Aalto University
School of Science

RoK, Paper, SISsors
Toolkit for Lattice-based Succinct Arguments

Michael Klooß[1,2], Russell W. F. Lai[1], Ngoc Khanh Nguyen[2], and **Michał Osadnik**[1]

[1] Aalto University, Espoo, Finland
[2] ETH Zurich, Switzerland
[3] King's College London, United Kingdom

Lattice-Based Argument Systems

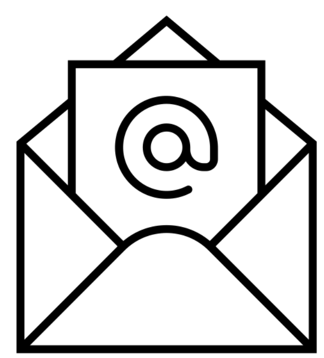
Goal: prove knowledge of vector **u** such that

$$\mathbf{A} \cdot \mathbf{u} = \mathbf{v} \bmod q \qquad 0 \leq ||\mathbf{u}|| \leq \beta$$

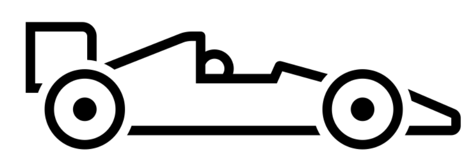
Various objectives:

Witness privacy

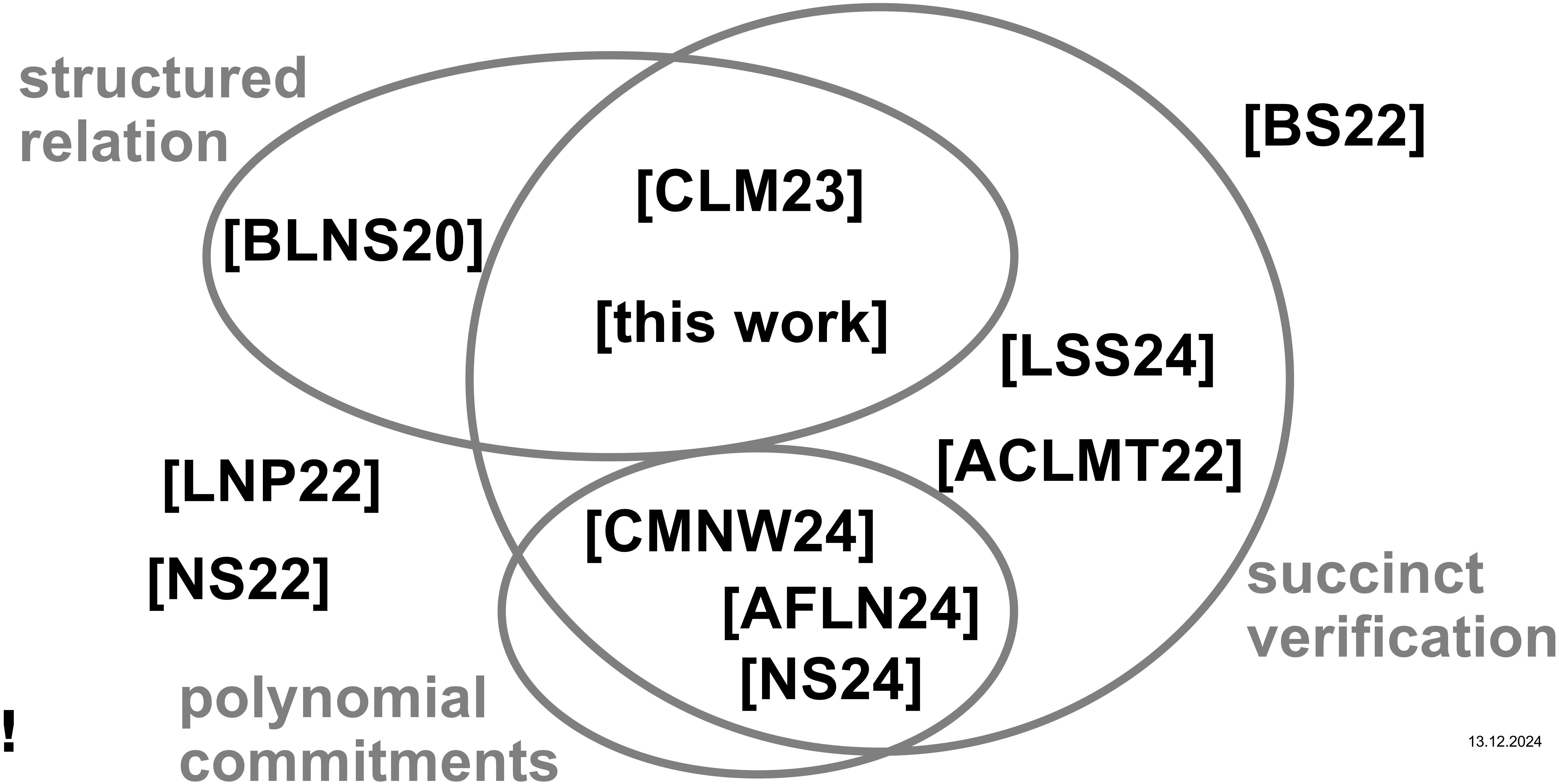
Communication succintness



Verifier runtime succintness



Lattice-Based Argument Systems (and polynomial commitments)



Folding-based protocols

High level idea:

Turn ”big” relation into a “smaller” one, verifiable succinctly in plain.

Problem:

The relation proved is “degraded”, i.e. too weak in many applications.

To be more precise, we need some background knowledge…

Reduction of Knowledge – definition

Reduction of Knowledge (RoK) is a pair of algorithms *P* and *V turning a relation* from Ξ_0 to Ξ_1.

- RoK is correct from Ξ_0 to Ξ_1 if reduces the correct input statement $\mathrm{stmt}_0 \in \Xi_0$ to $\mathrm{stmt}_1 \in \Xi_1$.
- RoK is relaxed knowledge sound from Ξ_0^{KS} to Ξ_1^{KS} if there exists an efficient extractor.

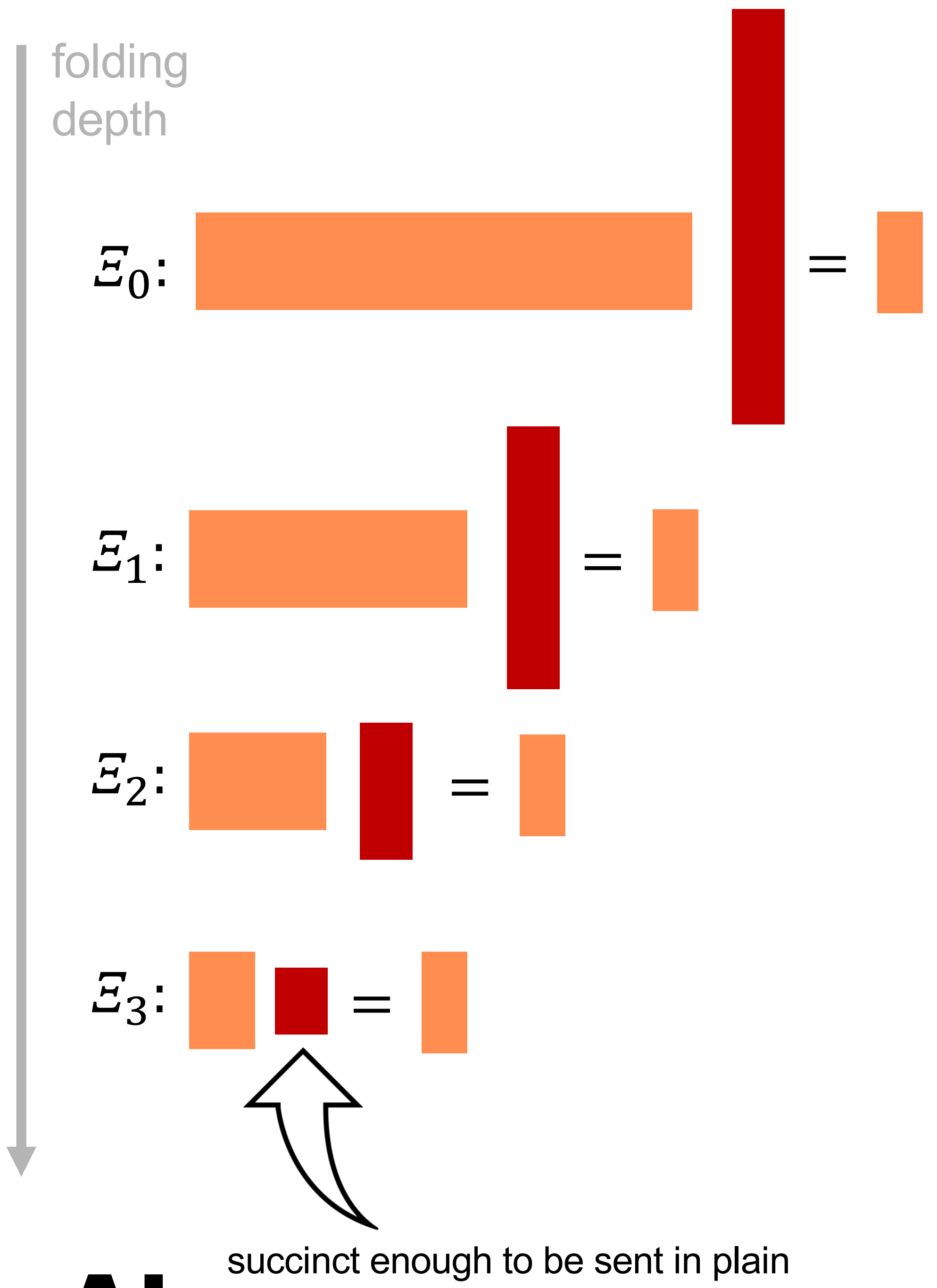
(extractor is an algorithm to "recover" the witness to Ξ_0^{KS} from Ξ_1^{KS} by "interacting" with the prover.)

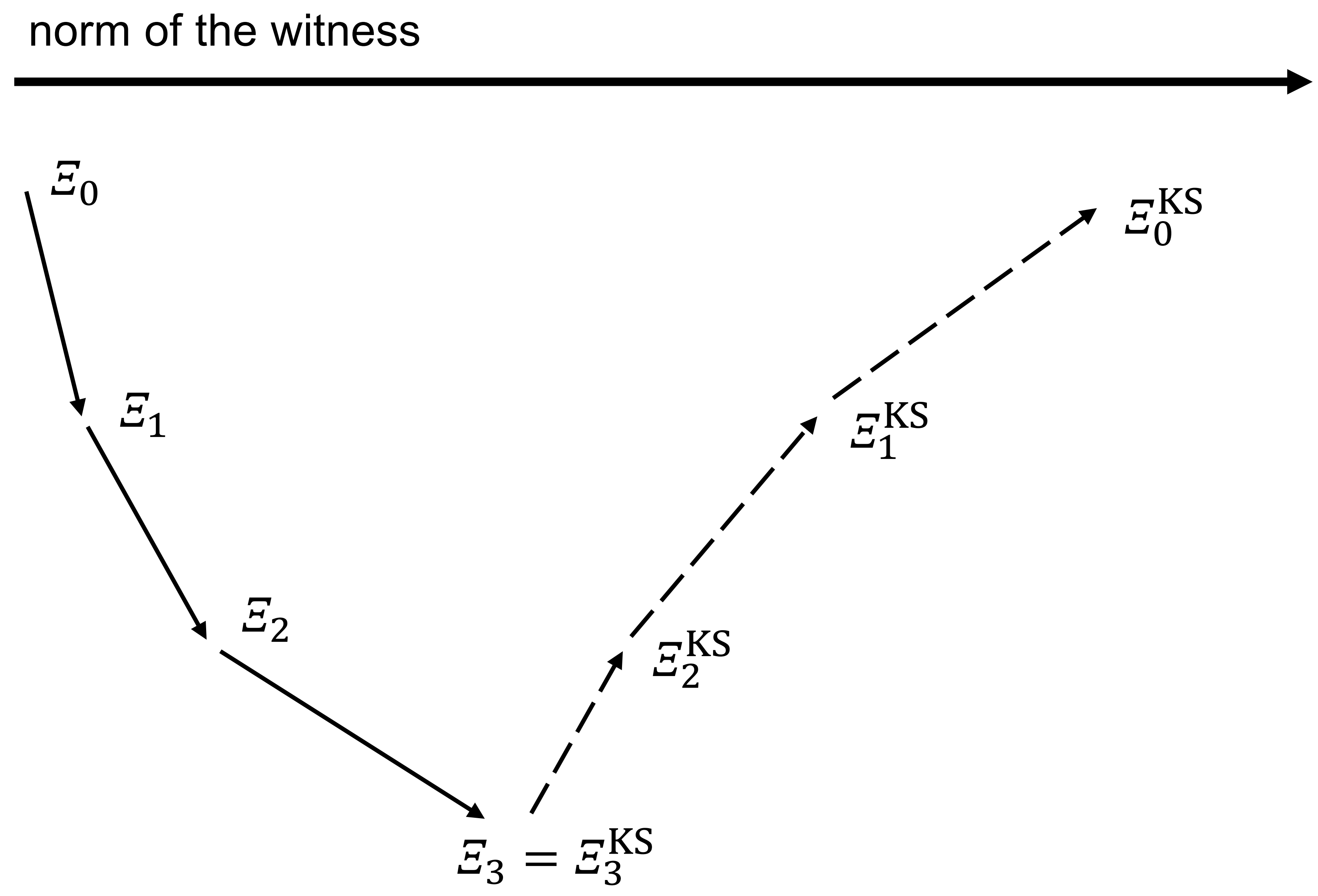
Traditionally, the properties correspond to correctness and extractability of an argument system.

Folding-based protocol are viewed as a series of RoKs.

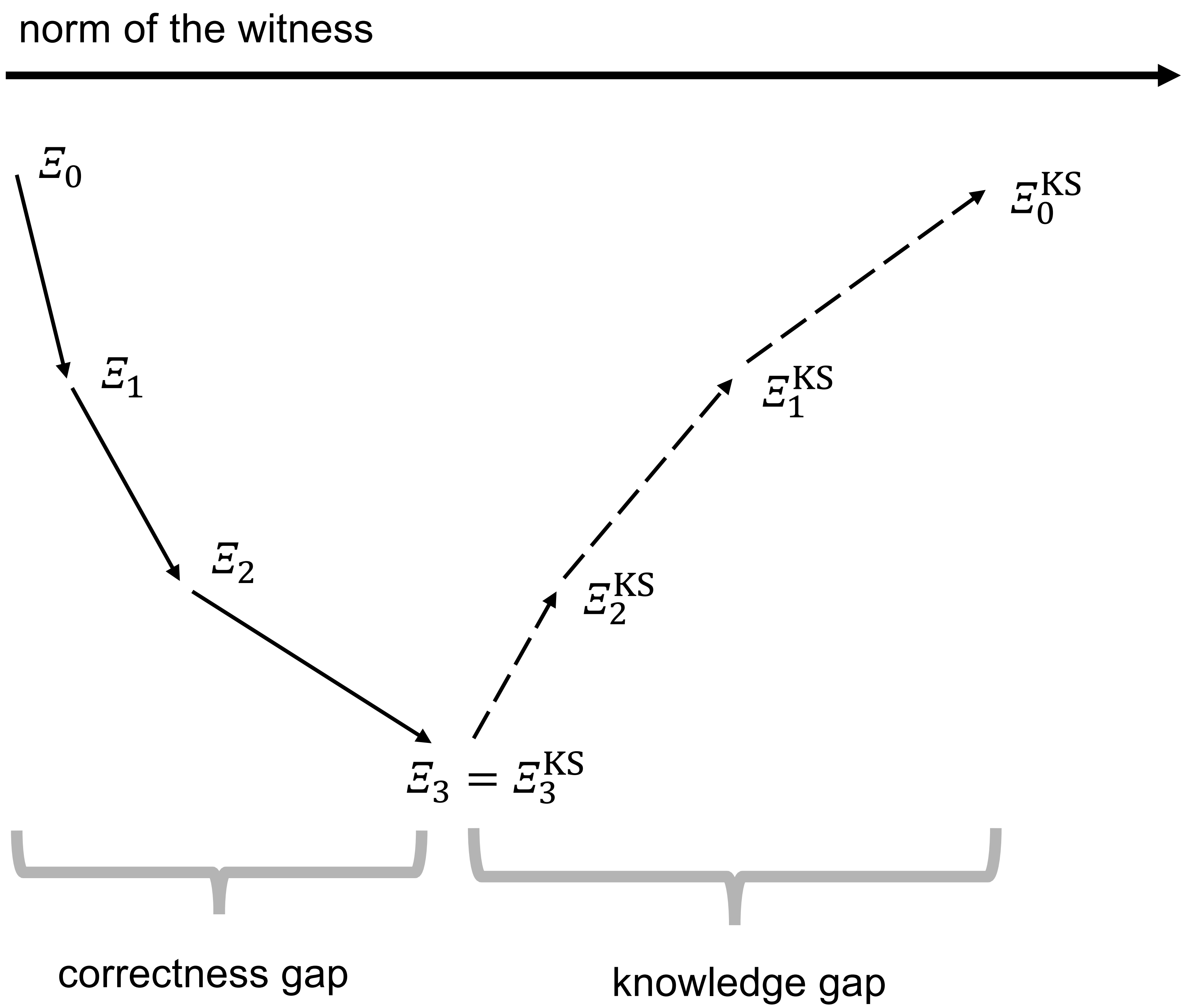
Issues: knowledge and soudness gaps

Example: proving SIS relation with [CLM23]





Issues: knowledge and soudness gaps



<u>Consequence:</u>
Instead of proving Ξ_0, we prove only a relaxed variant Ξ_0^{KS} with weaker norm guarantee.

Hence, Ξ_0^{KS} needs to be also ”meaningful”, e.g. hard, which impacts drastically the parameters selection.

Can we design a series of RoKs

eliminating correctness and knowledge gaps?

Contributions.

Topic of this presentation

We present:

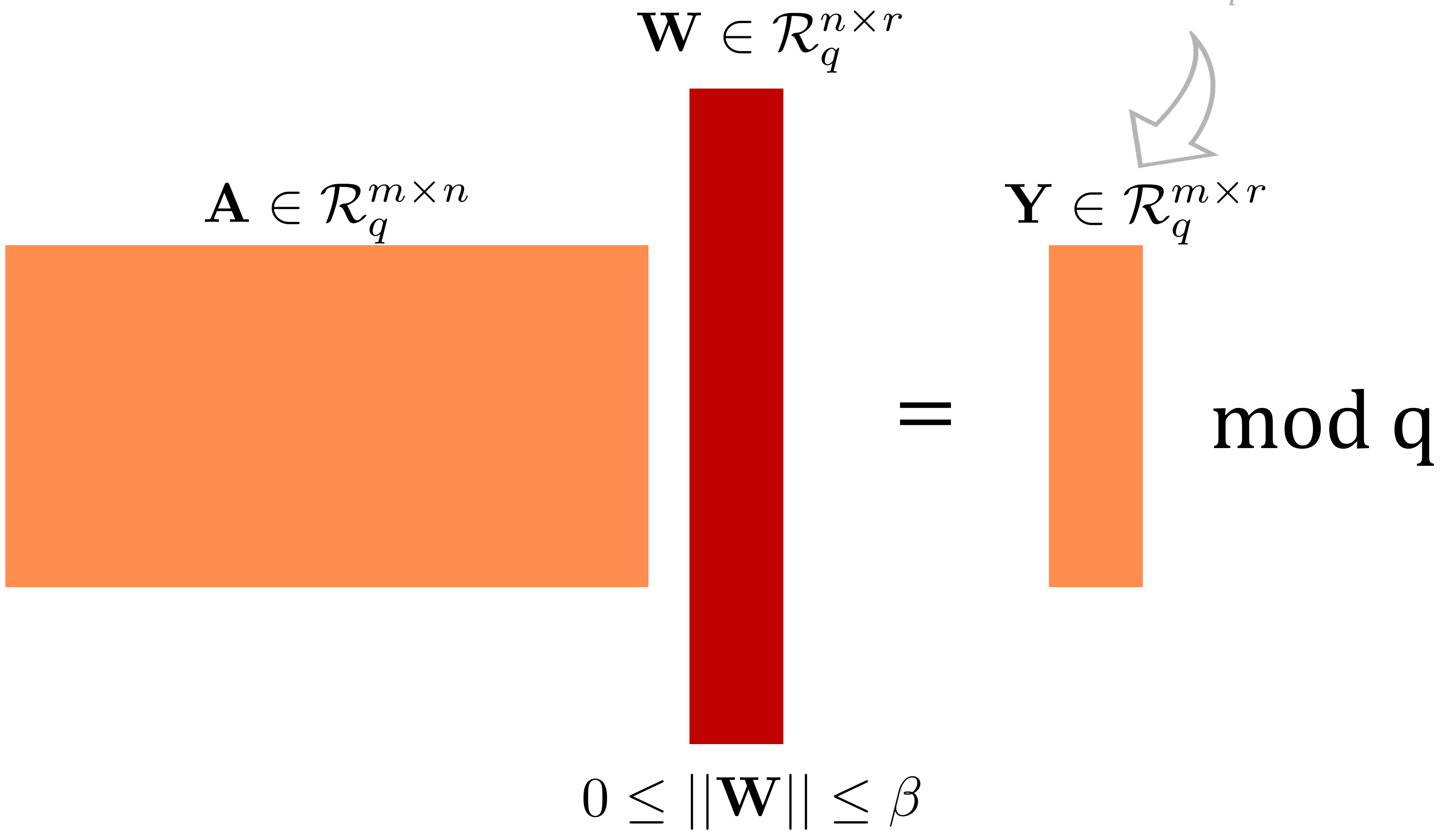
- Lattice-based series of RoKs with no correctness and soundness gap.
- New tools and techniques for lattice RoKs:
  - new subtractive sets
  - new inner-product embedding techniques
  - succinct consistency proof of CRT transform.

Principal relation Ξ

$(\mathbf{A}, \mathbf{Y}), \mathbf{W} \in \Xi$

statement witness

some cyclotomic ring,
but $\mathbb{Z}_q$ is enough for us.



Note: witness here is matrix

Principal relation Ξ

Furthermore,

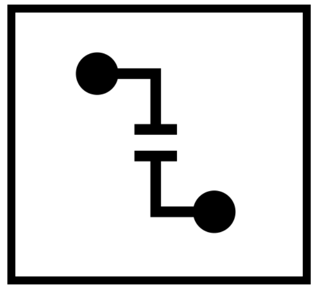
$$\mathbf{A} \in \mathcal{R}_q^{m \times n}$$

$$= \begin{pmatrix} \begin{pmatrix} a_0^{(0)} & a_1^{(0)} \end{pmatrix} \otimes \widetilde{\mathbf{A}}^{(0)} \\ \begin{pmatrix} a_0^{(1)} & a_1^{(1)} \end{pmatrix} \otimes \widetilde{\mathbf{A}}^{(1)} \\ \dots \end{pmatrix}$$

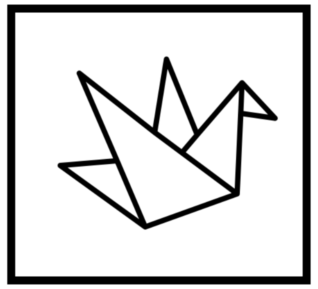
is “structured”, i.e. is row-tensor.

Four RoKs

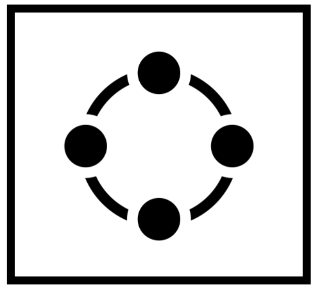
"Almost" folklore construction for reducing the witness size for structured relation.



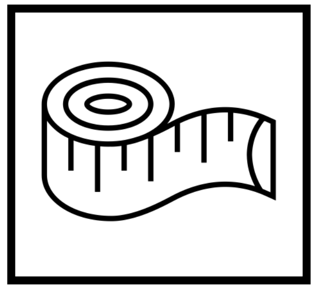
Split



Fold



Decomp

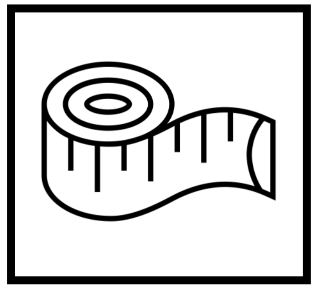


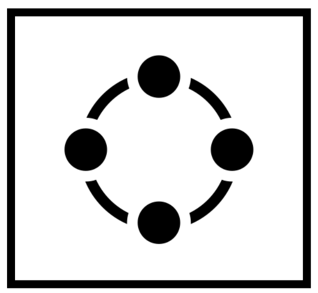
Norm-check

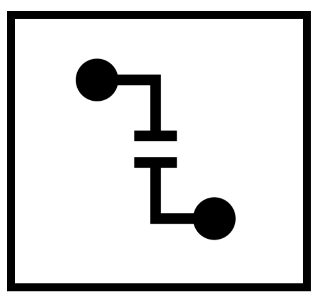
Standard decomposition with a radix, i.e. shink of the witness norm in the "correctness" direction.

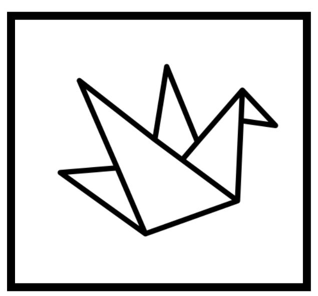
Intermediate opening to the norm of the witness acting as an "upgrade" of the norm in the "knowledge soundness" direction

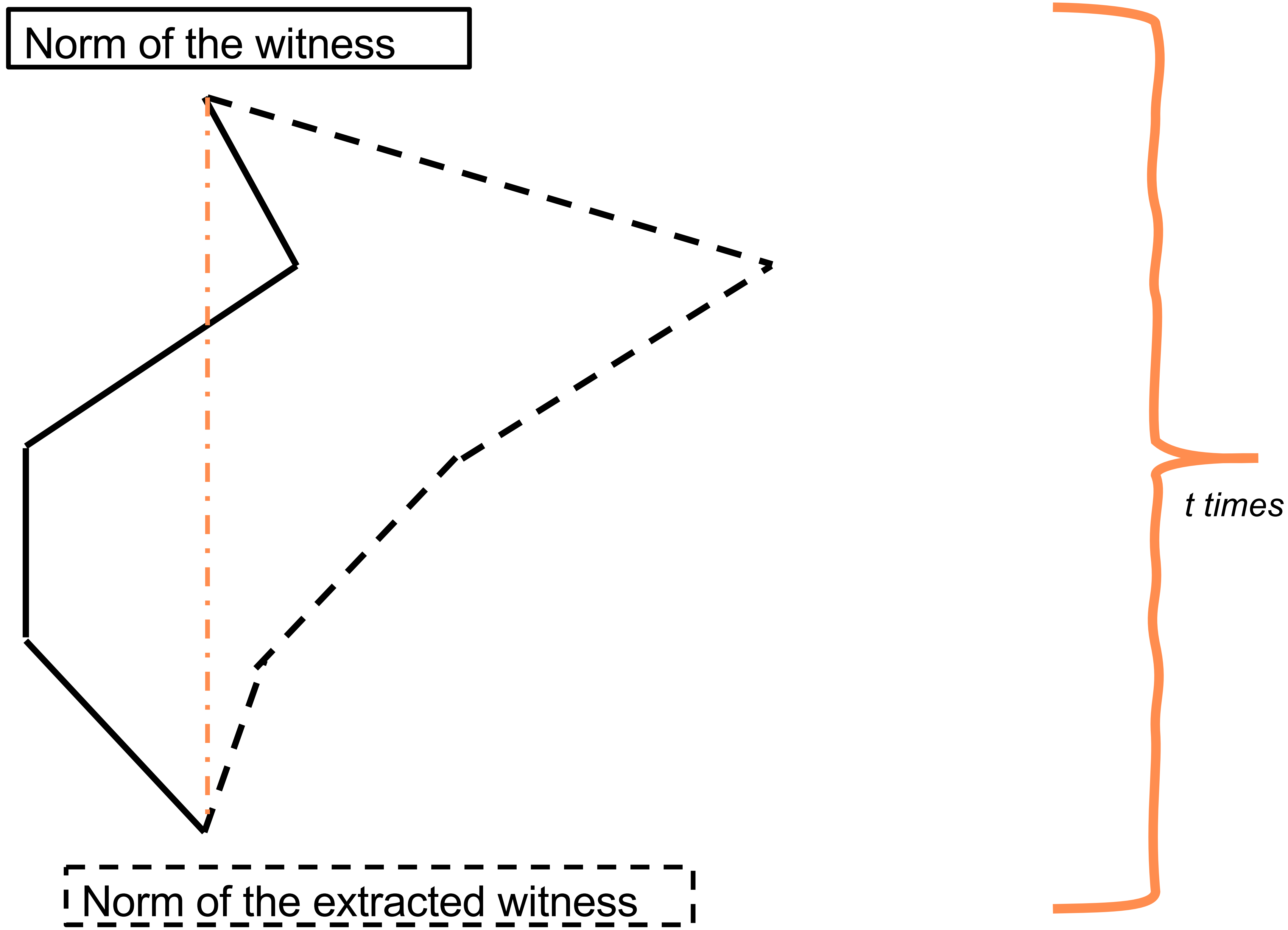
Combining RoKs


Norm-check

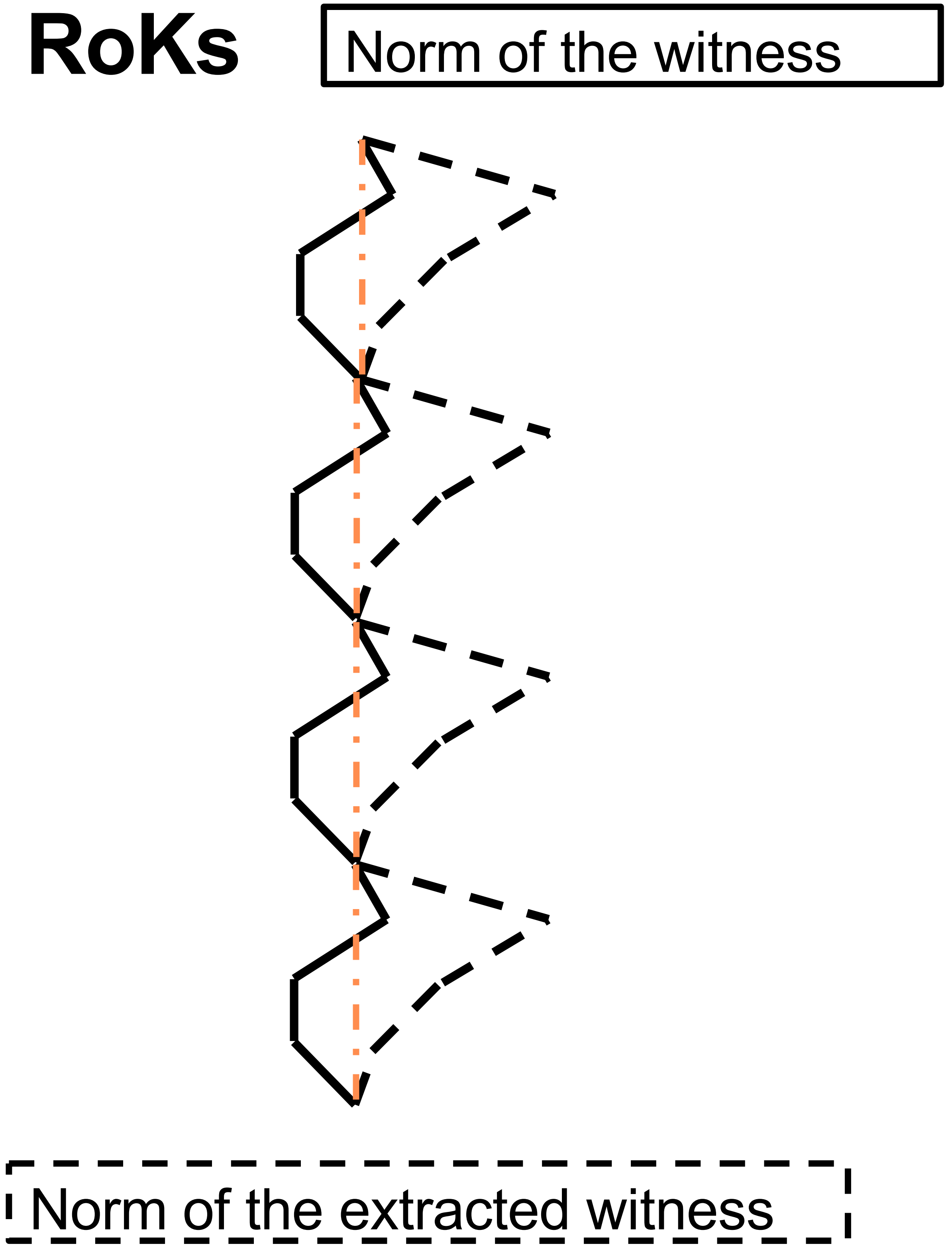

Decomp

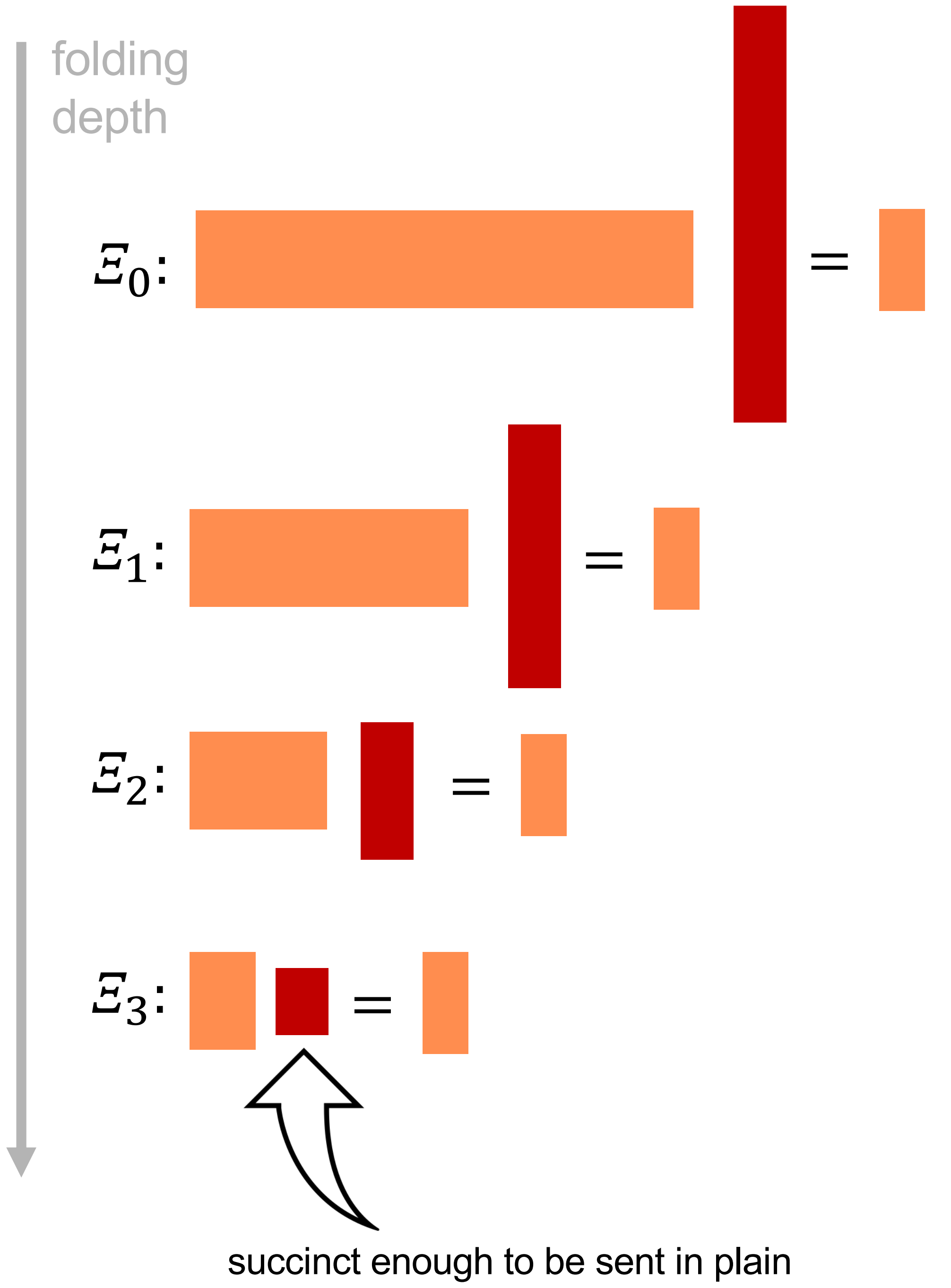

Split


Fold



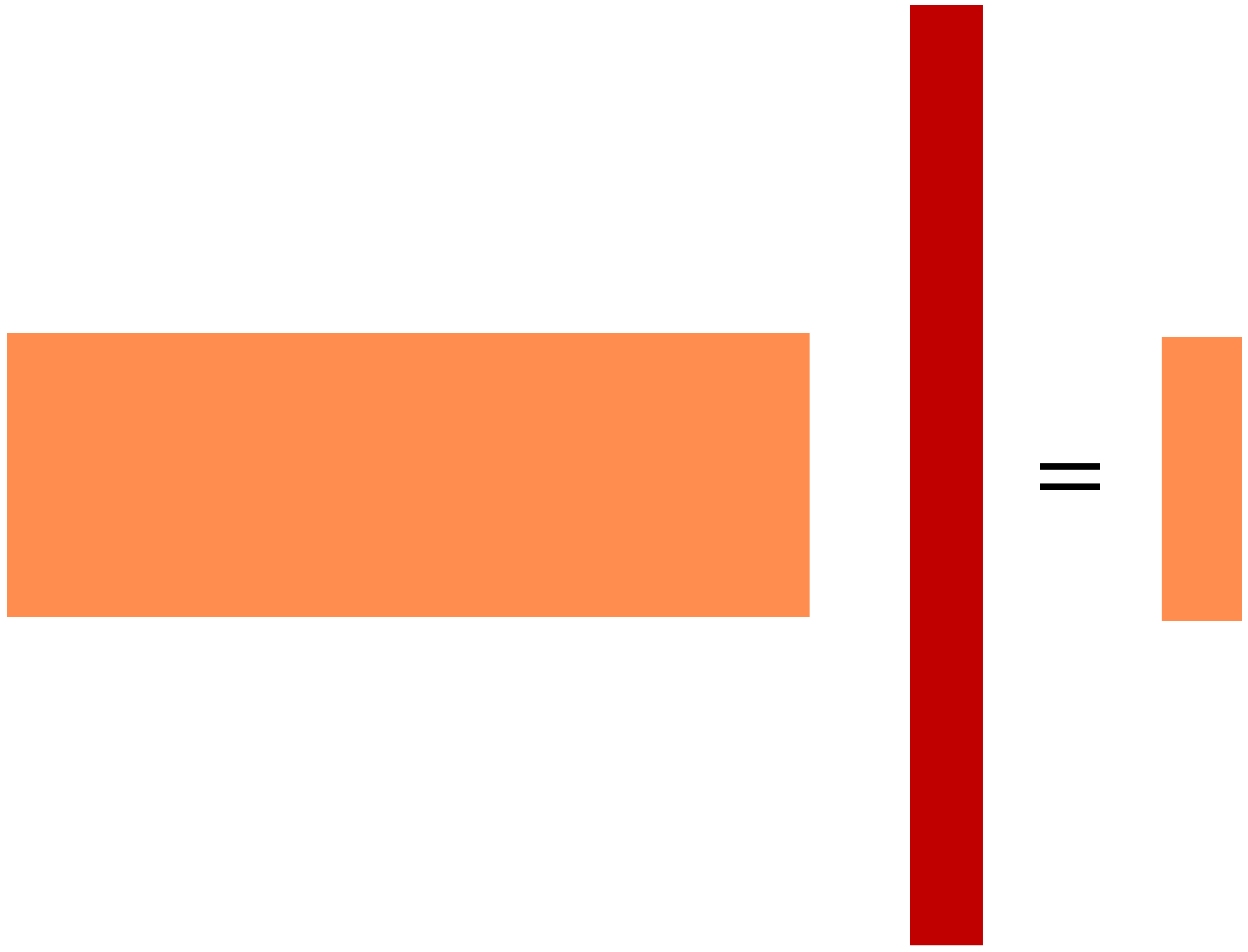
Combining RoKs





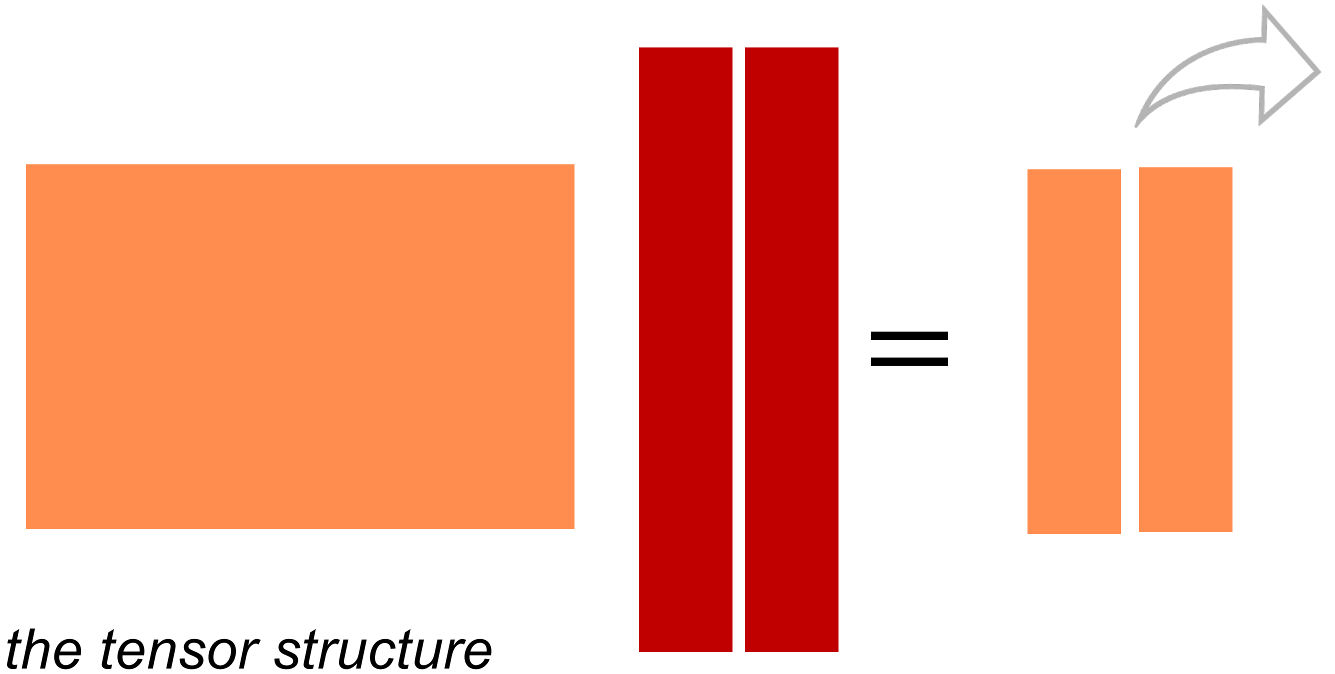
Split

RoK reduces Ξ_0 to Ξ_1*, rearranging the witness into smaller in height, but wider.*



Split

RoK reduces Ξ_0 to Ξ_1, rearranging the witness into smaller in height, but wider.



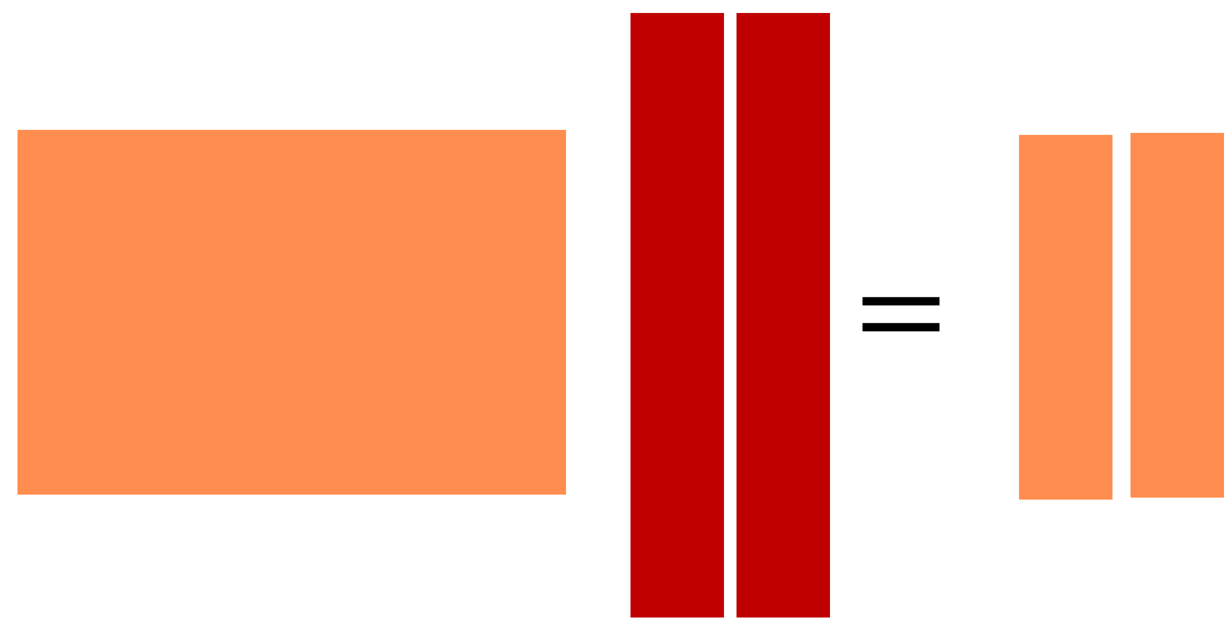
Sent to verifier and consistency check

possible due to the tensor structure

Correctness and knowledge soundness immediate – rearranging of the witness.

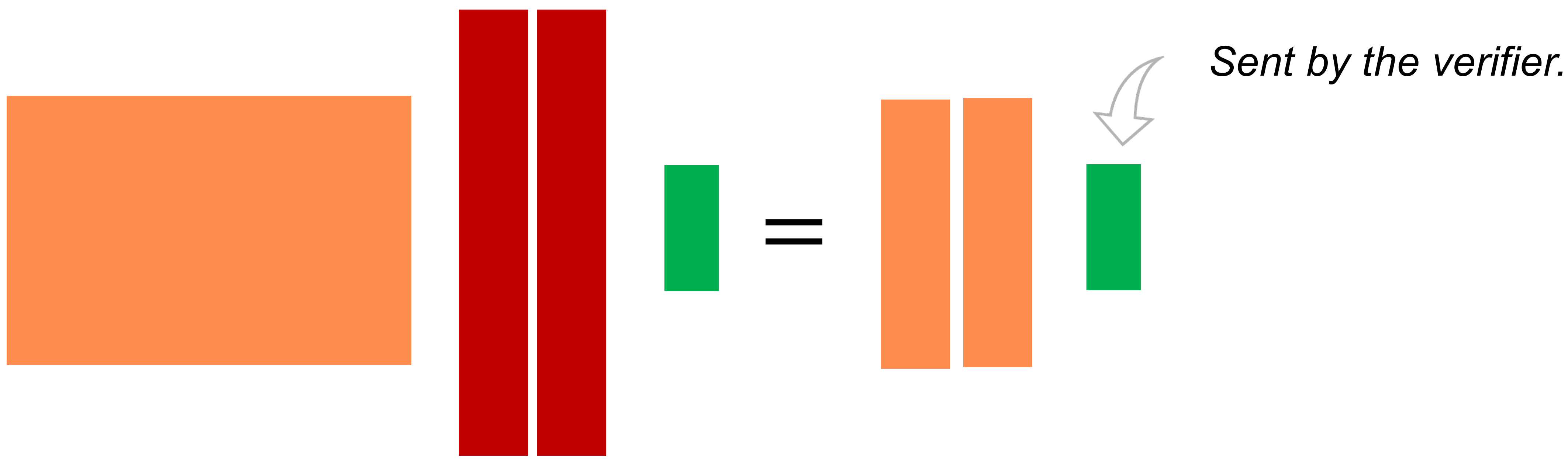
Fold

RoK reduces Ξ_0 to Ξ_1, combing the r_{in} columns of the witness into r_{out} columns.



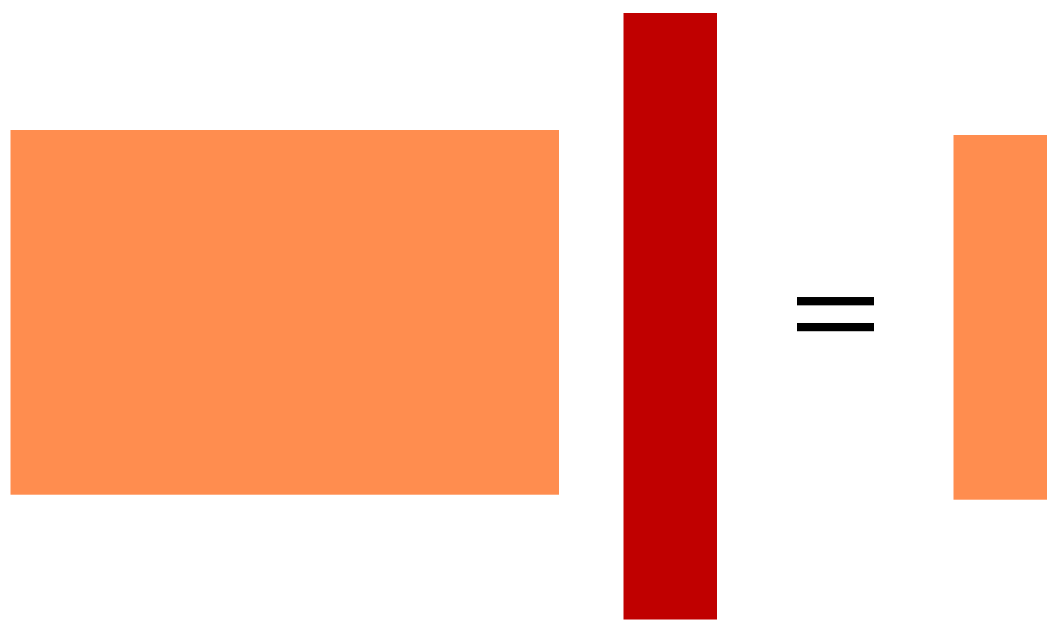
Fold

RoK reduces Ξ_0 to Ξ_1, combing the r_{in} columns of the witness into r_{out} columns.



Fold

RoK reduces Ξ_0 to Ξ_1*, combing the* r_{in} *columns of the witness into* r_{out} *columns.*



Correctness and knowledge soundness due to folklore results – similar to [CLM23]

Decomp

RoK reduces Ξ_0 to Ξ_1, decomposing the witness, reducing its norm, but increasing its width.

Example: radix b = 2, $\mathcal{R}_q = \mathbb{Z}_q$

$$\begin{pmatrix} 7 & 6 \\ 5 & 1 \end{pmatrix} \rightarrow 4 \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Decomp

RoK reduces Ξ_0 to Ξ_1, decomposing the witness, reducing its norm, but increasing its width.

Ξ_0 $\mathbf{A} \cdot \mathbf{W} = \mathbf{Y}$

RoK:

$\mathcal{P}$ $\mathcal{V}$

$(\widetilde{\mathbf{W}}_0, \widetilde{\mathbf{W}}_0, \ldots, \widetilde{\mathbf{W}}_\ell) \leftarrow \mathsf{decomp}_b(\mathbf{W})$

$(\widetilde{\mathbf{Y}}_0, \widetilde{\mathbf{Y}}_0, \ldots, \widetilde{\mathbf{Y}}_\ell) := \mathbf{A} \cdot (\widetilde{\mathbf{W}}_0, \widetilde{\mathbf{W}}_0, \ldots, \widetilde{\mathbf{W}}_\ell)$

$$\sum_{i \in [\ell]} \widetilde{\mathbf{Y}}_i \stackrel{?}{=} b^i \cdot \mathbf{Y}$$

Ξ_1

$$\mathbf{A} \cdot (\widetilde{\mathbf{W}}_0, \widetilde{\mathbf{W}}_0, \ldots, \widetilde{\mathbf{W}}_\ell) = (\widetilde{\mathbf{Y}}_0, \widetilde{\mathbf{Y}}_0, \ldots, \widetilde{\mathbf{Y}}_\ell)$$

Decomp is correct and knowledge sound and reduces the norm of the witness.

Norm-check

RoK reduces Ξ_0 to Ξ_1 such that Ξ_0^{KS} has a better norm guarantee than Ξ_1^{KS}

Fact: $\langle \mathbf{w}, \mathbf{w} \rangle \approx ||\mathbf{w}||_2^2$

inner-product 2-norm squared

Idea: give the opening to the inner product.

(assume the witness to Ξ_0 is a vector, i.e. single column matrix)

Step 1: compute “convoluted” witness and append horizontally

Norm-check

RoK reduces Ξ_0 to Ξ_1 such that Ξ_0^{KS} has a better norm guarantee than Ξ_1^{KS}

Step 1: compute "convoluted" witness and append horizontally

$$\mathsf{L}_{\mathbf{w}}(X) = \sum_{i \in [m]} w_i \cdot X^{i-1}$$

$$\mathsf{L}_{\mathbf{w}}(X) \cdot \mathsf{L}_{\mathbf{w}}(X^{-1}) = \sum_{i \in [1,m]} w_i X^i \cdot \sum_{i \in [1,m]} w_i X^{-i} = \sum_{i,j \in [1,m]} w_i w_j X^{i-j} = \begin{cases} \sum_{\substack{i,j \in [1,m] \\ i \neq j}} w_i w_j X^{i-j} + \langle \mathbf{w}, \mathbf{w} \rangle \\ \sum_{i \in [-m+1, m-1]} v^i X^i \end{cases}$$

$$\mathbf{v}^{(R)} = \mathbf{v}^{(L)}$$

$\mathcal{P}$ $\qquad\qquad$ $\mathcal{V}$

$$\widetilde{\mathbf{Y}} := \mathbf{A} \cdot \left(\mathbf{w} \quad \mathbf{v}^{(R)} \right)$$

Norm-check

RoK reduces Ξ_0 to Ξ_1 such that Ξ_0^{KS} has a better norm guarantee than Ξ_1^{KS}

Step 2: The verifier chooses a challenge ξ and sends to the prover.

<u>RoK:</u>

$\mathcal{P}$ $\mathcal{V}$

$\xi \leftarrow_{\$} \mathcal{R}_q^{\times}$

$$\underbrace{\overset{\widetilde{\mathbf{Y}}}{\begin{pmatrix} c_{\mathbf{w}} & c_{\mathbf{v}}^{(R)} \\ c_{\mathbf{w}}^{\vee} & c_{\mathbf{v}}^{(L)} \\ - & v_0 \end{pmatrix}}}_{\widehat{\mathbf{Y}}} := \underbrace{\begin{pmatrix} & & \mathbf{A} & & \\ \xi & \xi^2 & \xi^3 & \dots & \xi^m \\ \xi^{-1} & \xi^{-2} & \xi^{-3} & \dots & \xi^{-m} \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}}_{\widehat{\mathbf{A}}} \cdot \begin{pmatrix} \mathbf{w} & \mathbf{v}^{(R)} \end{pmatrix}$$

Norm-check

RoK reduces Ξ_0 to Ξ_1 *such that* Ξ_0^{KS} *has a better norm guarantee than* Ξ_1^{KS}

Step 3: Verifier checks statements about the right-hand side

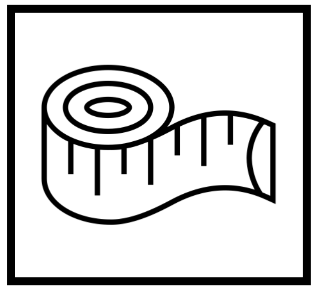
$$\underbrace{\overset{\widetilde{\mathbf{Y}}}{\begin{pmatrix} c_{\mathbf{w}} & c_{\mathbf{v}}^{(R)} \\ c_{\mathbf{w}}^{\vee} & c_{\mathbf{v}}^{(L)} \\ - & v_0 \end{pmatrix}}}_{\widehat{\mathbf{Y}}} := \underbrace{\overset{\mathbf{A}}{\begin{pmatrix} \xi & \xi^2 & \xi^3 & \dots & \xi^m \\ \xi^{-1} & \xi^{-2} & \xi^{-3} & \dots & \xi^{-m} \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}}}_{\widehat{\mathbf{A}}} \cdot \begin{pmatrix} \mathbf{w} & \mathbf{v}^{(R)} \end{pmatrix}$$

$$c_{\mathbf{w}} \cdot c_{\mathbf{w}}^{\vee} \stackrel{?}{=} c_{\mathbf{v}}^{(R)} + c_{\mathbf{v}}^{(L)} - v_0$$

$v_0 \leq \mu^2 \quad \mu -$ norm claim

Step 4: Final relation

$$\widehat{\mathbf{A}} \cdot \begin{pmatrix} \mathbf{x} & \mathbf{v}^{(R)} \end{pmatrix} = \widehat{\mathbf{Y}}$$



Norm-check

RoK reduces Ξ_0 to Ξ_1 *such that* Ξ_0^{KS} *has a better norm guarantee than* Ξ_1^{KS}

$$c_{\mathbf{w}} \cdot c_{\mathbf{w}}^{\vee} \stackrel{?}{=} c_{\mathbf{v}}^{(R)} + c_{\mathbf{v}}^{(L)} - v_0$$

$v_0 \leq \mu^2 \quad \mu -$ norm claim

$$\overset{\widetilde{\mathbf{Y}}}{\begin{pmatrix} c_{\mathbf{w}} & c_{\mathbf{v}}^{(R)} \\ c_{\mathbf{w}}^{\vee} & c_{\mathbf{v}}^{(L)} \\ - & v_0 \end{pmatrix}} := \overset{\mathbf{A}}{\begin{pmatrix} \xi & \xi^2 & \xi^3 & \dots & \xi^m \\ \xi^{-1} & \xi^{-2} & \xi^{-3} & \dots & \xi^{-m} \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}} \cdot \begin{pmatrix} \mathbf{w} & \mathbf{v}^{(R)} \end{pmatrix}$$

<u>Correctness</u>

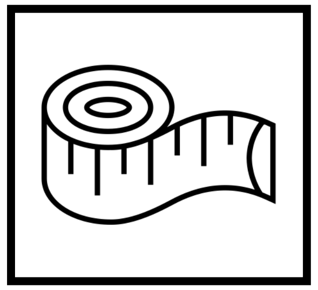
Honest verifier correctly computes new RHS.
Therefore, remains to prove that verifier's checks pass

$$v_0 = \langle \mathbf{w}, \mathbf{w} \rangle$$

$$c_{\mathbf{w}} \cdot c_{\mathbf{w}}^{\vee} = \sum_{i \in [1,m]} w_i \xi^i \cdot \sum_{i \in [1,m]} w_i \xi^{-i} = \sum_{i,j \in [-m+1, m-1]} w_i w_j \xi^{i-j}$$

$$c_{\mathbf{v}}^{(R)} + c_{\mathbf{v}}^{(L)} - v_0 = \sum_{i \in [0, m-1]} v_i \xi^i + \sum_{i \in [-m+1, 0]} v_i \xi^i - v_0 = \sum_{i \in [-m+1, m-1]} v_i \xi^i + v_0 - v_0 = \sum_{i,j \in [-m+1, m-1]} w_i w_j \xi^{i-j}$$

$$v_0 = ||\mathbf{w}||_2^2 \leq \mu^2$$



Norm-check

RoK reduces Ξ_0 to Ξ_1 such that Ξ_0^{KS} has a better norm guarantee than Ξ_1^{KS}

<u>Knowledge soundness</u>

We argue that we extract:

- vSIS break, or
- witness with a stronger (μ) norm guarantee.

or ξ is a non-trivial root of a polynomial defined by the witness
→ unlikely under the Schwartz-Zippel lemma.

Combining RoKs

- The suggested way produces a small proof size, while maintaining the modulus under 2^{64}. Concretely, we obtain the following numbers.

	I	II	III
Witness size [MB]	**128**	**1280**	**5120**
Proof size [MB]	**5.3**	**5.7**	**7.1**

- However, many ways of combining RoKs might be subject of interest, while focusing on different factors, i.e.:
  - verifier runtime,
  - prover runtime,
  - maintaining very low modulus, e.g. 2^{40},
  - selection of application-specific rings.
- We provide a script for estimation of the concrete parameters.

Remarks

The protocol is “public coin”, i.e. the verifier sends only random challenges.
Therefore, Fiat-Shamir transform applies turning the protocol into SNARK.

The protocol requires subtractive set, i.e. set with differences invertible over $\mathcal{R}$.
We identify subtractive set over composite cyclotomics with low expansion factor.

In the protocol, we usually operate over “canonical 2-norm”.
We also provide results for coefficient ∞-norm — practical in some applications.

Aalto University
School of Science

RoK, Paper, SISsors

a versatile framework for combining reductions of knowledge without knowledge and correctness gaps.

Thanks

Michał Osadnik
Michal.osadnik@aalto.fi

ia.cr/2024/1972

Witness-managing RoKs:

- Split
- Fold

Norm-control RoKs:

- Norm-check
- Decomp