Zero Knowledge Proofs

Benjamin Schmid

2019-02-14

Swiss Olympiad in Informatics

Zero Knowledge Proofs

What is an (interactive) proof?

Zero Knowledge Proof of Knowledge

Commitments

Based on Lecture “Cryptographic Protocols” by Ueli Maurer and Martin Hirt.

https://www.crypto.ethz.ch/teaching/lectures/KP18

What is an (interactive) proof?

Sudoku

						4		
2					1		5	
4	3		7	5		1		2
				7			6	
	5	3				2	4	
	4			1				
3		1		8	2		7	4
	2		9					5
		8						

Proof System

- Statements (e.g. Sudoku Field)
- Semantics (which statements are true)
  (e.g. solvable Sudoku)
- Proof
- Verification Function (statement, proof) $\rightarrow$ {accept, reject}

Static Proof

- Prover and Verifier know statement
- Prover sends proof to Verifier
- Verifier checks statement and proof $\rightarrow$ {accept, reject}

Static Proof

- Prover and Verifier know statement
- Prover sends proof to Verifier
- Verifier checks statement and proof $\rightarrow$ {accept, reject}

Example:

- Statement is Sudoku S is solvable
- Proof is solution for S
- Verification checks whether solution correct

Interactive Proof

- Prover and Verifier know statement
- Exchange of messages
- Verifier checks statement and all messages $\rightarrow$ {accept, reject}

- More Powerful
- Allows Zero Knowledge Proofs

Zero Knowledge Proof of Knowledge

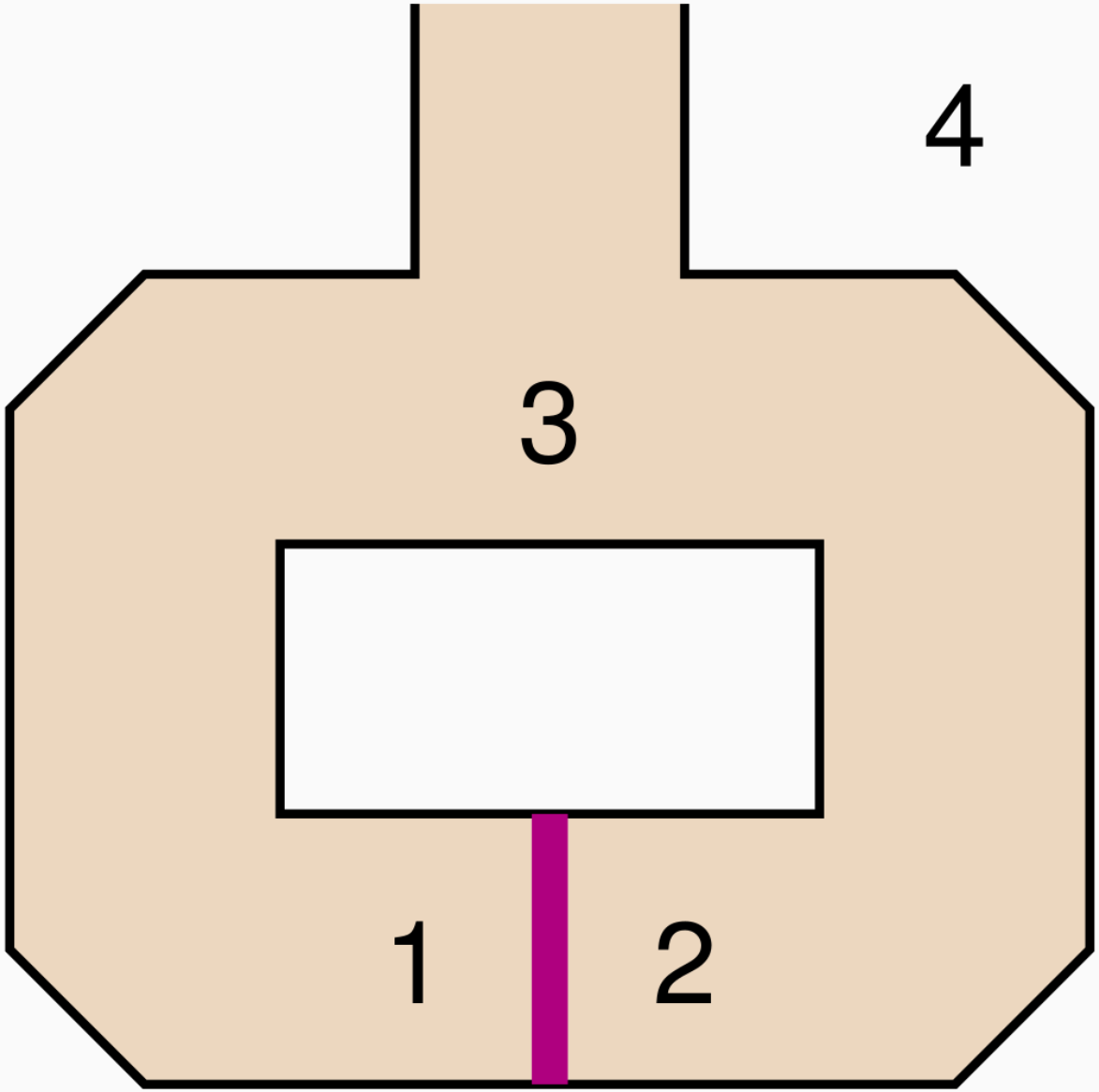
Proof of Knowledge

- Want to proof knowledge
- Contrary to proving a statement
- Statement: “This Sudoku has a solution”
- Knowledge: “I know the solution of this Sudoku”
- Often, knowledge implies statement

What is Knowledge?

- Knowledge extractor
- Can interact with Prover
- Can rewind Prover (with same randomness)
- Has to compute knowledge

Zero Knowledge: Cave Example



Zero Knowledge

- Verifier should not learn anything new
- Verifier can not prove knowledge to other party

Zero Knowledge

- Verifier should not learn anything new
- Verifier can not prove knowledge to other party
- Communication can be simulated $\rightarrow$ nothing learned
- Often three round protocol:
  - P $\rightarrow$ V: Value t based on secret and randomness
  - P $\leftarrow$ V: Challenge c
  - P $\rightarrow$ V: Challenge response r depending on initial t
- Given c, can simulate valid t and r
- Prover does not know c before selecting t

Example: Schnorr

Prover

knows $x \in \mathbb{Z}_q$ s.t. $h^x = z$

$k \in_R \mathbb{Z}_q$

$t = h^k$

$r = k + xc$

Verifier

knows z

$c \in_R \mathcal{C} \subseteq \mathbb{Z}_q$

$h^r = t \cdot z^c$

Commitments

Commitments

- New primitive: Commitment
- Can commit to value
- Value is secret
- Can only reveal committed value
- Like magic Post-It
- Example: commit to $x \in \mathbb{Z}_q$ with $b = h^x$ or $b = g^x h^r$

Sudoku Protocol

- Given unfinished Sudoku
- Want to prove knowledge of solution
- Zero Knowledge
- Use interactive proof with commitments

Sudoku Protocol

- Permute numbers of solution
- Commit to whole field
- Send commitments
- Challenges:
  - One row
  - One column
  - One field
  - Original values
- Open requested values

Sudoku Demo

Sudoku

						4		
2					1		5	
4	3		7	5		1		2
				7			6	
	5	3				2	4	
	4			1				
3		1		8	2		7	4
	2		9					5
		8						

Sudoku

1	6	5	8	2	9	4	3	7
2	8	7	3	4	1	9	5	6
4	3	9	7	5	6	1	8	2
9	1	2	4	7	3	5	6	8
7	5	3	6	9	8	2	4	1
8	4	6	2	1	5	7	9	3
3	9	1	5	8	2	6	7	4
6	2	4	9	3	7	8	1	5
5	7	8	1	6	4	3	2	9