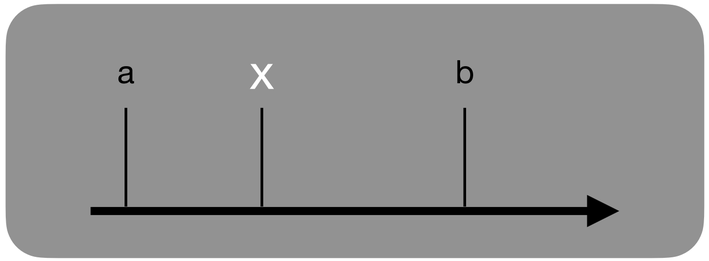
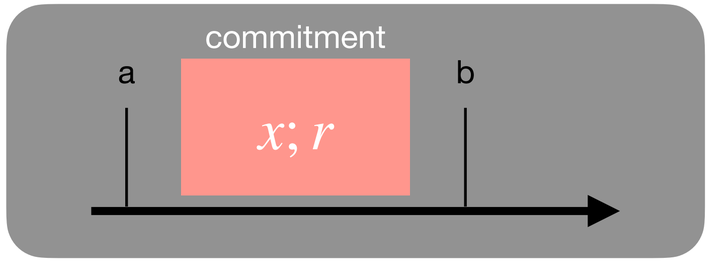
Efficient Range Proofs

with Transparent Setup from Bounded Integer Commitments

- Geoffroy Couteau — IRIF — CNRS
- Michael Klooß — KIT
- Huang Lin — Mercury's Wing — Suterusu
- Michael Reichle — INRIA — ENS — CNRS — PSL University

Setting



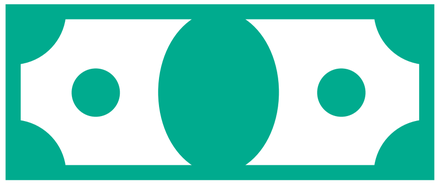


prover

“I know that the committed value **x**
is in range **[a,b]**”

verifier

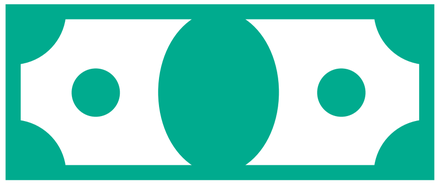
Applications



Anonymous Transactions

“I have enough money”

Applications



Anonymous Transactions

“I have enough money”

Anonymous Credentials

“I am old enough”

“My ticket in still valid”

Approach

[Bou00], [Lip03], [Gro05], [CPP17]

$$(x-a)(b-x) = \sum_{i=1}^{4} x_i^2$$

- Shows $x \in [a, b]$
- Requires integer commitments
  - trusted setup
  - large parameters

$x \in \mathbb{N}; r$

Approach

[Bou00], [Lip03], [Gro05], [CPP17]

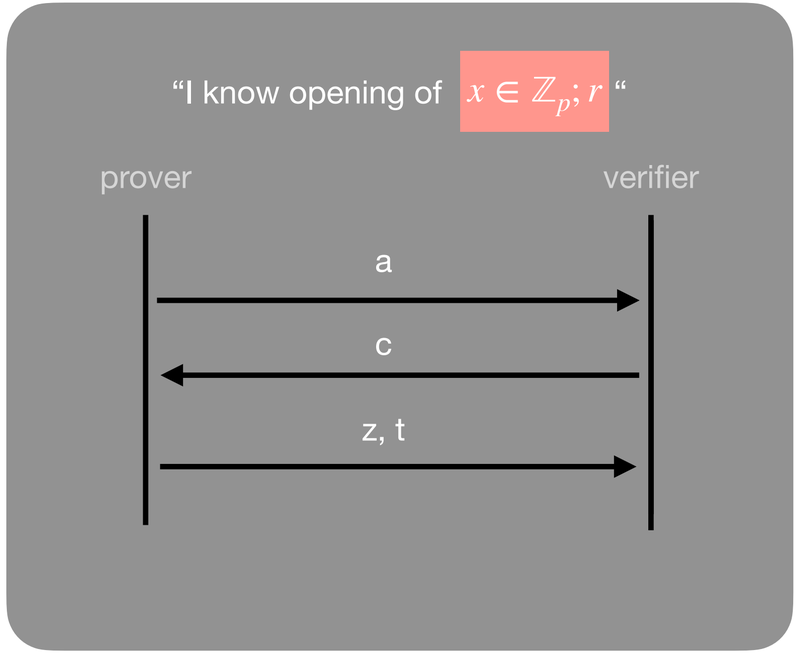
$$(x-a)(b-x) = \sum_{i=1}^{4} x_i^2$$

- Shows $x \in [a, b]$
- Requires integer commitments
  - trusted setup
  - large parameters
- **Idea:** show decomposition over $\mathbb{Z}_p$
  - need that x is short (no overflow)

$x \in \mathbb{N}; r$

$x \in \mathbb{Z}_p; r$

Proof of Opening

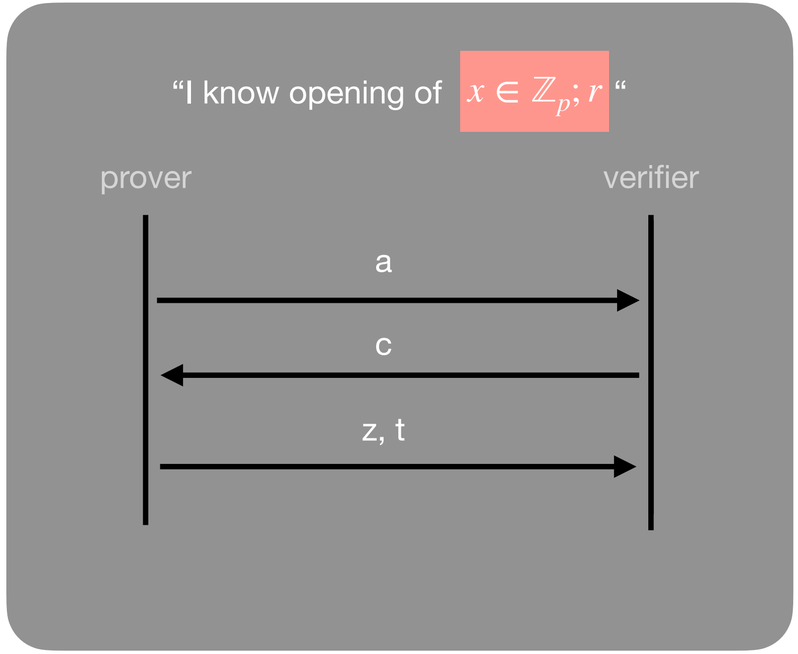


- Homomorphic commitment over $\mathbb{Z}_p$

Zero-Knowledge:
reveals no information about witness

Soundness:
witness can be extracted from transcripts

Proof of Opening

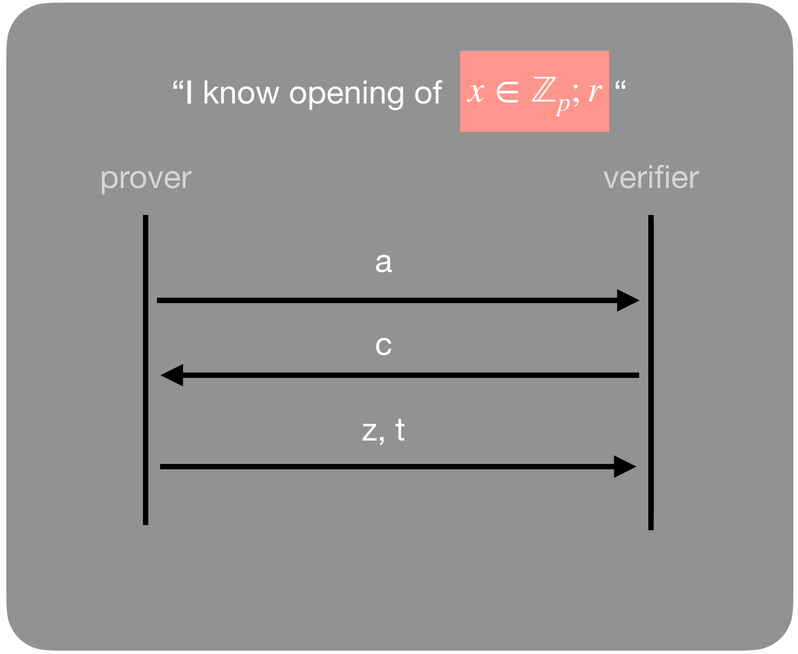


Zero-Knowledge:
reveals no information about witness

Soundness:
witness can be extracted from transcripts

- Homomorphic commitment over $\mathbb{Z}_p$
- **Extraction:**
  - $x = \frac{z - z'}{c - c'} \mod p$
  - can ensure that $z - z'$ and $c - c'$ are short

Proof of Opening

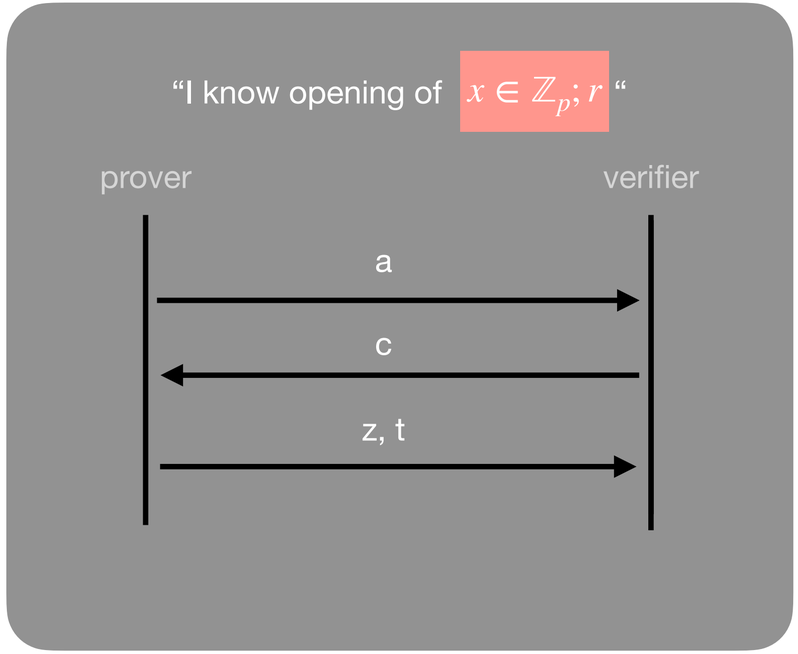


Zero-Knowledge:
reveals no information about witness

Soundness:
witness can be extracted from transcripts

- Homomorphic commitment over $\mathbb{Z}_p$
- **Extraction:**
  - $x = \frac{z - z'}{c - c'} \mod p$
  - can ensure that $z - z'$ and $c - c'$ are short
- **Problem:** extracted x not short

Proof of Opening



Zero-Knowledge:
reveals no information about witness

Soundness:
witness can be extracted from transcripts

- Homomorphic commitment over $\mathbb{Z}_p$
- **Extraction:**
  - $x = \frac{z - z'}{c - c'} \mod p$
  - can ensure that $z - z'$ and $c - c'$ are short
- **Problem:** extracted x not short
- **Idea:** map $x = \frac{z - z'}{c - c'} \in \mathbb{Z}_p$ to $x = \left\lfloor \frac{z - z'}{c - c'} \right\rfloor \in \mathbb{N}$

Protocol

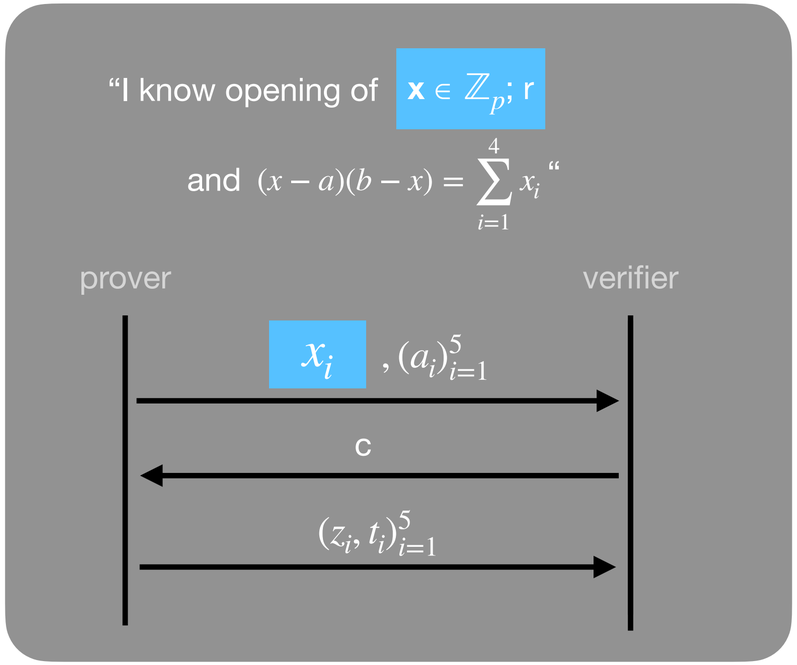
- Relax commitment scheme:
  - $\frac{z}{c} \in \mathbb{Z}_p; r$ commits to $x = \left\lfloor \frac{z}{c} \right\rfloor \in \mathbb{Z}$

Protocol

- Relax commitment scheme:
  - $\frac{z}{c} \in \mathbb{Z}_p; r$ commits to $x = \left\lfloor \frac{z}{c} \right\rfloor \in \mathbb{Z}$
- (Some) properties
  - binding if z, c are short
  - retains restricted homomorphic properties
  - retains shortness

Protocol

- Relax commitment scheme:
  - $\frac{z}{c} \in \mathbb{Z}_p; r$ commits to $x = \left\lfloor \frac{z}{c} \right\rceil \in \mathbb{Z}$
- (Some) properties
  - binding if z, c are short
  - retains restricted homomorphic properties
  - retains shortness



Evaluation

- Simple Scheme
- Good Efficiency
- Transparent Setup

- Large groups required
- Weaker homomorphic properties

Thank You

ia.cr/2021/540