Set Membership and Range Proofs

Rafik Chaabouni

28 January 2012

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

TARTU ÜLIKOOL
1632
UNIVERSITAS TARTUENSIS

Outline

- What?
  - Set Membership
  - Range Proofs
- Why?
  - COP Initiative
- How? (intuitions)

What?

Set Membership

What?

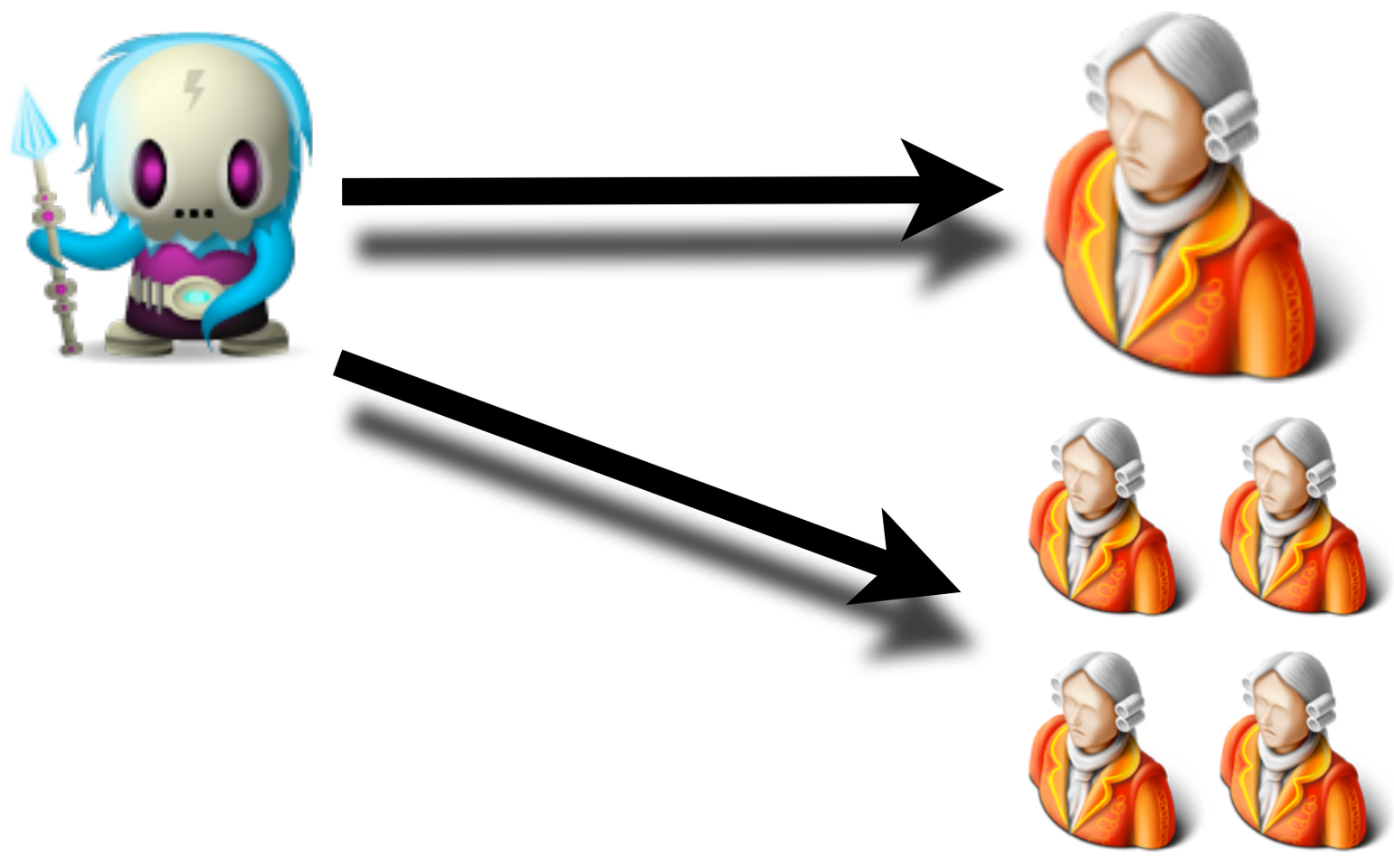
Range Proofs

x

$[0, 1, 2, ..., H]$

What?

Non-Interactive Proofs



Why?

- E-Voting:
  Valid ballot without revealing content

Why?

- E-Auctions:
  Valid secret bids before end of auction
  Sufficient wealth in bank account

- E-Cash (internal construction)

Why?

- Anonymous Credentials:
  Reveal only limited information of ID attributes

Why?

Why?

- Increased connectivity of Children
  (2009: 93% 12-17 USA teens regularly online)
- Age of first connectivity is dropping
- Children often left alone
  (2009: 72% French children surf alone)
- Internet brings outside world
  inside home

Why?

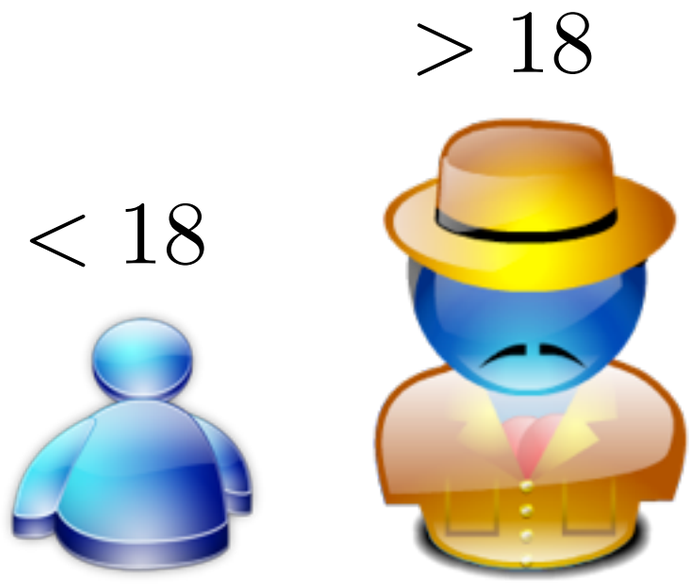
- Adult contents (pornography, violence)
- Adult predators
- Bullying
- Racism
- ...

Why?

- Child Online Protection (COP) Initiative:
  - ITU and other Stakeholders
  - November 2008

Why?

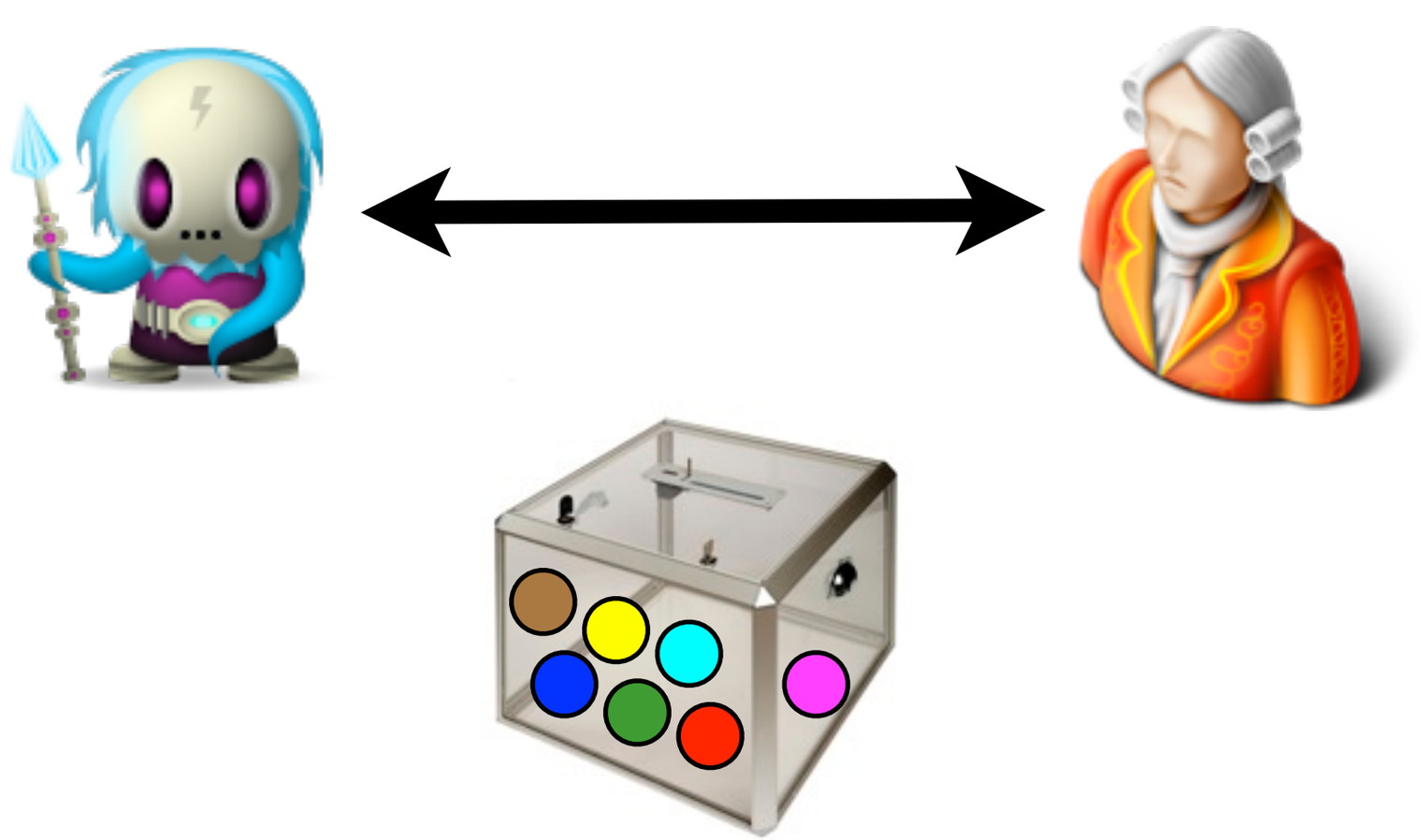
- Range Proofs & e-ID
  - secret: date of birth
  - restrict adult contents
  - protect children from adult predators on youth's platforms (forums, social networking services)



How Set Membership?

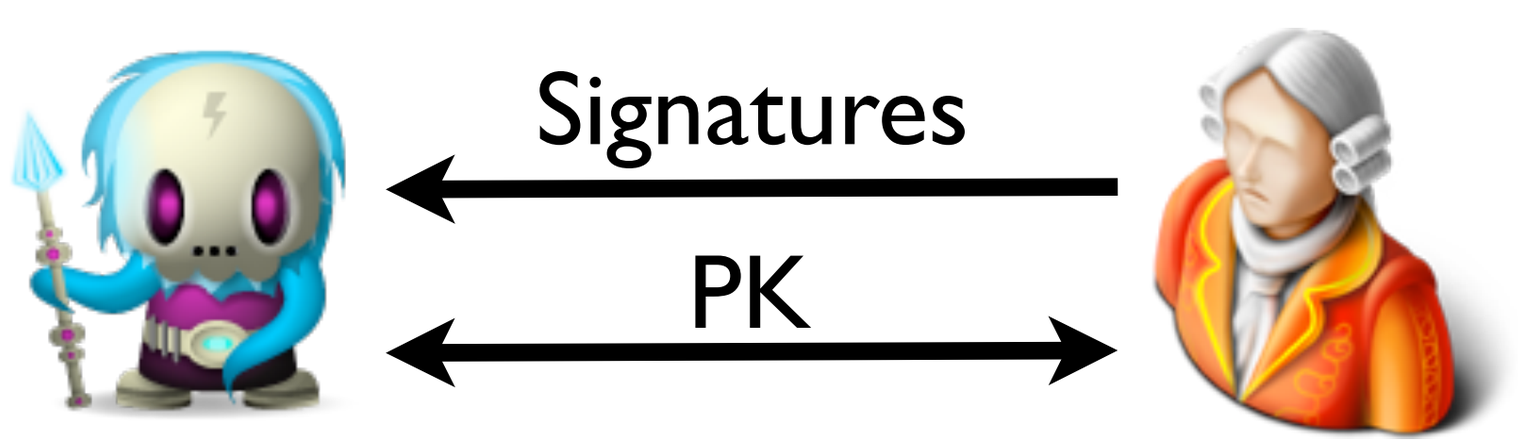
- Combination of ZK OR-proofs

  ➡ naive & inefficient



How Set Membership?

- Efficient idea [CamenischCs08]



How Range Proof?

- Naive approaches n°1

  ➡ advantage of regular set structure lost

$$[0, 1, 2, ..., H] =$$

How Range Proof?

- Naive approaches n°2:
  binary decomposition

➡ inefficient

x

$$[0, 1, 2, ..., H]$$

How Range Proof?

- Optimal solution: "Divide and Conquer"
  - Special structured set decomposition
  - Tradeoff needed between
    number of sets VS. *size of sets*

How Range Proof?

- Most recent efficient techniques based on Progression-Free Sets (cf. previous talk)
  - Interactive [ChaabouniLs10]
  - Non-Interactive [ChaabouniLZ12]

Questions?

1. [CamenischCs08]
   Jan Camenisch, Rafik Chaabouni, and abhi shelat.
   Efficient Protocols for Set Membership and Range Proofs.
   In Josef Pieprzyk, editor, ASIACRYPT 2008, volume 5350 of LNCS, pages 234–252, Melbourne, Australia, December 7–11, 2008. Springer-Verlag.

2. [ChaabouniLs10]
   Rafik Chaabouni, Helger Lipmaa, and abhi shelat.
   Additive Combinatorics and Discrete Logarithm Based Range Protocols.
   In Ron Steinfeld and Philip Hawkes, editors, ACISP 2010, volume 6168 of LNCS, pages 336–351, Sydney, Australia, July 5–7, 2010. Springer-Verlag.

3. [ChaabouniLZ12]
   Rafik Chaabouni, Helger Lipmaa, and Bingsheng Zhang.
   A Non-Interactive Range Proof with Constant Communication.
   In Angelos Keromytis, editor, FC 2012, volume ? of LNCS pages ?--?, Bonaire, The Netherlands, February 27–March 2, 2012. Springer-Verlag.