$  is the text  $(\text{mod } q)$ . A blue arrow points from the word "commitment" on the far right to the  $t$  box.

$$A \cdot s = t \pmod{q}$$

commitment

# Ajtai commitment [Ajt96]

- Let  $\mathbb{Z}_q$  be a ring of integers modulo  $q$ .
- To commit to a **short** message vector  $s$ , we compute:

$$A \cdot s = t \pmod{q}$$

commitment

Binding holds under the Shortest Integer Solution (SIS) problem:

Given a random matrix  $A$ , find a short non-zero vector  $s$  s.t.

$$As = \mathbf{0} \pmod{q}$$



# Lova, take 1

# Lova, take 1

$$R = \{(t, s) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Prover  $(t_1, t_2; s_1, s_2)$

Verifier  $(t_1, t_2)$

$$R = \{(t, s) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Prover  $(t_1, t_2; s_1, s_2)$

$$\begin{bmatrix} t_1 \\ t_2 \end{bmatrix} = A \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \pmod{q}$$

Verifier  $(t_1, t_2)$

$$R = \{(t, s) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Prover  $(t_1, t_2; s_1, s_2)$

$$\begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} = \begin{array}{|c|} \hline A \\ \hline \end{array} \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \pmod q$$

Verifier  $(t_1, t_2)$

$$c \leftarrow C \subseteq \mathbb{Z}_q$$

$$R = \{(t, s) \mid t = As \pmod q \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Prover  $(t_1, t_2; s_1, s_2)$

$$\begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} = \begin{array}{|c|} \hline A \\ \hline \end{array} \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \pmod q$$

Verifier  $(t_1, t_2)$

$$c \leftarrow C \subseteq \mathbb{Z}_q$$



$$R = \{(t, s) \mid t = As \pmod q \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Prover  $(t_1, t_2; s_1, s_2)$

$$\begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} = A \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \pmod q$$

Verifier  $(t_1, t_2)$

$$c \leftarrow C \subseteq \mathbb{Z}_q$$



$$s' = \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline c \\ \hline \end{array}$$

$$R = \{(t, s) \mid t = As \pmod q \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Prover  $(t_1, t_2; s_1, s_2)$

$$\begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} = A \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \pmod q$$

Verifier  $(t_1, t_2)$

$$c \leftarrow C \subseteq \mathbb{Z}_q$$



$$s' = \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline c \\ \hline \end{array}$$

$$t' = \begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline c \\ \hline \end{array}$$

$$R = \{(t, s) \mid t = As \pmod q \wedge \|s\| \leq \beta\}$$



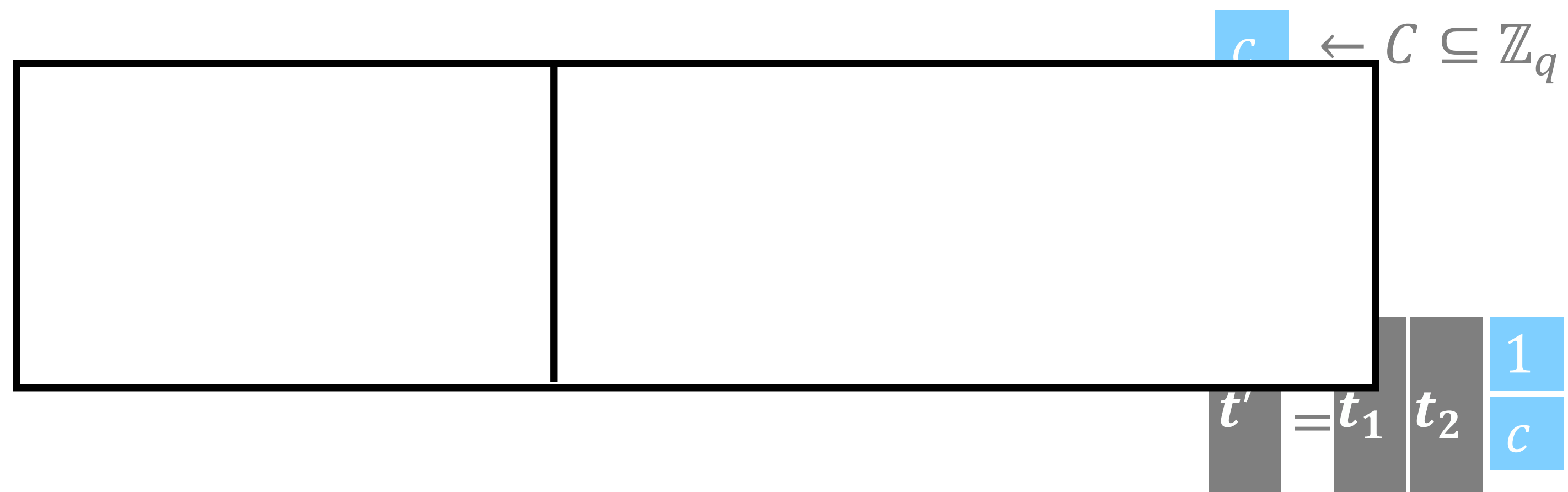
# Lova, take 1

Prover  $(t_1, t_2; s_1, s_2)$

$$\begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} = A \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \pmod q$$

Verifier  $(t_1, t_2)$

$$s' = \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline c \\ \hline \end{array}$$



$$R = \{(t, s) \mid t = As \pmod q \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Prover  $(t_1, t_2; s_1, s_2)$

$$\begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} = A \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \pmod q$$

Verifier  $(t_1, t_2)$

$$s' = \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline c \\ \hline \end{array}$$

$$\begin{aligned} As' &= A(s_1 + cs_2) \\ &= As_1 + cAs_2 \\ &= t_1 + ct_2 \\ &= t' \end{aligned}$$

$$c \leftarrow C \subseteq \mathbb{Z}_q$$

$$t' = \begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline c \\ \hline \end{array}$$

$$R = \{(t, s) \mid t = As \pmod q \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Prover  $(t_1, t_2; s_1, s_2)$

$$\begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} = A \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \pmod q$$

Verifier  $(t_1, t_2)$

$$s' = \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline c \\ \hline \end{array}$$

$$\begin{aligned} As' &= A(s_1 + cs_2) \\ &= As_1 + cAs_2 \\ &= t_1 + ct_2 \\ &= t' \end{aligned}$$

$$\|s'\| \leq \beta \left( \max_{c \in C} |c| + 1 \right) \stackrel{\text{def}}{=} \beta'$$

$c \leftarrow C \subseteq \mathbb{Z}_q$

$$t' = \begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline c \\ \hline \end{array}$$

$$R = \{(t, s) \mid t = As \pmod q \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Knowledge soundness via special soundness:  $c_1 \neq c_2$

$$\begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} = A \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \pmod q$$

$$c \leftarrow C \subseteq \mathbb{Z}_q$$



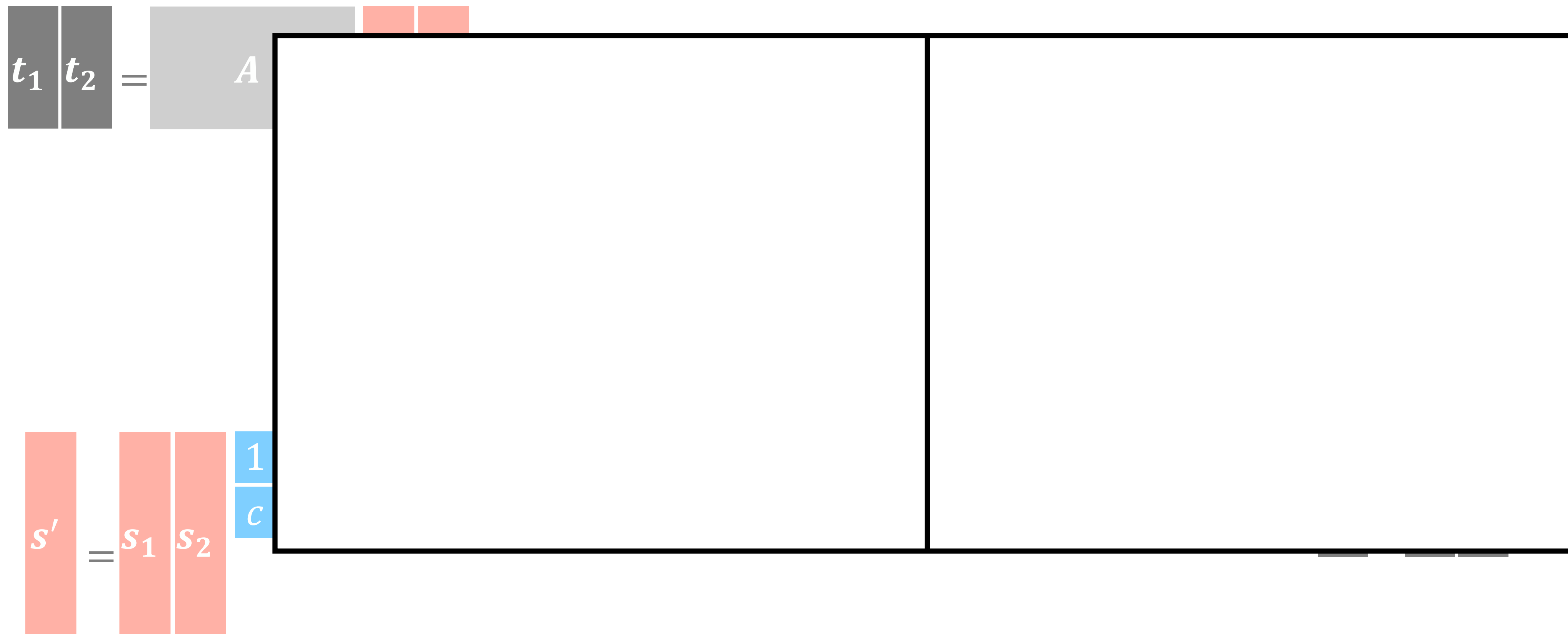
$$s' = \begin{array}{|c|c|} \hline s_1 & s_2 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline c \\ \hline \end{array}$$

$$t' = \begin{array}{|c|c|} \hline t_1 & t_2 \\ \hline \end{array} \begin{array}{|c|} \hline 1 \\ \hline c \\ \hline \end{array}$$

$$R = \{(t, s) \mid t = As \pmod q \wedge \|s\| \leq \beta\}$$

# Lova, take 1

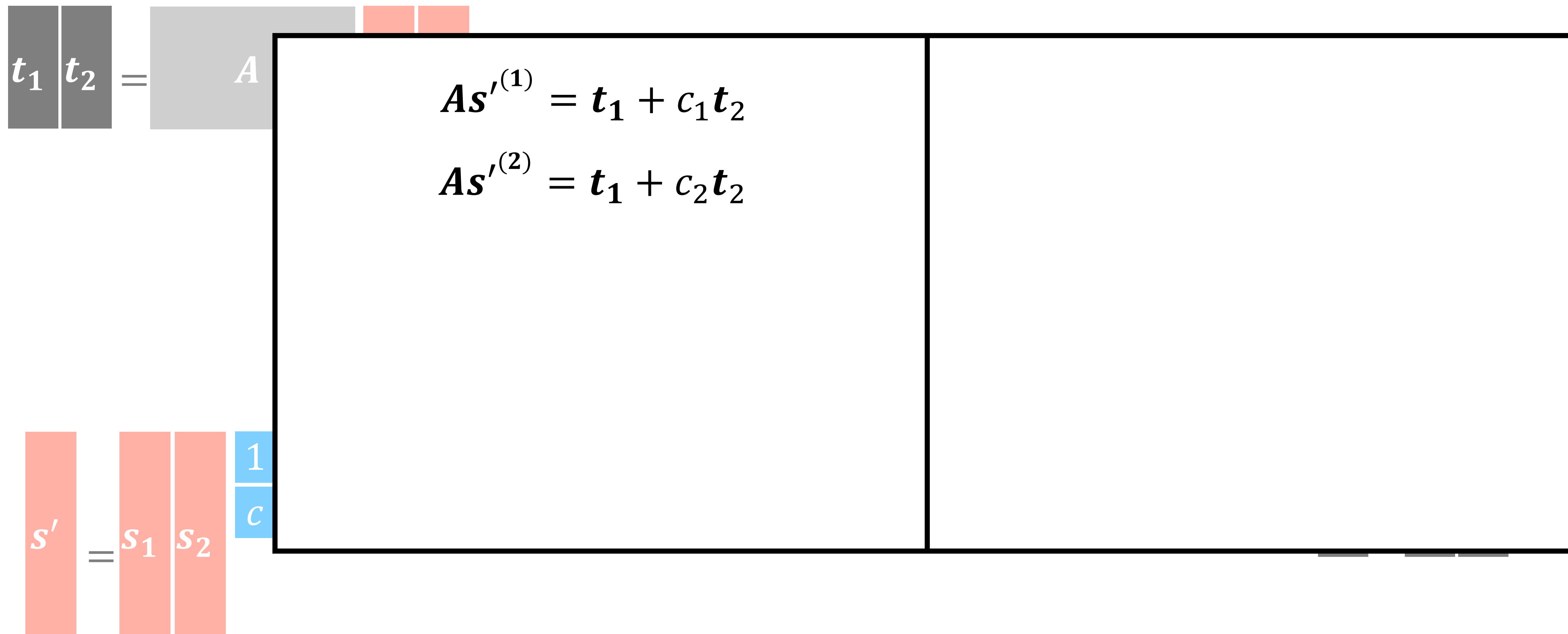
Knowledge soundness via special soundness:  $c_1 \neq c_2$



$$R = \{(t, s) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Knowledge soundness via special soundness:  $c_1 \neq c_2$



$$R = \{(t, s) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Knowledge soundness via special soundness:  $c_1 \neq c_2$

Diagram illustrating the relationship between variables and matrices:

- Top left:  $t_1$  and  $t_2$  are shown as a vector, with an equals sign pointing to a matrix  $A$ .
- Bottom left:  $s'$  is shown as a vector, with an equals sign pointing to a vector composed of  $s_1$  and  $s_2$ , followed by a blue box containing the vector  $\begin{bmatrix} 1 \\ c \end{bmatrix}$ .
- Central box (left side):
 
$$As'^{(1)} = t_1 + c_1 t_2$$

$$As'^{(2)} = t_1 + c_2 t_2$$

$$A \begin{pmatrix} s'^{(1)} - s'^{(2)} \\ c_1 - c_2 \end{pmatrix} = t_2$$

$$A \begin{pmatrix} c_2 s'^{(1)} - c_1 s'^{(2)} \\ c_2 - c_1 \end{pmatrix} = t_1$$

$$R = \{(t, s) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Knowledge soundness via special soundness:  $c_1 \neq c_2$

Diagram illustrating the derivation of special soundness from knowledge soundness. The diagram shows the relationship between vectors  $t_1$ ,  $t_2$ ,  $s'$ , and matrix  $A$ .

Visual representation of  $t_1$  and  $t_2$  as two grey blocks, and  $A$  as a grey block with two red blocks to its right.

Visual representation of  $s'$  as a single red block, and  $s_1$  and  $s_2$  as two red blocks, with a blue block containing  $\frac{1}{c}$  to the right.

Equations derived from the diagram:

$$As'^{(1)} = t_1 + c_1 t_2$$

$$As'^{(2)} = t_1 + c_2 t_2$$

$$A \begin{pmatrix} \overline{s_2} \frac{s'^{(1)} - s'^{(2)}}{c_1 - c_2} \\ \frac{c_2 s'^{(1)} - c_1 s'^{(2)}}{c_2 - c_1} \end{pmatrix} = t_2$$

$$A \begin{pmatrix} \frac{c_2 s'^{(1)} - c_1 s'^{(2)}}{c_2 - c_1} \\ \frac{1}{c} \end{pmatrix} = t_1$$

$$R = \{(t, s) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$$



# Lova, take 1

Knowledge soundness via special soundness:  $c_1 \neq c_2$

Diagram illustrating the relationship between variables  $t_1$ ,  $t_2$ ,  $s'$ ,  $s_1$ ,  $s_2$ , and matrix  $A$ .

Top left:  $t_1$  and  $t_2$  are shown as a vector, with  $t_2$  highlighted in red. This vector is multiplied by matrix  $A$ .

Bottom left:  $s'$  is shown as a vector, which is equal to the concatenation of  $s_1$  and  $s_2$ .  $s_1$  and  $s_2$  are highlighted in red. This vector is multiplied by a matrix with entries  $1$  and  $c$ .

Right side (enclosed in a box):

$$As'^{(1)} = t_1 + c_1 t_2$$

$$As'^{(2)} = t_1 + c_2 t_2$$

$$A \begin{pmatrix} \overline{s_2}^{(1)} - \overline{s_2}^{(2)} \\ c_1 - c_2 \end{pmatrix} = t_2$$

$$A \begin{pmatrix} \overline{s_1}^{(1)} - \overline{s_1}^{(2)} \\ c_2 - c_1 \end{pmatrix} = t_1$$

$$R = \{(t, s) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Knowledge soundness via special soundness:  $c_1 \neq c_2$

$t_1$

$t_2$

=

$A$

$As'^{(1)} = t_1 + c_1 t_2$

$As'^{(2)} = t_1 + c_2 t_2$

$\overline{s_2}$ 
 $A \left( \frac{s'^{(1)} - s'^{(2)}}{c_1 - c_2} \right) = t_2$

$\overline{s_1}$ 
 $A \left( \frac{c_2 s'^{(1)} - c_1 s'^{(2)}}{c_2 - c_1} \right) = t_1$

$s'$

=

$s_1$

$s_2$

$1$

$c$

Suppose  $C = \{0,1\}$ .  
Then,

$\|\overline{s}_i\| \leq 2 \cdot \beta'$  for  $i = 1,2$

$$R = \{(t, s) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$$

# Lova, take 1

Folding Norm Growth

Soundness error

Extractor Norm Growth

# Lova, take 1

Folding Norm Growth

$$\beta \mapsto \beta' = 2\beta$$

Soundness error

Extractor Norm Growth

# Lova, take 1

Folding Norm Growth

$$\beta \mapsto \beta' = 2\beta$$

Soundness error

$$\frac{1}{2}$$

Extractor Norm Growth

# Lova, take 1

Folding Norm Growth

$$\beta \mapsto \beta' = 2\beta$$

Soundness error

$$\frac{1}{2}$$

Extractor Norm Growth

$$\beta' \mapsto 2\beta'$$

# Lova, take 1

Folding Norm Growth

$$\beta \mapsto \beta' = 2\beta$$

Decompose [BS23]!

Soundness error

$$\frac{1}{2}$$

Extractor Norm Growth

$$\beta' \mapsto 2\beta'$$

**Lova, take 2**  $R = \{(\mathbf{t} \in \mathbb{Z}_q^h, \mathbf{s} \in \mathbb{Z}_q^n) \mid \mathbf{t} = \mathbf{A}\mathbf{s} \pmod{q} \wedge \|\mathbf{s}\| \leq \beta\}$

Prover  $(\mathbf{t}_j; \mathbf{s}_j)$

Verifier  $(\mathbf{t}_1, \mathbf{t}_2)$



**Lova, take 2**  $R = \{(\mathbf{t} \in \mathbb{Z}_q^h, \mathbf{s} \in \mathbb{Z}_q^n) \mid \mathbf{t} = \mathbf{A}\mathbf{s} \pmod{q} \wedge \|\mathbf{s}\| \leq \beta\}$

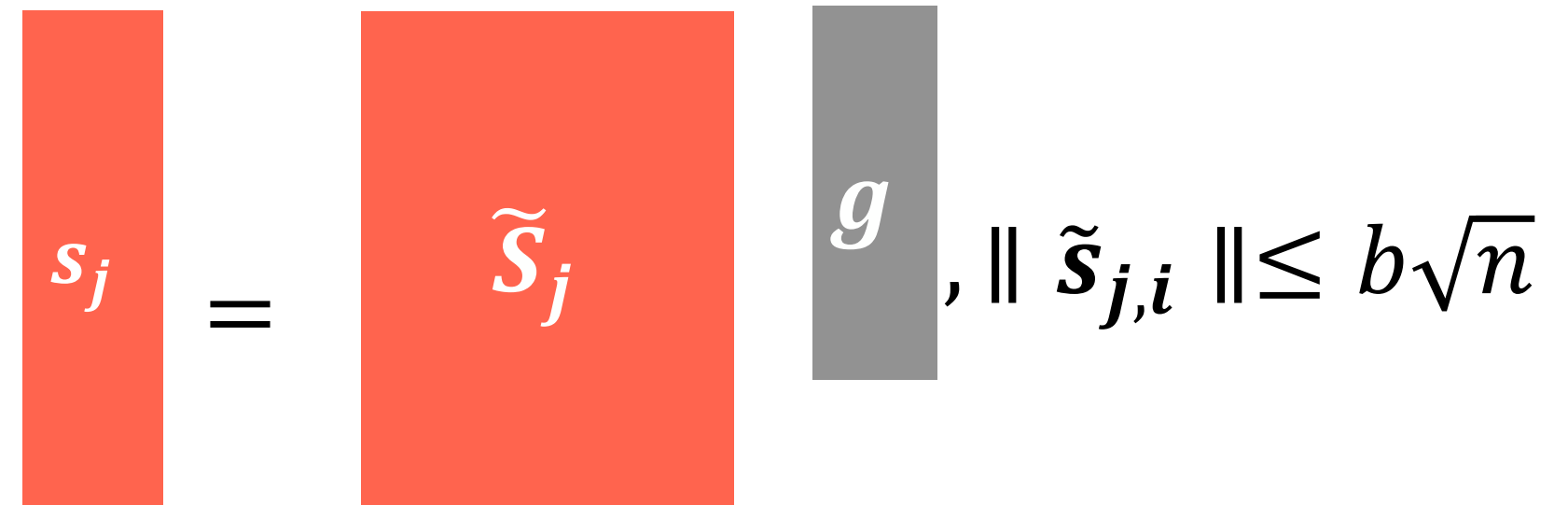
Prover  $(\mathbf{t}_j; \mathbf{s}_j)$

$$\mathbf{s}_j = \sum_{i=0}^k b^i \tilde{\mathbf{s}}_{j,i}, \quad \|\tilde{\mathbf{s}}_{j,i}\| \leq b\sqrt{n}$$

Verifier  $(\mathbf{t}_1, \mathbf{t}_2)$

**Lova, take 2**  $R = \{(\mathbf{t} \in \mathbb{Z}_q^h, \mathbf{s} \in \mathbb{Z}_q^n) \mid \mathbf{t} = \mathbf{A}\mathbf{s} \pmod{q} \wedge \|\mathbf{s}\| \leq \beta\}$

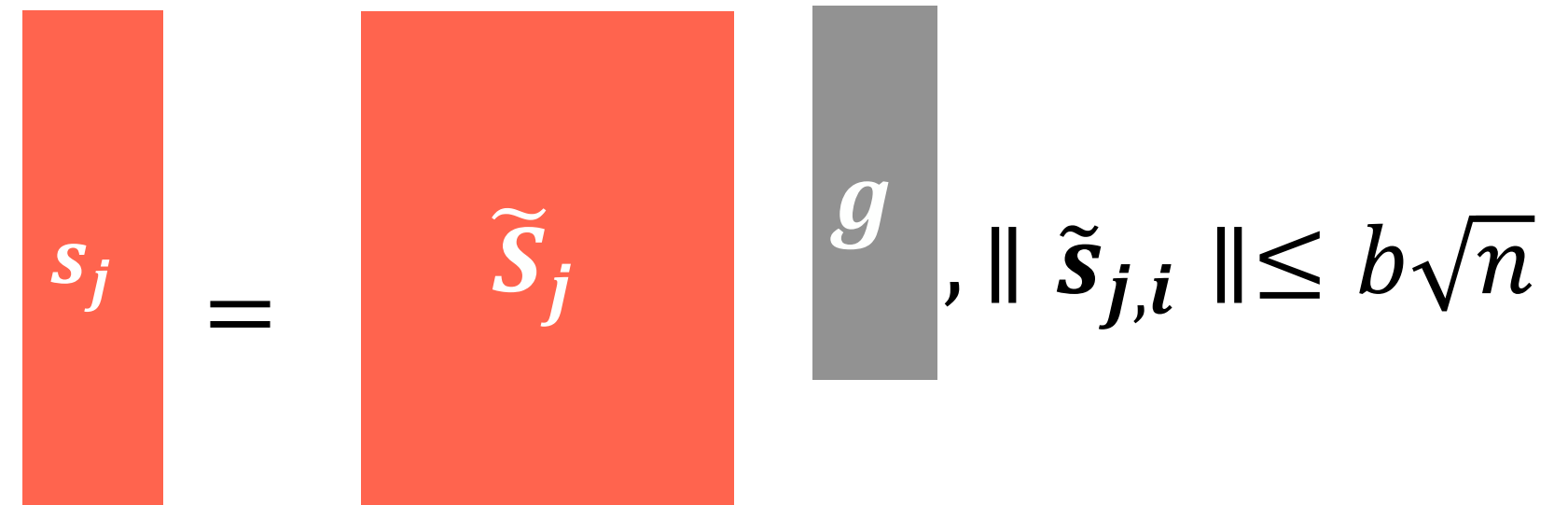
Prover  $(\mathbf{t}_j; \mathbf{s}_j)$



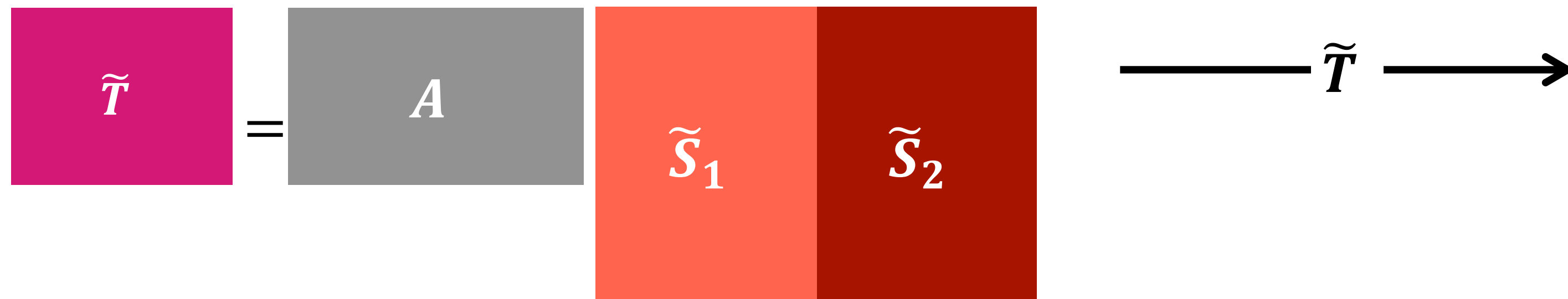
Verifier  $(\mathbf{t}_1, \mathbf{t}_2)$

# Lova, take 2 $R = \{(t \in \mathbb{Z}_q^h, s \in \mathbb{Z}_q^n) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$

Prover  $(t_j; s_j)$

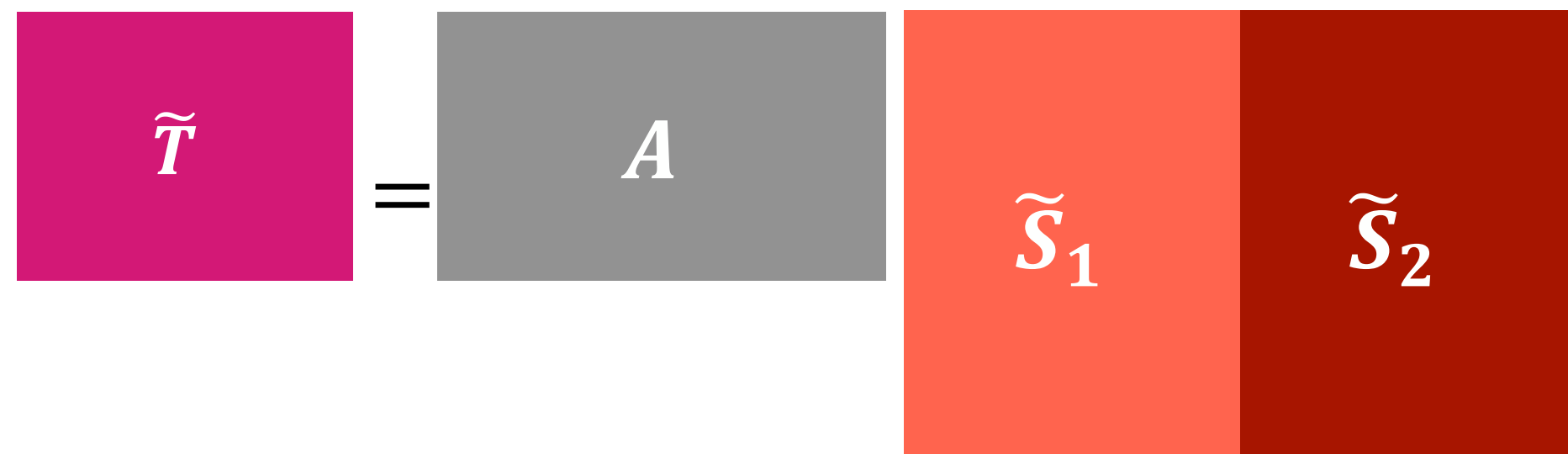
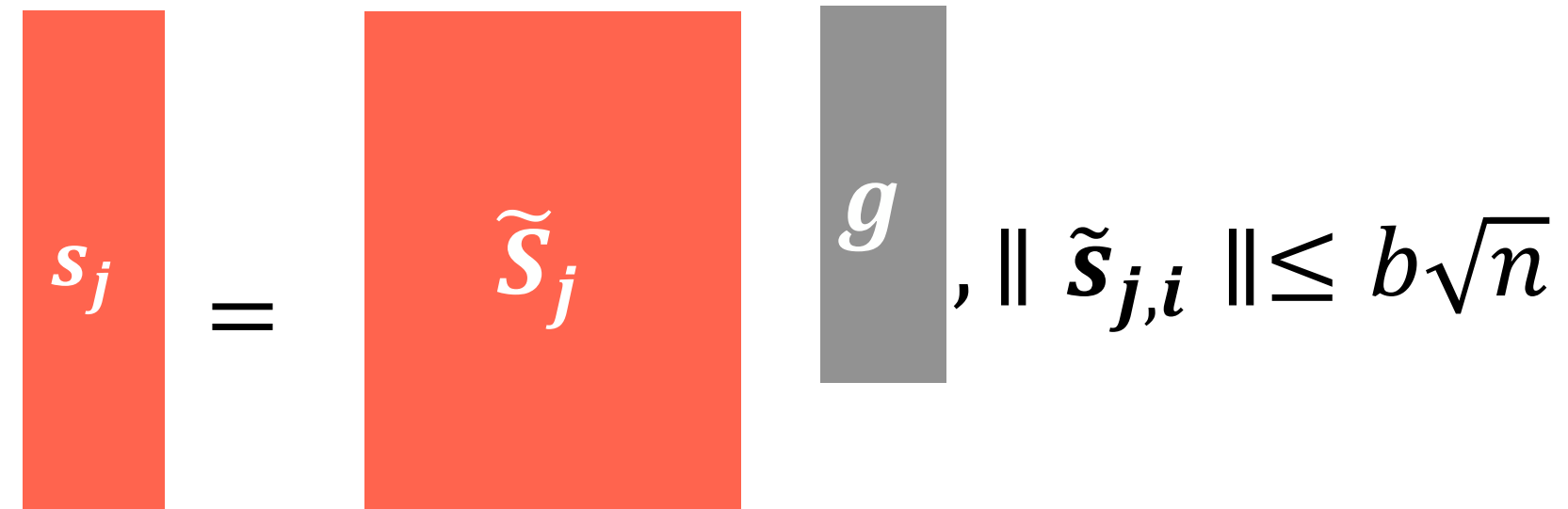


Verifier  $(t_1, t_2)$

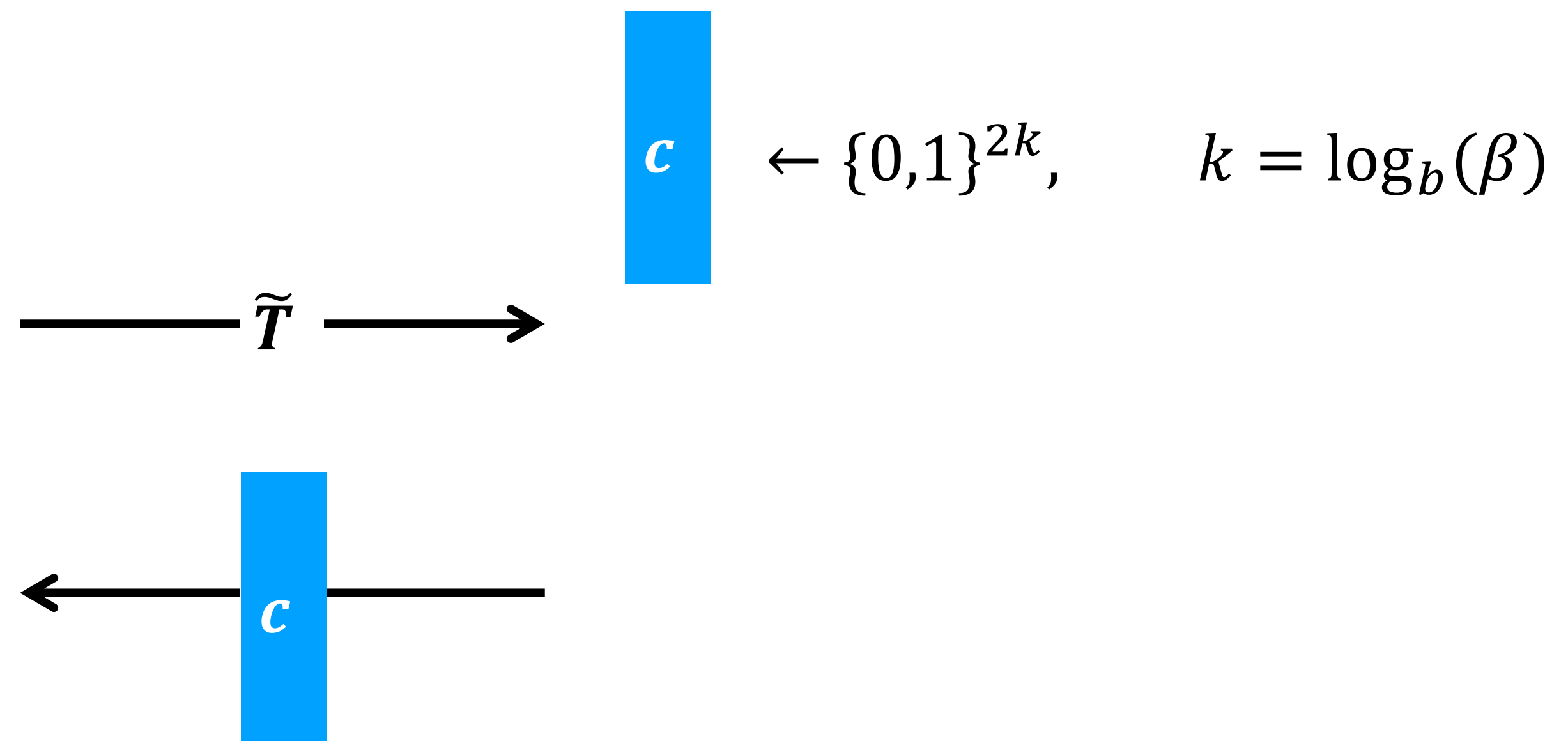


# Lova, take 2 $R = \{(t \in \mathbb{Z}_q^h, s \in \mathbb{Z}_q^n) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$

Prover ( $t_j; s_j$ )

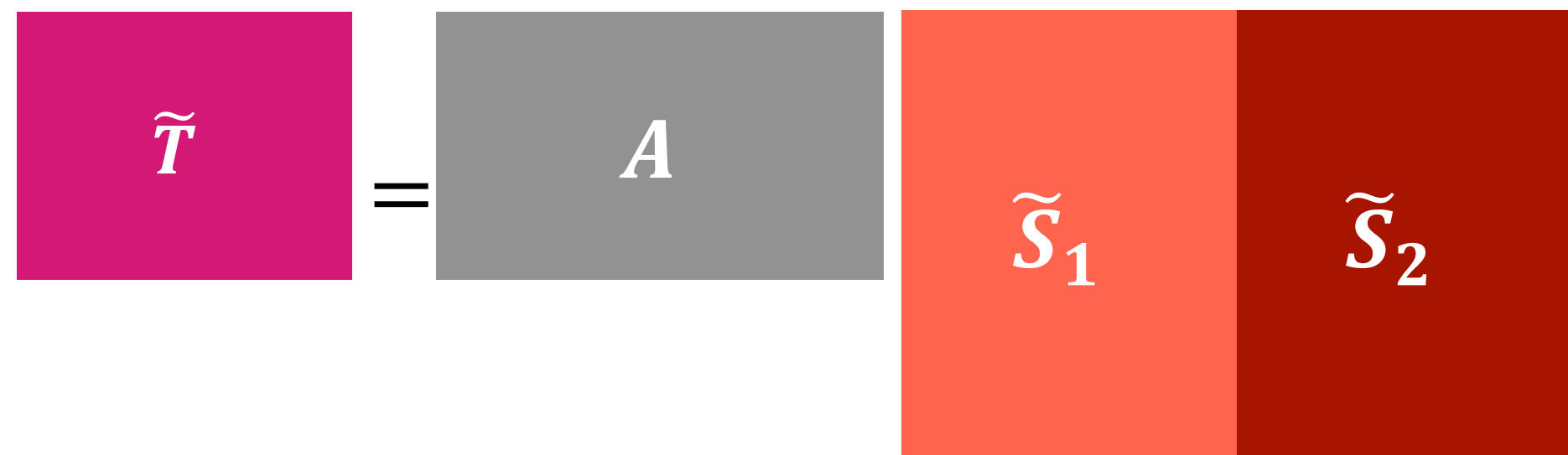
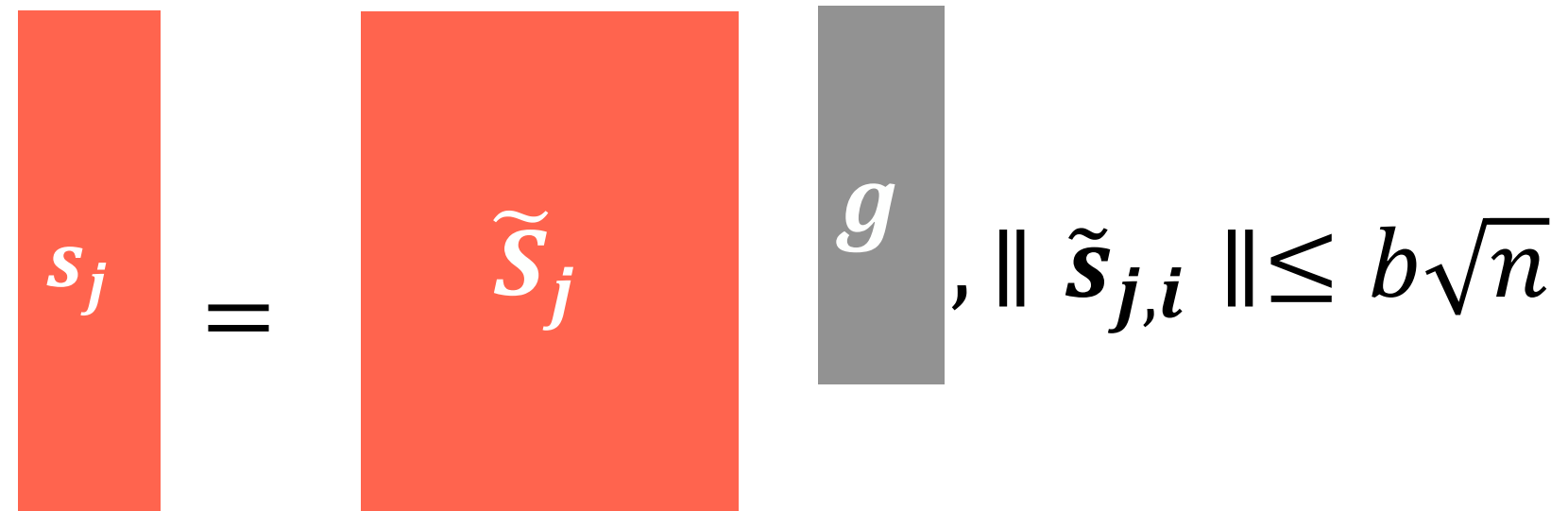


Verifier ( $t_1, t_2$ )

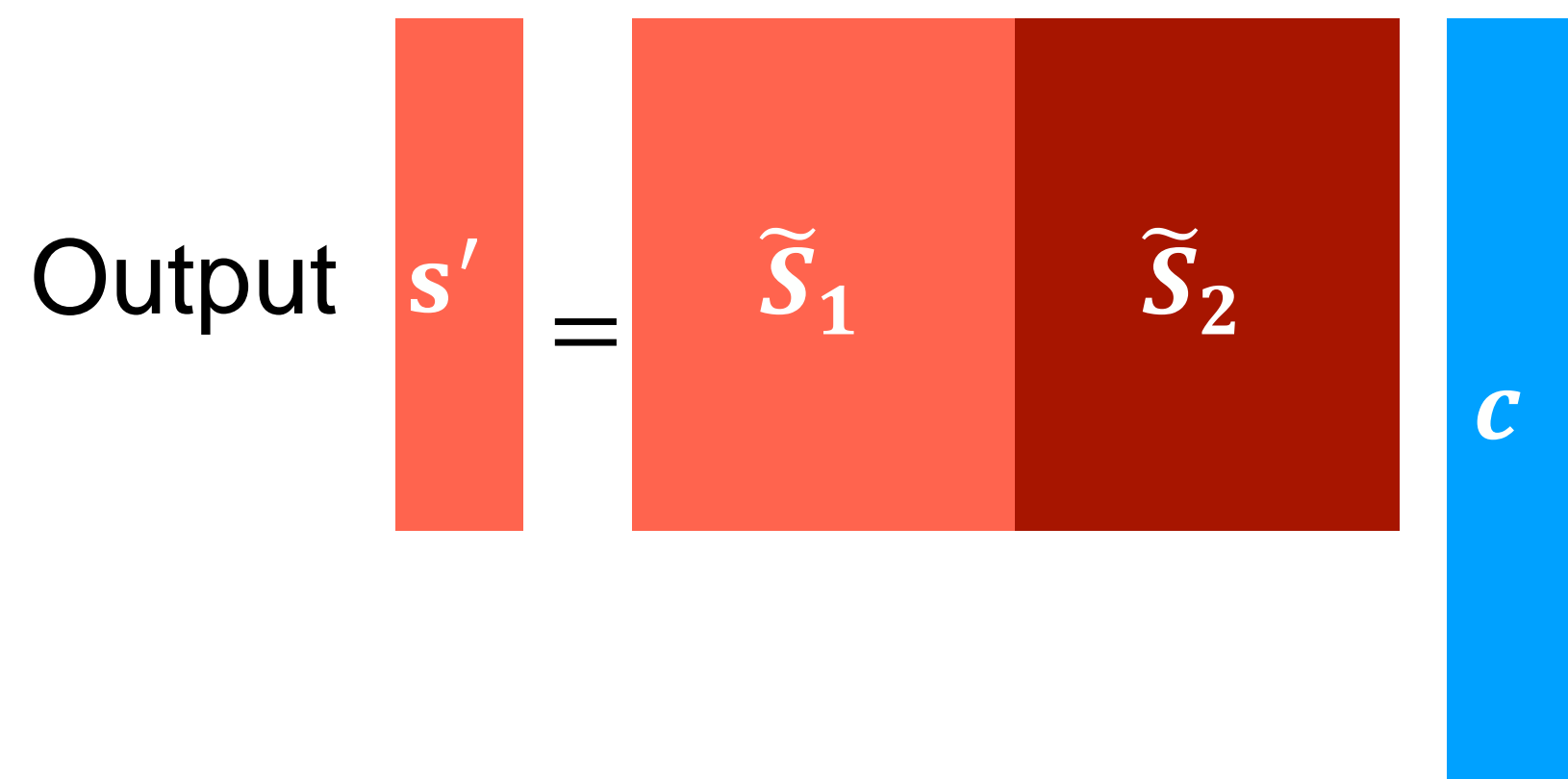
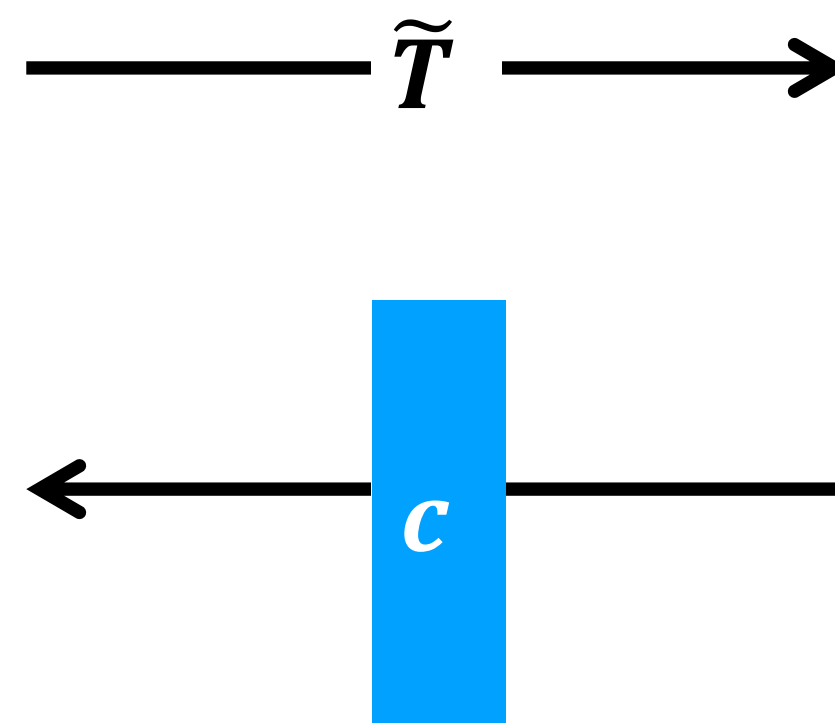
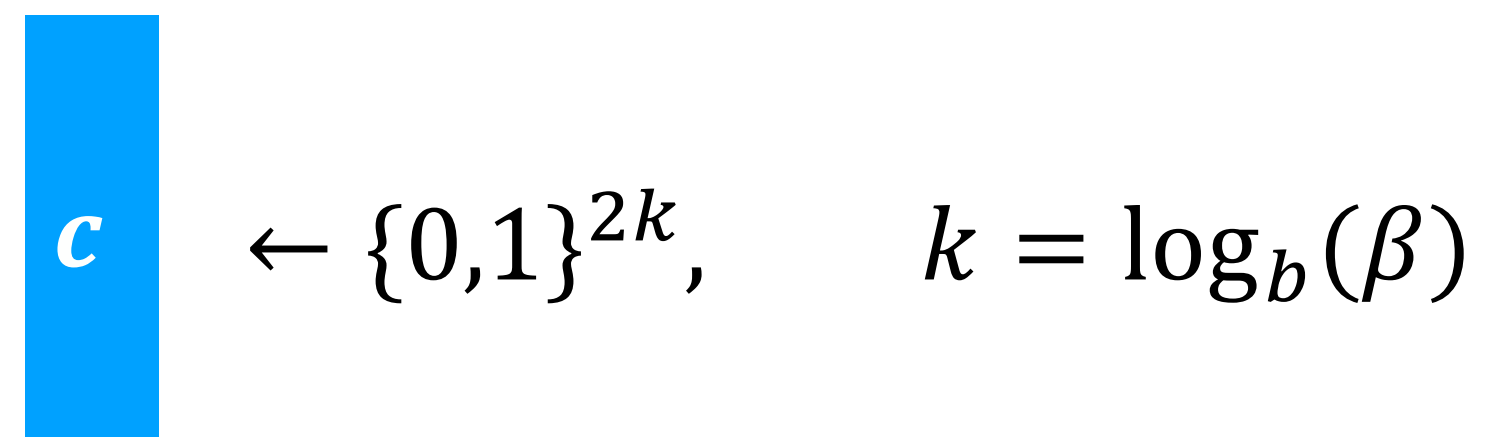


# Lova, take 2 $R = \{(t \in \mathbb{Z}_q^h, s \in \mathbb{Z}_q^n) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$

Prover ( $t_j; s_j$ )



Verifier ( $t_1, t_2$ )



# Lova, take 2 $R = \{(t \in \mathbb{Z}_q^h, s \in \mathbb{Z}_q^n) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$

Prover  $(t_j; s_j)$

$$s_j = \tilde{s}_j \cdot g, \quad \|\tilde{s}_{j,i}\| \leq b\sqrt{n}$$

$$\tilde{T} = A \begin{bmatrix} \tilde{s}_1 \\ \tilde{s}_2 \end{bmatrix}$$

$\xrightarrow{\tilde{T}}$

Verifier  $(t_1, t_2)$

$$c \leftarrow \{0,1\}^{2k}, \quad k = \log_b(\beta)$$

$\xleftarrow{c}$

Check

$$\begin{bmatrix} t_1 \\ t_2 \end{bmatrix} \stackrel{?}{=} \tilde{T} \begin{bmatrix} g \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ g \end{bmatrix}$$

Output

$$s' = \begin{bmatrix} \tilde{s}_1 \\ \tilde{s}_2 \end{bmatrix} \cdot c$$

# Lova, take 2 $R = \{(t \in \mathbb{Z}_q^h, s \in \mathbb{Z}_q^n) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$

Prover  $(t_j; s_j)$

$$s_j = \tilde{s}_j \cdot g, \quad \|\tilde{s}_{j,i}\| \leq b\sqrt{n}$$

$$\tilde{T} = A \begin{bmatrix} \tilde{s}_1 \\ \tilde{s}_2 \end{bmatrix}$$

$\tilde{T}$

$c$

Output  $s' = \begin{bmatrix} \tilde{s}_1 \\ \tilde{s}_2 \end{bmatrix} \cdot c$

Verifier  $(t_1, t_2)$

$$c \leftarrow \{0,1\}^{2k}, \quad k = \log_b(\beta)$$

Check  $\begin{bmatrix} t_1 \\ t_2 \end{bmatrix} \stackrel{?}{=} \tilde{T} \begin{bmatrix} g \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ g \end{bmatrix}$

Output  $t' = \tilde{T} \cdot c$

# Lova, take 2 $R = \{(t \in \mathbb{Z}_q^h, s \in \mathbb{Z}_q^n) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$

Prover  $(t_j; s_j)$

$$s_j = \tilde{s}_j \cdot g, \quad \|\tilde{s}_{j,i}\| \leq b\sqrt{n}$$

$$\tilde{T} = A \begin{bmatrix} \tilde{s}_1 \\ \vdots \\ \tilde{s}_j \end{bmatrix}$$

$\|s'\| \leq 2kb\sqrt{n} \leq \beta$   
 for a suitable choice of parameters

Output  $s' = \begin{bmatrix} \tilde{s}_1 \\ \vdots \\ \tilde{s}_j \end{bmatrix} \cdot c$

Verifier  $(t_1, t_2)$

$$c \leftarrow \{0,1\}^{2k}, \quad k = \log_b(\beta)$$

Check  $\begin{bmatrix} t_1 \\ t_2 \end{bmatrix} \stackrel{?}{=} \tilde{T} \begin{bmatrix} g \\ 0 \end{bmatrix} \begin{bmatrix} 0 \\ g \end{bmatrix}$

Output  $t' = \tilde{T} \cdot c$



# Lova, take 2

Folding Norm Growth

Soundness error

Extractor Norm Growth

# Lova, take 2

Folding Norm Growth

$$\| \mathbf{s}' \| \leq 2kb\sqrt{n} \leq \beta$$

Soundness error

Extractor Norm Growth

# Lova, take 2

Folding Norm Growth

$$\| \mathbf{s}' \| \leq 2kb\sqrt{n} \leq \beta$$

Soundness error

$$\frac{1}{2^{2k}} + ???$$

Extractor Norm Growth

$$\beta' \mapsto 2\beta'$$

# Lova, take 2

Folding Norm Growth

$$\|s'\| \leq 2kb\sqrt{n} \leq \beta$$

Soundness error

$$\frac{1}{2^{2k}} + ???$$

parallel repetition  
+ clever analysis!

Extractor Norm Growth

$$\beta' \mapsto 2\beta'$$

**Lova, take 3**  $R = \{(T \in \mathbb{Z}_q^{h \times t}, S \in \mathbb{Z}_q^{n \times t}) \mid T = AS \pmod{q} \wedge \|S_{:,i}\| \leq \beta\}$

Prover  $(T_1, T_2; S_1, S_2)$

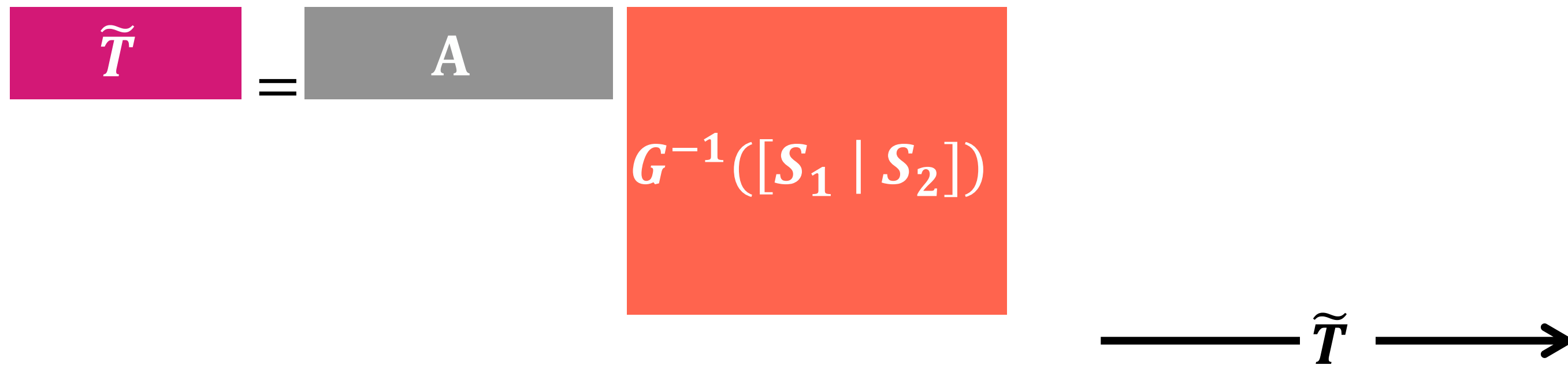
Verifier  $(T_1, T_2)$

# Lova, take 3

$$R = \{(T \in \mathbb{Z}_q^{h \times t}, S \in \mathbb{Z}_q^{n \times t}) \mid T = AS \pmod{q} \wedge \|S_{:,i}\| \leq \beta\}$$

Prover  $(T_1, T_2; S_1, S_2)$

Verifier  $(T_1, T_2)$

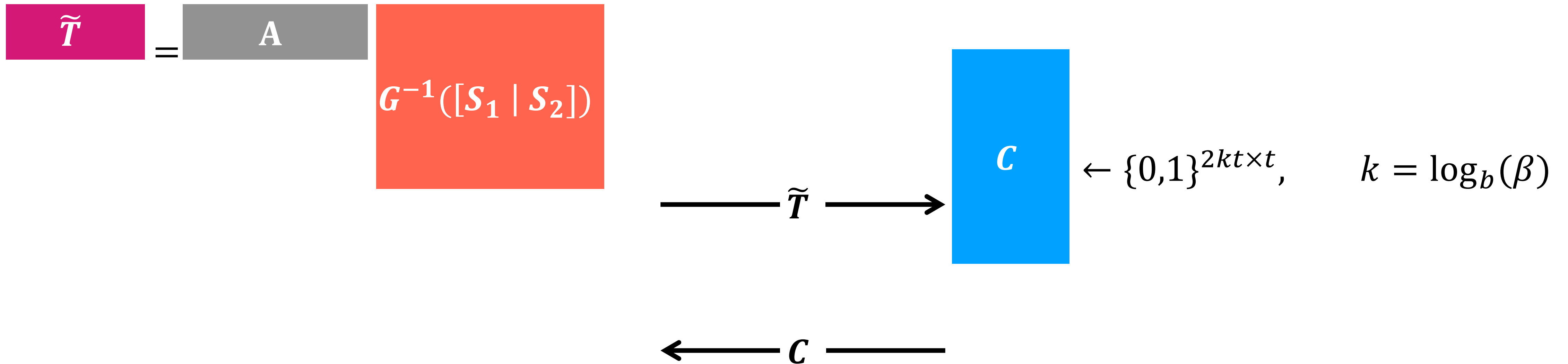


# Lova, take 3

$$R = \{(T \in \mathbb{Z}_q^{h \times t}, S \in \mathbb{Z}_q^{n \times t}) \mid T = AS \pmod{q} \wedge \|S_{:,i}\| \leq \beta\}$$

Prover  $(T_1, T_2; S_1, S_2)$

Verifier  $(T_1, T_2)$

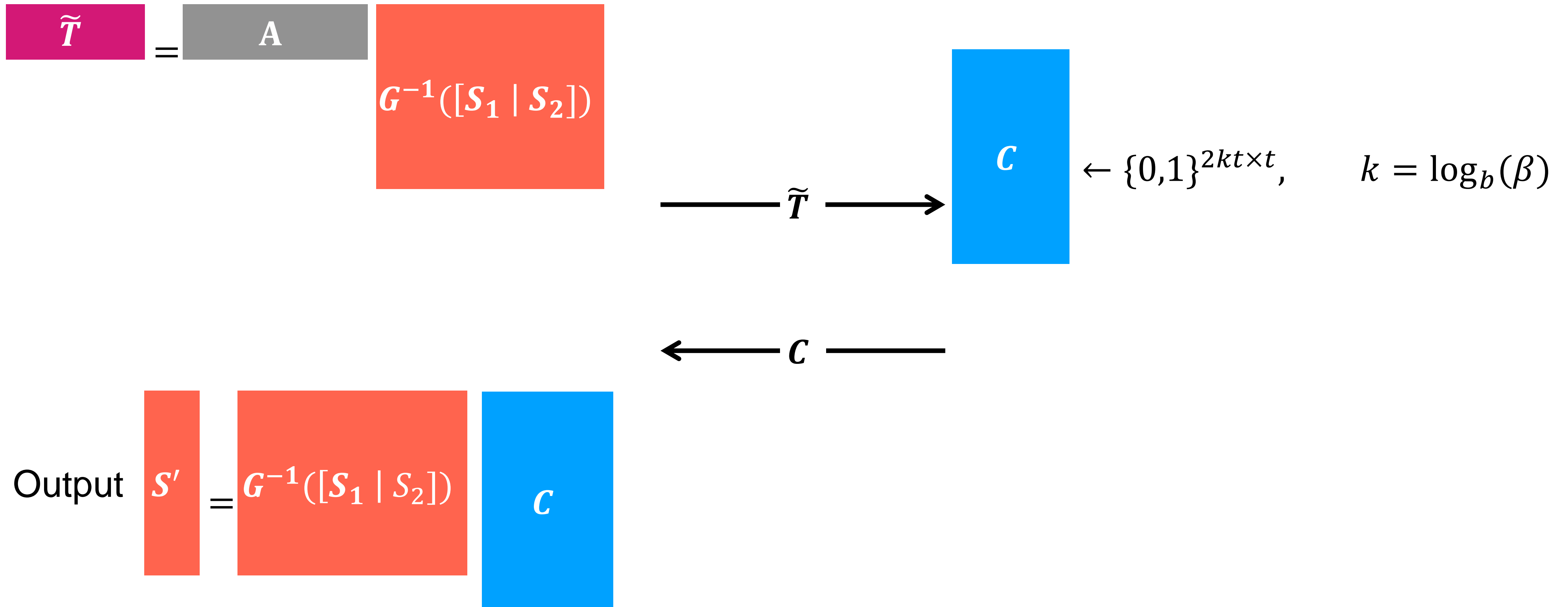


# Lova, take 3

$$R = \{(T \in \mathbb{Z}_q^{h \times t}, S \in \mathbb{Z}_q^{n \times t}) \mid T = AS \pmod{q} \wedge \|S_{:,i}\| \leq \beta\}$$

Prover  $(T_1, T_2; S_1, S_2)$

Verifier  $(T_1, T_2)$



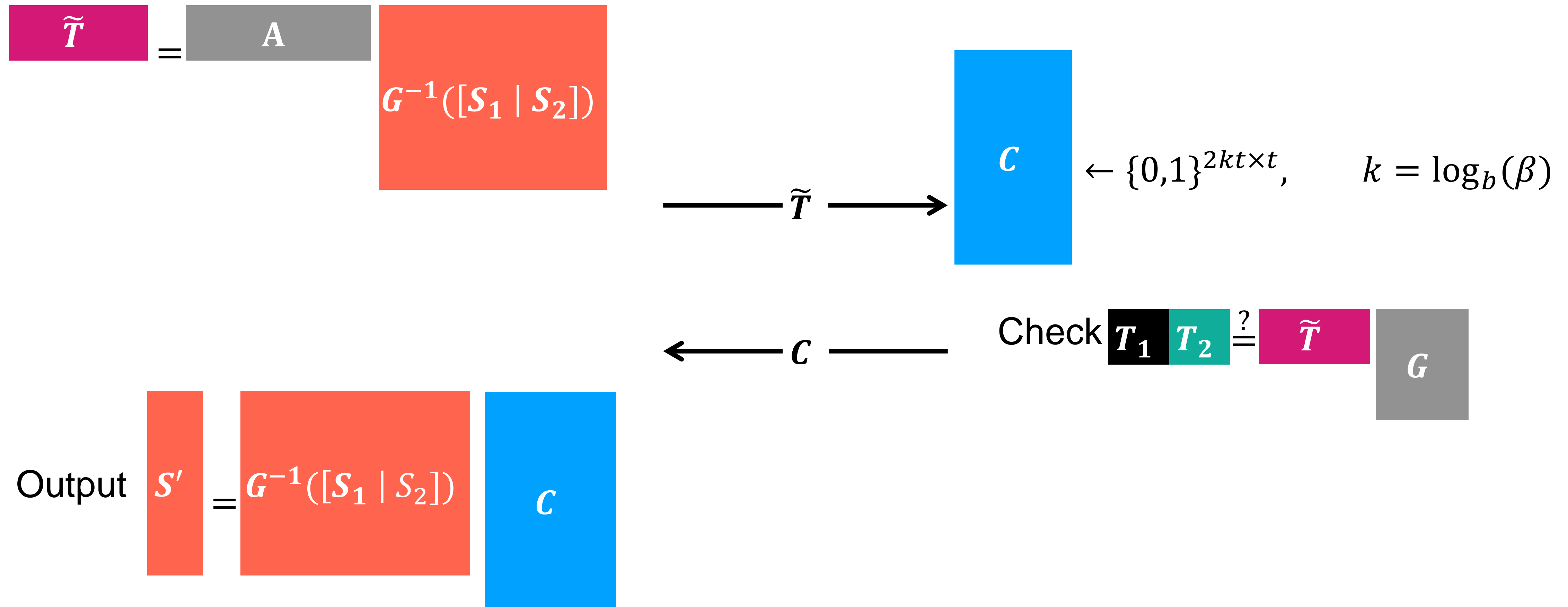


# Lova, take 3

$$R = \{(T \in \mathbb{Z}_q^{h \times t}, S \in \mathbb{Z}_q^{n \times t}) \mid T = AS \pmod{q} \wedge \|S_{:,i}\| \leq \beta\}$$

Prover  $(T_1, T_2; S_1, S_2)$

Verifier  $(T_1, T_2)$

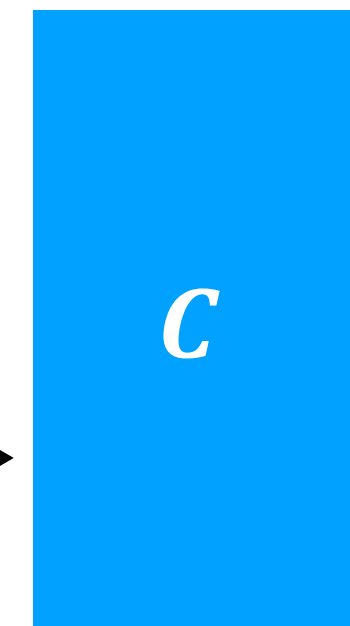
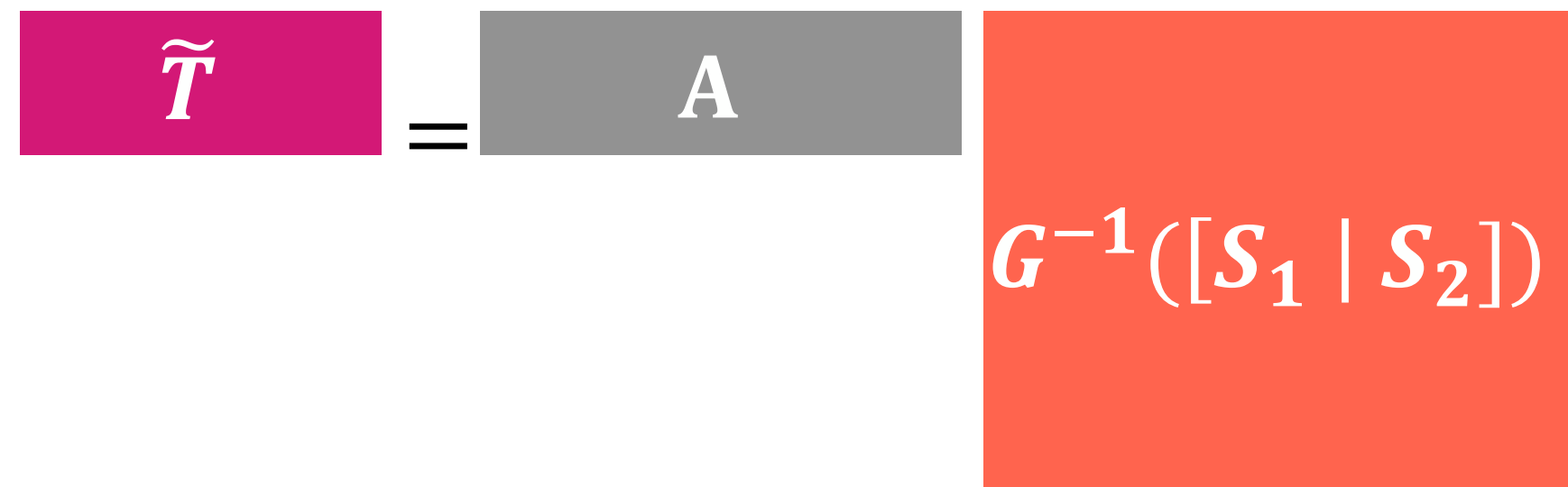


# Lova, take 3

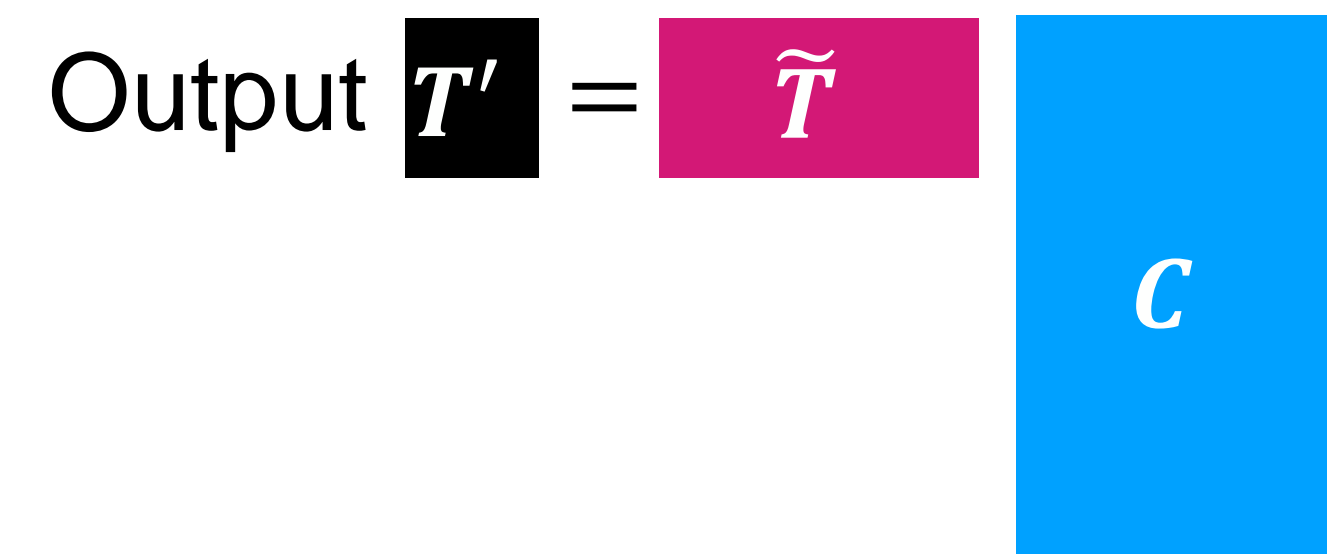
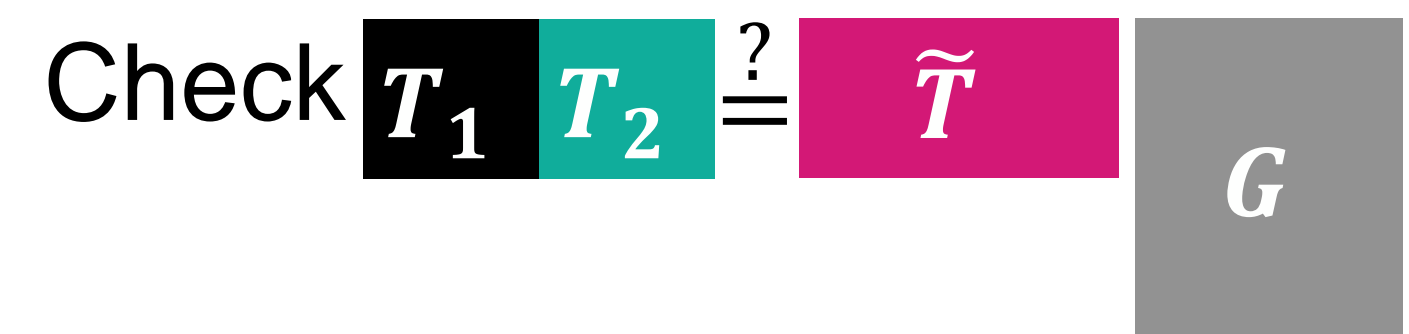
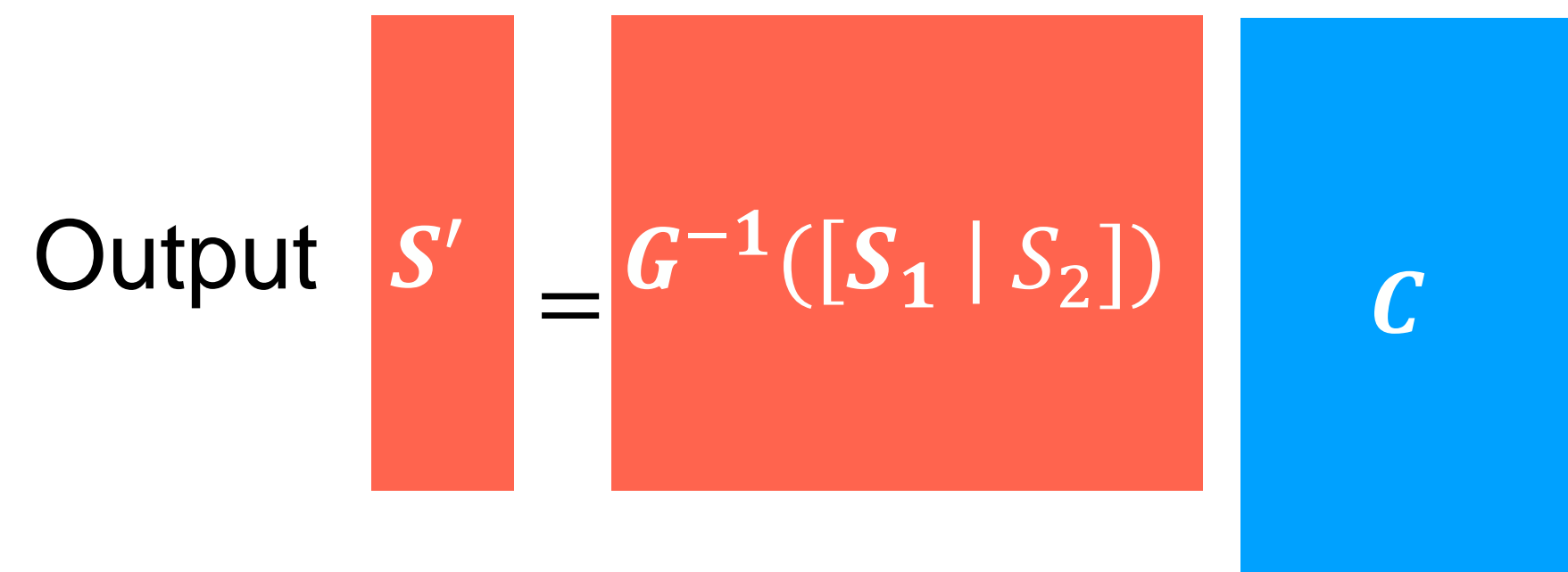
$$R = \{(T \in \mathbb{Z}_q^{h \times t}, S \in \mathbb{Z}_q^{n \times t}) \mid T = AS \pmod{q} \wedge \|S_{:,i}\| \leq \beta\}$$

Prover  $(T_1, T_2; S_1, S_2)$

Verifier  $(T_1, T_2)$



$$C \leftarrow \{0,1\}^{2kt \times t}, \quad k = \log_b(\beta)$$



**Lova, take 3**  $R = \{(T \in \mathbb{Z}_q^{k \times k}, S \in \mathbb{Z}_q^{2k \times k}) \mid T = AS \pmod{q} \wedge \|S_i\| \leq \beta\}$   
 Prover  $(T_1, T_2; S_1, S_2)$  Verifier  $(T_1, T_2)$

$\gamma = A$   $g^{-1}(S_1 | S_2)$   $C$   $\leftarrow \{0,1\}^{2k \times k}$

Output  $S' = g^{-1}(S_1 | S_2)$   $C$

Check  $T_1, T_2 \stackrel{?}{=} T$   $G$

Output  $T' = \gamma$   $C$

**Lova, take 2**  $R = \{(t \in \mathbb{Z}_q^k, s \in \mathbb{Z}_q^k) \mid t = As \pmod{q} \wedge \|s\| \leq \beta\}$   
 Prover  $(t_j; s_j)$  Verifier  $(t_1, t_2)$

$s_j = \tilde{s}_j$   $g$   $\|s_j\| \leq b\sqrt{n}$   $C$   $\leftarrow \{0,1\}^{2k}$

$\gamma = A$   $S_1$   $S_2$   $C$

Output  $s' = \tilde{s}_1$   $\tilde{s}_2$   $C$

Check  $t_1, t_2 \stackrel{?}{=} T$   $G$   $\begin{bmatrix} g & 0 \\ 0 & g \end{bmatrix}$

Output  $t' = \tilde{t}$   $C$

**+ parallel repetition**

**Corporate needs you to find the differences between this picture and this picture.**

**They're the same picture.**

# Lova, take 3

Folding Norm Growth

$$\| \mathbf{s}' \| \leq 2kb\sqrt{n} \leq \| \mathbf{s} \|$$

Soundness error

Extractor Norm Growth

# Lova, take 3

Folding Norm Growth

$$\| \mathbf{s}' \| \leq 2kb\sqrt{n} \leq \| \mathbf{s} \|$$

Soundness error

$$2kt/2^t$$

Coordinate-wise Special  
Soundness [FMN24]

Extractor Norm Growth

# Lova, take 3

Folding Norm Growth

$$\| \mathbf{s}' \| \leq 2kb\sqrt{n} \leq \| \mathbf{s} \|$$

Soundness error

$$2kt/2^t$$

Coordinate-wise Special  
Soundness [FMN24]

Extractor Norm Growth

$$\beta' \mapsto 2\beta'$$

# Lova, take 3

Folding Norm Growth

$$\| \mathbf{s}' \| \leq 2kb\sqrt{n} \leq \| \mathbf{s} \|$$

Soundness error

$$2kt/2^t$$

Coordinate-wise Special  
Soundness [FMN24]

Extractor Norm Growth

$$\beta' \mapsto 2\beta'$$

We need exact norm proofs

# Ideas for proving exact norm bounds

## Observation 1



# Ideas for proving exact norm bounds

## Observation 1

# Ideas for proving exact norm bounds

## Observation 1

- If a vector  $s$  satisfies  $|\langle s, s \rangle \bmod q| \leq \beta^2$  and  $\|s\| \ll q$  then we must have

$$\|s\| \leq \beta.$$

Hence, we reduce the problem to proving inner products modulo  $q$ .

# New relation

$$R_{q,\beta,t}^{\text{SIS}} = \left\{ \left( \mathbf{T} \in \mathbb{Z}_q^{h \times t}, \mathbf{S} \in \mathbb{Z}_q^{n \times t} \right) \mid \begin{array}{l} \mathbf{T} = \mathbf{A}\mathbf{S} \pmod{q} \\ \wedge \|\mathbf{S}_{:,i}\| \leq \beta \end{array} \right\}$$

$$R_{q,\beta,t}^{\text{SIS}} = \left\{ \left( \left( \mathbf{T} \in \mathbb{Z}_q^{h \times t}, \mathbf{D} \in \mathbb{Z}^{t \times t} \right), \mathbf{S} \in \mathbb{Z}_q^{n \times t} \right) \mid \begin{array}{l} \mathbf{T} = \mathbf{A}\mathbf{S} \pmod{q} \\ \wedge \mathbf{D} = \mathbf{S}^T \mathbf{S} \\ \wedge \|\mathbf{D}_{i,i}\| \leq \beta^2 \end{array} \right\}$$

# Ideas for proving exact norm bounds

## Observation 2

- Suppose  $S_1^\top S_1 = D_1$  and  $S_2^\top S_2 = D_2$ .

- Denote  $S^* := G^{-1}([S_1 | S_2])$ . Then,

- $$\begin{bmatrix} D_1 & \begin{matrix} \color{yellow}{\vdots} \end{matrix} \\ \begin{matrix} \color{red}{\vdots} \end{matrix} & D_2 \end{bmatrix} = G^\top S^{*\top} S^* G.$$

- Hence, reveal  $\tilde{D} := S^{*\top} S^*$ .

# Lova, take 4 (final)

$$R_{q,\beta,t}^{\text{SIS}} = \left\{ \left( \left( \mathbf{T} \in \mathbb{Z}_q^{h \times t}, \mathbf{D} \in \mathbb{Z}^{t \times t} \right), \mathbf{S} \in \mathbb{Z}_q^{n \times t} \right) \mid \begin{array}{l} \mathbf{T} = \mathbf{A}\mathbf{S} \pmod{q} \\ \wedge \mathbf{D} = \mathbf{S}^T \mathbf{S} \\ \wedge \|\mathbf{D}_{i,i}\| \leq \beta^2 \end{array} \right\}$$

Prover  $(\mathbf{T}_j, \mathbf{D}_j; \mathbf{S}_j)$

$$\tilde{\mathbf{T}} = \mathbf{A} \mathbf{G}^{-1}([\mathbf{S}_1 | \mathbf{S}_2])$$

Verifier  $(\mathbf{T}_0, \mathbf{T}_1, \mathbf{D}_0, \mathbf{D}_1)$

$$\mathbf{C} \leftarrow \{0,1\}^{2kt \times t}$$

Check  $\mathbf{T}_1 \mathbf{T}_2 \stackrel{?}{=} \tilde{\mathbf{T}} \mathbf{G} \pmod{q}$

$$\xrightarrow{\tilde{\mathbf{T}}}$$

$$\xleftarrow{\mathbf{C}}$$

Output  $\mathbf{T}' = \tilde{\mathbf{T}} \mathbf{C} \pmod{q}$

Output  $\mathbf{S}' = \mathbf{G}^{-1}([\mathbf{S}_1 | \mathbf{S}_2]) \mathbf{C}$

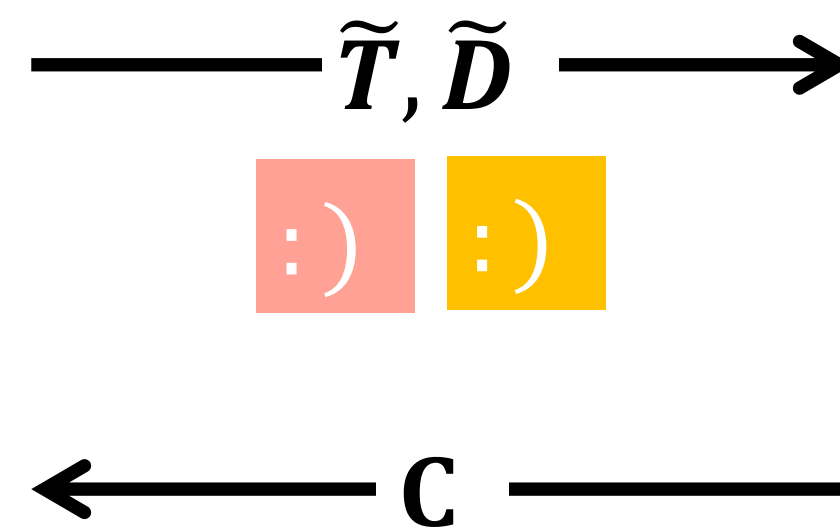
# Lova, take 4 (final)

$$R_{q,\beta,t}^{\text{SIS}} = \left\{ \left( (T \in \mathbb{Z}_q^{h \times t}, D \in \mathbb{Z}^{t \times t}), S \in \mathbb{Z}_q^{n \times t} \right) \mid \begin{array}{l} T = AS \pmod q \\ \wedge D = S^T S \\ \wedge \|D_{i,i}\| \leq \beta^2 \end{array} \right\}$$

Prover  $(T_j, D_j; S_j)$

$$\tilde{T} = A G^{-1}([S_1 | S_2])$$

$$\tilde{D} = G^{-1}([S_1 | S_2])^T G^{-1}([S_1 | S_2])$$



Output  $S' = G^{-1}([S_1 | S_2]) C$

Verifier  $(T_0, T_1, D_0, D_1)$

$$C \leftarrow \{0,1\}^{2kt \times t}$$

Check  $T_1 T_2 \stackrel{?}{=} \tilde{T} G \pmod q$

Output  $T' = \tilde{T} C \pmod q$

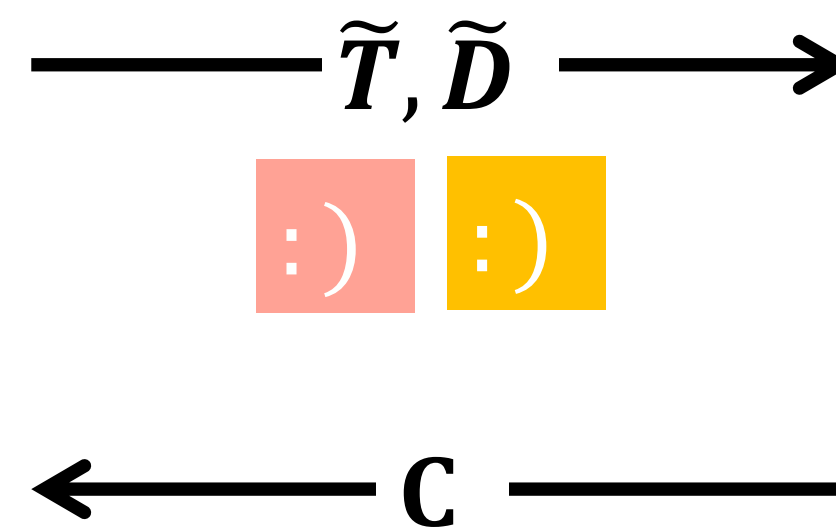
# Lova, take 4 (final)

$$R_{q,\beta,t}^{\text{SIS}} = \left\{ \left( (T \in \mathbb{Z}_q^{h \times t}, D \in \mathbb{Z}^{t \times t}), S \in \mathbb{Z}_q^{n \times t} \right) \mid \begin{array}{l} T = AS \pmod{q} \\ \wedge D = S^T S \\ \wedge \|D_{i,i}\| \leq \beta^2 \end{array} \right\}$$

Prover  $(T_j, D_j; S_j)$

$$\tilde{T} = A G^{-1}([S_1 | S_2])$$

$$\tilde{D} = G^{-1}([S_1 | S_2])^T G^{-1}([S_1 | S_2])$$



Output  $S' = G^{-1}([S_1 | S_2]) C$

Verifier  $(T_0, T_1, D_0, D_1)$

$$C \leftarrow \{0,1\}^{2kt \times t}$$

Check  $T_1 T_2 \stackrel{?}{=} \tilde{T} G \pmod{q}$

Check  $\begin{pmatrix} D_1 & :) \\ :) & D_2 \end{pmatrix} \stackrel{?}{=} G^T \tilde{D} G$

Output  $T' = \tilde{T} C \pmod{q}$

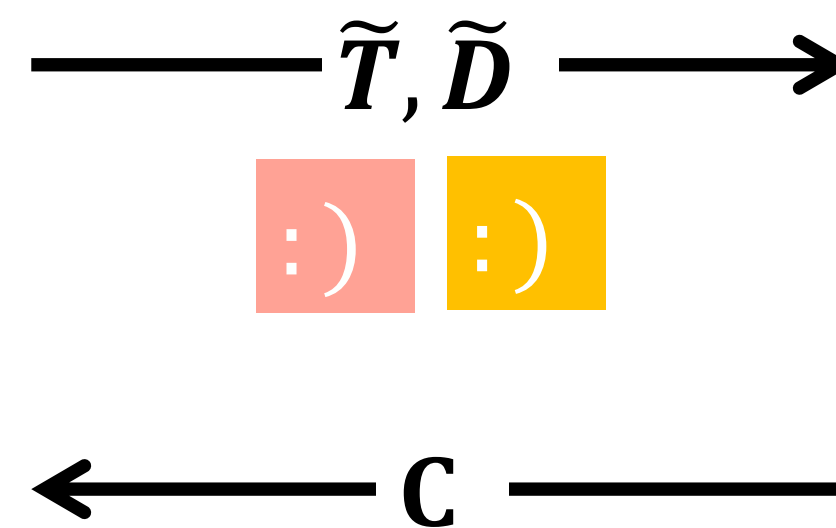
# Lova, take 4 (final)

$$R_{q,\beta,t}^{\text{SIS}} = \left\{ \left( (T \in \mathbb{Z}_q^{h \times t}, D \in \mathbb{Z}^{t \times t}), S \in \mathbb{Z}_q^{n \times t} \right) \mid \begin{array}{l} T = AS \pmod{q} \\ \wedge D = S^T S \\ \wedge \|D_{i,i}\| \leq \beta^2 \end{array} \right\}$$

Prover  $(T_j, D_j; S_j)$

$$\tilde{T} = A G^{-1}([S_1 | S_2])$$

$$\tilde{D} = G^{-1}([S_1 | S_2])^T G^{-1}([S_1 | S_2])$$



Output  $S' = G^{-1}([S_1 | S_2]) C$

Verifier  $(T_0, T_1, D_0, D_1)$

$$C \leftarrow \{0,1\}^{2kt \times t}$$

Check  $T_1 T_2 \stackrel{?}{=} \tilde{T} G \pmod{q}$

Check  $\begin{pmatrix} D_1 & :) \\ :) & D_2 \end{pmatrix} \stackrel{?}{=} G^T \tilde{D} G$

Output  $T' = \tilde{T} C \pmod{q}$

Output  $D' = C^T \tilde{D} C$



# Lova, take 4 (final)

Knowledge Soundness



# Lova, take 4 (final)

## Knowledge Soundness



1. Arguing knowledge soundness will boil down to random evaluation of some quadratic polynomial

# Lova, take 4 (final)



## Knowledge Soundness

1. Arguing knowledge soundness will boil down to random evaluation of some quadratic polynomial
2. To this end, relying on the  $\{0,1\}$  set is not enough

# Lova, take 4 (final)



## Knowledge Soundness

1. Arguing knowledge soundness will boil down to random evaluation of some quadratic polynomial
2. To this end, relying on the  $\{0,1\}$  set is not enough
3. So, instead we take the set  $\{-1,0,1\}$

# Lova, take 4 (final)



## Knowledge Soundness

1. Arguing knowledge soundness will boil down to random evaluation of some quadratic polynomial
2. To this end, relying on the  $\{0,1\}$  set is not enough
3. So, instead we take the set  $\{-1,0,1\}$

Fix  $c \in \{-1,0,1\}$ . With probability  $\frac{1}{3}$   
 $c' - c = \pm 1$ .

# Lova, take 4 (final)



## Knowledge Soundness

1. Arguing knowledge soundness will boil down to random evaluation of some quadratic polynomial

2. To this end, relying on the  $\{0,1\}$  set is not enough

3. So, instead we take the set  $\{-1,0,1\}$

Fix  $c \in \{-1,0,1\}$ . With probability  $\frac{1}{3}$   
 $c' - c = \pm 1$ .

Set big enough for the Schwartz-Zippel argument.

# Lova - Single folding step (ouch)

Instance length	$2^{17}$	$2^{18}$	$2^{19}$
Proof size ( $\kappa_C = 0$ )	44.45 MB	46.32 MB	48.20 MB
Proof size ( $\kappa_C \leq 2^{-128}$ )	42.37 MB	44.23 MB	46.11 MB
Prover time ( $\kappa_C = 0$ )	725.35 s	1568.5 s	3243.8 s
Prover time ( $\kappa_C \leq 2^{-128}$ )	702.11 s	1492.8 s	3002.9 s
Verifier time ( $\kappa_C = 0$ )	3.0337 s	3.0723 s	3.0986 s
Verifier time ( $\kappa_C \leq 2^{-128}$ )	3.1306 s	3.0185 s	3.1768 s

$\lambda = 128, q = 2^{64}, b = \sqrt{\beta}, k = 4, 64$ -bit Fiat-Shamir security loss  
AWC EC2 m5.8xlarge, 128GB RAM, 32 Intel Xeon vCPUs @ 3.1GHz

# Summary

- Decompose-and-fold for folding norm growth
- Amplify soundness by consider many instances (i.e., parallel repetition)
- Exact Euclidean norm proof (i.e., inner product + probabilistic check) for extracted norm growth

**THANKS!**