Zero-Knoweldge Proofs

Abhishek Jain

Zero Knowledge: History

- Invented by Shafi Goldwasser, Silvio Micali, Charlie Rackoff in 1980s

Zero Knowledge: History

- Invented by Shafi Goldwasser, Silvio Micali, Charlie Rackoff in 1980s

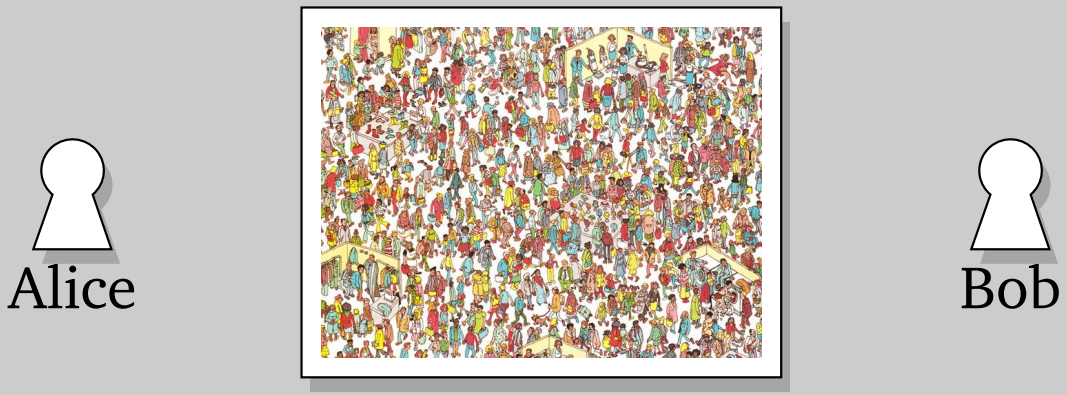
- Paper rejected three times! Accepted the 4th time in 1985.

Zero Knowledge: History

- Invented by Shafi Goldwasser, Silvio Micali, Charlie Rackoff in 1980s

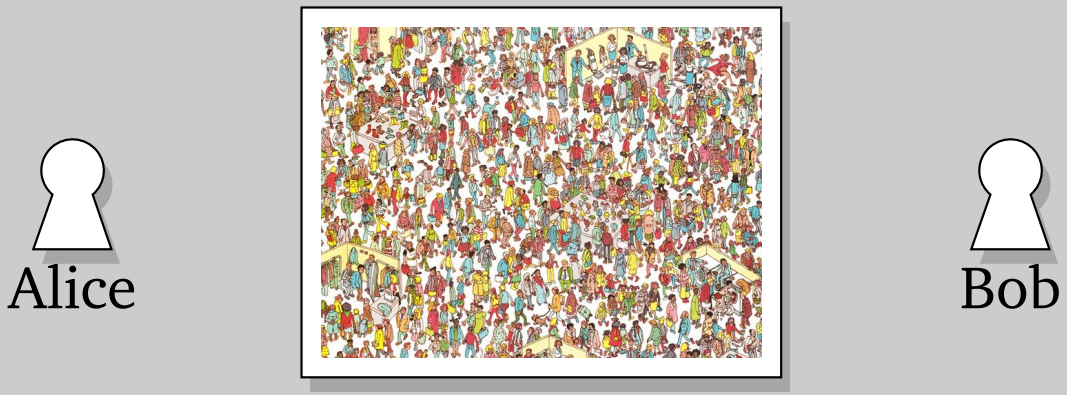
- Paper rejected three times! Accepted the 4th time in 1985.
- Shafi and Silvio won the 2012 Turing Award for work on encryption and proof systems.

Scenario: Where's Waldo?



A "Hey Bob, I found Waldo!"

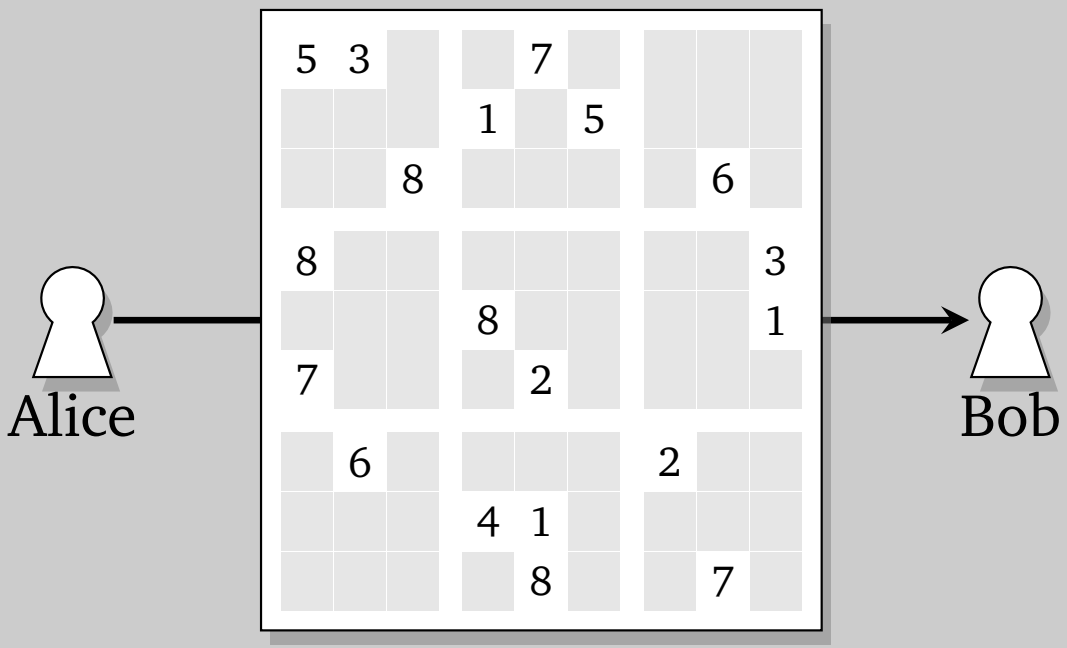
Scenario: Where's Waldo?



A "Hey Bob, I found Waldo!"

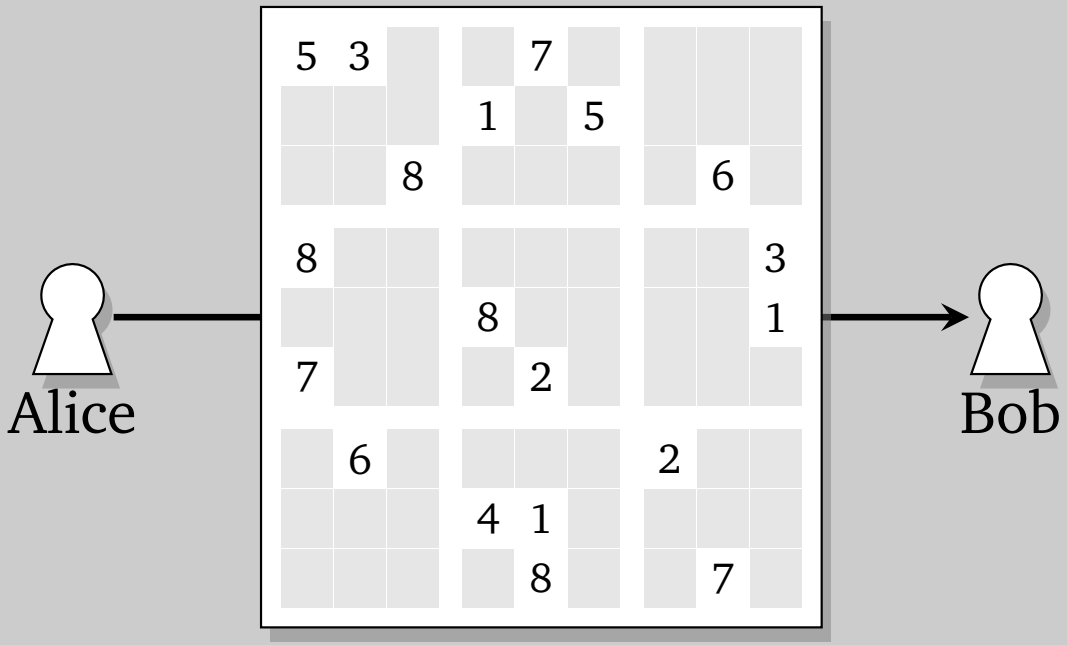
B "That was way too fast, I don't believe you."

Scenario: Sudoku



A "Hey Bob, check out this brutal Sudoku puzzle!"

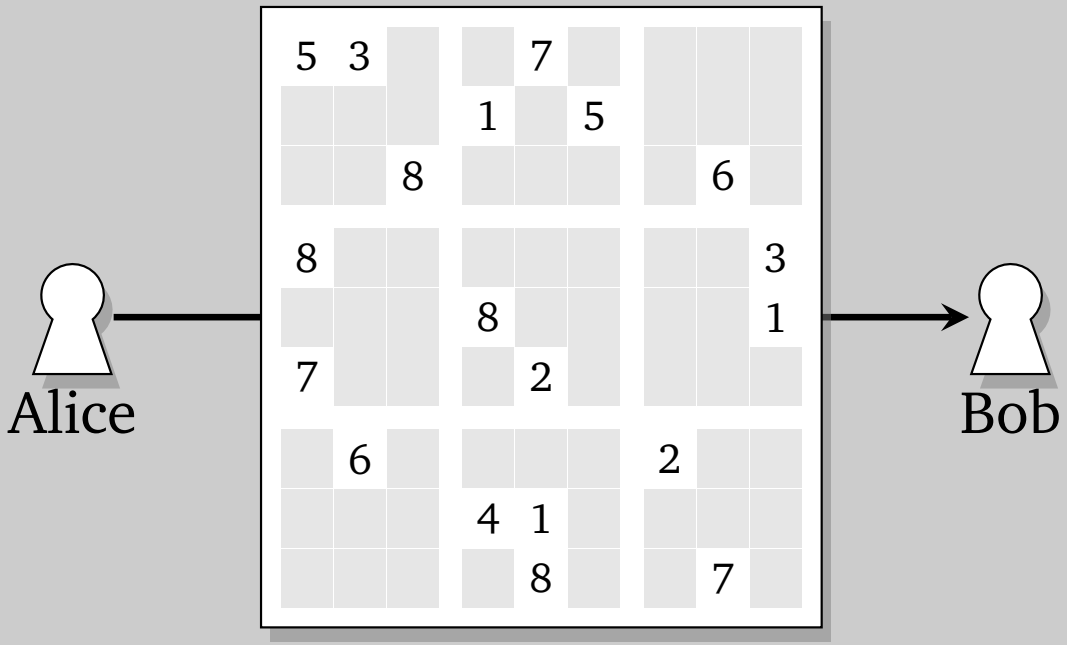
Scenario: Sudoku



A "Hey Bob, check out this brutal Sudoku puzzle!"

B "Last week you gave me a puzzle with no solution. I wasted 3 hours."

Scenario: Sudoku

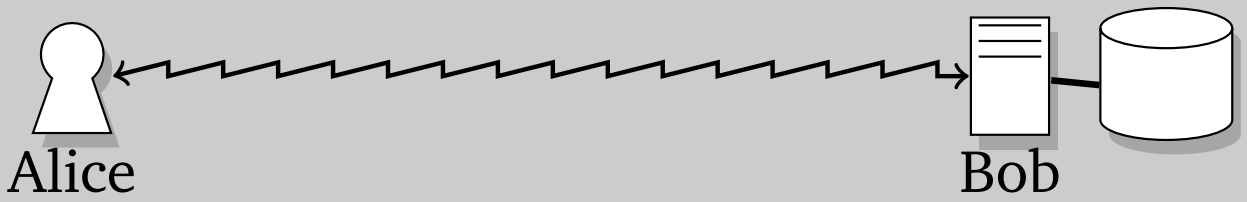


A "Hey Bob, check out this brutal Sudoku puzzle!"

B "Last week you gave me a puzzle with no solution. I wasted 3 hours."

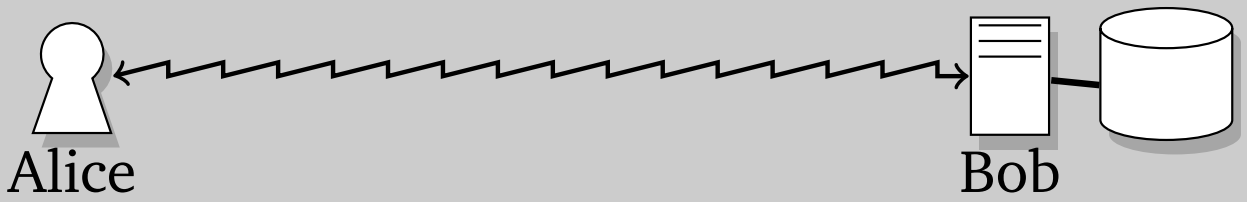
A "This one has a solution, trust me."

Scenario: Authentication



A "Can I have access to the database? It's me, Alice."

Scenario: Authentication



A "Can I have access to the database? It's me, Alice."

B "OK, send me your password so I know it's you."

A Problem of Trust and Information

Alice wants to convince Bob of something

- Waldo is in the picture
- Sudoku puzzle has a solution
- Alice is not an imposter

A Problem of Trust and Information

Alice wants to convince Bob of something

- Waldo is in the picture
- Sudoku puzzle has a solution
- Alice is not an imposter

Bob should not learn "too much"

- Waldo's location
- Sudoku solution
- Alice's password

A Problem of Trust and Information

Alice wants to convince Bob of something

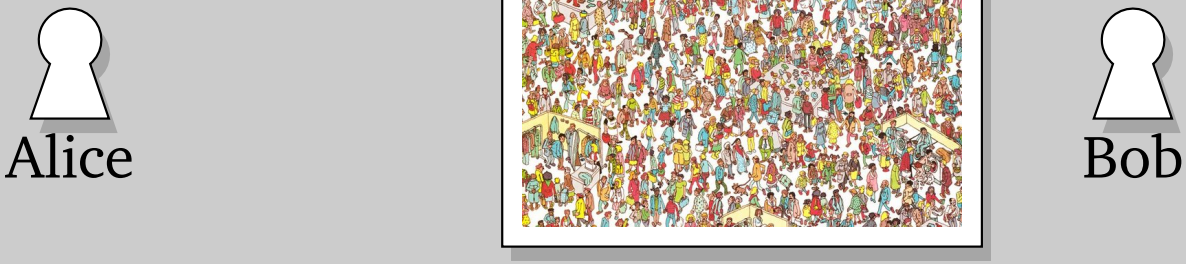
- Waldo is in the picture
- Sudoku puzzle has a solution
- Alice is not an imposter

Bob should not learn "too much"

- Waldo's location
- Sudoku solution
- Alice's password

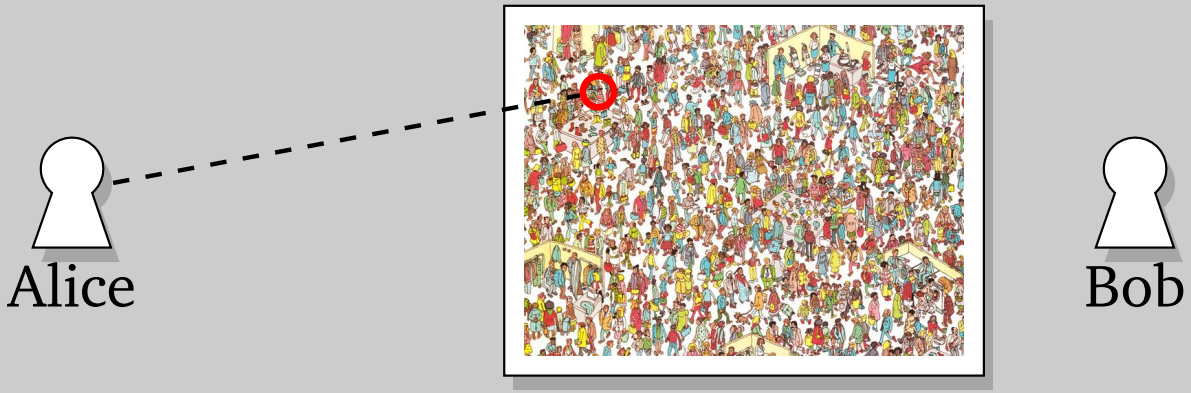
What might a possible solution look like?

Where's Waldo? Solution



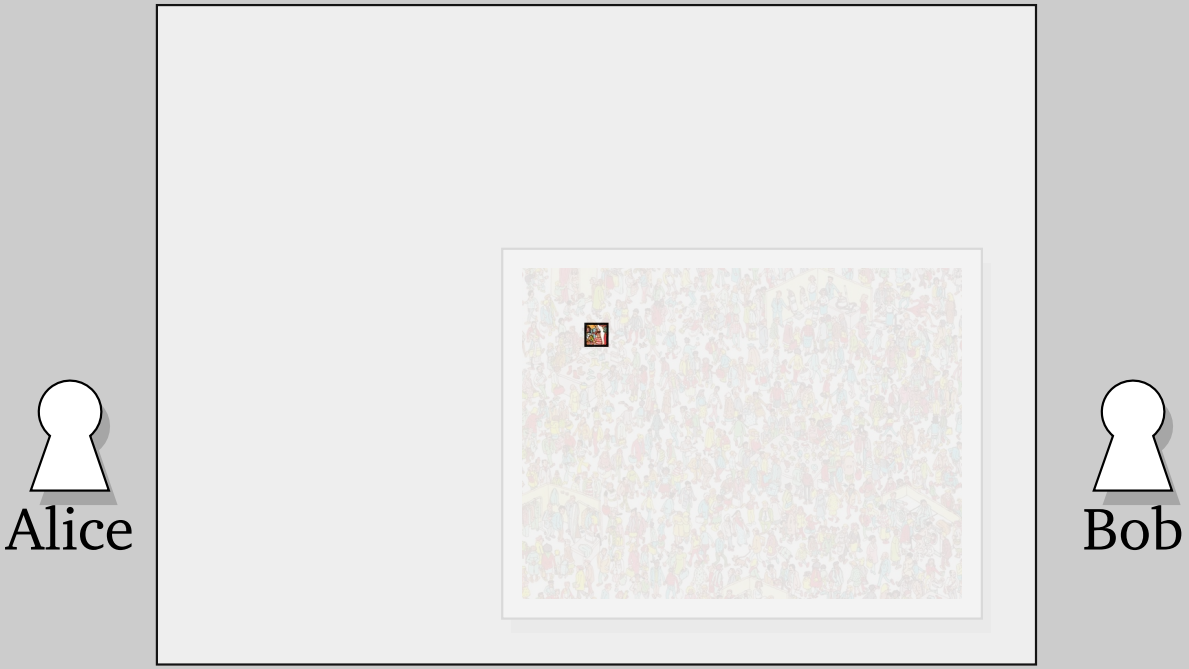
Solution:

Where's Waldo? Solution



Solution:

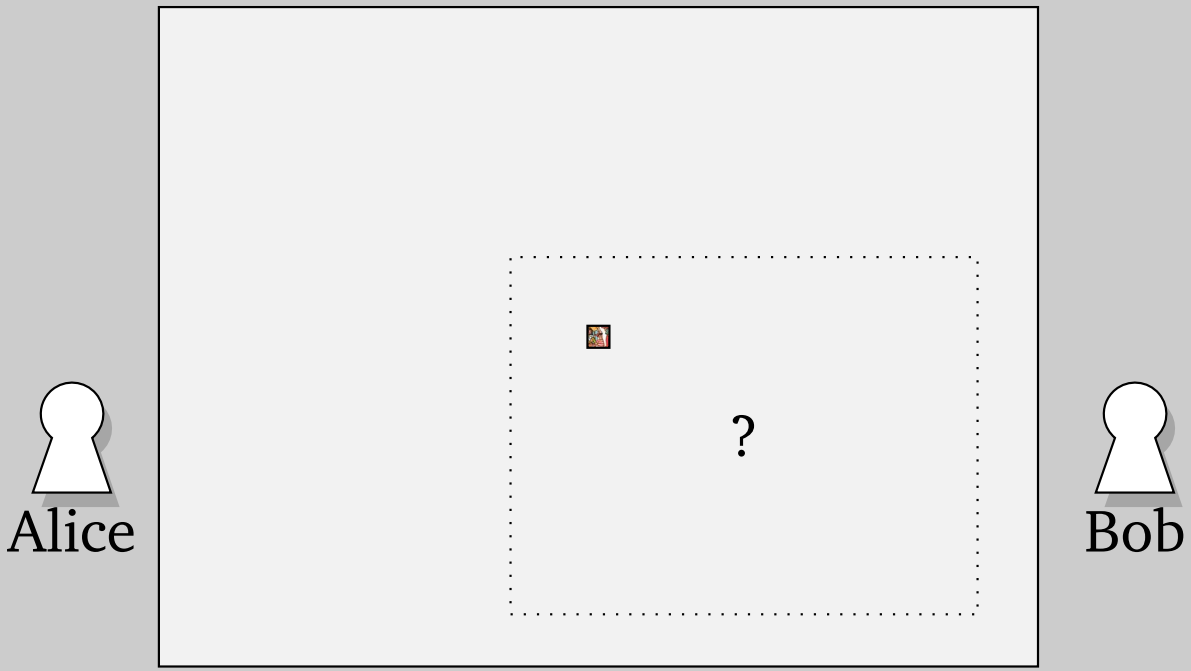
Where's Waldo? Solution



Solution:

1. Alice places opaque cardboard with hole over picture, revealing Waldo

Where's Waldo? Solution

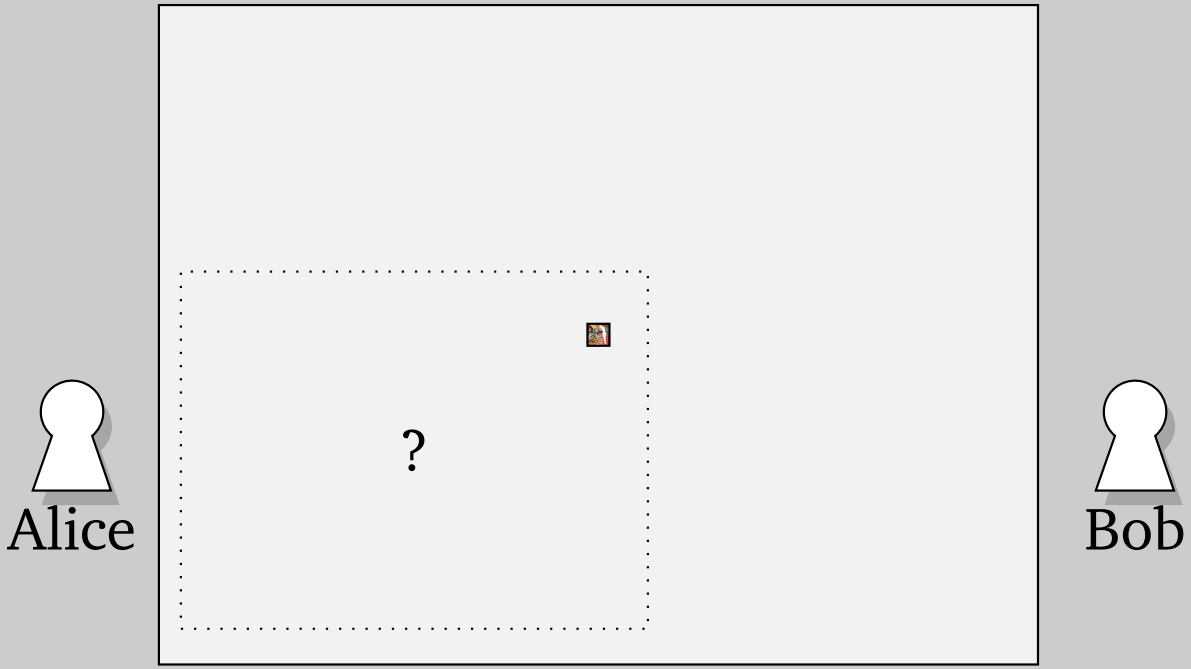


Solution:

1. Alice places opaque cardboard with hole over picture, revealing Waldo

Bob gets no information about Waldo's location within picture!

Where's Waldo? Solution

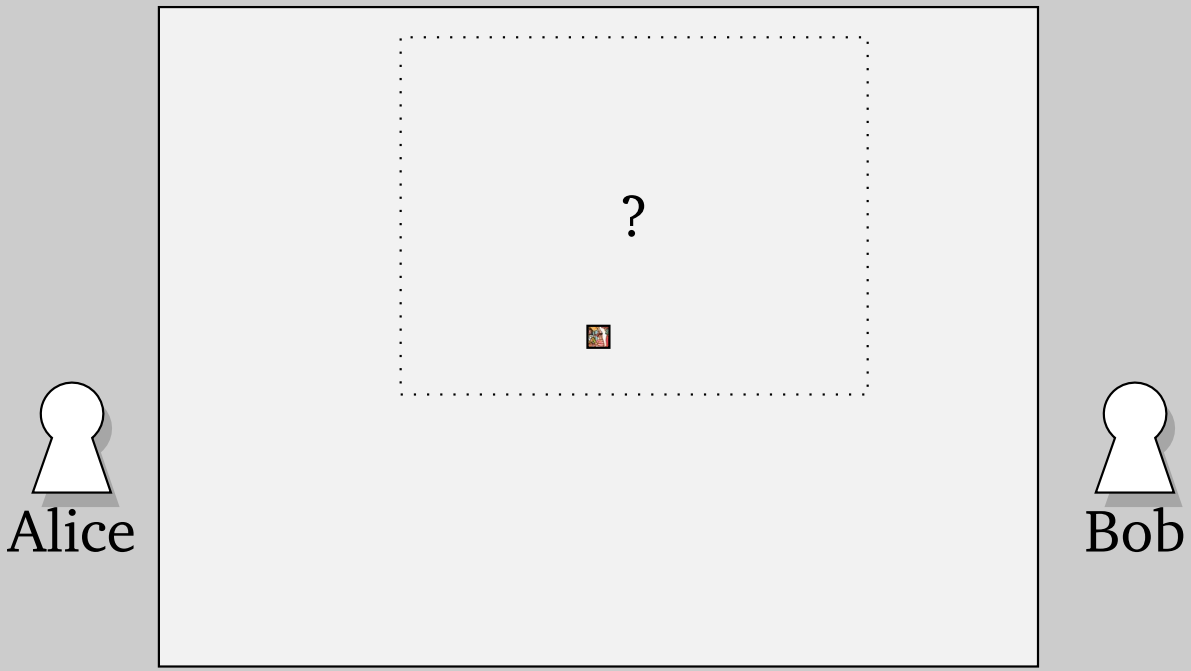


Solution:

1. Alice places opaque cardboard with hole over picture, revealing Waldo

Bob gets no information about Waldo's location within picture!

Where's Waldo? Solution



Solution:

1. Alice places opaque cardboard with hole over picture, revealing Waldo

Bob gets no information about Waldo's location within picture!

Philosophy

Fuzzy Definition

A zero-knowledge proof is a way to convince someone of a fact without giving out "any additional information"

Philosophy

Fuzzy Definition

A zero-knowledge proof is a way to convince someone of a fact without giving out "any additional information"

What does it mean to

- prove something?
- give out information?

What is a proof?

Classical Definition

A proof is a list of logical steps. Something that Alice can write down and send to Bob.

What is a proof?

Classical Definition

A proof is a list of logical steps. Something that Alice can write down and send to Bob.

Must a proof be "non-interactive?"

What is a proof?

Classical Definition

A proof is a list of logical steps. Something that Alice can write down and send to Bob.

Must a proof be "non-interactive?"

Today: Interactive Proofs

A Lady Testing Tea

Muriel

Ronald

A true story [R. Fisher, *Mathematics of a Lady Testing Tea*, 1956]:

A Lady Testing Tea

A true story [R. Fisher, *Mathematics of a Lady Testing Tea*, 1956]:

- M "Tea poured into milk tastes different than milk poured into tea."

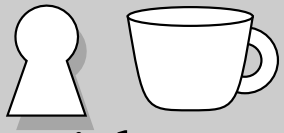
A Lady Testing Tea

A true story [R. Fisher, *Mathematics of a Lady Testing Tea*, 1956]:

M "Tea poured into milk tastes different than milk poured into tea."

R "Intriguing. Can you prove it?"

A Lady Testing Tea



A true story [R. Fisher, *Mathematics of a Lady Testing Tea*, 1956]:

M "Tea poured into milk tastes different than milk poured into tea."

R "Intriguing. Can you prove it?"

M "I'm just a tea connoisseur. *You're* the statistician."

A Lady Testing Tea

A true story [R. Fisher, *Mathematics of a Lady Testing Tea*, 1956]:

M "Tea poured into milk tastes different than milk poured into tea."

R "Intriguing. Can you prove it?"

M "I'm just a tea connoisseur. *You're* the statistician."

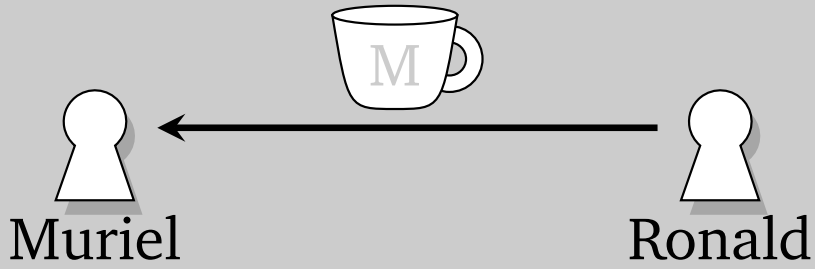
R "..."

Fisher's Smart Idea: Interactive Proof

Fisher's Smart Idea: Interactive Proof

Random challenge In private, flip a coin to decide which to pour first (tea or milk).

Fisher's Smart Idea: Interactive Proof



Random challenge In private, flip a coin to decide which to pour first (tea or milk). Give cup to Muriel.

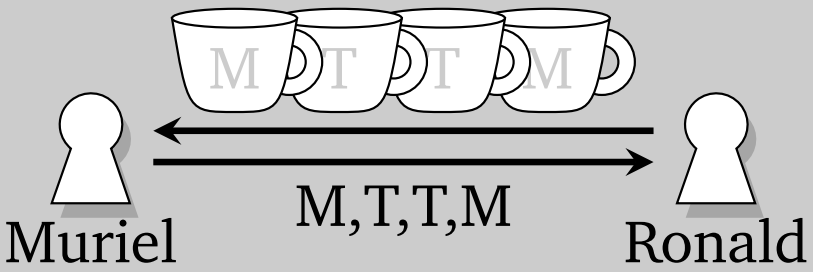
Fisher's Smart Idea: Interactive Proof

Random challenge In private, flip a coin to decide which to pour first (tea or milk). Give cup to Muriel.

Response Muriel guesses.

- If Muriel can really tell, she gets it right.
- If no difference in two kinds of teas, she has 1/2 chance of guessing correctly.

Fisher's Smart Idea: Interactive Proof



Random challenge In private, flip a coin to decide which to pour first (tea or milk). Give cup to Muriel.

Response Muriel guesses.

- If Muriel can really tell, she gets it right.
- If no difference in two kinds of teas, she has 1/2 chance of guessing correctly.

Repeat Repeat n times.

- If no difference in two kinds of teas, she has $(1/2)^n$ chance of guessing *all* correctly.

Epistemology: What is Knowledge?

Bad situation

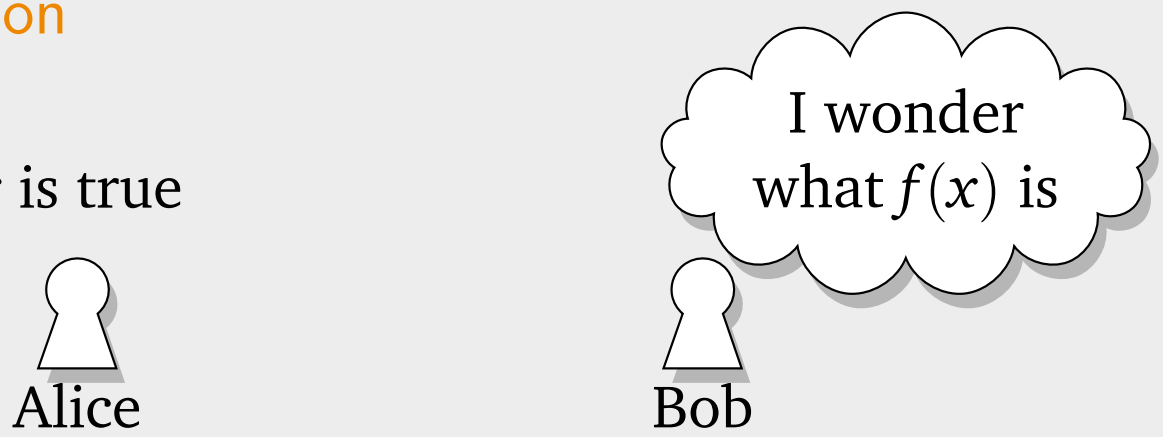
x is true

Alice

Bob

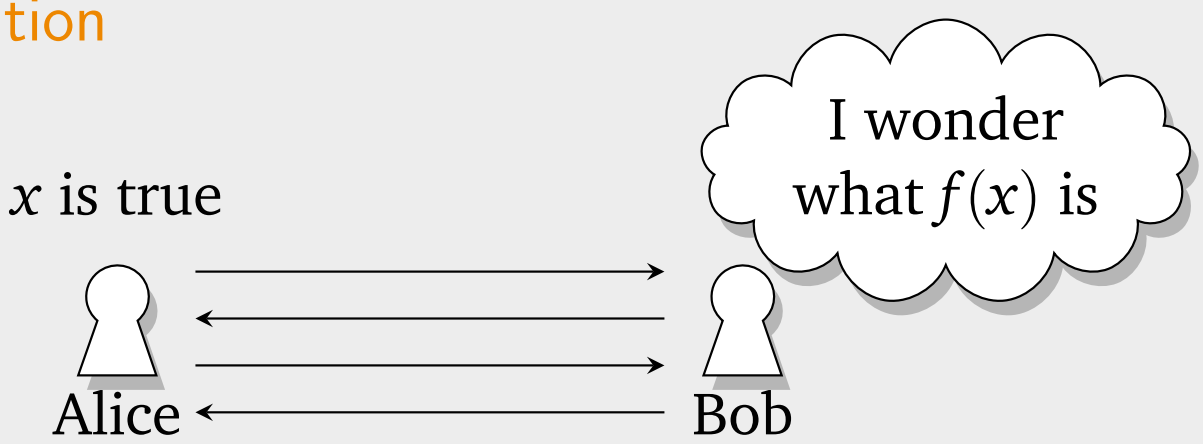
Epistemology: What is Knowledge?

Bad situation



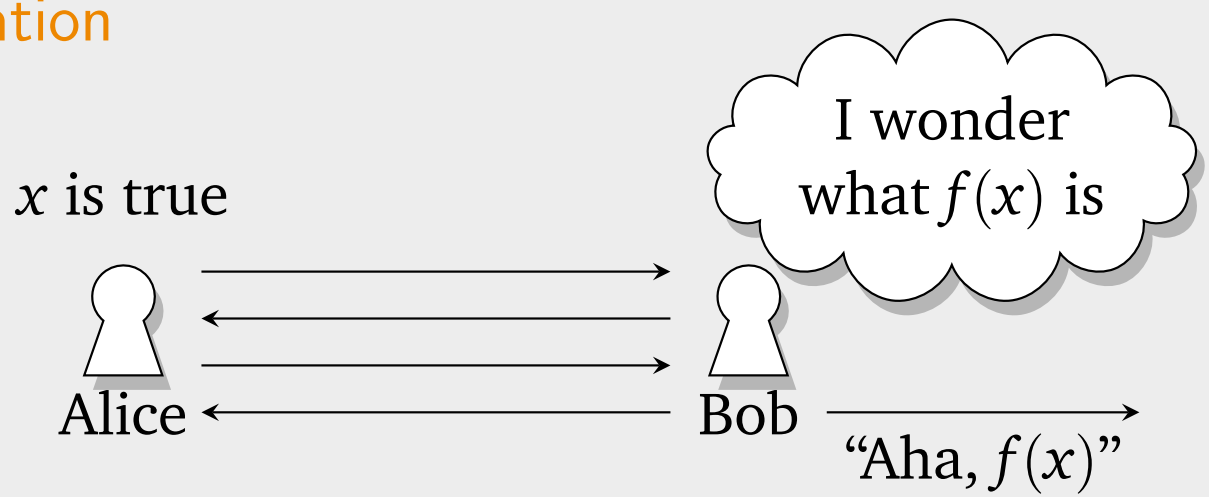
Epistemology: What is Knowledge?

Bad situation



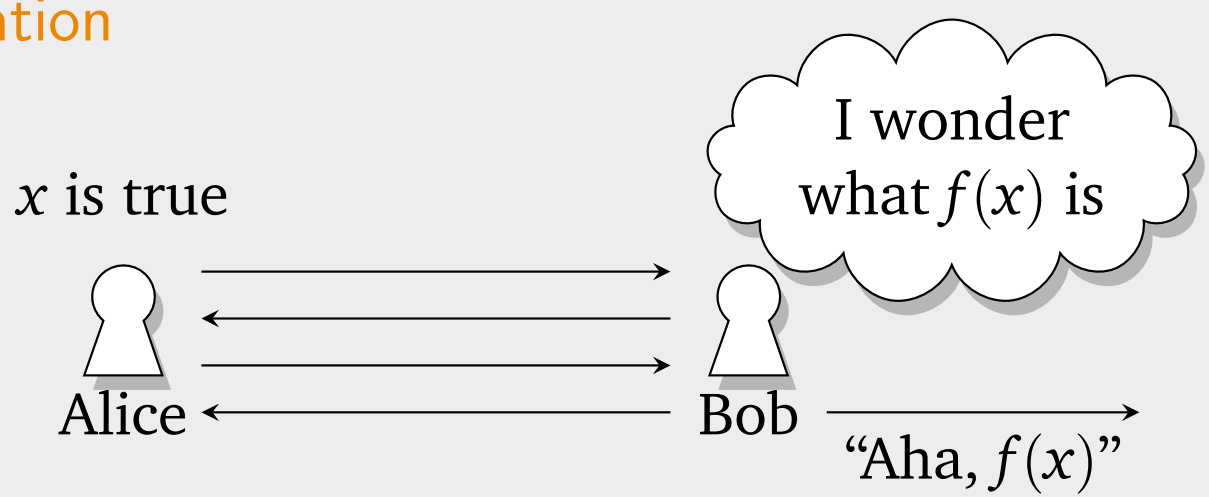
Epistemology: What is Knowledge?

Bad situation



Epistemology: What is Knowledge?

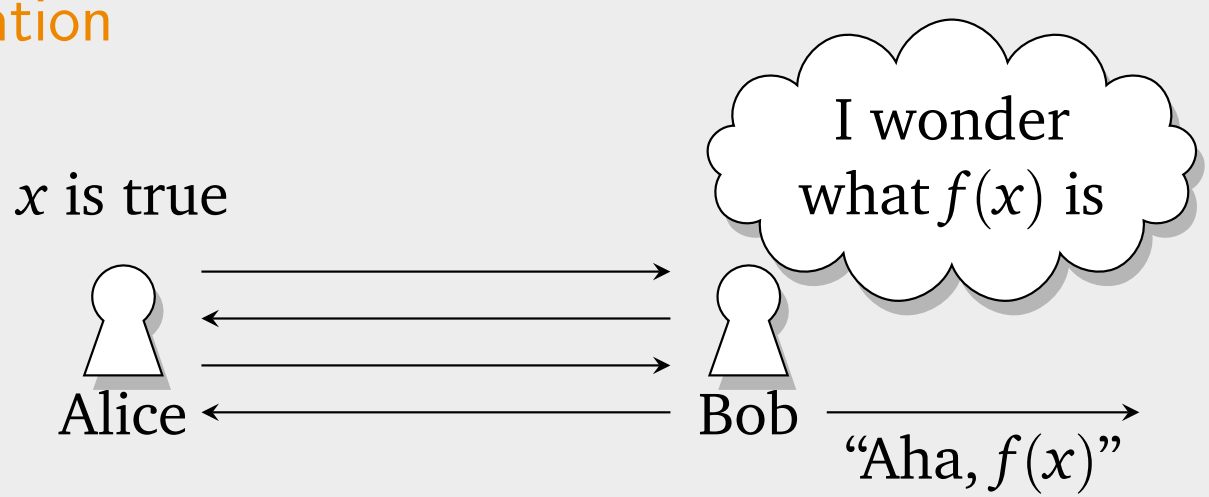
Bad situation



- This situation is bad if Bob couldn't have computed $f(x)$ before the interaction

Epistemology: What is Knowledge?

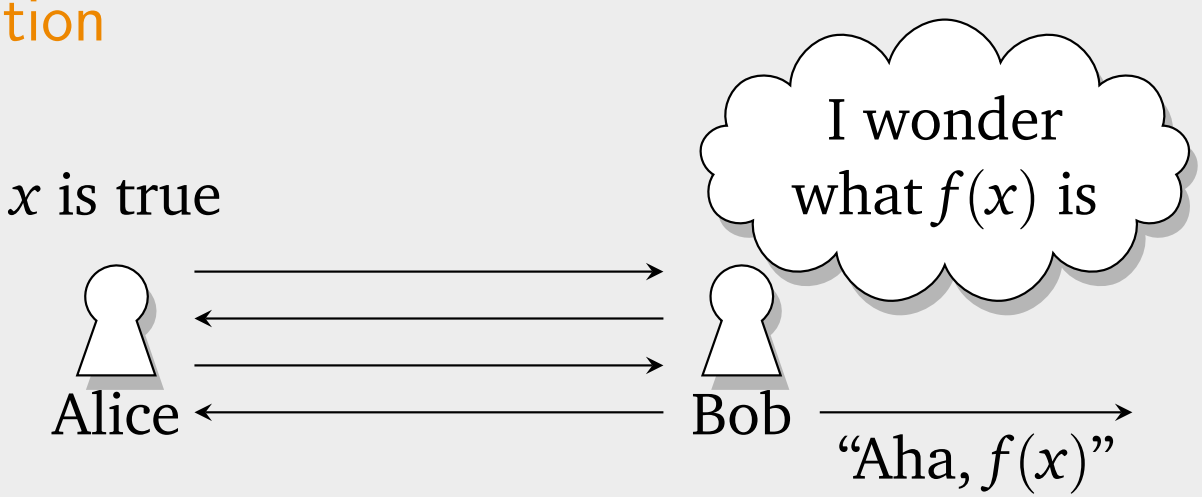
Bad situation



- This situation is bad if Bob couldn't have computed $f(x)$ before the interaction
- Interaction transcript gives him knowledge

Epistemology: What is Knowledge?

Bad situation



- This situation is bad if Bob couldn't have computed $f(x)$ before the interaction
- Interaction transcript gives him knowledge

Zero Knowledge (Want to say):

Everything Bob can compute *after* seeing the transcript, he could have computed *before* seeing the transcript.

Transcript Simulation

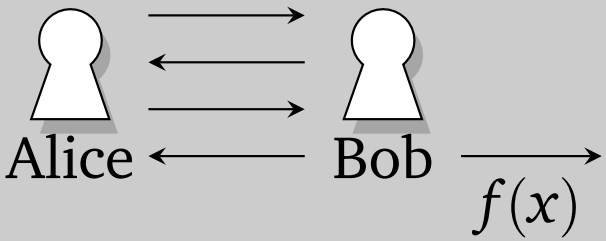
Clever Definition

Interaction is zero-knowledge if Bob could generate transcripts without interacting with Alice:

Transcript Simulation

Clever Definition

Interaction is zero-knowledge if Bob could generate transcripts without interacting with Alice:

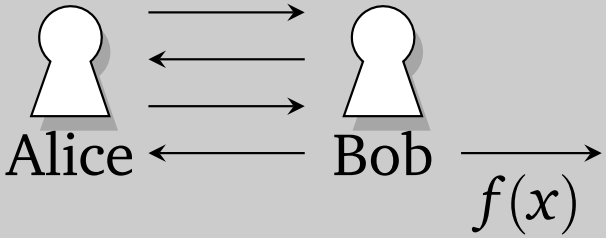


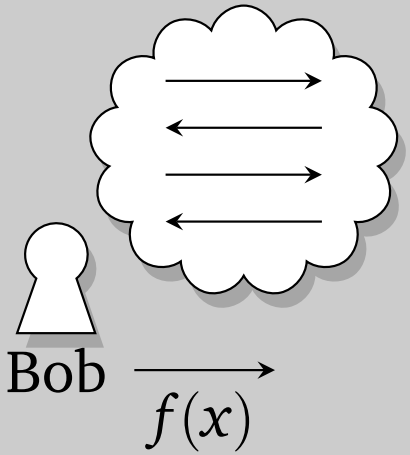
Whatever Bob could compute *after* seeing the transcript ...

Transcript Simulation

Clever Definition

Interaction is zero-knowledge if Bob could generate transcripts without interacting with Alice:





Whatever Bob could compute *after* seeing the transcript ...

... there is a way to compute without interaction!

Apparent Paradox

Paradox?

- Transcript should *convince* Bob of something new
- Bob could have generated transcript himself

Apparent Paradox


Bob


Charlie

- “Alice can tell whether tea is poured into milk or vice-versa!”

Apparent Paradox


Bob


Charlie

B "Alice can tell whether tea is poured into milk or vice-versa!"

C "Oh really?"

Apparent Paradox

B "Alice can tell whether tea is poured into milk or vice-versa!"

C "Oh really?"

B "Yes, see all these correctly identified tea cups??"

Apparent Paradox

B "Alice can tell whether tea is poured into milk or vice-versa!"

C "Oh really?"

B "Yes, see all these correctly identified tea cups??"

C "You dummy, anyone can fill a tea cup and label it!"

Apparent Paradox

B "Alice can tell whether tea is poured into milk or vice-versa!"

C "Oh really?"

B "Yes, see all these correctly identified tea cups??"

C "You dummy, anyone can fill a tea cup and label it!"

B "But I picked the kind of pouring at random, and she was able to answer every time!"

Apparent Paradox

B "Alice can tell whether tea is poured into milk or vice-versa!"

C "Oh really?"

B "Yes, see all these correctly identified tea cups??"

C "You dummy, anyone can fill a tea cup and label it!"

B "But I picked the kind of pouring at random, and she was able to answer every time!"

Bob already knew the correct responses to challenges

- Convinced by *how* the transcript was generated (in response to his challenges)

Formal Definition

Definition [GMR 1985]

A zero-knowledge proof is an interactive protocol satisfying:

- The prover can always convince the verifier of any true statement

Formal Definition

Definition [GMR 1985]

A zero-knowledge proof is an interactive protocol satisfying:

- The prover can always convince the verifier of any true statement
- The verifier can't be convinced of a false statement (even by a cheating prover), except with very low probability

Formal Definition

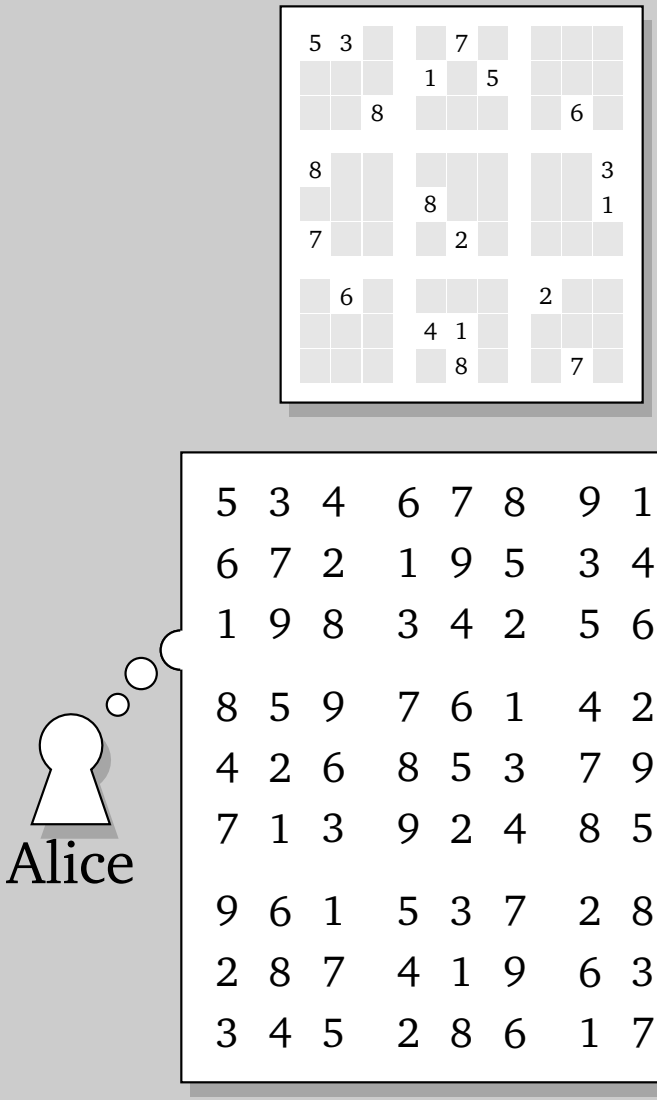
Definition [GMR 1985]

A zero-knowledge proof is an interactive protocol satisfying:

- The prover can always convince the verifier of any true statement
- The verifier can't be convinced of a false statement (even by a cheating prover), except with very low probability
- There is an efficient procedure to output "same-looking" protocol transcripts

Sudoku Zero-Knowledge Proof

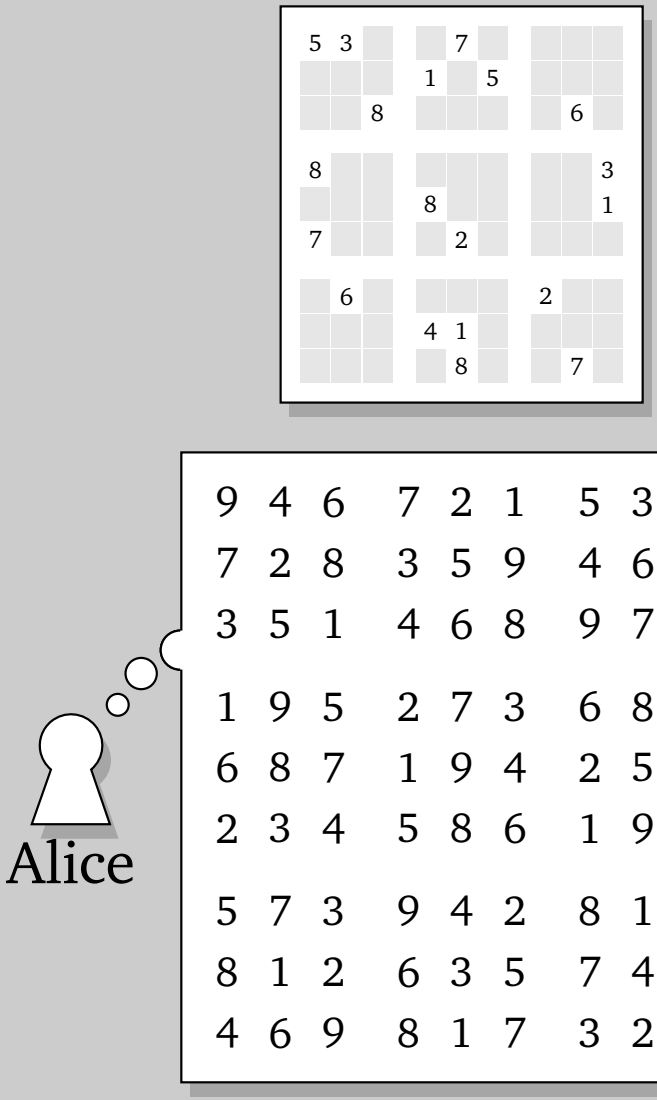
Zero-knowledge protocol:



Sudoku Zero-Knowledge Proof

Zero-knowledge protocol:

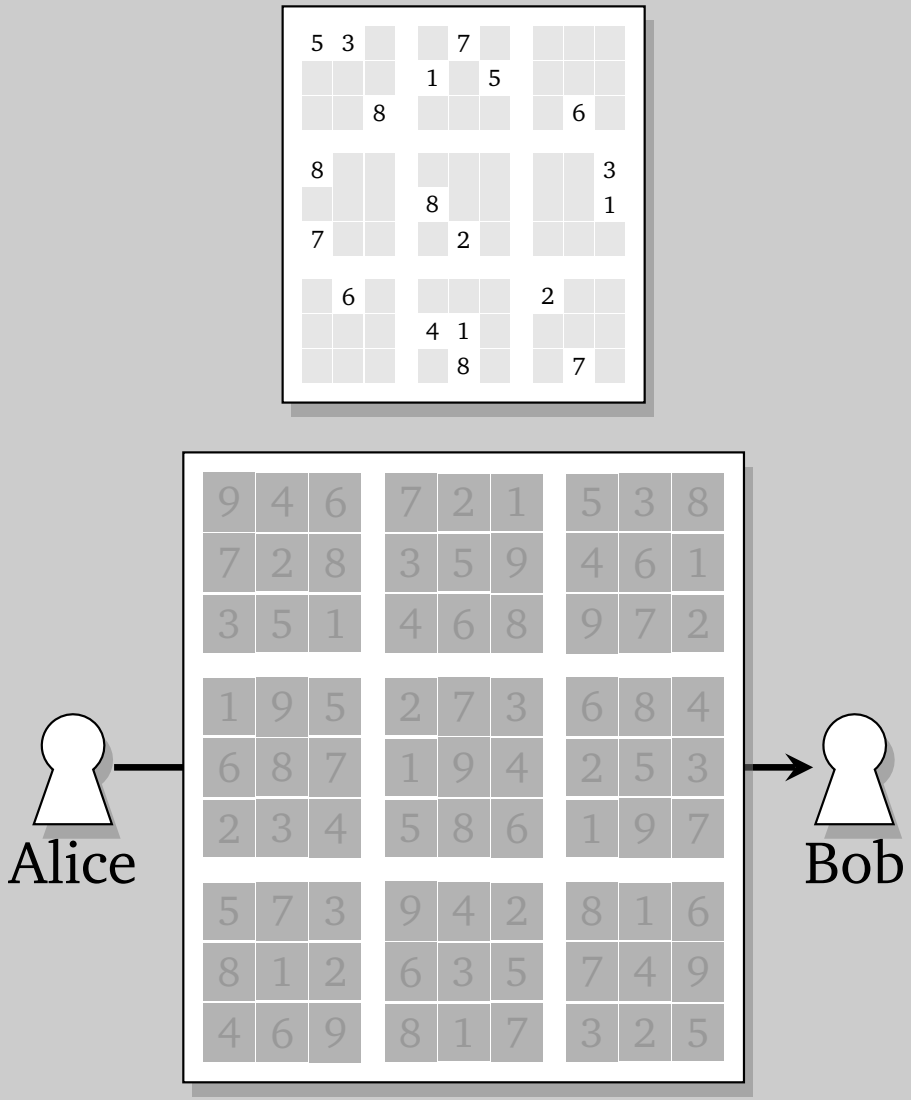
1. Alice randomly relabels $\{1, \ldots, 9\}$



Sudoku Zero-Knowledge Proof

Zero-knowledge protocol:

1. Alice randomly relabels $\{1, \ldots, 9\}$
2. Alice writes relabeled solution on scratch card, shows to Bob

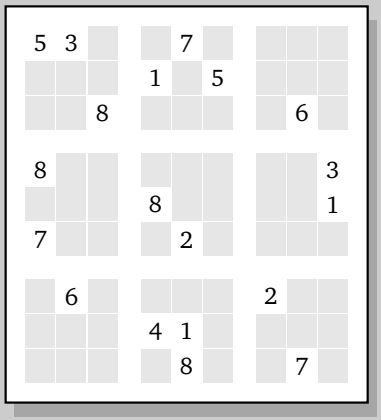


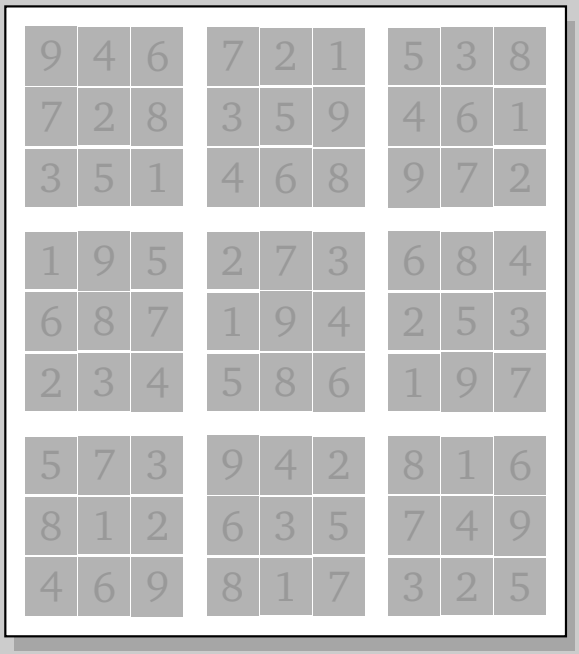
Sudoku Zero-Knowledge Proof

Zero-knowledge protocol:

1. Alice randomly relabels $\{1, \ldots, 9\}$
2. Alice writes relabeled solution on scratch card, shows to Bob
3. Bob asks Alice to scratch off either:

and checks consistency



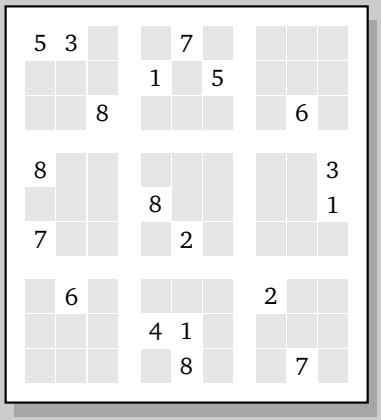


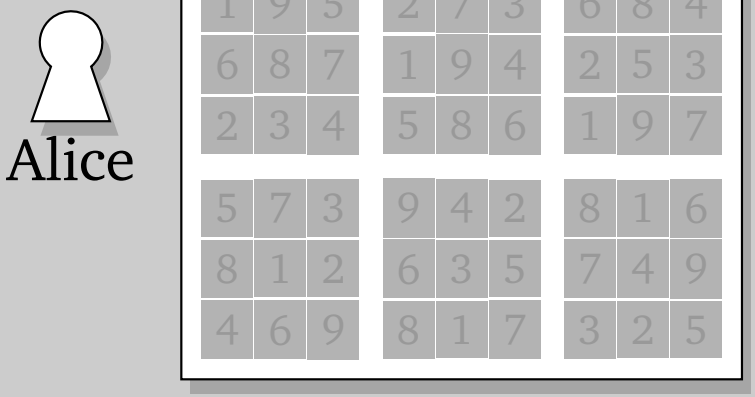
Sudoku Zero-Knowledge Proof

Zero-knowledge protocol:

1. Alice randomly relabels $\{1, \ldots, 9\}$
2. Alice writes relabeled solution on scratch card, shows to Bob
3. Bob asks Alice to scratch off either:
   - A particular row

and checks consistency





Alice

row 2

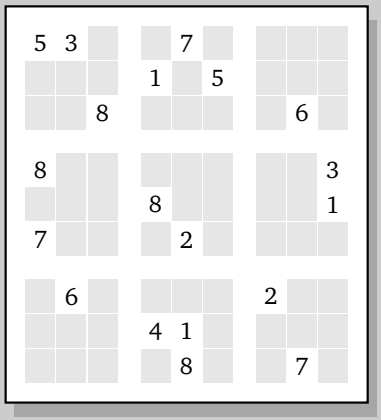
Bob

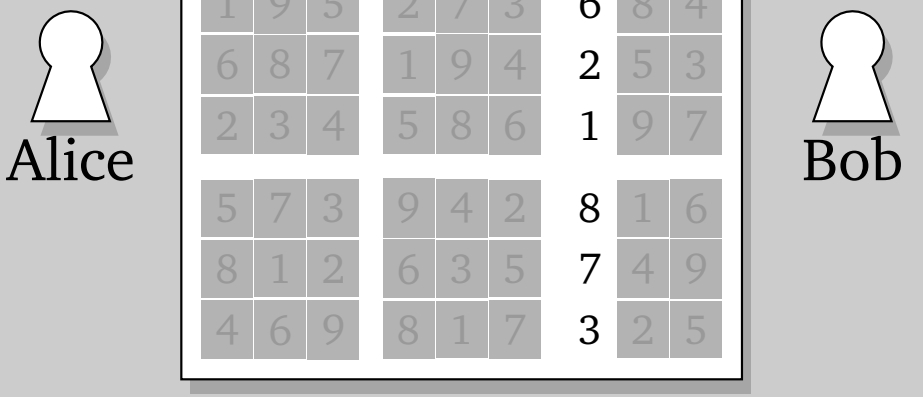
Sudoku Zero-Knowledge Proof

Zero-knowledge protocol:

1. Alice randomly relabels $\{1, \ldots, 9\}$
2. Alice writes relabeled solution on scratch card, shows to Bob
3. Bob asks Alice to scratch off either:
   - A particular row
   - A particular column

and checks consistency



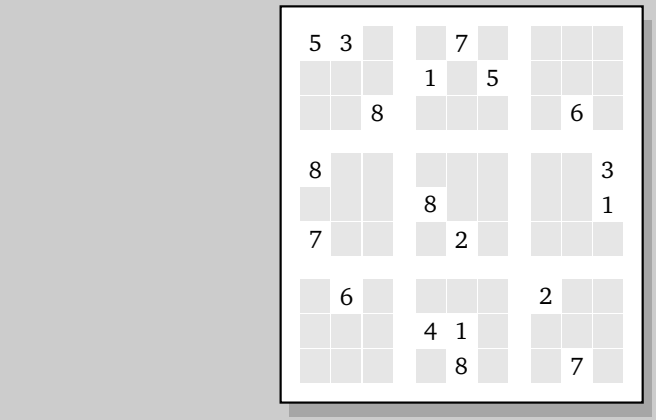


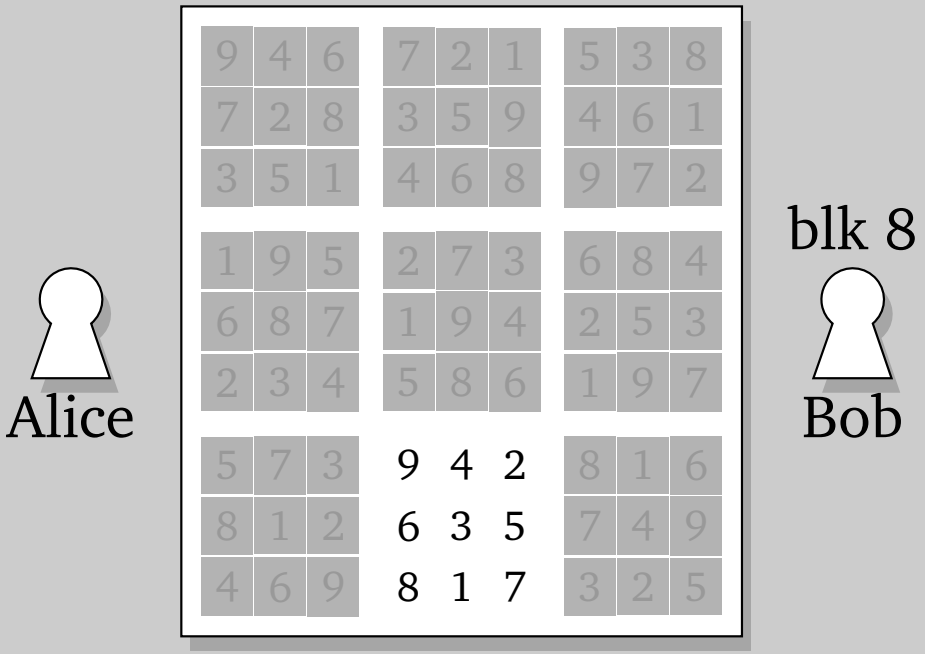
Sudoku Zero-Knowledge Proof

Zero-knowledge protocol:

1. Alice randomly relabels $\{1, \ldots, 9\}$
2. Alice writes relabeled solution on scratch card, shows to Bob
3. Bob asks Alice to scratch off either:
   - A particular row
   - A particular column
   - A particular 3×3 block

   and checks consistency



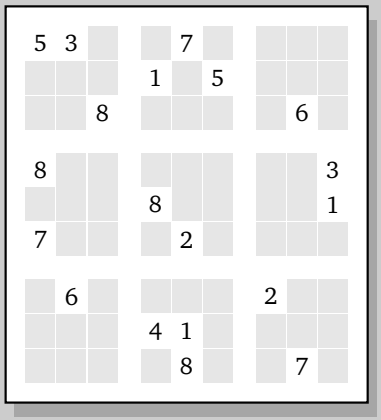


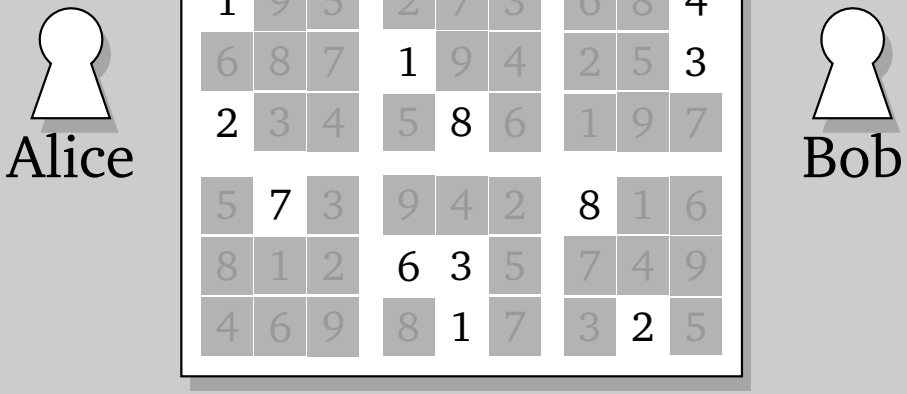
Sudoku Zero-Knowledge Proof

Zero-knowledge protocol:

1. Alice randomly relabels $\{1, \ldots, 9\}$
2. Alice writes relabeled solution on scratch card, shows to Bob
3. Bob asks Alice to scratch off either:
   - A particular row
   - A particular column
   - A particular 3×3 block
   - Initial positions

   and checks consistency



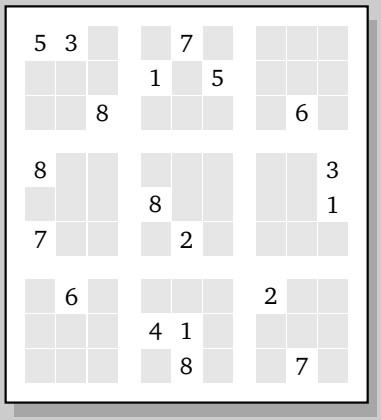


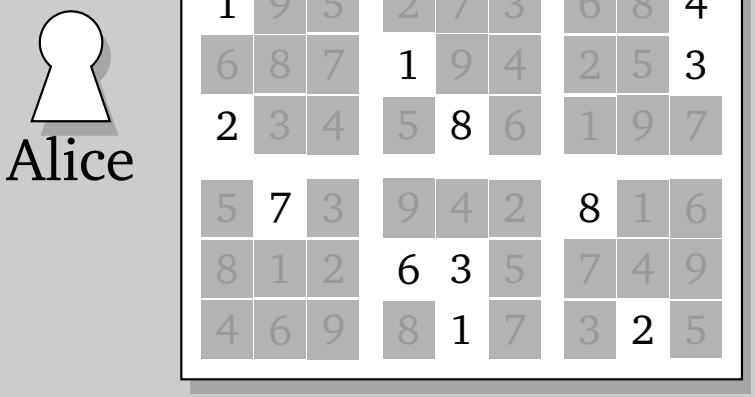
Sudoku Zero-Knowledge Proof

Zero-knowledge protocol:

1. Alice randomly relabels $\{1, \ldots, 9\}$
2. Alice writes relabeled solution on scratch card, shows to Bob
3. Bob asks Alice to scratch off either:
   - A particular row
   - A particular column
   - A particular 3×3 block
   - Initial positions

   and checks consistency
4. Repeat n times





Sudoku Zero-Knowledge Proof, Analysis

Observation

If Alice can answer all challenges successfully, her scratch card satisfies:

- Every row, column, block is permutation of $\{1, \ldots, 9\}$
- Initial positions consistent with relabeling of $\{1, \ldots, 9\}$ in original puzzle

Sudoku Zero-Knowledge Proof, Analysis

Observation

If Alice can answer all challenges successfully, her scratch card satisfies:

- Every row, column, block is permutation of $\{1, \ldots, 9\}$
- Initial positions consistent with relabeling of $\{1, \ldots, 9\}$ in original puzzle

Then the original puzzle has a solution.

Sudoku Zero-Knowledge Proof, Analysis

Observation

If Alice can answer all challenges successfully, her scratch card satisfies:

- Every row, column, block is permutation of $\{1, \ldots, 9\}$
- Initial positions consistent with relabeling of $\{1, \ldots, 9\}$ in original puzzle

Then the original puzzle has a solution.

What if Alice is cheating (there really is no solution)?

Sudoku Zero-Knowledge Proof, Analysis

Observation

If Alice can answer all challenges successfully, her scratch card satisfies:

- Every row, column, block is permutation of $\{1, \ldots, 9\}$
- Initial positions consistent with relabeling of $\{1, \ldots, 9\}$ in original puzzle

Then the original puzzle has a solution.

What if Alice is cheating (there really is no solution)?

$\Rightarrow$ No scratch card can correctly answer all challenges.

Sudoku Zero-Knowledge Proof, Analysis

Suppose Alice tries to prove an incorrect statement. Let c be a challenge that is bad for Alice's scratch card.

- Bob picks random challenge (28 choices)
- With probability 1/28, Bob chooses c and Alice is caught!
- With probability $\leq 27/28$, Alice's cheating undetected

Sudoku Zero-Knowledge Proof, Analysis

Suppose Alice tries to prove an incorrect statement. Let c be a challenge that is bad for Alice's scratch card.

- Bob picks random challenge (28 choices)
- With probability 1/28, Bob chooses c and Alice is caught!
- With probability $\leq 27/28$, Alice's cheating undetected

Key Idea

Repeat protocol n times. Alice cheats undetected in all rounds with probability $(27/28)^n \approx (1/2)^{0.05n}$

Sudoku Zero-Knowledge Proof, Analysis

Suppose Alice tries to prove an incorrect statement. Let c be a challenge that is bad for Alice's scratch card.

- Bob picks random challenge (28 choices)
- With probability 1/28, Bob chooses c and Alice is caught!
- With probability $\leq 27/28$, Alice's cheating undetected

Key Idea

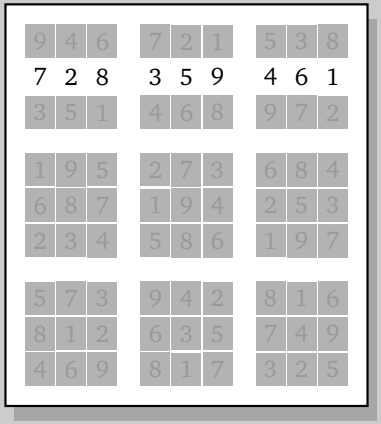
Repeat protocol n times. Alice cheats undetected in all rounds with probability $(27/28)^n \approx (1/2)^{0.05n}$

When $n = 2500$, Alice caught with 99% probability.

Sudoku Zero-Knowledge Proof, Analysis

If Alice follows protocol (there is a solution), then each round transcript is:

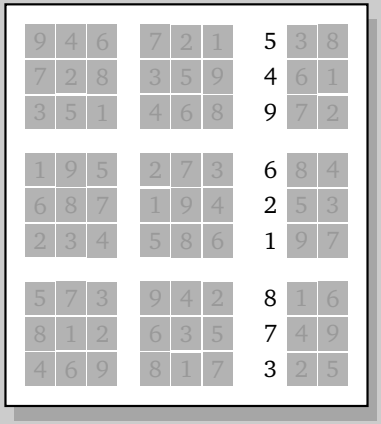
Sudoku Zero-Knowledge Proof, Analysis



If Alice follows protocol (there is a solution), then each round transcript is:

- Random permutation of $\{1, \ldots, 9\}$ in random row,

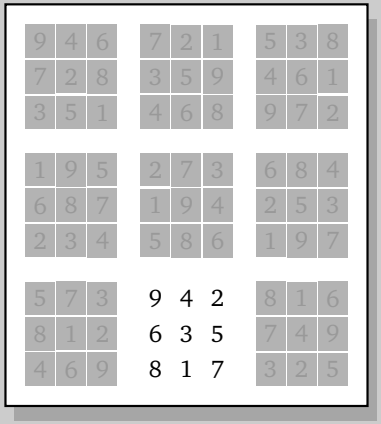
Sudoku Zero-Knowledge Proof, Analysis



If Alice follows protocol (there is a solution), then each round transcript is:

- Random permutation of $\{1, \ldots, 9\}$ in random row,
- Random permutation of $\{1, \ldots, 9\}$ in random column,

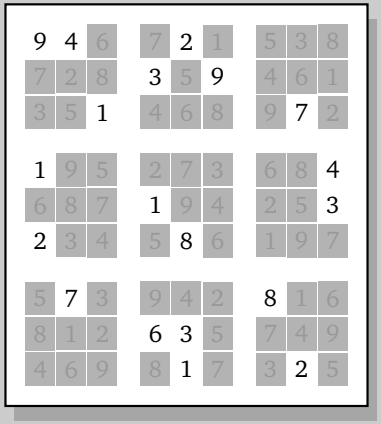
Sudoku Zero-Knowledge Proof, Analysis



If Alice follows protocol (there is a solution), then each round transcript is:

- Random permutation of $\{1, \ldots, 9\}$ in random row,
- Random permutation of $\{1, \ldots, 9\}$ in random column,
- Random permutation of $\{1, \ldots, 9\}$ in random block, or

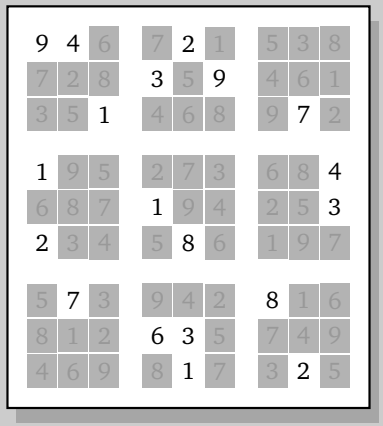
Sudoku Zero-Knowledge Proof, Analysis



If Alice follows protocol (there is a solution), then each round transcript is:

- Random permutation of $\{1, \ldots, 9\}$ in random row,
- Random permutation of $\{1, \ldots, 9\}$ in random column,
- Random permutation of $\{1, \ldots, 9\}$ in random block, or
- Random relabeling of original puzzle's initial positions

Sudoku Zero-Knowledge Proof, Analysis



If Alice follows protocol (there is a solution), then each round transcript is:

- Random permutation of $\{1, \ldots, 9\}$ in random row,
- Random permutation of $\{1, \ldots, 9\}$ in random column,
- Random permutation of $\{1, \ldots, 9\}$ in random block, or
- Random relabeling of original puzzle's initial positions

Each of these Bob could have generated himself (without the solution)!

Zero-Knowledge Proofs for *Everything?*

We have a zero-knowledge proof protocol for Sudoku, so what?

Zero-Knowledge Proofs for *Everything?*

We have a zero-knowledge proof protocol for Sudoku, so what?

Theorem [Yato 2003]

$n \times n$ Sudoku is NP-complete. (Take 600.271 and 600.363)

Zero-Knowledge Proofs for *Everything?*

We have a zero-knowledge proof protocol for Sudoku, so what?

Theorem [Yato 2003]

$n \times n$ Sudoku is NP-complete. (Take 600.271 and 600.363)

Every (practical) statement can be expressed in terms of the solvability of a (generalized) Sudoku instance.

Zero-Knowledge Proofs for *Everything?*

We have a zero-knowledge proof protocol for Sudoku, so what?

Theorem [Yato 2003]

$n \times n$ Sudoku is NP-complete. (Take 600.271 and 600.363)

Every (practical) statement can be expressed in terms of the solvability of a (generalized) Sudoku instance.

- Given statement x, can compute puzzle $S(x)$

Zero-Knowledge Proofs for *Everything?*

We have a zero-knowledge proof protocol for Sudoku, so what?

Theorem [Yato 2003]

$n \times n$ Sudoku is NP-complete. (Take 600.271 and 600.363)

Every (practical) statement can be expressed in terms of the solvability of a (generalized) Sudoku instance.

- Given statement x, can compute puzzle $S(x)$
- x is true $\iff$ $S(x)$ is a solvable Sudoku puzzle

Zero-Knowledge Proofs for *Everything?*

We have a zero-knowledge proof protocol for Sudoku, so what?

Theorem [Yato 2003]

$n \times n$ Sudoku is NP-complete. (Take 600.271 and 600.363)

Every (practical) statement can be expressed in terms of the solvability of a (generalized) Sudoku instance.

- Given statement x, can compute puzzle $S(x)$
- x is true $\iff$ $S(x)$ is a solvable Sudoku puzzle
- To prove x, use Sudoku ZK on $S(x)$

Zero-Knowledge Proofs for *Everything?*

We have a zero-knowledge proof protocol for Sudoku, so what?

Theorem [Yato 2003]

$n \times n$ Sudoku is NP-complete. (Take 600.271 and 600.363)

Every (practical) statement can be expressed in terms of the solvability of a (generalized) Sudoku instance.

- Given statement x, can compute puzzle $S(x)$
- x is true $\iff$ $S(x)$ is a solvable Sudoku puzzle
- To prove x, use Sudoku ZK on $S(x)$

Theorem

Every NP statement can be proven in zero-knowledge.

What are They Good For?

Lots of things!

What are They Good For?

Lots of things!

- Authentication without passwords

What are They Good For?

Lots of things!

- Authentication without passwords
- Proving Physical Statements! (e.g., Nuclear Disarmament, Glaser-Barak-Goldston, 2012)

What are They Good For?

Lots of things!

- Authentication without passwords
- Proving Physical Statements! (e.g., Nuclear Disarmament, Glaser-Barak-Goldston, 2012)
- Stronger encryption

What are They Good For?

Lots of things!

- Authentication without passwords
- Proving Physical Statements! (e.g., Nuclear Disarmament, Glaser-Barak-Goldston, 2012)
- Stronger encryption
- Forcing people to behave ”honestly”...

What are They Good For?

Lots of things!

- Authentication without passwords
- Proving Physical Statements! (e.g., Nuclear Disarmament, Glaser-Barak-Goldston, 2012)
- Stronger encryption
- Forcing people to behave ”honestly”...

Disclaimer: ZK proofs **very bad** for teaching courses:

- Students convinced that professor knows a lot
- Students gained no additional knowledge

Like Cryptography?

Take 600.442!

Thanks for your attention!

fin.

I hope this was a “talk about zero knowledge,”
not a “zero-knowledge talk.”