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

THX for the slides

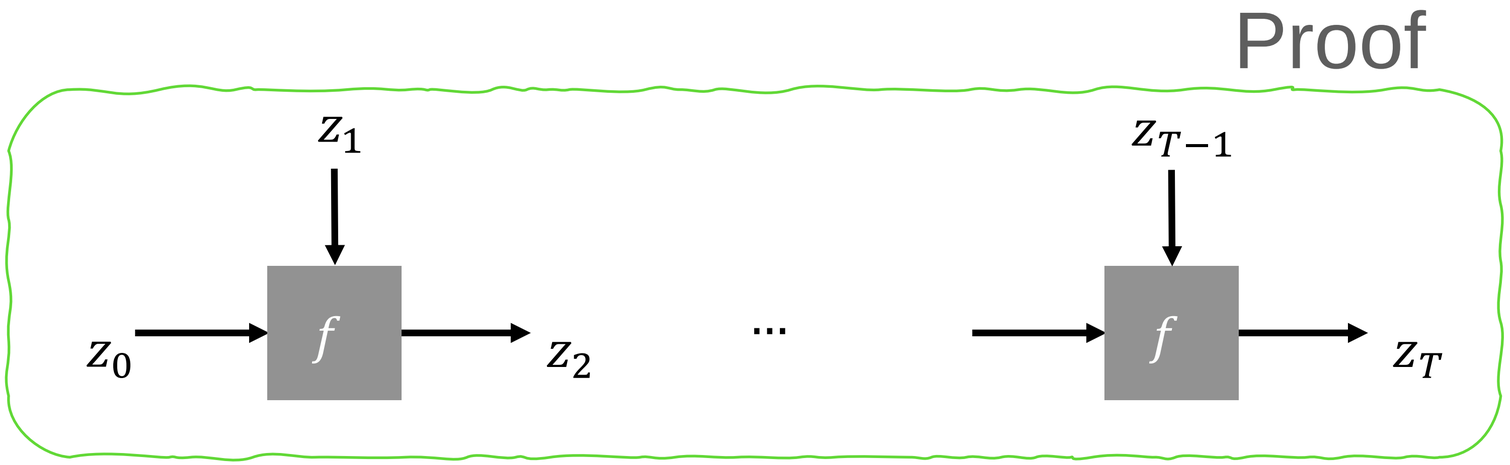
EPFL

1794 ENS ÉCOLE NORMALE SUPÉRIEURE

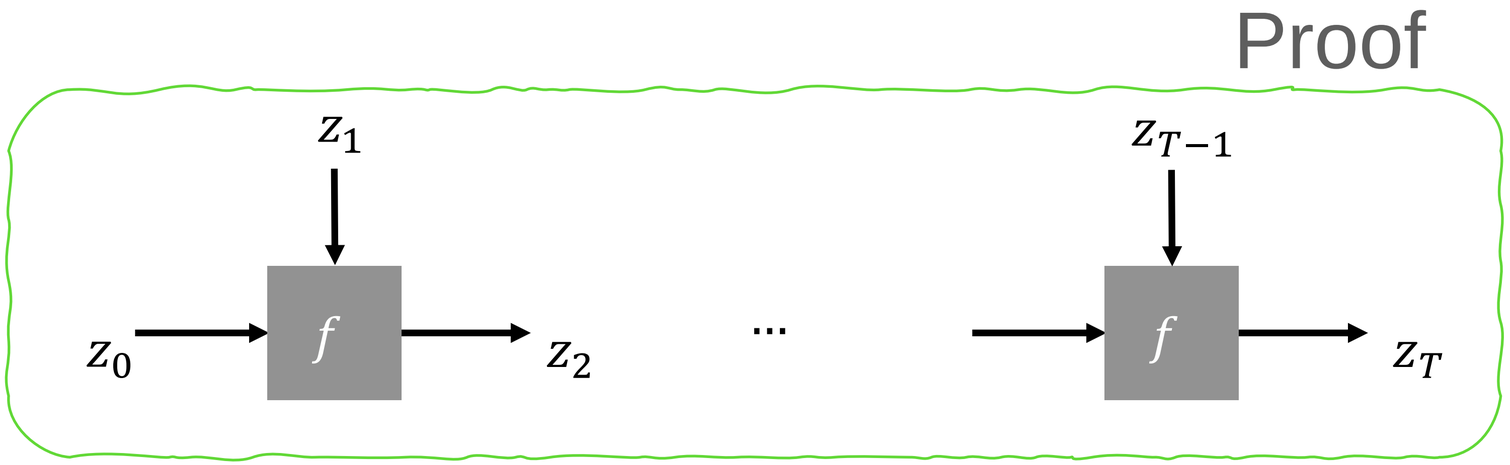
KING'S College LONDON

Folding Scheme

Incrementally Verifiable Computation [Val08]



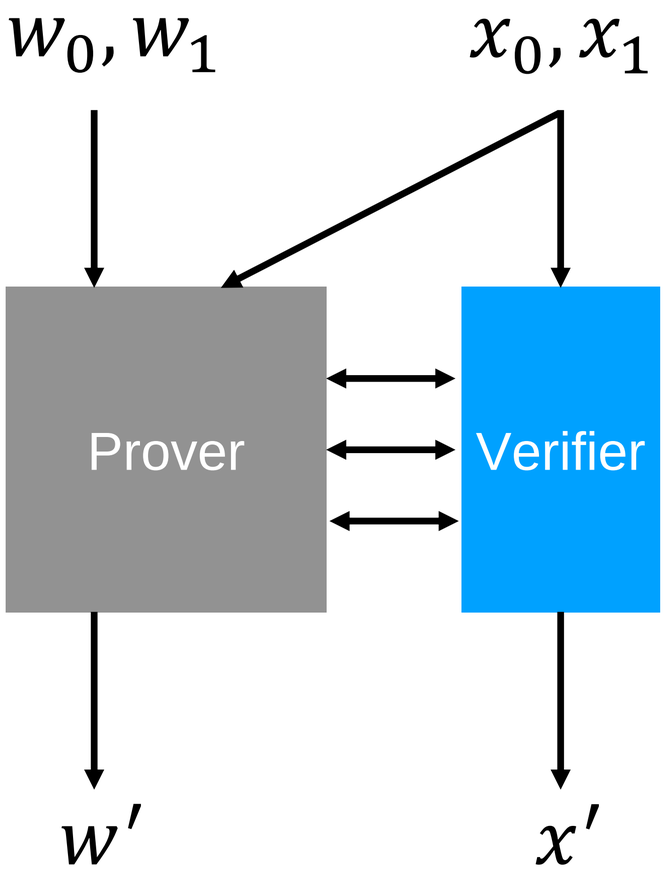
Incrementally Verifiable Computation [Val08]



Applications:

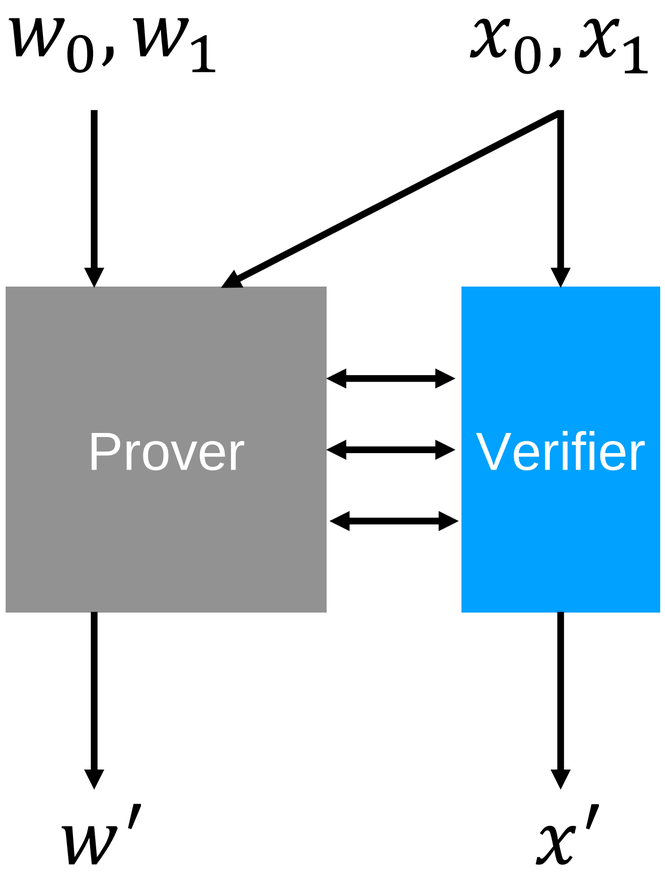
- Verifiable Delay Functions
- ZK-Virtual Machine
- zkRollups

Folding scheme [KST22]



Folding scheme [KST22]

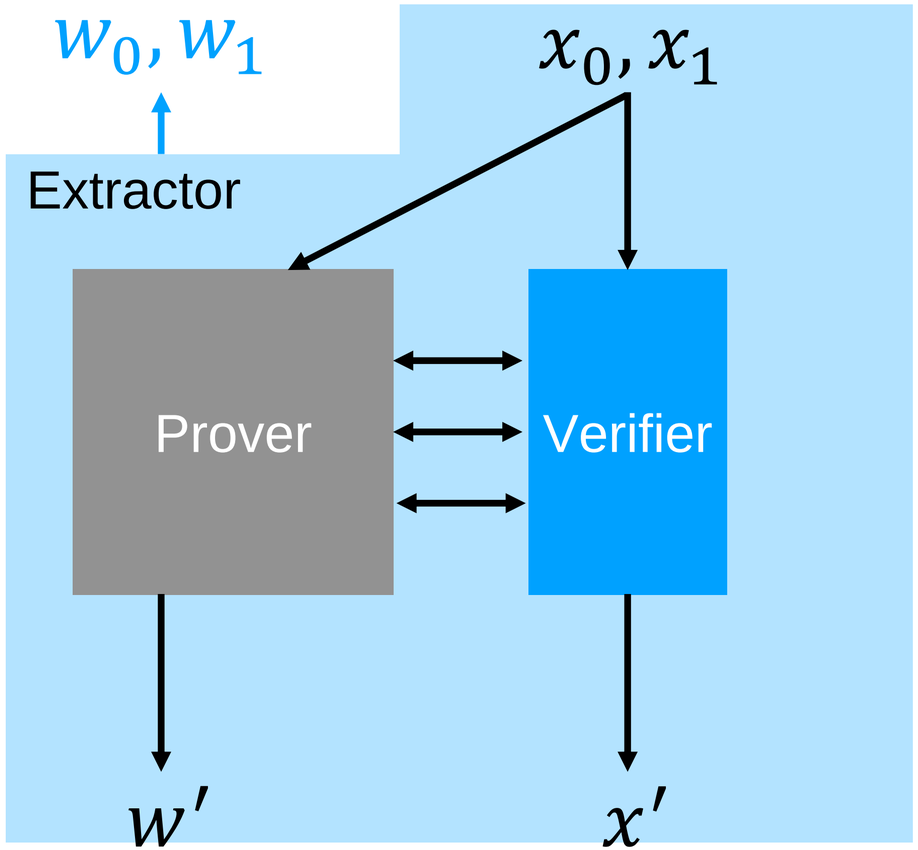
Completeness



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

Folding scheme [KST22]

Knowledge Soundness

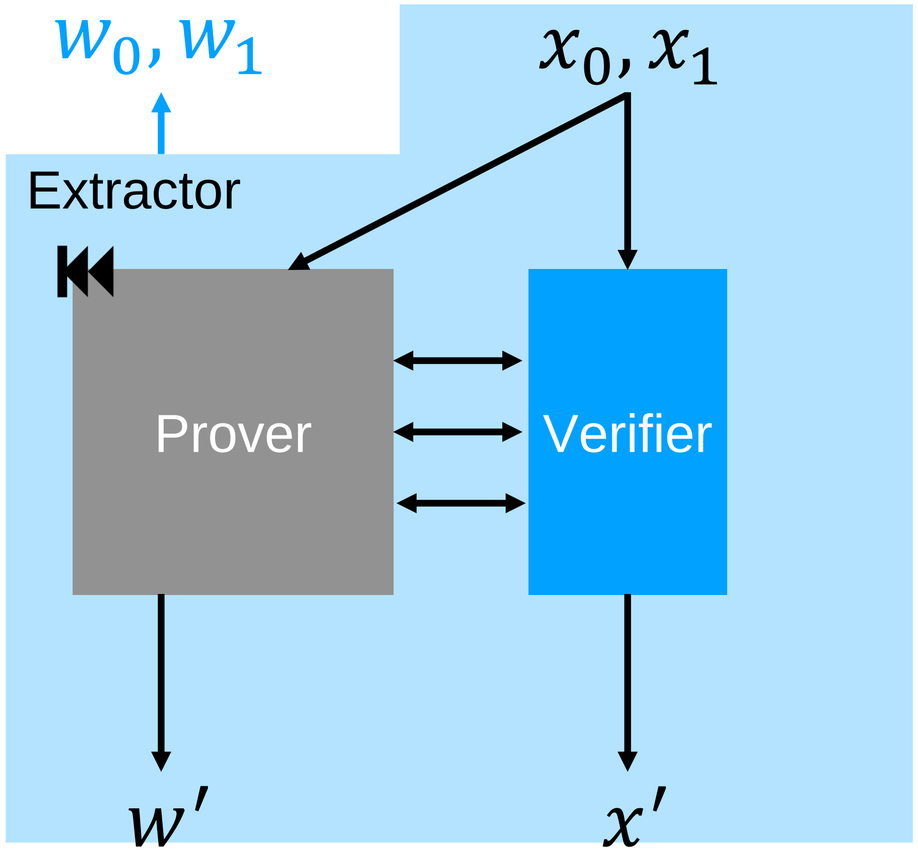


W.h.p.,

$(x', w') \in R \Longrightarrow$ The prover must have known valid w_0, w_1 for x_0, x_1

Folding scheme [KST22]

Knowledge Soundness

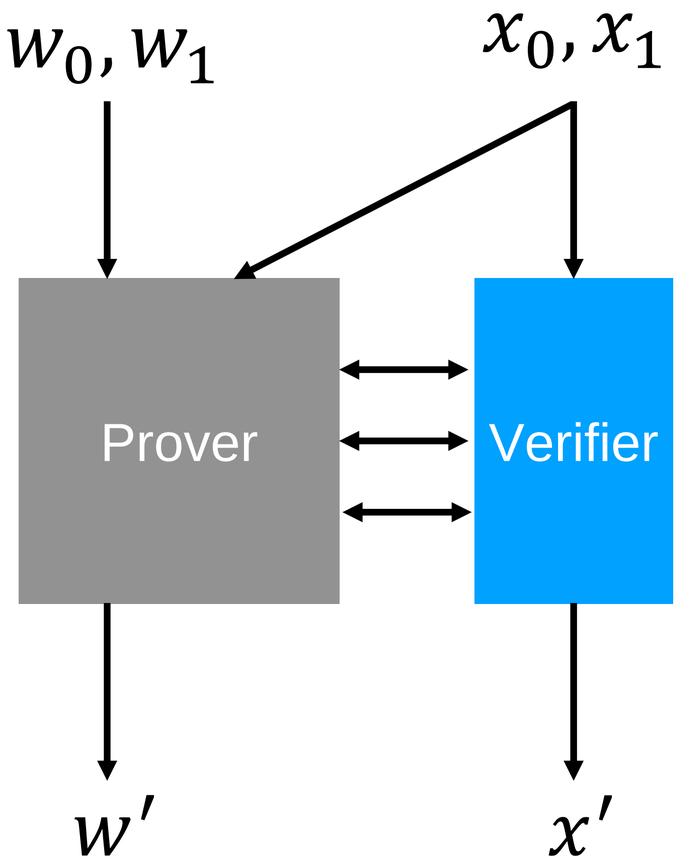


W.h.p.,

$(x', w') \in R \Longrightarrow$ 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

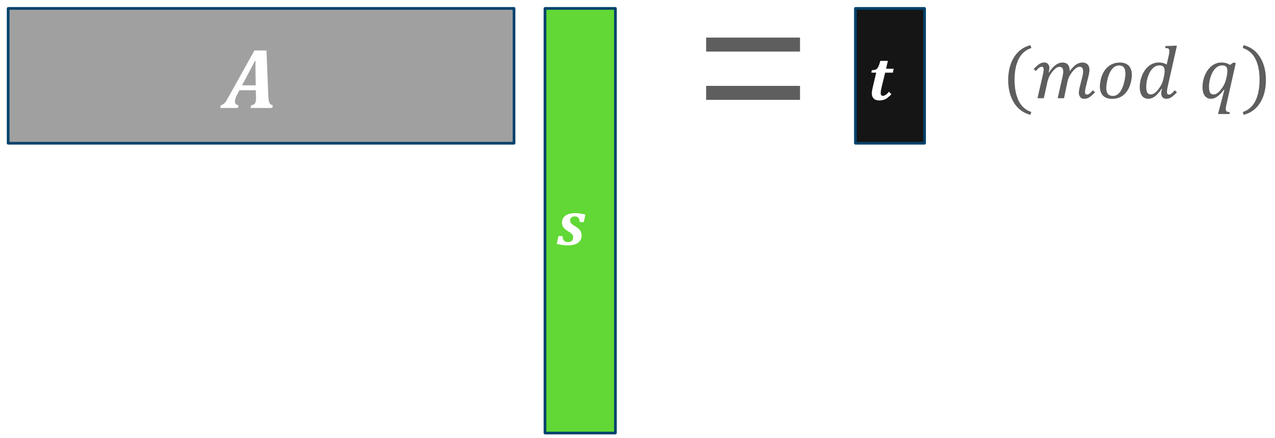
- First lattice-based folding scheme
- Based on the (unstructured) SIS assumption
- Exact Euclidean norm proof

Ajtai commitment [Ajt96]

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

Ajtai commitment [Ajt96]

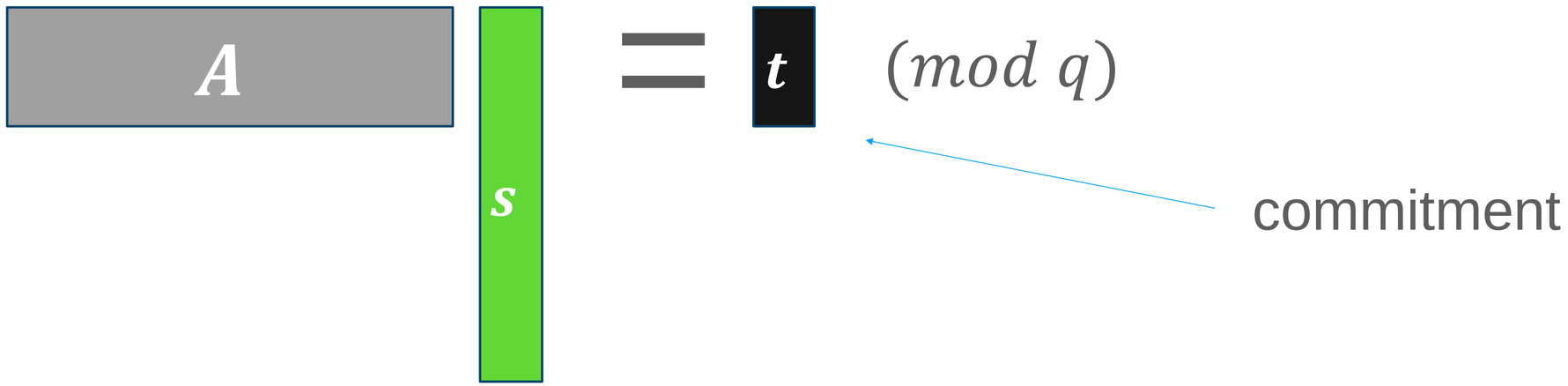
- Let $\mathbb{Z}_q$ be a ring of integers modulo q.
- To commit to a short message vector $\boldsymbol{s}$, we compute:



$$(mod\ q)$$

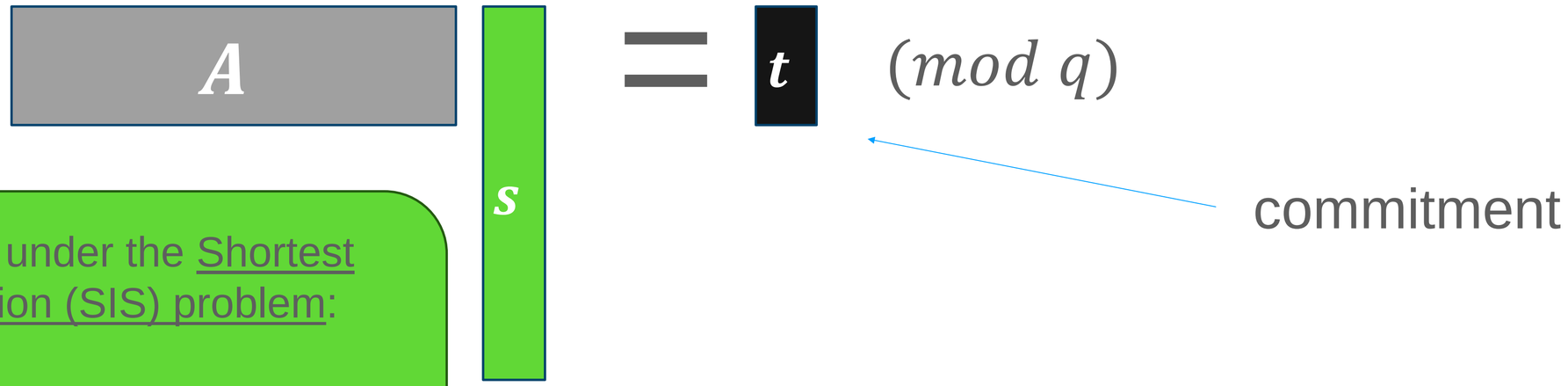
Ajtai commitment [Ajt96]

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



Ajtai commitment [Ajt96]

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



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

Given a random matrix $\boldsymbol{A}$, find a short non-zero vector $\boldsymbol{s}$ s.t.
$\boldsymbol{As} = \boldsymbol{0}\ (mod\ q)$

Lova, take 1

Lova, take 1

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

Lova, take 1

Prover $(\boldsymbol{t_1}, \boldsymbol{t_2}; \boldsymbol{s_1}, \boldsymbol{s_2})$

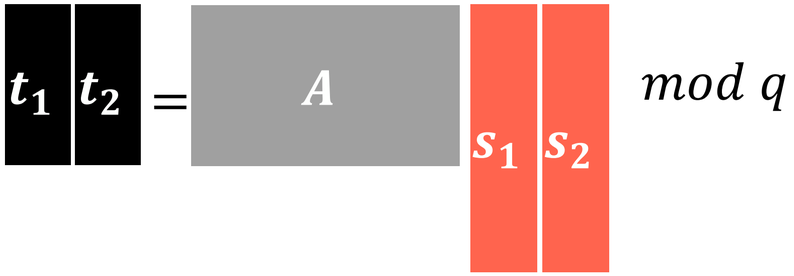
Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$

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

Lova, take 1

Prover $(\boldsymbol{t_1}, \boldsymbol{t_2}; \boldsymbol{s_1}, \boldsymbol{s_2})$

Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$

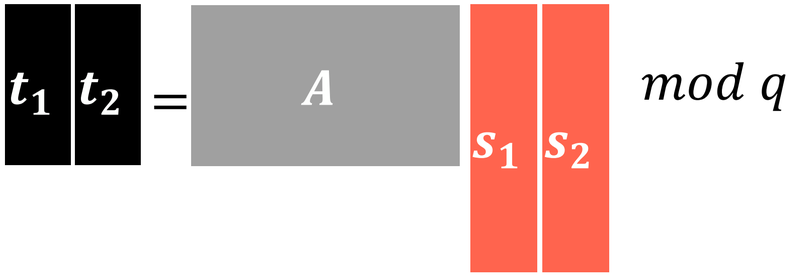


$$R = \{(\boldsymbol{t}, \boldsymbol{s}) | \boldsymbol{t} = \boldsymbol{As}\ (\boldsymbol{mod}\ \boldsymbol{q}) \wedge \| \boldsymbol{s} \| \leq \boldsymbol{\beta}\}$$

Lova, take 1

Prover $(\boldsymbol{t_1}, \boldsymbol{t_2}; \boldsymbol{s_1}, \boldsymbol{s_2})$

Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$



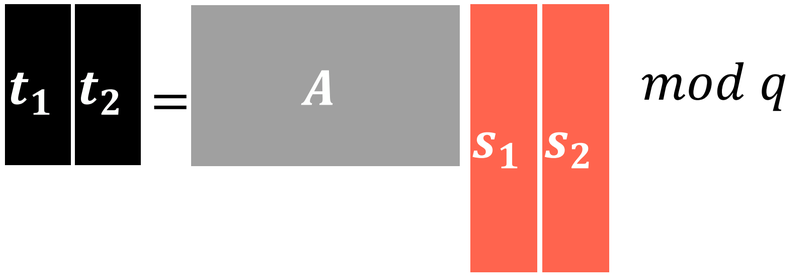
$c \leftarrow C \subseteq \mathbb{Z}_q$

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

Lova, take 1

Prover $(\boldsymbol{t_1}, \boldsymbol{t_2}; \boldsymbol{s_1}, \boldsymbol{s_2})$

Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$



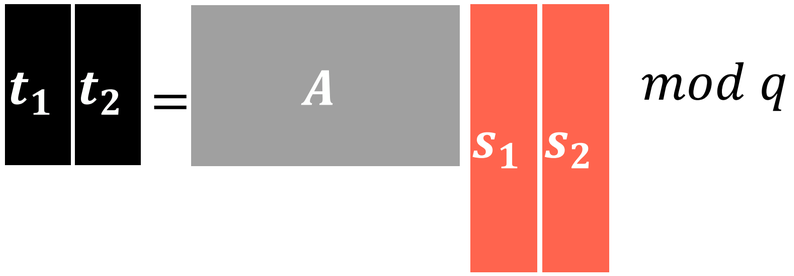
$c \leftarrow C \subseteq \mathbb{Z}_q$

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

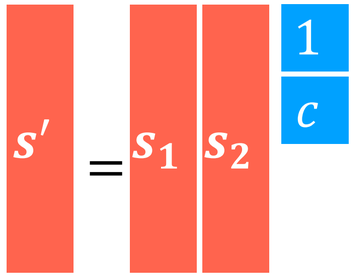
Lova, take 1

Prover $(\boldsymbol{t_1}, \boldsymbol{t_2}; \boldsymbol{s_1}, \boldsymbol{s_2})$

Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$



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

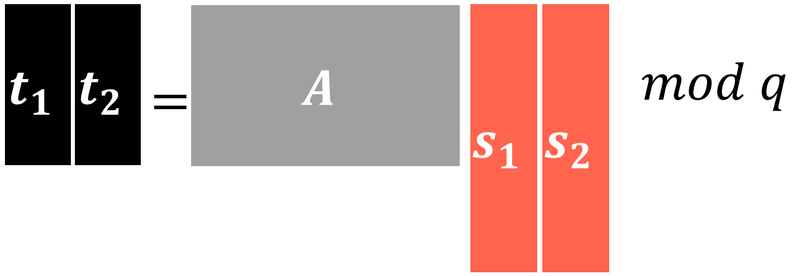


$$R = \{(\boldsymbol{t}, \boldsymbol{s}) | \boldsymbol{t} = \boldsymbol{As}\ (\boldsymbol{mod}\ \boldsymbol{q}) \wedge \| \boldsymbol{s} \| \leq \boldsymbol{\beta}\}$$

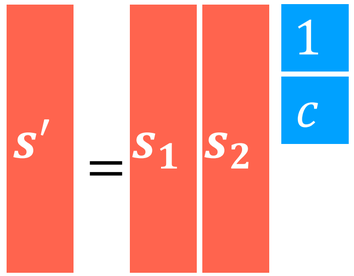
Lova, take 1

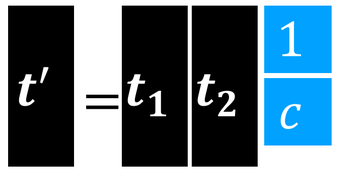
Prover $(\boldsymbol{t_1}, \boldsymbol{t_2}; \boldsymbol{s_1}, \boldsymbol{s_2})$

Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$



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



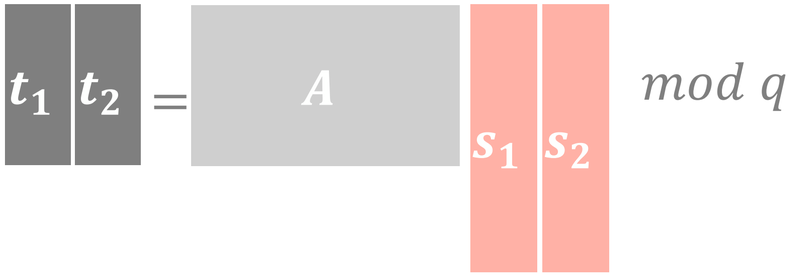


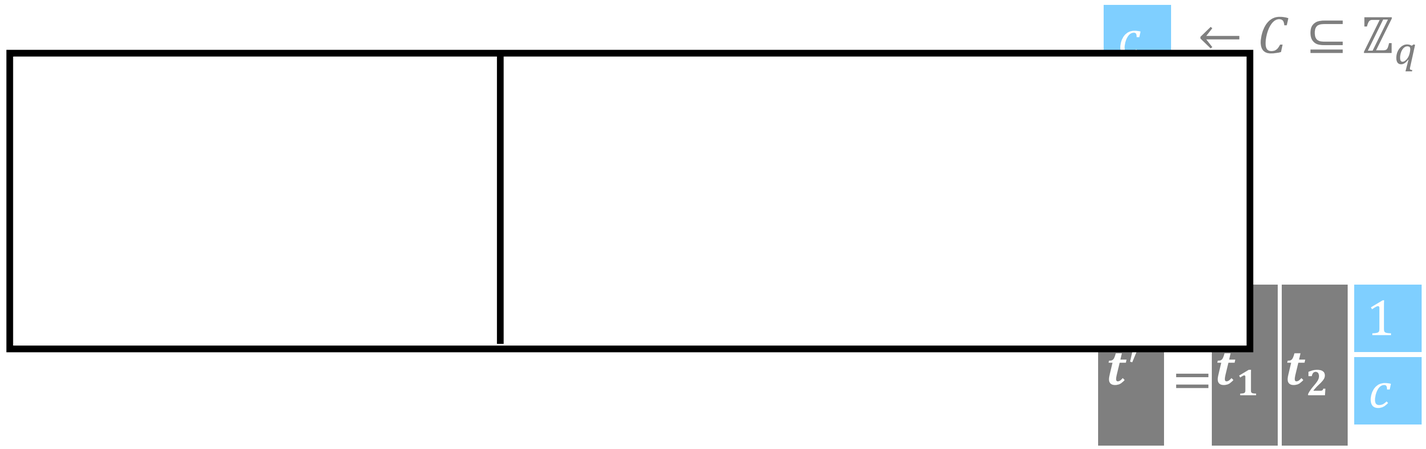
$$R = \{(\boldsymbol{t}, \boldsymbol{s}) | \boldsymbol{t} = \boldsymbol{As}\ (\boldsymbol{mod}\ \boldsymbol{q}) \wedge \| \boldsymbol{s} \| \leq \boldsymbol{\beta}\}$$

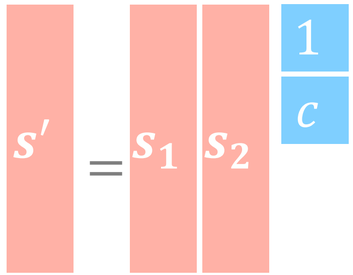
Lova, take 1

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

Verifier (t_1, t_2)





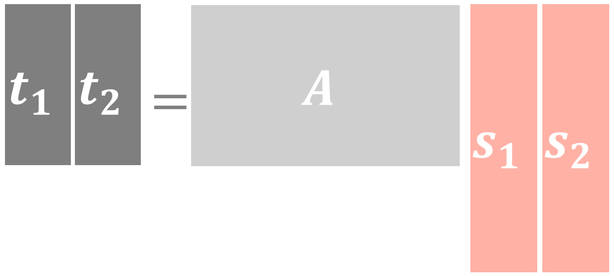


$$R = \{(\boldsymbol{t}, \boldsymbol{s}) | \boldsymbol{t} = \boldsymbol{As}\ (\boldsymbol{mod}\ \boldsymbol{q}) \wedge \| \boldsymbol{s} \| \leq \boldsymbol{\beta}\}$$

Lova, take 1

Prover $(\boldsymbol{t_1}, \boldsymbol{t_2}; \boldsymbol{s_1}, \boldsymbol{s_2})$

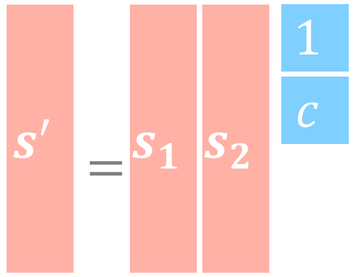
Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$

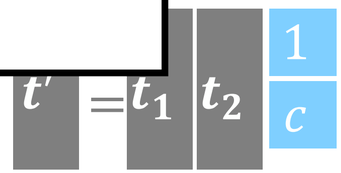


$mod\ q$

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

$$\begin{aligned} \boldsymbol{As'} &= \boldsymbol{A}(\boldsymbol{s_1} + c\boldsymbol{s_2}) \\ &= \boldsymbol{As_1} + c\boldsymbol{As_2} \\ &= \boldsymbol{t_1} + c\boldsymbol{t_2} \\ &= \boldsymbol{t'} \end{aligned}$$



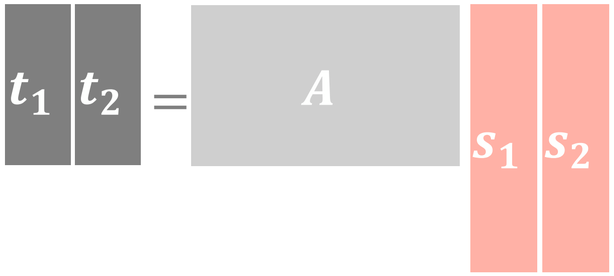


$$R = \{(\boldsymbol{t}, \boldsymbol{s}) | \boldsymbol{t} = \boldsymbol{As}\ (\boldsymbol{mod}\ \boldsymbol{q}) \wedge \| \boldsymbol{s} \| \leq \boldsymbol{\beta}\}$$

Lova, take 1

Prover $(\boldsymbol{t_1}, \boldsymbol{t_2}; \boldsymbol{s_1}, \boldsymbol{s_2})$

Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$

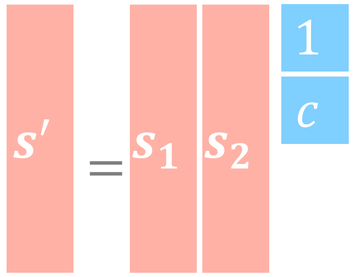


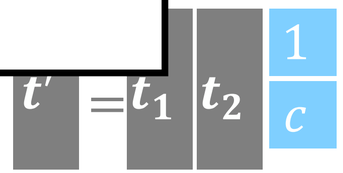
$mod\ q$

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

$$\boldsymbol{As'} = \boldsymbol{A}(\boldsymbol{s_1} + c\boldsymbol{s_2}) = \boldsymbol{As_1} + c\boldsymbol{As_2} = \boldsymbol{t_1} + c\boldsymbol{t_2} = \boldsymbol{t'}$$

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

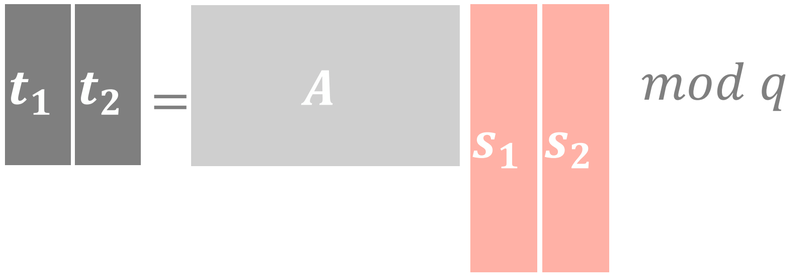




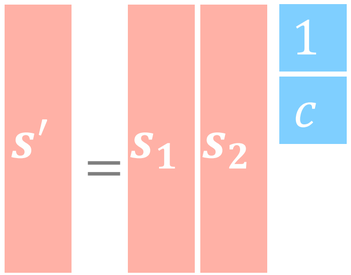
$$R = \{(\boldsymbol{t}, \boldsymbol{s}) | \boldsymbol{t} = \boldsymbol{As}\ (\boldsymbol{mod\ q}) \wedge \| \boldsymbol{s} \| \leq \boldsymbol{\beta}\}$$

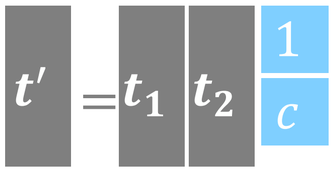
Lova, take 1

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



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

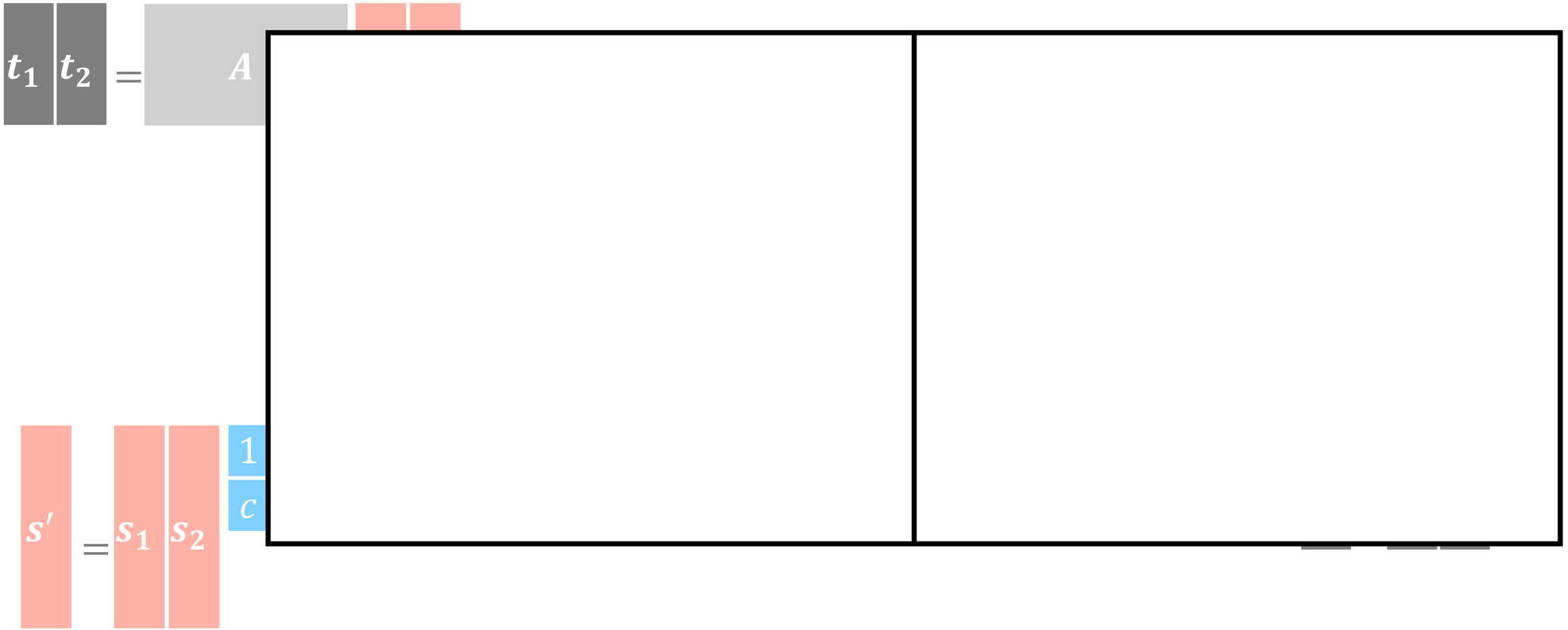




$$R = \{(\boldsymbol{t}, \boldsymbol{s}) | \boldsymbol{t} = \boldsymbol{As}\ (\boldsymbol{mod}\ \boldsymbol{q}) \wedge \| \boldsymbol{s} \| \leq \boldsymbol{\beta}\}$$

Lova, take 1

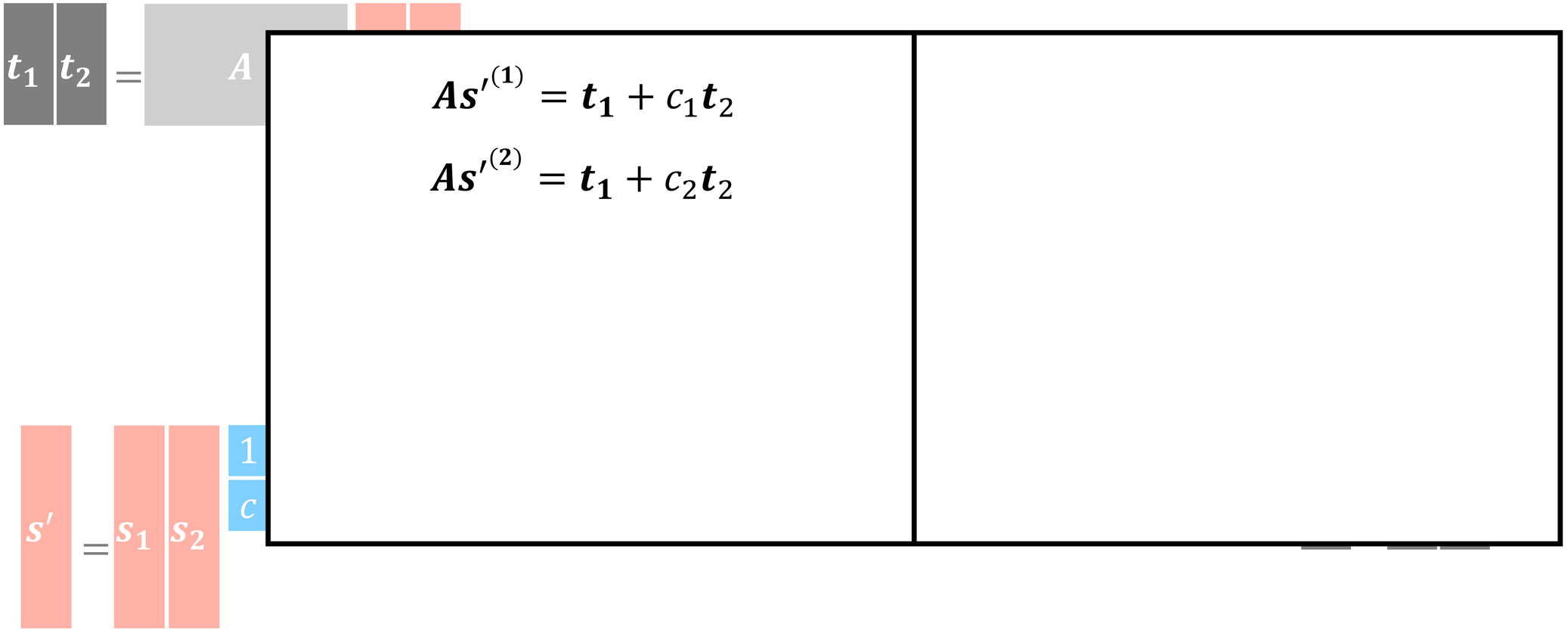
Knowledge soundness via special soundness: $c_1 \neq c_2$



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

Lova, take 1

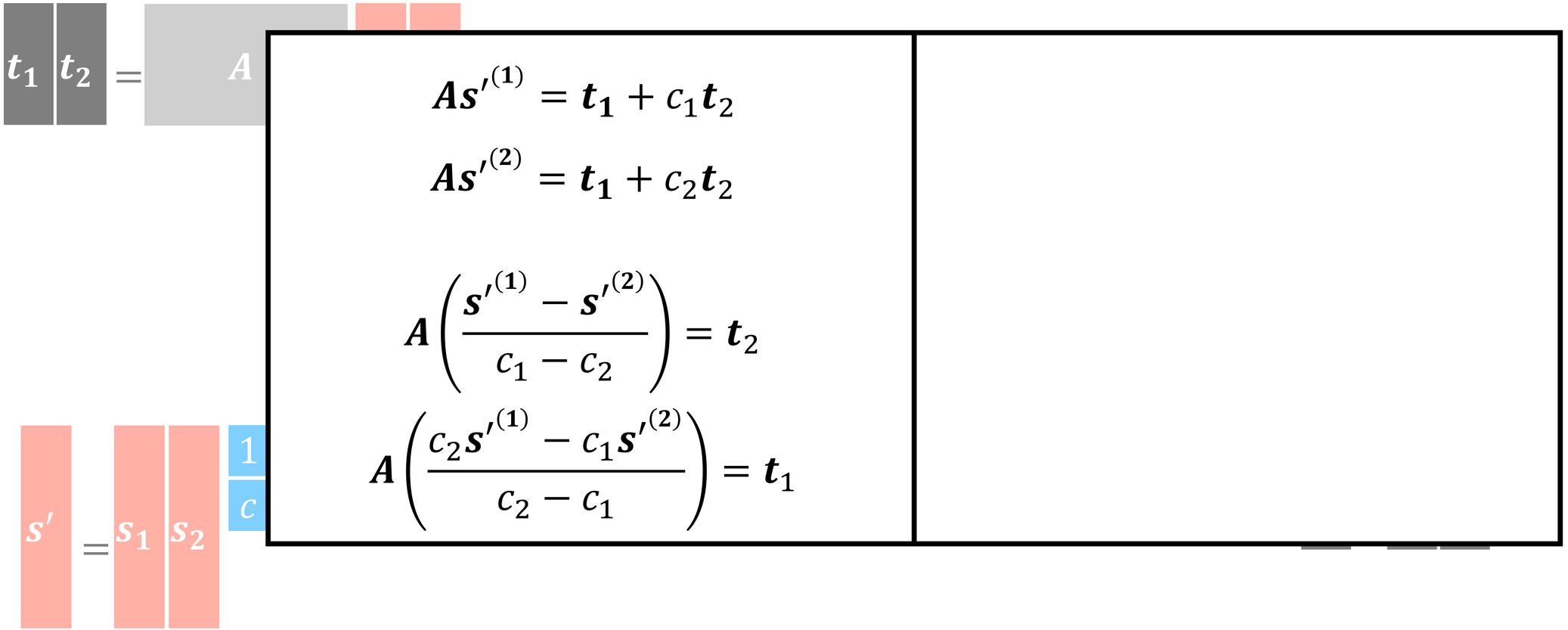
Knowledge soundness via special soundness: $c_1 \neq c_2$



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

Lova, take 1

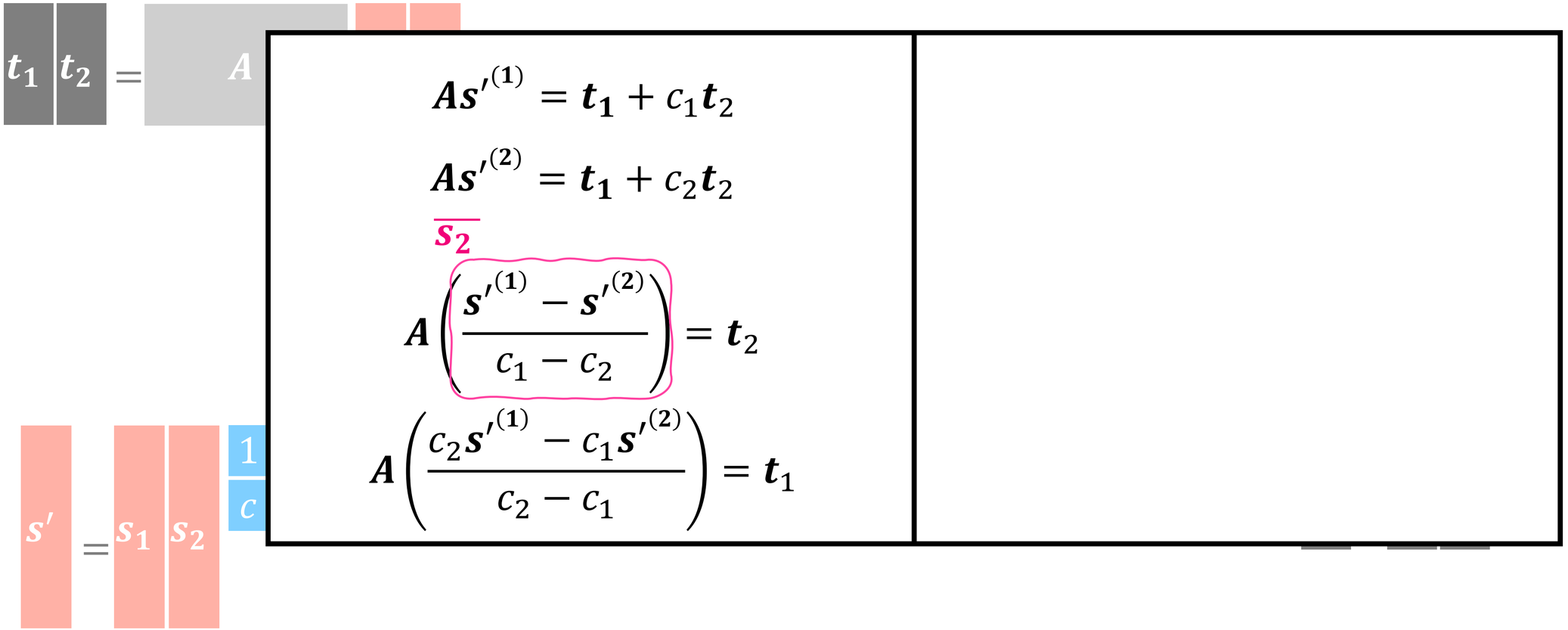
Knowledge soundness via special soundness: $c_1 \neq c_2$



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

Lova, take 1

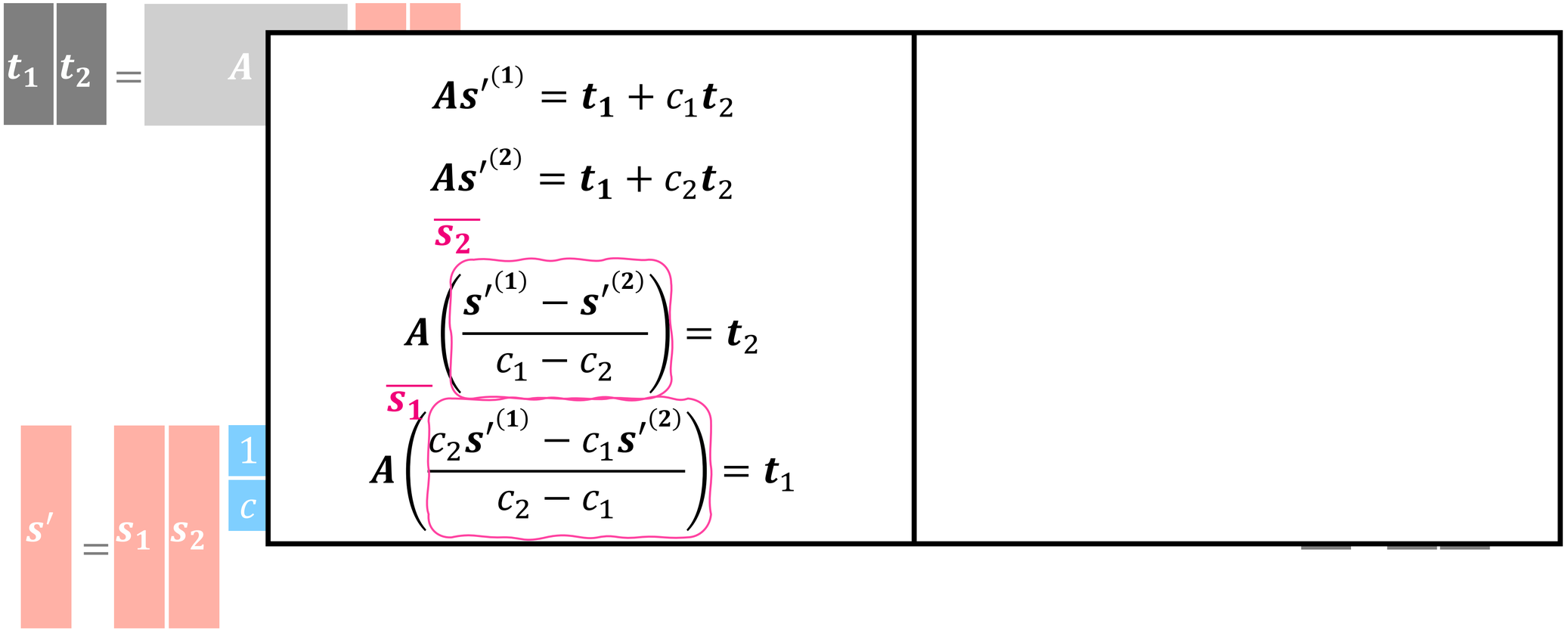
Knowledge soundness via special soundness: $c_1 \neq c_2$



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

Lova, take 1

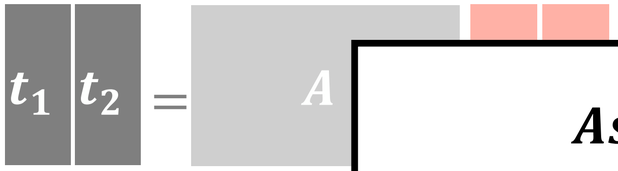
Knowledge soundness via special soundness: $c_1 \neq c_2$



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

Lova, take 1

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



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

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

$\overline{\boldsymbol{s_2}}$

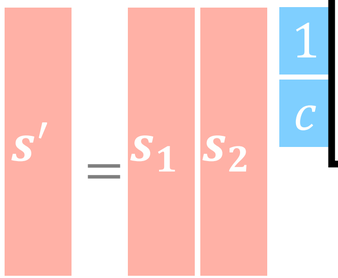
$$\boldsymbol{A}\left(\frac{\boldsymbol{s'^{(1)}} - \boldsymbol{s'^{(2)}}}{c_1 - c_2}\right) = \boldsymbol{t_2}$$

$\overline{\boldsymbol{s_1}}$

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

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

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



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

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 $R = \{(\boldsymbol{t} \in \mathbb{Z}_q^h, \boldsymbol{s} \in \mathbb{Z}_q^n) | \boldsymbol{t} = \mathbf{A}\boldsymbol{s} \ (mod\ q) \wedge \| \ \boldsymbol{s} \ \| \leq \beta\}$

Prover $(\boldsymbol{t_j}; \boldsymbol{s_j})$

Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$

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

Prover $(\boldsymbol{t_j}; \boldsymbol{s_j})$

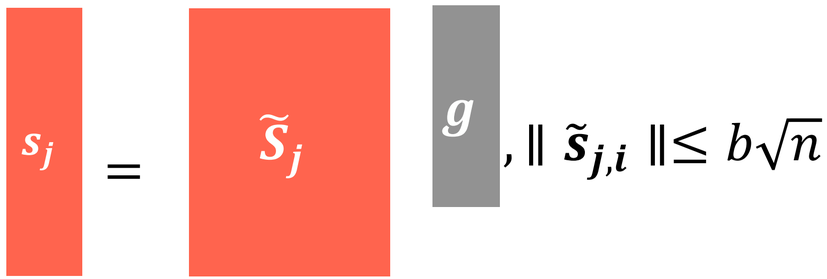
Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$

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

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

Prover $(\boldsymbol{t_j}; \boldsymbol{s_j})$

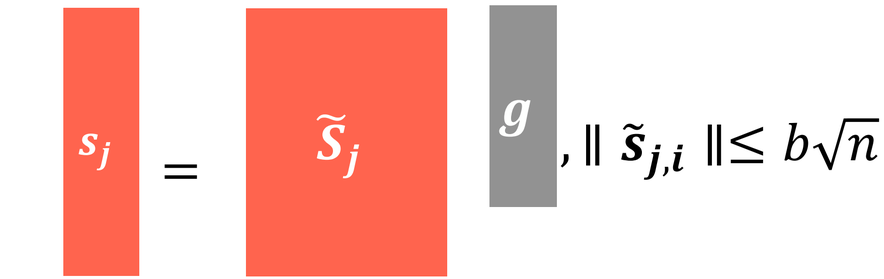
Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$

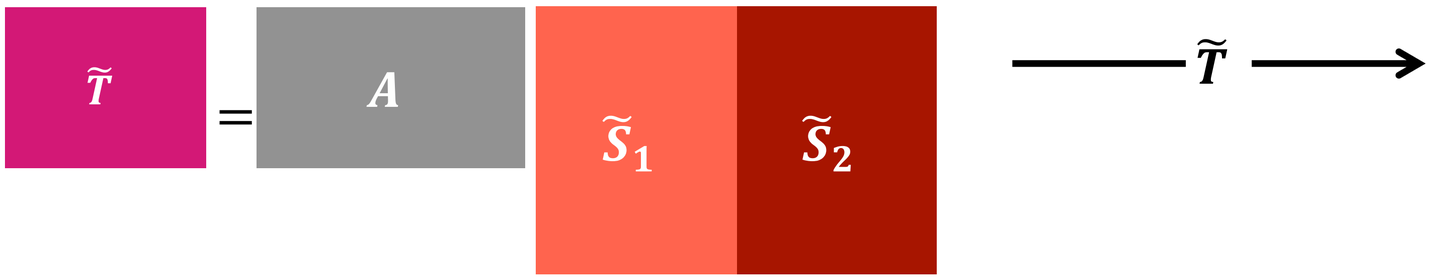


Lova, take 2 $R = \{(\boldsymbol{t} \in \mathbb{Z}_q^h, \boldsymbol{s} \in \mathbb{Z}_q^n) | \boldsymbol{t} = \mathbf{A}\boldsymbol{s} \ (mod\ q) \wedge \| \boldsymbol{s} \| \leq \beta\}$

Prover $(\boldsymbol{t_j}; \boldsymbol{s_j})$

Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$



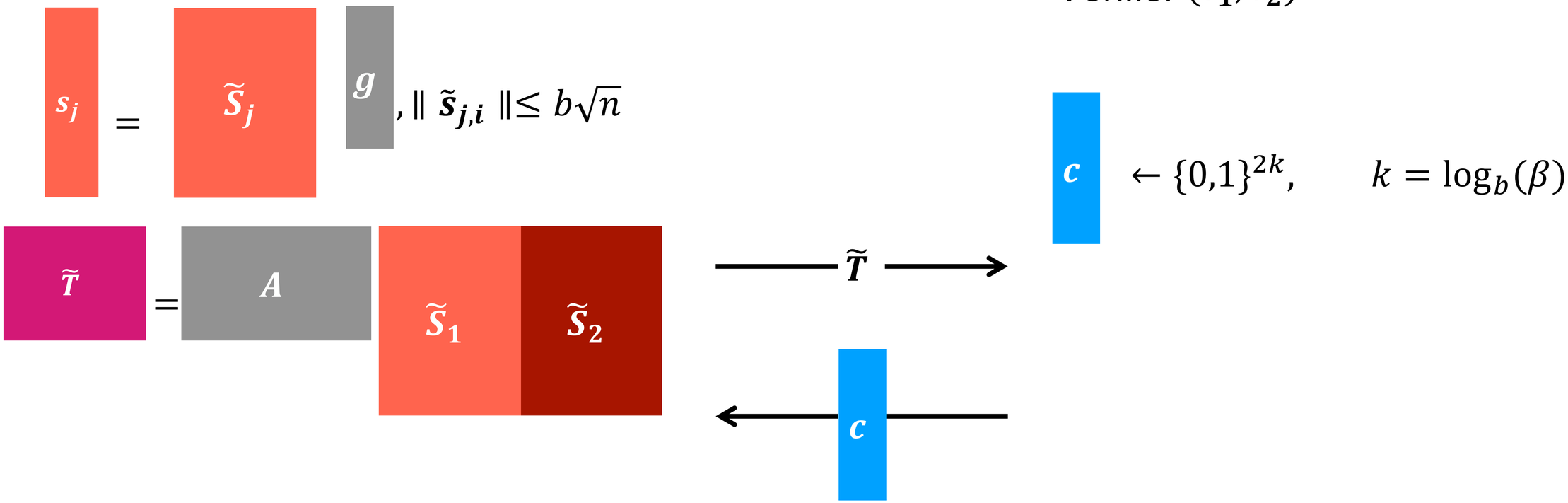


$\longrightarrow \widetilde{\boldsymbol{T}} \longrightarrow$

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

Prover $(\boldsymbol{t_j}; \boldsymbol{s_j})$

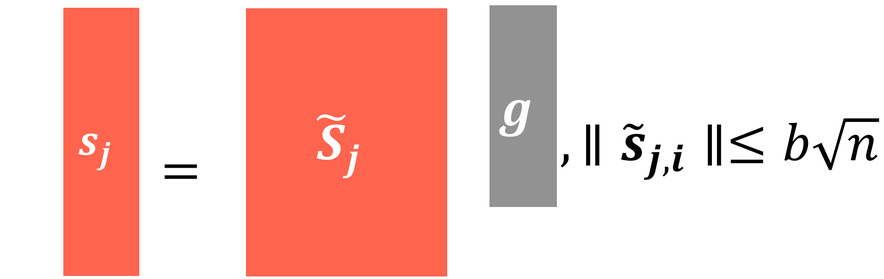
Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$

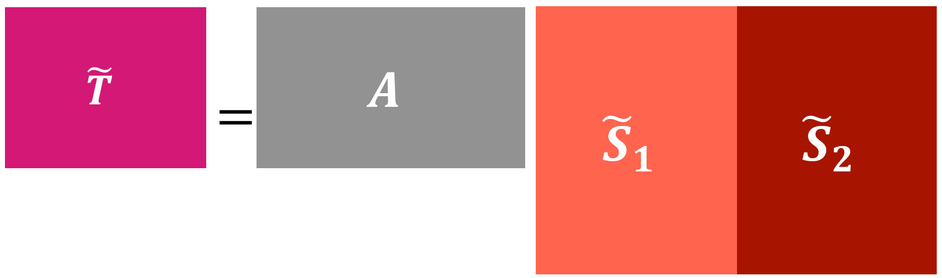


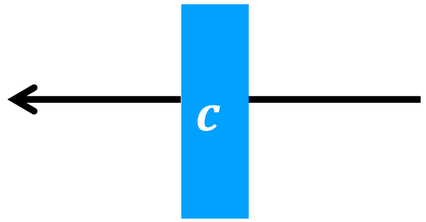
Lova, take 2 $R = \{(\boldsymbol{t} \in \mathbb{Z}_q^h, \boldsymbol{s} \in \mathbb{Z}_q^n) | \boldsymbol{t} = \mathbf{A}\boldsymbol{s} \ (mod\ q) \wedge \| \boldsymbol{s} \| \leq \beta\}$

Prover $(\boldsymbol{t_j}; \boldsymbol{s_j})$

Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$





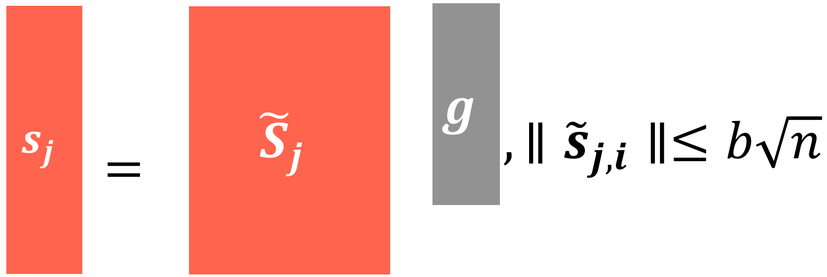


$\leftarrow \{0,1\}^{2k}, \qquad k = \log_b(\beta)$

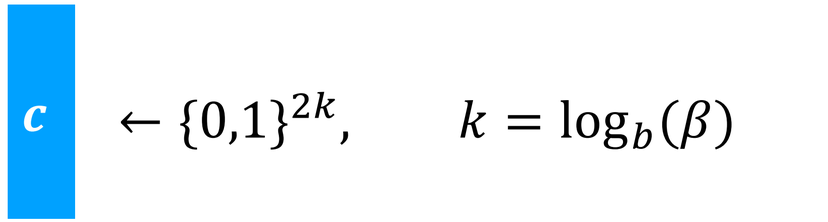
Output s' = $\widetilde{S}_1$ $\widetilde{S}_2$ c

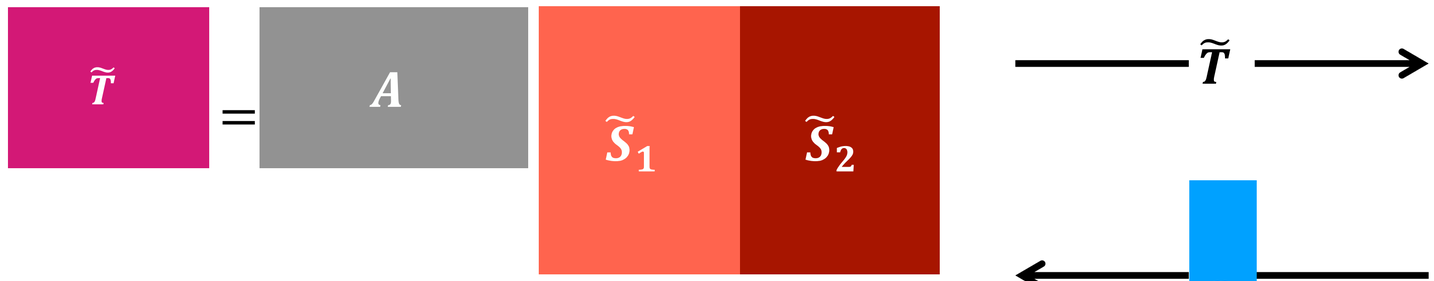
Lova, take 2 $R = \{(\boldsymbol{t} \in \mathbb{Z}_q^h, \boldsymbol{s} \in \mathbb{Z}_q^n) | \boldsymbol{t} = \mathbf{A}\boldsymbol{s} \ (mod\ q) \wedge \| \boldsymbol{s} \| \leq \beta\}$

Prover $(\boldsymbol{t_j}; \boldsymbol{s_j})$

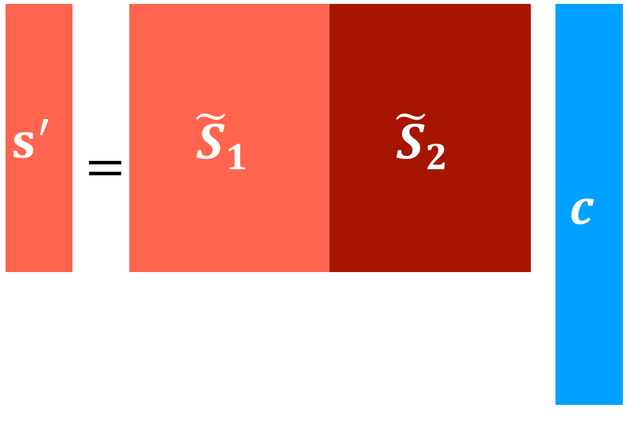


Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$



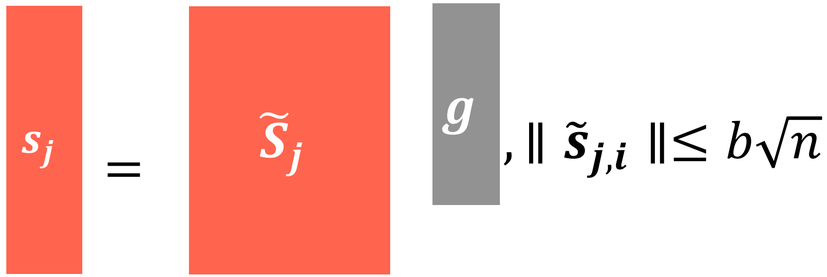


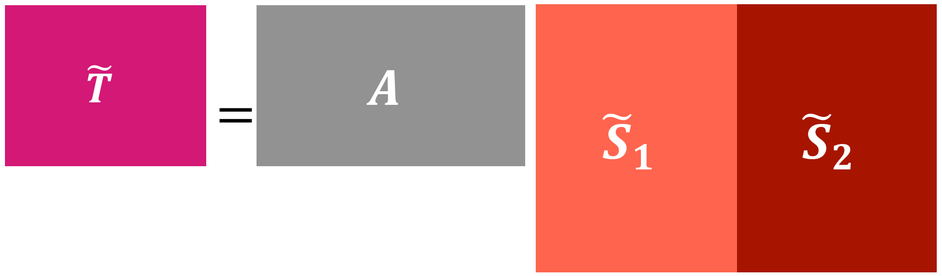
Check 

Output 

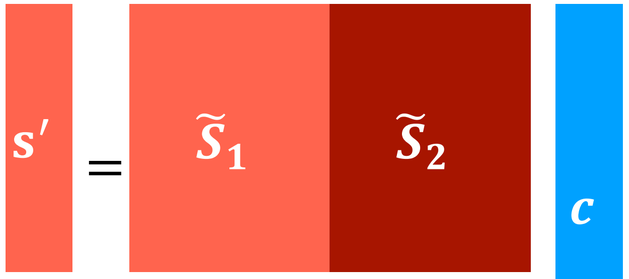
Lova, take 2 $R = \{(\boldsymbol{t} \in \mathbb{Z}_q^h, \boldsymbol{s} \in \mathbb{Z}_q^n) | \boldsymbol{t} = \mathbf{A}\boldsymbol{s} \ (mod\ q) \wedge \| \boldsymbol{s} \| \leq \beta\}$

Prover $(\boldsymbol{t_j}; \boldsymbol{s_j})$



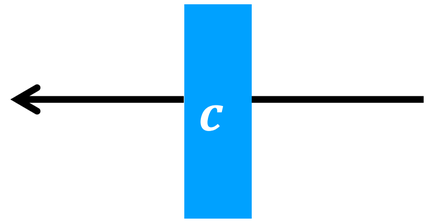


Output



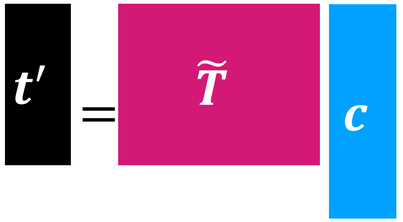
Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$

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



Check

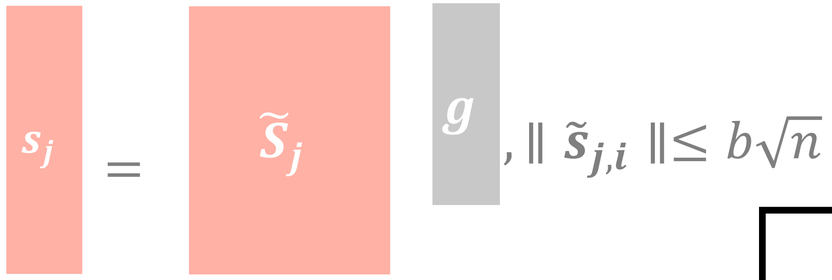
Output

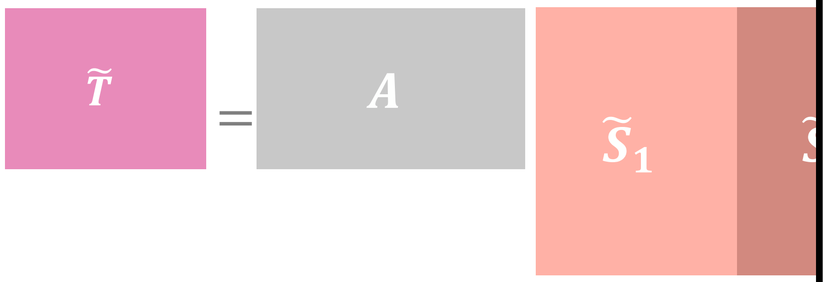


Lova, take 2

$$R = \{(\boldsymbol{t} \in \mathbb{Z}_q^h, \boldsymbol{s} \in \mathbb{Z}_q^n) | \boldsymbol{t} = \mathbf{A}\boldsymbol{s} \ (mod\ q) \wedge \| \boldsymbol{s} \| \leq \beta\}$$

Prover $(\boldsymbol{t_j}; \boldsymbol{s_j})$





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

$$\leq \beta$$

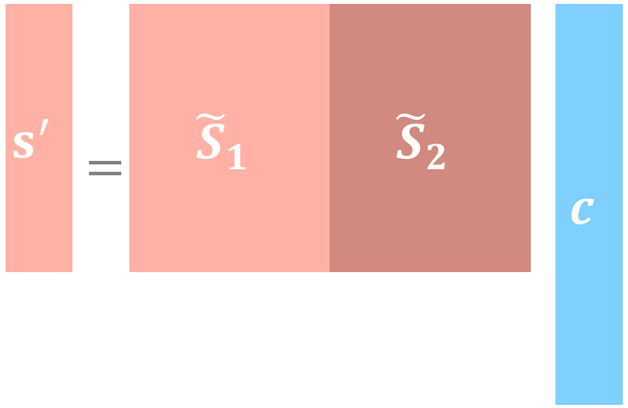
for a suitable choice of parameters

Verifier $(\boldsymbol{t_1}, \boldsymbol{t_2})$

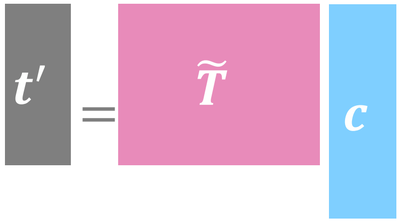
$\leftarrow \{0,1\}^{2k}$, $k = \log_b(\beta)$

Check

Output



Output



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

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

Soundness error

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

parallel repetition
+ clever analysis!

Extractor Norm Growth

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

Lova, take 3

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

Prover $(\boldsymbol{T_1}, \boldsymbol{T_2}; \boldsymbol{S_1}, \boldsymbol{S_2})$

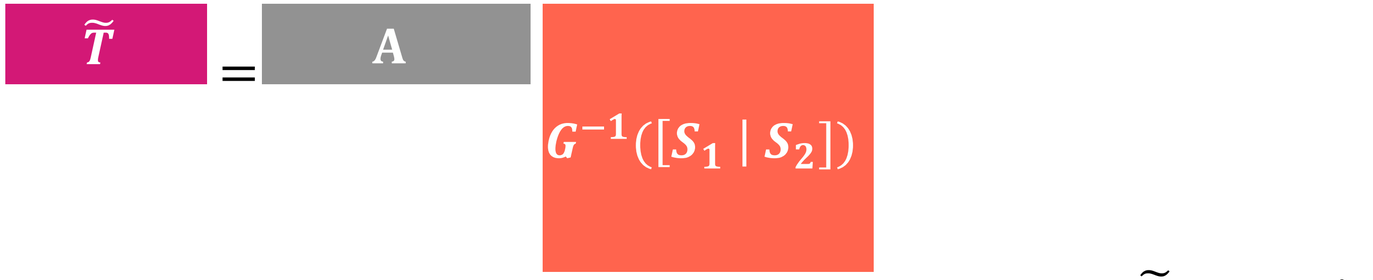
Verifier $(\boldsymbol{T_1}, \boldsymbol{T_2})$

Lova, take 3

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

Prover $(\boldsymbol{T_1}, \boldsymbol{T_2}; \boldsymbol{S_1}, \boldsymbol{S_2})$

Verifier $(\boldsymbol{T_1}, \boldsymbol{T_2})$

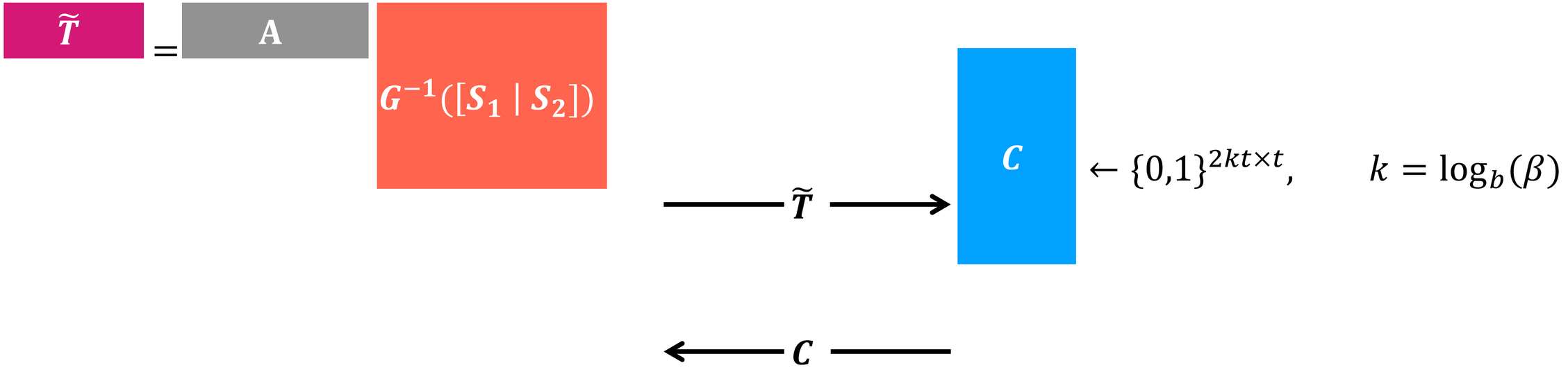


Lova, take 3

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

Prover $(\boldsymbol{T_1}, \boldsymbol{T_2}; \boldsymbol{S_1}, \boldsymbol{S_2})$

Verifier $(\boldsymbol{T_1}, \boldsymbol{T_2})$

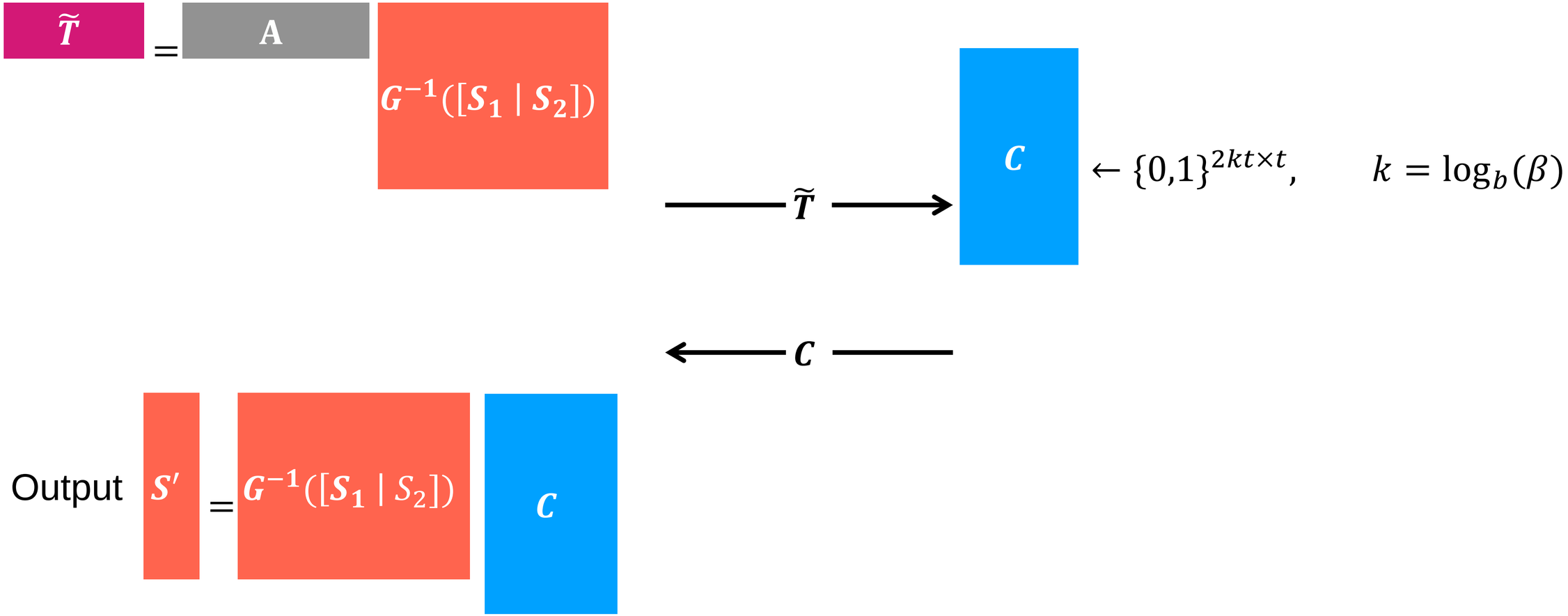


Lova, take 3

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

Prover $(\boldsymbol{T_1}, \boldsymbol{T_2}; \boldsymbol{S_1}, \boldsymbol{S_2})$

Verifier $(\boldsymbol{T_1}, \boldsymbol{T_2})$

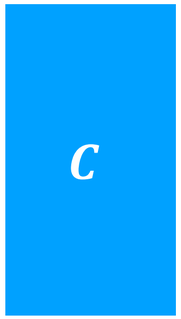


Lova, take 3

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

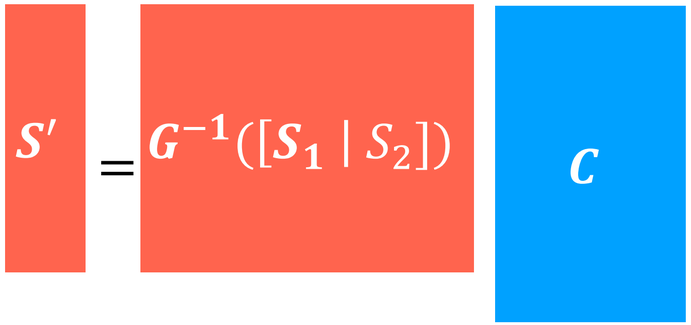
Prover $(\boldsymbol{T_1}, \boldsymbol{T_2}; \boldsymbol{S_1}, \boldsymbol{S_2})$

Verifier $(\boldsymbol{T_1}, \boldsymbol{T_2})$



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

Check 

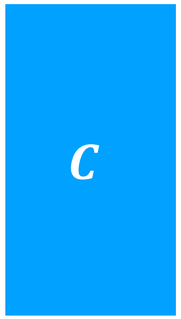
Output 

Lova, take 3

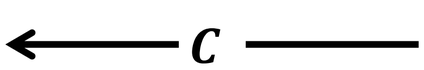
$$R = \{(\boldsymbol{T} \in \mathbb{Z}_q^{h \times t}, \boldsymbol{S} \in \mathbb{Z}_q^{n \times t}) | \boldsymbol{T} = \boldsymbol{AS} \ (mod\ q) \wedge \| \mathbf{S}_{:,i} \| \leq \beta\}$$

Prover $(\boldsymbol{T_1}, \boldsymbol{T_2}; \boldsymbol{S_1}, \boldsymbol{S_2})$

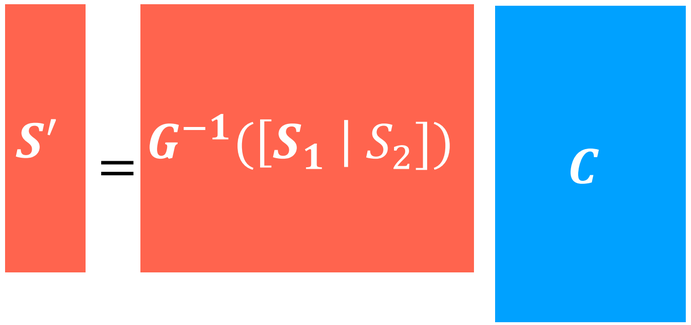
Verifier $(\boldsymbol{T_1}, \boldsymbol{T_2})$

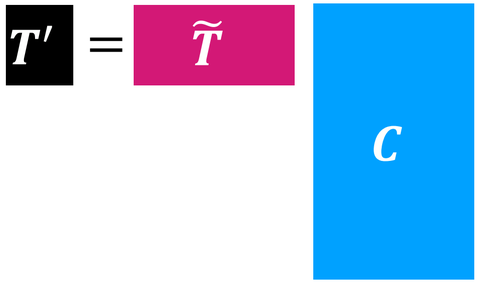


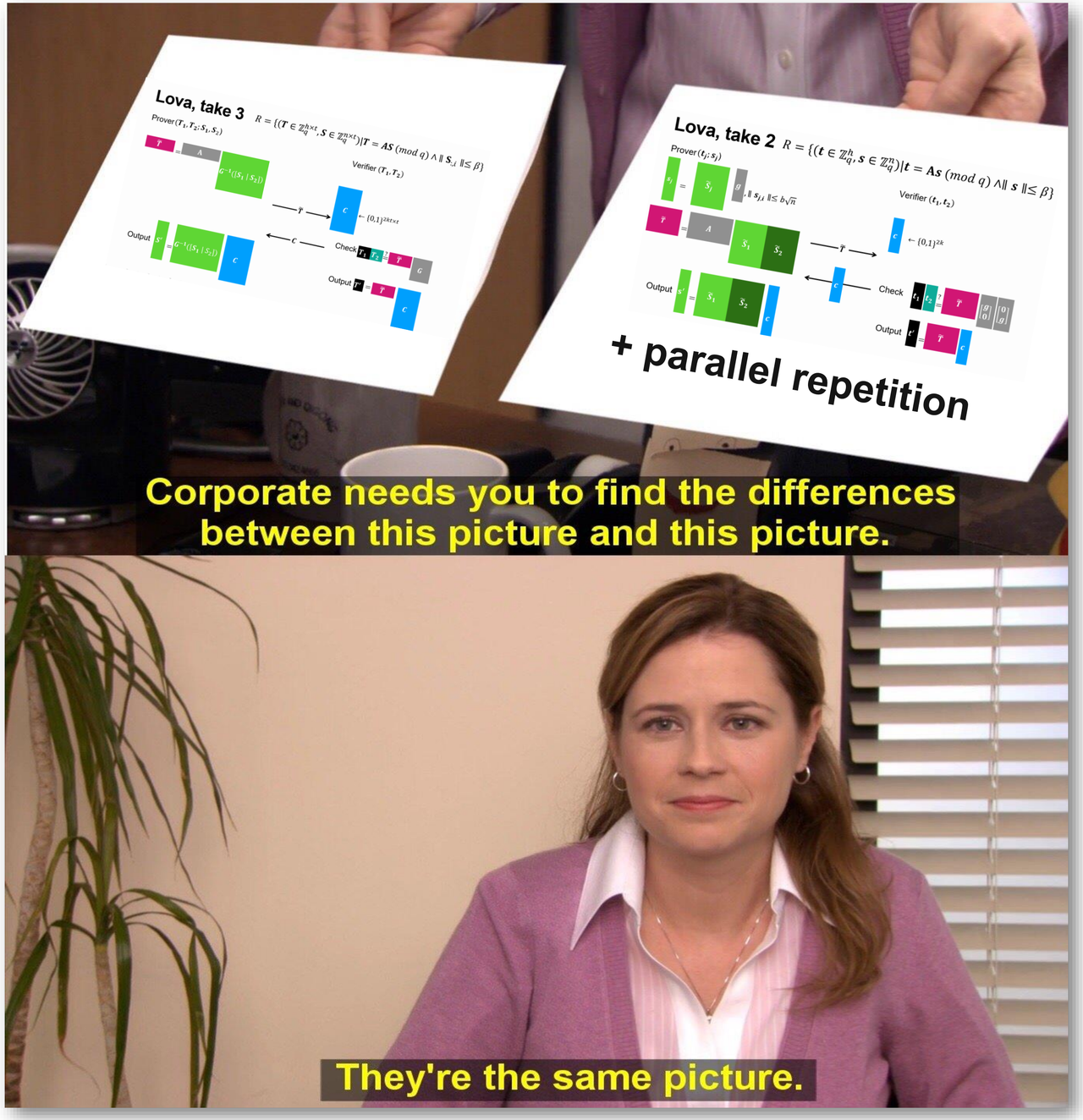
$\leftarrow \{0,1\}^{2kt \times t}, \qquad k = \log_b(\beta)$



Check 

Output 

Output 


Lova, take 3
Lova, take 2
+ 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 $\boldsymbol{s}$ satisfies $|\langle \boldsymbol{s}, \boldsymbol{s} \rangle \, mod \, q| \leq \beta^2$ and $||\boldsymbol{s}|| \ll q$ then we must have

$$||\boldsymbol{s}|| \leq \beta.$$

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

New relation

$$R^{\mathrm{SIS}}_{q,\beta,t} = \left\{ \left(\mathbf{T} \in \mathbb{Z}_q^{h \times t}, \mathbf{S} \in \mathbb{Z}_q^{n \times t} \right) \;\middle|\; \begin{array}{r} \mathbf{T} = \mathbf{AS} \mod q \\ \wedge \|\mathbf{S}_{:,i}\| \leq \beta \end{array} \right\}$$

$$R^{\mathrm{SIS}}_{q,\beta,t} = \left\{ \left(\left(\mathbf{T} \in \mathbb{Z}_q^{h \times t}, \mathbf{D} \in \mathbb{Z}^{t \times t} \right), \mathbf{S} \in \mathbb{Z}_q^{n \times t} \right) \;\middle|\; \begin{array}{r} \mathbf{T} = \mathbf{AS} \mod q \\ \wedge \mathbf{D} = \mathbf{S}^{\top}\mathbf{S} \\ \wedge \|\mathbf{D}_{i,i}\| \leq \beta^2 \end{array} \right\}$$

Ideas for proving exact norm bounds

Observation 2

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

- Denote $\boldsymbol{S^* \coloneqq G^{-1}([S_1|S_2])}$. Then,
  - $\begin{bmatrix} \boldsymbol{D_1} & :) \\ :) & \boldsymbol{D_2} \end{bmatrix} = \boldsymbol{G^\top S^{*\top} S^* G}$.
    - Hence, reveal $\boldsymbol{\widetilde{D} \coloneqq S^{*\top} S^*}$.

Lova, take 4 (final)

$$R^{\mathrm{SIS}}_{q,\beta,t} = \left\{ \left(\left(\mathbf{T} \in \mathbb{Z}_q^{h \times t}, \mathbf{D} \in \mathbb{Z}^{t \times t} \right), \mathbf{S} \in \mathbb{Z}_q^{n \times t} \right) \;\middle|\; \begin{array}{r} \mathbf{T} = \mathbf{AS} \mod q \\ \wedge\, \mathbf{D} = \mathbf{S}^{\mathsf{T}}\mathbf{S} \\ \wedge\, \|\mathbf{D}_{i,i}\| \le \beta^2 \end{array} \right\}$$

Prover $(\boldsymbol{T_j}, \boldsymbol{D_j}; \boldsymbol{S_j})$

Verifier $(\boldsymbol{T_0}, \mathbf{T_1}, \boldsymbol{D_0}, \mathbf{D_1})$

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

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

Check $\boldsymbol{T_1}\boldsymbol{T_2} \stackrel{?}{=} \widetilde{\boldsymbol{T}}\, \boldsymbol{G} \mod q$

$\widetilde{\boldsymbol{T}}$ →

← $\mathbf{C}$

Output $\boldsymbol{T'} = \widetilde{\boldsymbol{T}}\, \boldsymbol{C} \mod q$

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

Lova, take 4 (final)

$$R^{\mathrm{SIS}}_{q,\beta,t} = \left\{ \left(\left(\mathbf{T} \in \mathbb{Z}_q^{h \times t}, \mathbf{D} \in \mathbb{Z}^{t \times t} \right), \mathbf{S} \in \mathbb{Z}_q^{n \times t} \right) \;\middle|\; \begin{array}{l} \mathbf{T} = \mathbf{AS} \mod q \\ \wedge\, \mathbf{D} = \mathbf{S}^{\top}\mathbf{S} \\ \wedge\, \|\mathbf{D}_{i,i}\| \le \beta^2 \end{array} \right\}$$

Prover $(\boldsymbol{T_j}, \boldsymbol{D_j}; \boldsymbol{S_j})$

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

$\widetilde{\boldsymbol{D}} = G^{-1}([\boldsymbol{S_1}|\boldsymbol{S_2}])^{\top}\, G^{-1}([\boldsymbol{S_1}|\boldsymbol{S_2}])$

$\widetilde{\boldsymbol{T}}, \widetilde{\boldsymbol{D}} \longrightarrow$

:) :)

$\longleftarrow \mathbf{C}$

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

Verifier $(\boldsymbol{T_0}, \mathbf{T_1}, \boldsymbol{D_0}, \mathbf{D_1})$

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

Check $\boldsymbol{T_1}\boldsymbol{T_2} \stackrel{?}{=} \widetilde{\boldsymbol{T}}\, \boldsymbol{G} \mod q$

Output $\boldsymbol{T'} = \widetilde{\boldsymbol{T}}\, \boldsymbol{C} \mod q$

Lova, take 4 (final)

$$R^{\mathrm{SIS}}_{q,\beta,t} = \left\{ \left(\left(\mathbf{T} \in \mathbb{Z}_q^{h \times t}, \mathbf{D} \in \mathbb{Z}^{t \times t} \right), \mathbf{S} \in \mathbb{Z}_q^{n \times t} \right) \;\middle|\; \begin{array}{r} \mathbf{T} = \mathbf{AS} \mod q \\ \wedge\, \mathbf{D} = \mathbf{S}^{\top}\mathbf{S} \\ \wedge\, \|\mathbf{D}_{i,i}\| \le \beta^2 \end{array} \right\}$$

Prover $(\boldsymbol{T_j}, \boldsymbol{D_j}; \boldsymbol{S_j})$

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

$\widetilde{\boldsymbol{D}} = G^{-1}([S_1|S_2])^{\top}\, G^{-1}([S_1|S_2])$

$\widetilde{\boldsymbol{T}}, \widetilde{\boldsymbol{D}} \longrightarrow$

:) :)

$\longleftarrow \mathbf{C}$

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

Verifier $(\boldsymbol{T_0}, \mathbf{T_1}, \boldsymbol{D_0}, \mathbf{D_1})$

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

Check $\boldsymbol{T_1}\, \boldsymbol{T_2} \overset{?}{=} \widetilde{\boldsymbol{T}}\, G \mod q$

Check $\begin{matrix} \boldsymbol{D_1} & :) \\ :) & \boldsymbol{D_2} \end{matrix} \overset{?}{=} G^{\top}\, \widetilde{\boldsymbol{D}}\, G$

Output $\boldsymbol{T'} = \widetilde{\boldsymbol{T}}\, \boldsymbol{C} \mod q$

Lova, take 4 (final)

$$R^{\mathrm{SIS}}_{q,\beta,t} = \left\{ \left(\left(\mathbf{T} \in \mathbb{Z}_q^{h \times t}, \mathbf{D} \in \mathbb{Z}^{t \times t} \right), \mathbf{S} \in \mathbb{Z}_q^{n \times t} \right) \;\middle|\; \begin{array}{r} \mathbf{T} = \mathbf{AS} \mod q \\ \wedge\, \mathbf{D} = \mathbf{S}^{\mathsf{T}}\mathbf{S} \\ \wedge\, \|\mathbf{D}_{i,i}\| \le \beta^2 \end{array} \right\}$$

Prover $(\boldsymbol{T_j}, \boldsymbol{D_j}; \boldsymbol{S_j})$

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

$\widetilde{\boldsymbol{D}} = \boldsymbol{G^{-1}([S_1|S_2])^{\mathsf{T}}}\; \boldsymbol{G^{-1}([S_1|S_2])}$

$\widetilde{\boldsymbol{T}}, \widetilde{\boldsymbol{D}} \longrightarrow$

:) :)

$\longleftarrow \mathbf{C}$

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

Verifier $(\boldsymbol{T_0}, \mathbf{T_1}, \boldsymbol{D_0}, \mathbf{D_1})$

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

Check $\boldsymbol{T_1}\, \boldsymbol{T_2} \overset{?}{=} \widetilde{\boldsymbol{T}}\; \boldsymbol{G} \mod q$

Check $\begin{matrix} \boldsymbol{D_1} & :) \\ :) & \boldsymbol{D_2} \end{matrix} \overset{?}{=} \boldsymbol{G^{\mathsf{T}}}\; \widetilde{\boldsymbol{D}}\; \boldsymbol{G}$

Output $\boldsymbol{T'} = \widetilde{\boldsymbol{T}}\; \boldsymbol{C} \mod q$

Output $\boldsymbol{D'} = \boldsymbol{C^{\mathsf{T}}}\; \widetilde{\boldsymbol{D}}\; \boldsymbol{C}$

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!