A Compressed Σ-Protocol Theory for Lattices

Joint work with Thomas Attema and Ronald Cramer

Lisa Kohl, Cryptology Group

CWI Scientific Meetings, 17 June

About me

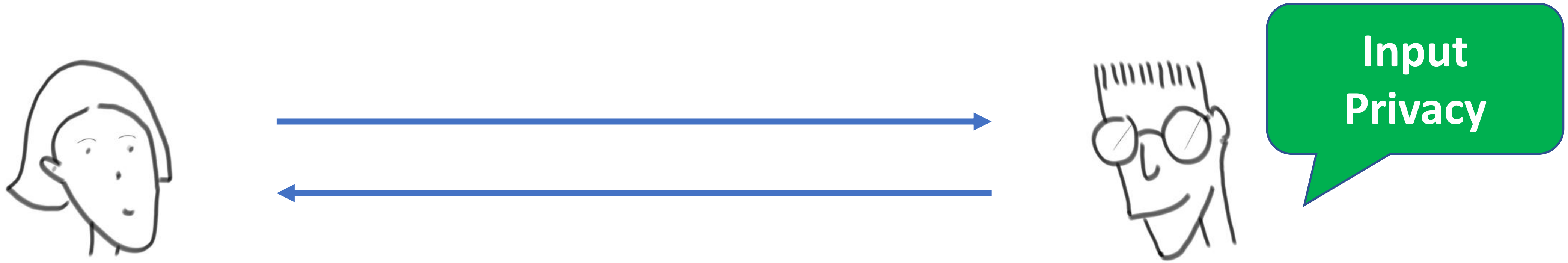
Jun – Dec 2015 • **Master's thesis** in the CWI Cryptology Group

• **PhD** at Karlsruhe Institute of Technology, Germany

• **Postdoc** at Technion, Israel

Since Oct 2020 • **TT** in the Cryptology Group

Research interest: Practical post-quantum secure multi-party computation



Proof of Knowledge (PoK)

Example:
y: description of a sudoku instance
x: solution to sudoku

(y, x)

y

s.t. x valid solution to sudoku

Goal: Alice wants to convince Bob that she *knows* x

Proof of Knowledge (PoK)

This work: Constraint-Satisfiability
f: description of a function
x: input such that $f(x) = 0$

(f, x)

f

s.t. $\mathrm{f}(x) = 0$

Goal: Alice wants to convince Bob that she *knows* x

Desired properties:

- **Zero-knowledge:** Bob learns *nothing* beyond (in particular: doesn't learn x)
- **Succinctness:** $|\text{Communication}| \ll |x|$

Possible?

Practical?

Yes (for all NP)!
"PCP theorem" AroraSafra'92, AroraLundMotwaniSudanSzedegy'92

Yes (for all NP)!
GoldwasserMicaliRackoff'85

Proof of Knowledge (PoK)

This work: Constraint-Satisfiability
f: description of a function
x: input such that $f(x) = 0$

s.t. $\mathrm{f}(x) = 0$

Goal: Alice wants to convince Bob that she *knows* x

Desired properties:

- **Zero-knowledge:** Bob learns *nothing* beyond (in particular: doesn't learn x)
- **Succinctness:** $|\text{Communication}| \ll |x|$

PCP-based approaches have *inherently* high concrete overhead

Alternative: Use "Bulletproof" folding [BCC+'16, BBB+'18, AC'20]

Problem: Not quantum-safe!

Part I: Compressed Σ-Protocols [AttemaCramer'20]

Compressed Σ-protocols [AC'20]

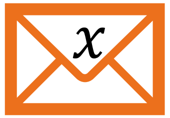
- **Fact:** Can write every function f as **arithmetic circuit** of *addition* (linear) and *multiplication* (non-linear) gates

- **High-level paradigm:**

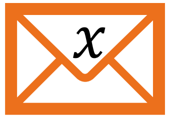
Solve linear instances first, and then linearize non-linear instances

1. **PoK for linear constraints** $f(\boldsymbol{x}) = \langle \boldsymbol{L}, \boldsymbol{x} \rangle$ from *homomorphic commitments*
2. **Communication** $\sim \log |\boldsymbol{x}|$ via *adaptation of Bulletproof PoK* [BCC+'16, BBB+'18]
3. **PoK for arbitrary constraints** via *arithmetic secret sharing*

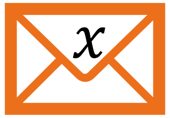
(Succinct) Homomorphic Commitments

Commitment scheme: Commit to x via 

such that:

- **Hiding:** 

hides x

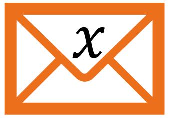
- **Binding:** 

can only be opened to x

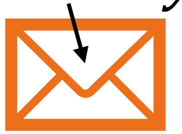
Simplified: Given $\boldsymbol{x}$ can verify if commitment is commitment to $\boldsymbol{x}$

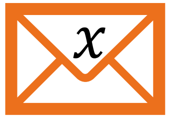
In this talk: $\boldsymbol{x}$ from large space, infeasible to guess

Additional required properties:

- **Homomorphic:** 

$+ \quad c \cdot$ 

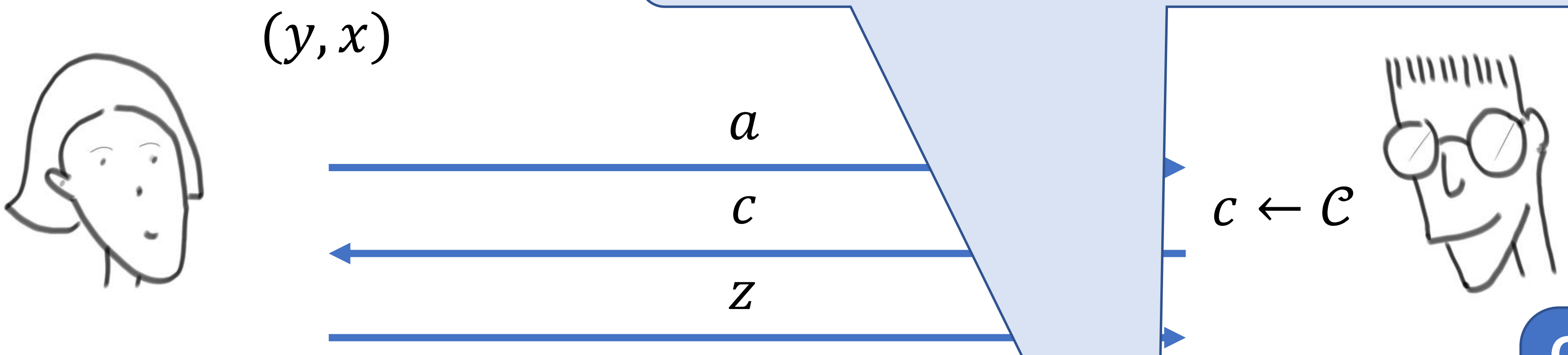
$=$ 
$x + c \cdot y$

- **Succinct:** $\Big|$ 

$\Big| \ll |x|$

Σ-Protocols [Cramer'96]

Verifier could have made up the transcript itself
→ did not *learn* anything from the interaction



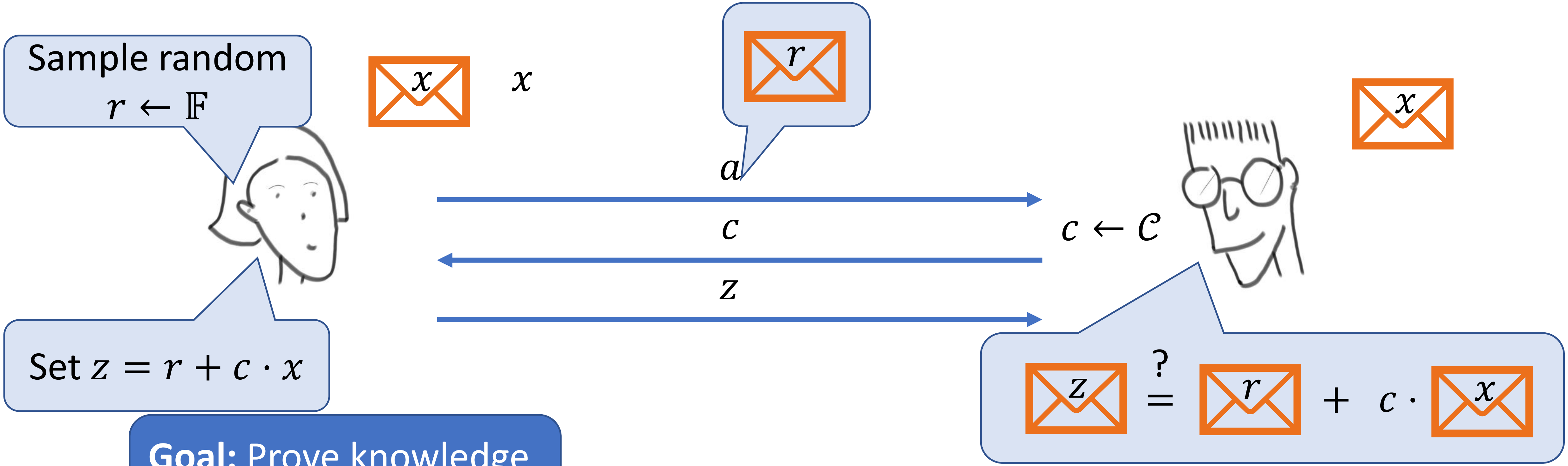
Output:
0: reject, or
1: accept

- **3-move protocol:**
  - **Completeness:** If the prover is honest and knows x, the verifier always accepts
  - **(Honest verifier) zero knowledge:** An accepting transcript can be efficiently simulated
  - **(Special) soundness:** Given accepting transcripts $(a, c, z), (a, c', z')$ one can efficiently extract a witness x

Knowledge error: $^1/_{|\mathcal{C}|}$

If the prover can successfully answer on two different challenges it must *know* the witness

Σ-Protocols for Commitment Opening



Goal: Prove knowledge of opening $x \in \mathcal{X}$

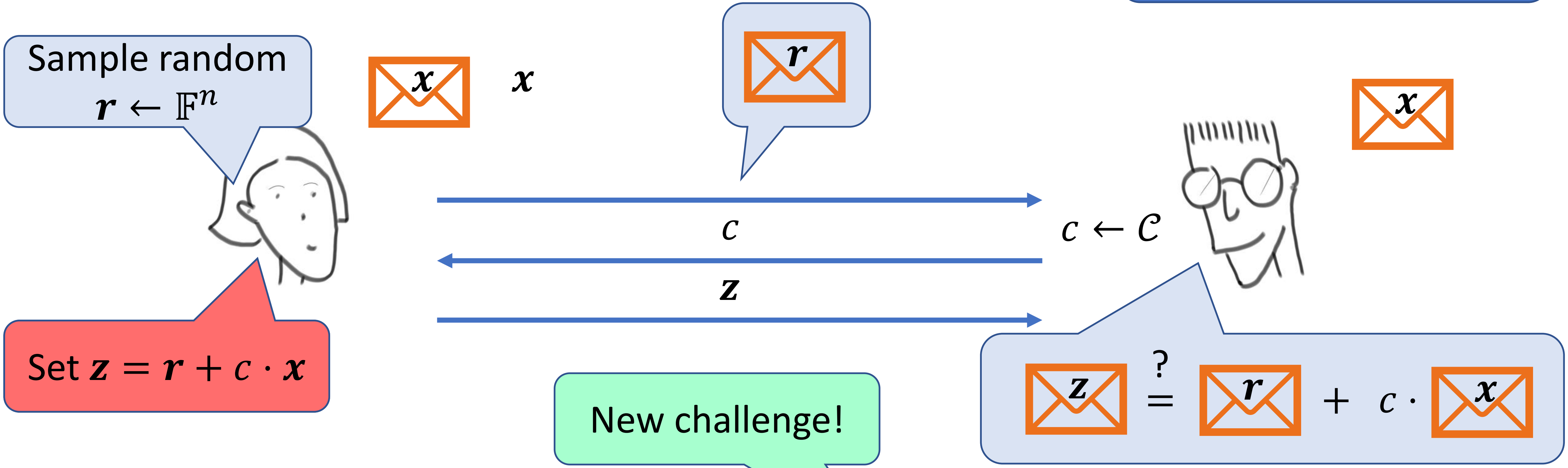
- **First attempt:** Send x
- **Second attempt:** Send random r

Cannot be efficiently simulated → not **zero knowledge**

Does not allow to extract witness → not **special sound**

Towards Compressed Σ-Protocols [

Goal: Prove knowledge of opening $\boldsymbol{x} \in \mathbb{F}^n$



- **Problem:** $|\boldsymbol{z}| = |\boldsymbol{x}| = n \cdot \log|\mathbb{F}|$
- **Idea:** "Fold" $\boldsymbol{z} = (\boldsymbol{z}_1, \boldsymbol{z}_2)$ as $\boldsymbol{z}' := \boldsymbol{z}_1 + \mathrm{d} \cdot \boldsymbol{z}_2$ and send $\boldsymbol{z}'$
- **Problem:** Bob can compute  but not 

How to verify??

Folding Commitments [BCC+'16, BBB+'18]

- **Recall:** $z' := z_1 + \mathrm{d} \cdot z_2$

$$z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

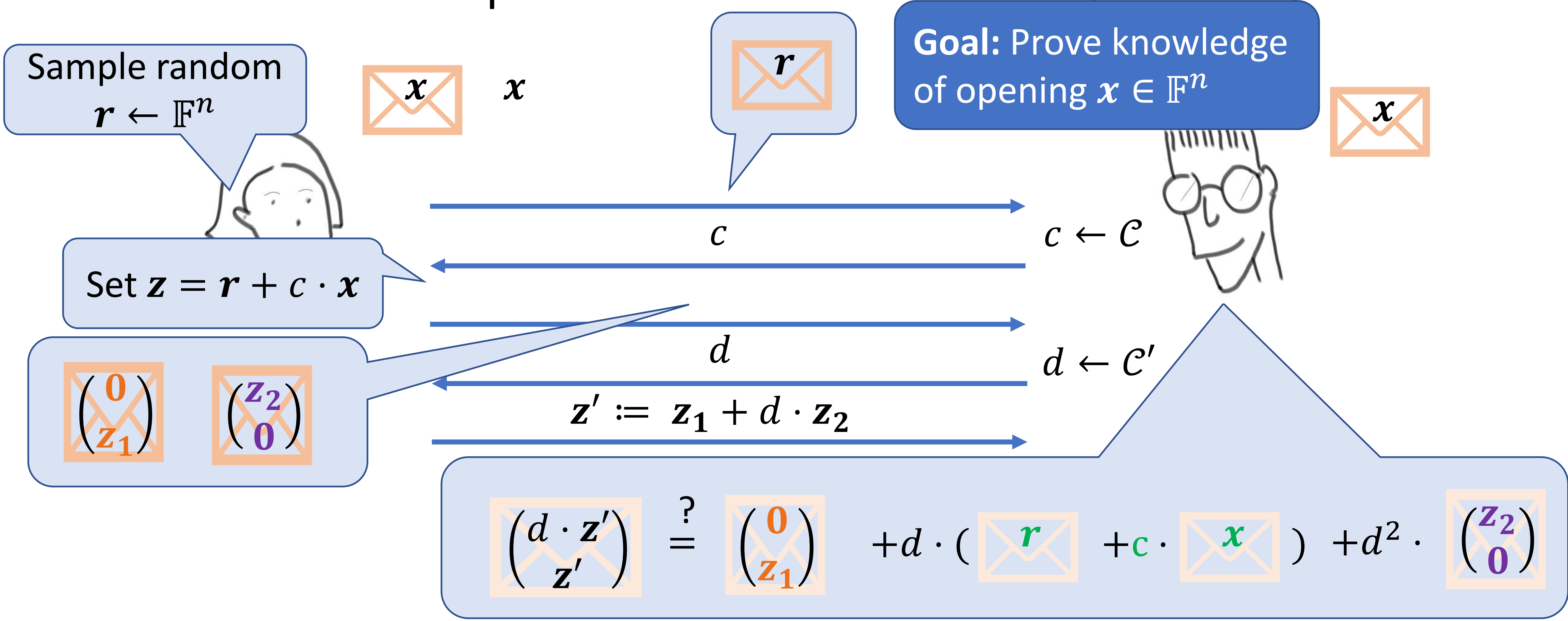
Can be computed from transcript

- **Observation:**

$$\begin{pmatrix} d \cdot z' \\ z' \end{pmatrix} = \begin{pmatrix} d \cdot (z_1 + d \cdot z_2) \\ z_1 + d \cdot z_2 \end{pmatrix} = \begin{pmatrix} 0 \\ z_1 \end{pmatrix} + d \cdot \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} + d^2 \cdot \begin{pmatrix} z_2 \\ 0 \end{pmatrix}$$

Have to be provided by prover

Towards Compressed Σ-Protocols [AC'20]



- **After $\log n$ repetitions:** Communication $\approx \log n \cdot \log|\mathbb{F}|$ (in $\log n$ rounds)

Instantiating Compressed Σ-Protocols [AC’20]

- **Discrete logarithm, strong-RSA:** (poly)logarithmic communication
- **Knowledge of exponent assumption:** constant communication
- **Assumptions in pairing groups:** direct ZK for bilinear circuits [ACR’20]

⇒ All broken by quantum computer

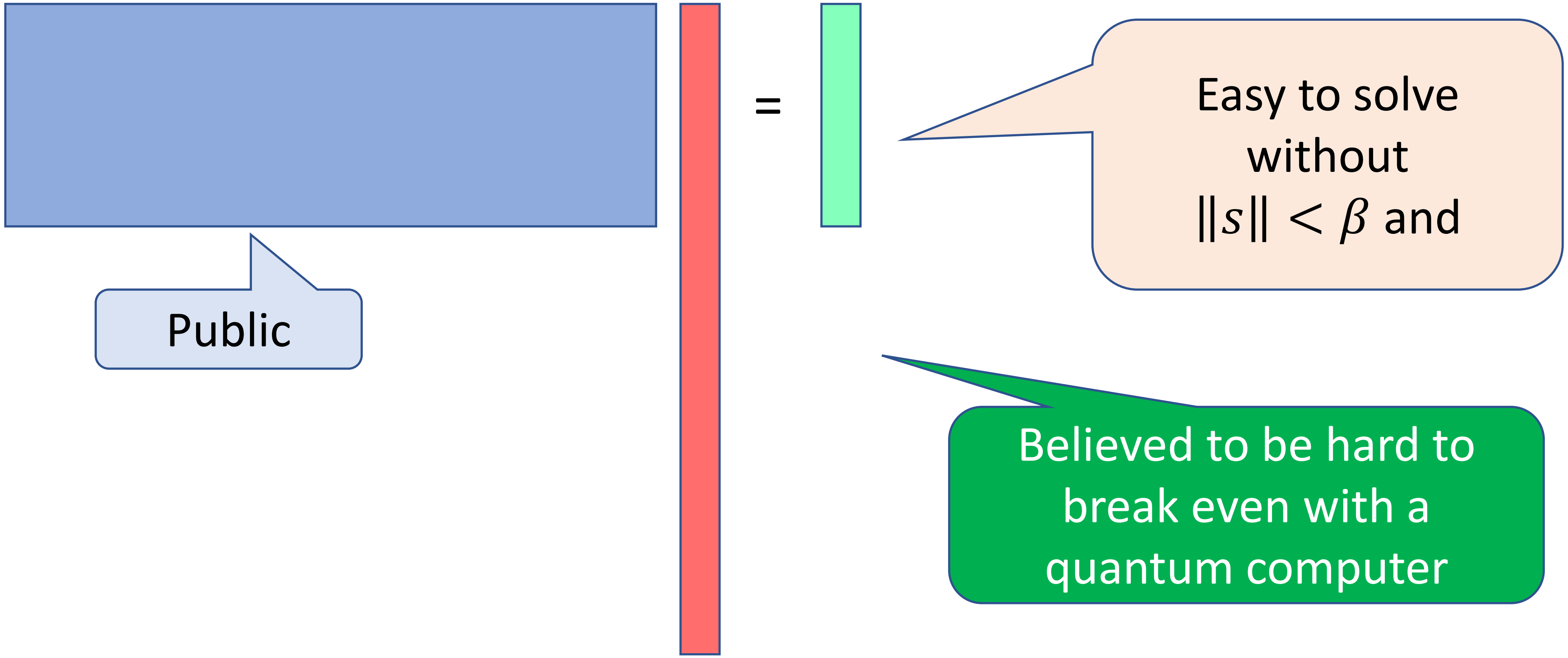
Towards quantum-safe Σ-protocol theory:

- Have to build on quantum-safe assumption

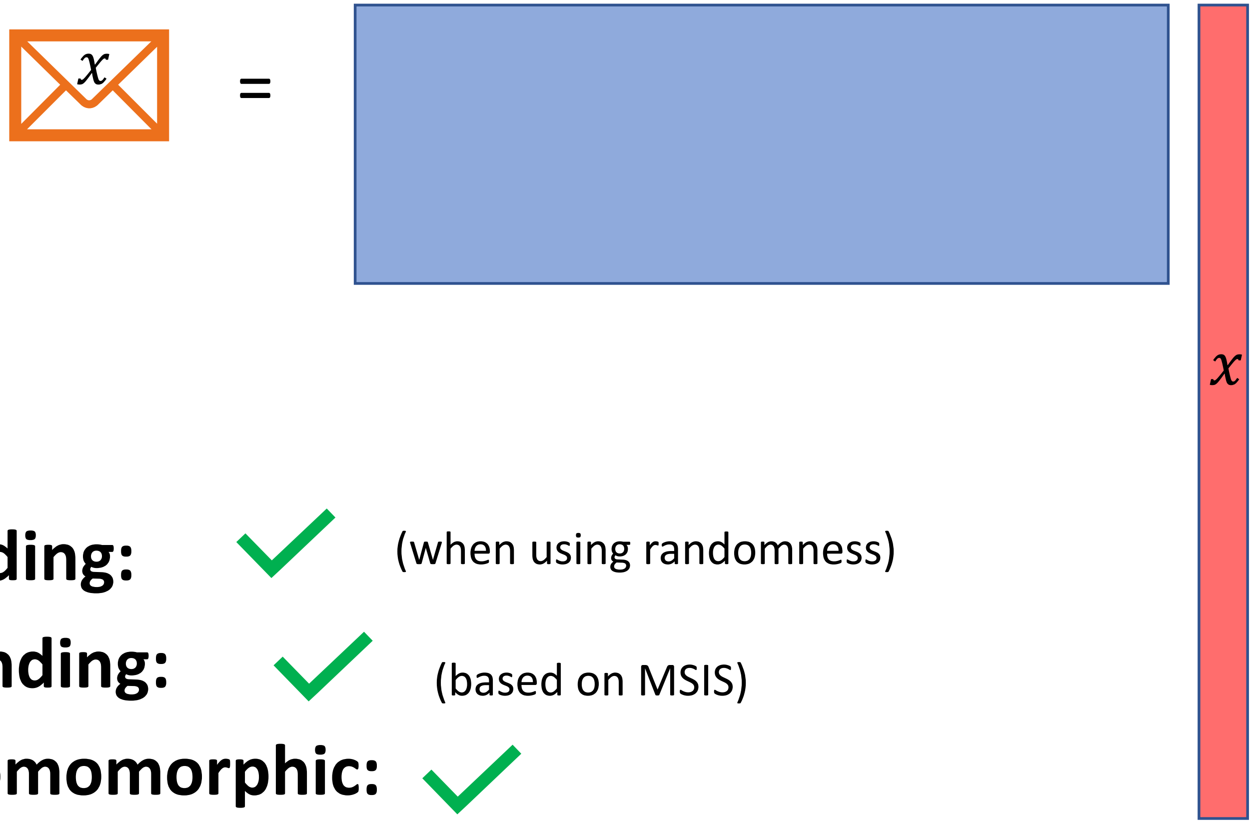
Part II: Compressed Σ-Protocols from Lattices

(Module-)Short Integer Solution ((M-)SIS)

- **(Module-)SIS Assumption:** It is difficult to find short integer solution s with $\|s\| < \beta$ and $A \cdot s = 0$ (over ring $R := \mathbb{Z}_q\,[X]/(f\,(X))$).



Homomorphic Commitments from MSIS



Simplified

Has to be small, e.g., in binary representation

- **Hiding:** ✓ (when using randomness)
- **Binding:** ✓ (based on MSIS)
- **Homomorphic:** ✓
- **Succinct:** ✓

This Work

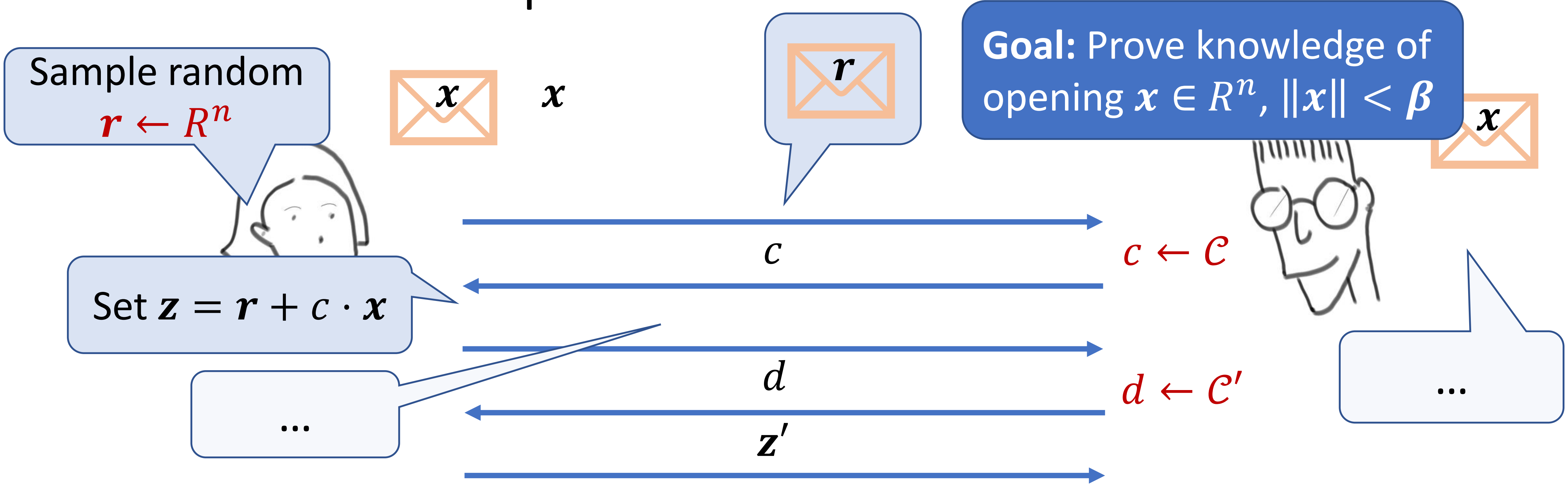
Lattice-based instantiation of compressed Σ-protocol theory

- **Idea:** Instantiate  with MSIS-based commitment scheme

⇒ general constraint zero-knwoledge with (poly-)logarithmic communication?

- **What goes wrong?**

Towards Compressed Σ-Protocols for Lattices



- **Problem:** Protocol allows to extract $\boldsymbol{x}'$ s.t. [envelope $\boldsymbol{x}'$] = [envelope $\boldsymbol{x}$]
- **(Standard-)Solution:** change distribution of $\boldsymbol{r}, c, d$

In particular: Require $(c - c')^{-1}$ small for all $c, c' \in \mathcal{C}$

Without additional guarantee $\|\boldsymbol{x}'\| < \beta'$ meaningless!!

Towards Compressed Σ-Protocols for Lattices

Require: Require $(c - c')^{-1}$ small for all $c, c' \in \mathcal{C}$

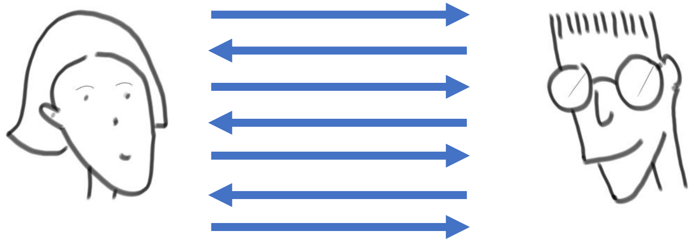
$|\mathcal{C}|$ small (e.g., $\mathcal{C}$={0,1})

Knowledge error $^1/_{|\mathcal{C}|}$ large!!

Need sequential or parallel repetition

- **Main challenge:**
  - $\log n$-round Σ-protocols more challenging than 3-round Σ-protocols
- **Previously:**
  - No *tight extractor analysis* for $\log n$-round Σ-protocols
  - No suitable *parallel repitition theorem* for multi-round PoKs

Summary



Open questions:
- Improve concrete parameters
- Give quantum proof of security

Compressed Σ-protocols for lattices:

- **Motivation:** Practical quantum-safe succinct zero-knowledge PoK
- **This work:**
  - **Abstract framework** to uniformize & simplify analysis
  - **Tight extractor analysis** (also improving non-lattice instantiations)
  - **New parallel repetition** theorem for PoKs (recently improved by [AttemaFehr'21])
  - **Adaptation of linearization techniques** to work over rings

Thank you!!