Secrets Kept, Truth Proved: The Magic of Zero Knowledge Proofs

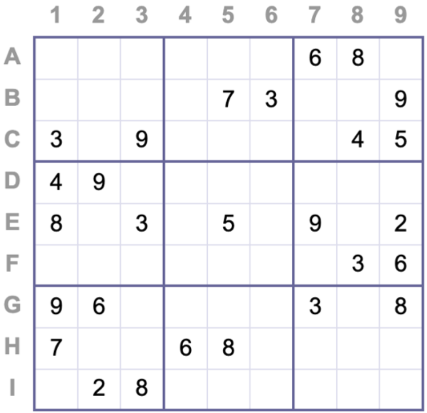
Nilanjan Datta

Associate Professor, IAI, TCG CREST

CCSS 2025

June 26, 2025

Solving Sudoku



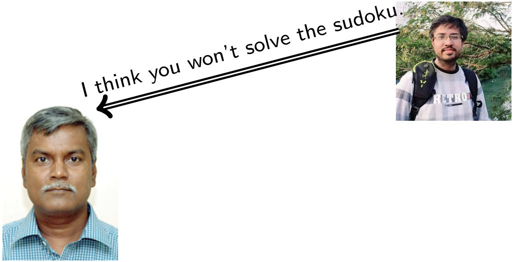
	1	2	3	4	5	6	7	8	9
A							6	8	
B					7	3			9
C	3		9					4	5
D	4	9							
E	8		3		5		9		2
F								3	6
G	9	6					3		8
H	7			6	8				
I		2	8						

Each cell must contain a number (1–9) that is unique to the row, column, and 3x3 grid.

Motivation

World Sudoku Championship

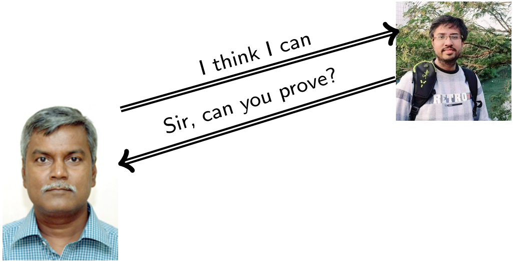
Motivation



I think you won't solve the sudoku.

World Sudoku Championship

Motivation



I think I can

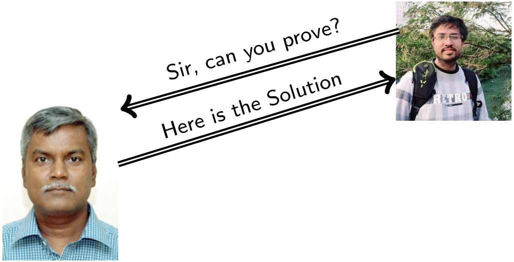
Sir, can you prove?

SUDOKU & PUZZLE WORLD CHAMPIONSHIPS 2022

News WSC WPC Location & fee FAQ Pictures Register Forum

World Sudoku Championship

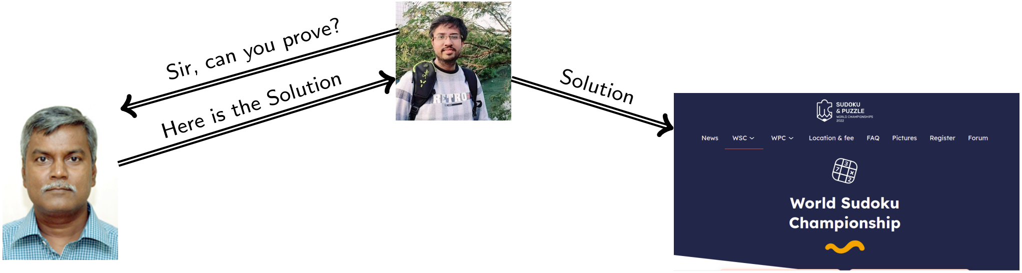
Motivation



Sir, can you prove?

Here is the Solution

Motivation



Sir, can you prove?

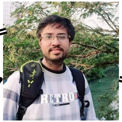
Here is the Solution

Solution

Motivation

Sir, can you prove?

Here is the Solution



Solution

World Sudoku Championship

Zero Knowledge Proof [GMR]

- Conceived in 1985 by Shafi Goldwasser, Silvio Micali, and Charles Rackoff **[SIAM'85]**.
- Received **Godel Prize** in 1993 for advances in Theoretical Computer Science.

I. Proofs and Proof System

Notion of Proof

What is Proof ?

Notion of Proof

What is Proof ?

“A proof is whatever convinces me” – Shimon Even (1978)

Notion of Proof

A proof involves two parties:

- Prover – One who supplies the proof in favor of the statement
- Verifier – One who verifies the proof

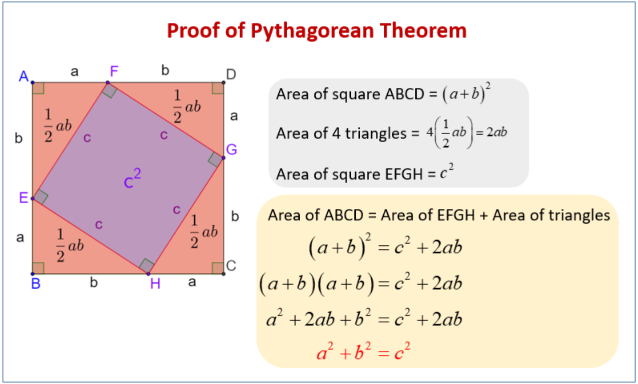
Notion of Proof

A proof involves two parties:

- Prover – One who supplies the proof in favor of the statement
- Verifier – One who verifies the proof

A proof should be easily verifiable.

Types of Proofs: Classical Proof



Proof of Pythagorean Theorem

Area of square ABCD = $(a+b)^2$

Area of 4 triangles = $4\left(\frac{1}{2}ab\right) = 2ab$

Area of square EFGH = c^2

Area of ABCD = Area of EFGH + Area of triangles

$$(a+b)^2 = c^2 + 2ab$$

$$(a+b)(a+b) = c^2 + 2ab$$

$$a^2 + 2ab + b^2 = c^2 + 2ab$$

$$a^2 + b^2 = c^2$$

Types of Proofs: Classical Proof

- The proof is fixed and written somewhere which is either
    - Self-evident, or
    - Derived from self-evident rules.
- These proofs are static in nature.
- Examples: Mathematical proofs.

Types of Proofs: Interactive Proof

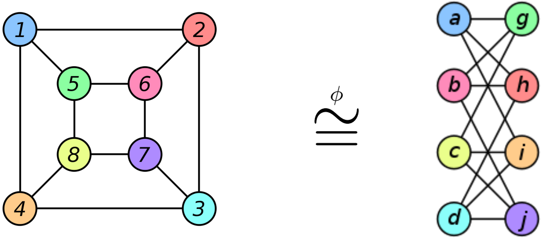
- Proof involves exchanges of information in multiple rounds between prover and verifier.
- Truth is established when the verifier accepts the hypothesis.
- Proof is dynamic in nature.
- Example: Legal Proofs in Court.

The Notion of Proof System

- Efficient - Verification of the proof should be simple
- Completeness - True statement must have a proof
- Soundness - False statement does not have any proof

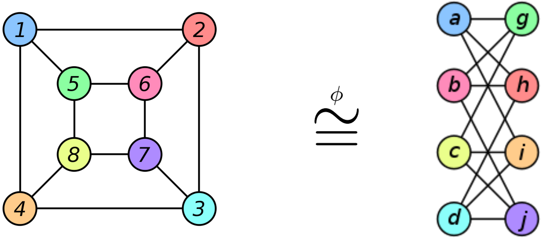
An Example of a Classical Valid Proof System

Graph Isomorphism



An Example of a Classical Valid Proof System

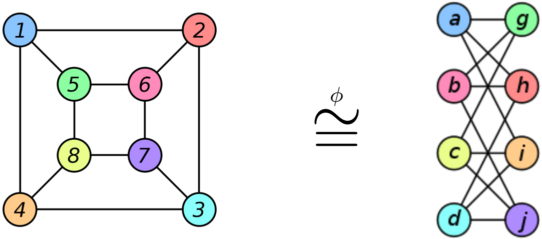
Graph Isomorphism



Isomorphism

$$\{\phi(1) = a, \phi(2) = h, \phi(3) = d, \phi(4) = i, \phi(5) = g, \phi(6) = b, \phi(7) = j, \phi(8) = c\}$$

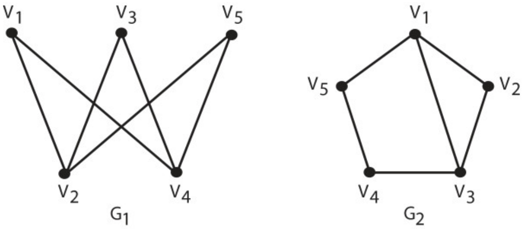
An Example of a Classical Valid Proof System



- Prover (P) sends ϕ as the proof to the verifier (V)
- V verifies ϕ is a valid permutation.
- Proof is complete and sound.
- No interaction between P and V

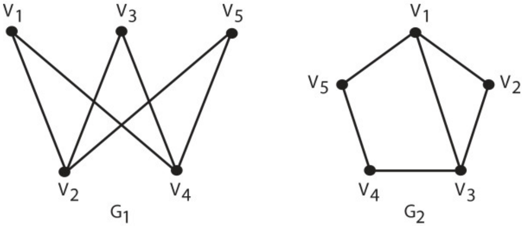
An Example where a Classical Proof System does not Work

Graph Non-Isomorphism (GNI)



An Example where a Classical Proof System does not Work

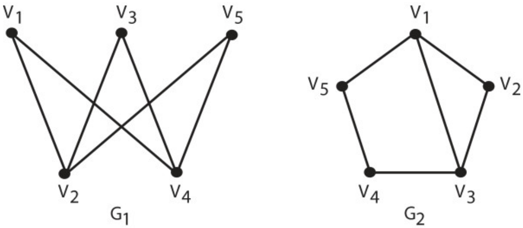
Graph Non-Isomorphism (GNI)



- Prover (P) sends all possible permutations ϕ on G_1 to V.
- Hard to verify..!!

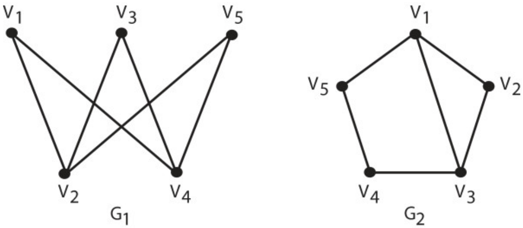
An Example where a Classical Proof System does not Work

Graph Non-Isomorphism (GNI)



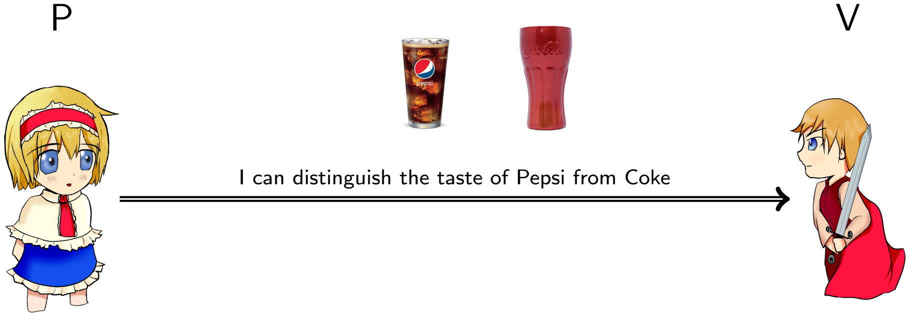
An Example where a Classical Proof System does not Work

Graph Non-Isomorphism (GNI)



- Need Interactive Proof System.

Distinguishing Problem – An Example of IP



P

V

I can distinguish the taste of Pepsi from Coke

Distinguishing Problem – An Example of IP

P

V

I can distinguish the taste of Pepsi from Coke

I don't believe you

Distinguishing Problem – An Example of IP

P

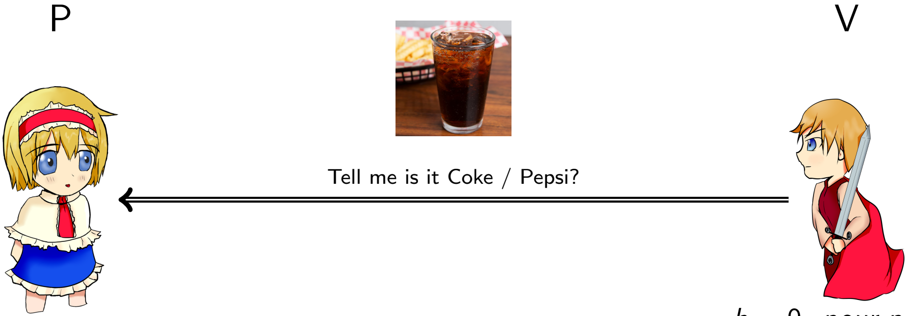
V

I can distinguish the taste of Pepsi from Coke

I don't believe you

How does P prove her claim to V ?

Distinguishing Problem – An Example of IP



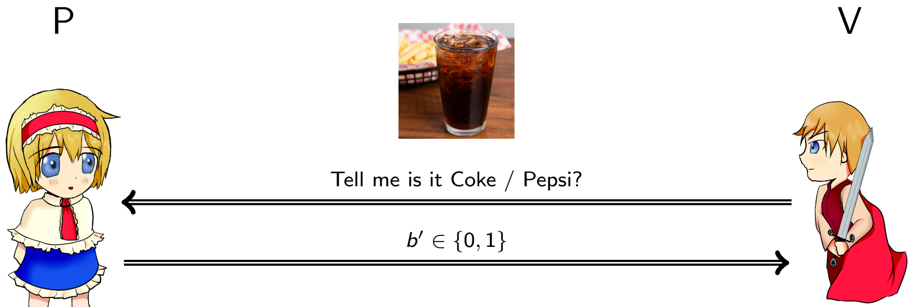
P

V

Tell me is it Coke / Pepsi?

$b = 0$, pour pepsi
$b = 1$, pour coke

Distinguishing Problem – An Example of IP



P

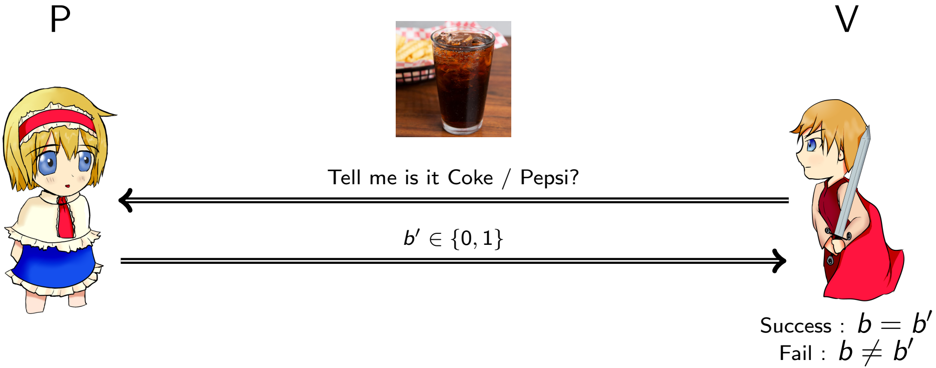
V

Tell me is it Coke / Pepsi?

$b' \in \{0, 1\}$

$b = 0,$ pour pepsi
$b = 1,$ pour coke

Distinguishing Problem – An Example of IP



P

V

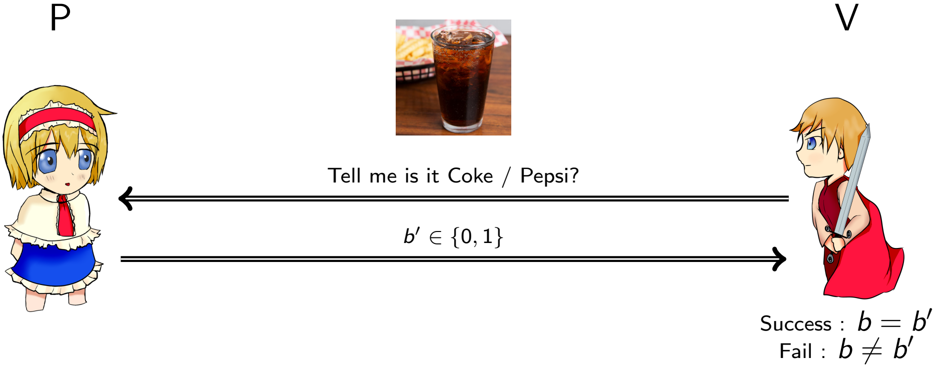
Tell me is it Coke / Pepsi?

$b' \in \{0, 1\}$

Success : $b = b'$

Fail : $b \neq b'$

Distinguishing Problem – An Example of IP



P

V

Tell me is it Coke / Pepsi?

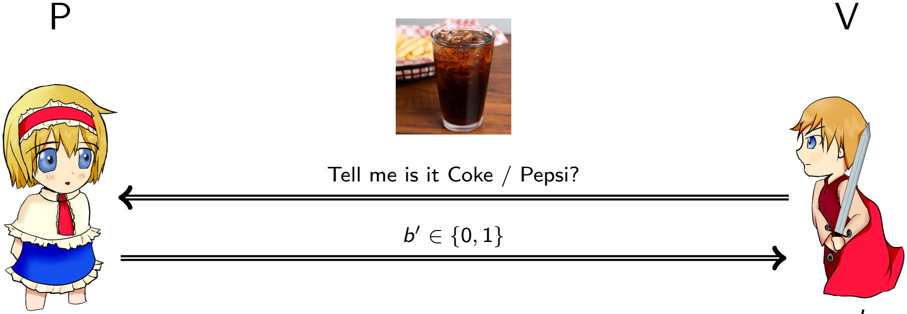
$b' \in \{0, 1\}$

Success : $b = b'$

Fail : $b \neq b'$

- If P really knows the difference then it always succeeds – **(Complete)**

Distinguishing Problem – An Example of IP



P

V

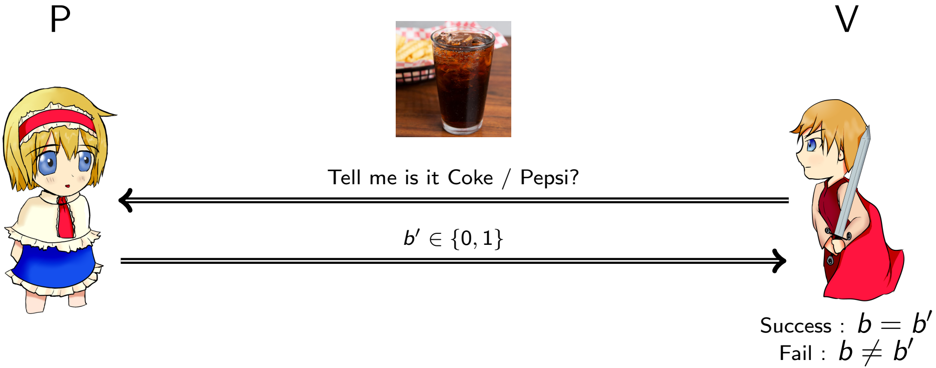
Tell me is it Coke / Pepsi?

$b' \in \{0,1\}$

Success : $b = b'$
Fail : $b \neq b'$

- If P really knows the difference then it always succeeds – **(Complete)**
- If P does not know, then it fails with probability (?)

Distinguishing Problem – An Example of IP



P

V

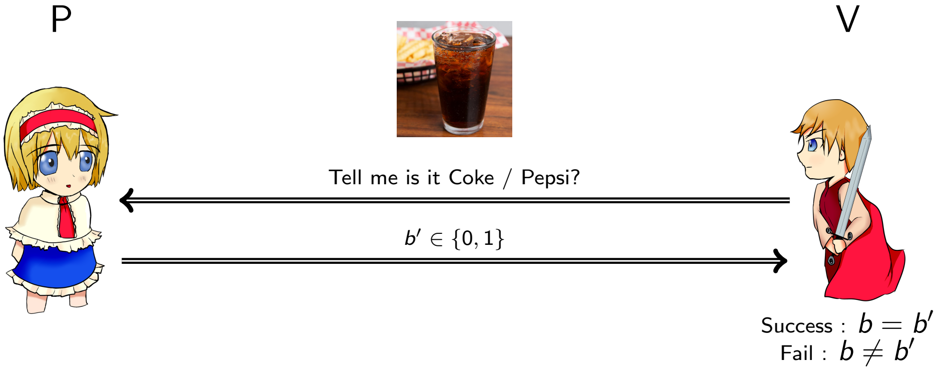
Tell me is it Coke / Pepsi?

$b' \in \{0, 1\}$

Success : $b = b'$
Fail : $b \neq b'$

- If P really knows the difference then it always succeeds – **(Complete)**
- If P does not know, then it fails with probability (?) 1/2

Distinguishing Problem – An Example of IP



P

V

Tell me is it Coke / Pepsi?

$b' \in \{0,1\}$

Success : $b = b'$

Fail : $b \neq b'$

- If P really knows the difference then it always succeeds – **(Complete)**
- If P does not know, then it fails with probability (?) 1/2

Distinguishing Problem – An Example of IP

P

V

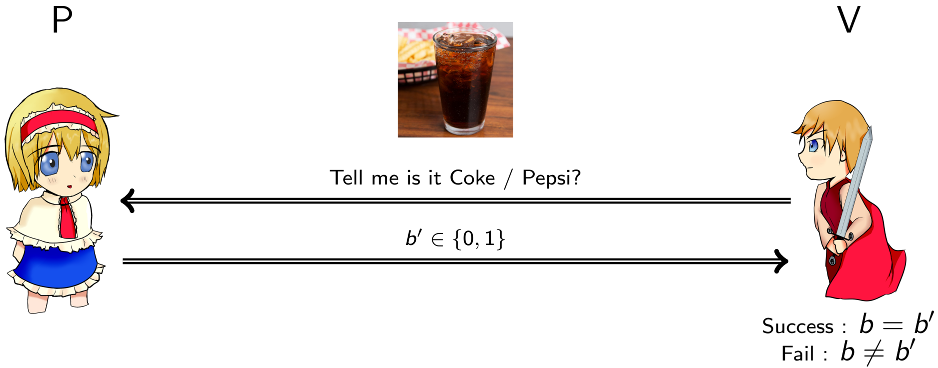
Tell me is it Coke / Pepsi?

$b' \in \{0,1\}$

Success : $b = b'$

Fail : $b \neq b'$

Distinguishing Problem – An Example of IP



P

V

Tell me is it Coke / Pepsi?

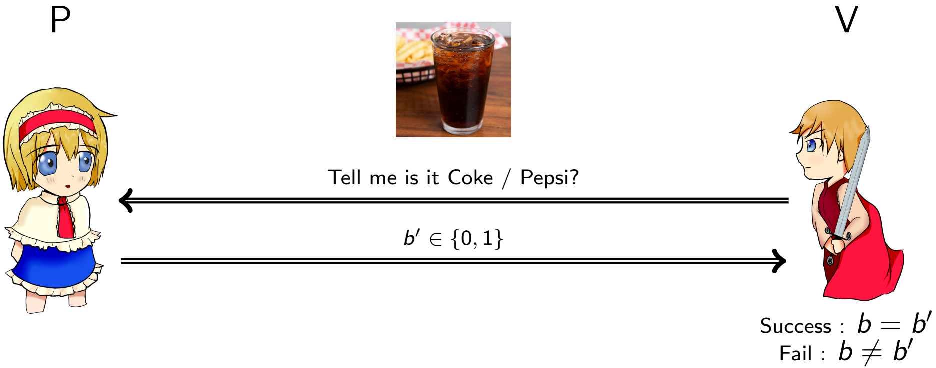
$b' \in \{0, 1\}$

Success : $b = b'$

Fail : $b \neq b'$

- Repeat the expermient afresh and continues for 10 times.
- If P does not know, then it fails with probability (?)

Distinguishing Problem – An Example of IP



P

V

Tell me is it Coke / Pepsi?

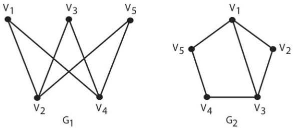
$b' \in \{0,1\}$

Success : $b = b'$
Fail : $b \neq b'$

- Repeat the expermient afresh and continues for 10 times.
- If P does not know, then it fails with probability (?) 1023/1024
- **Soundness error** 2^{-10}

GNI has an Interactive Proof

P

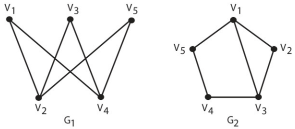


V

I can prove these two graphs are non-isomorphic

GNI has an Interactive Proof

P

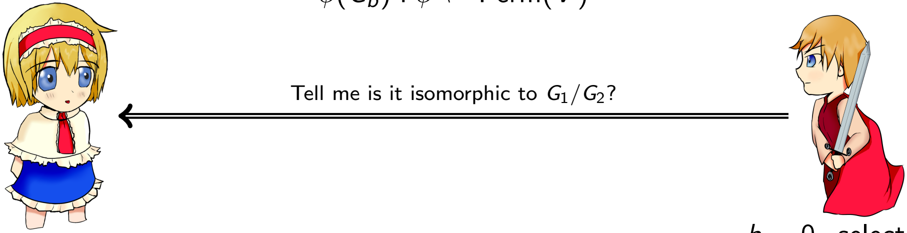


V

I can prove these two graphs are non-isomorphic →

← I don't believe you

GNI has an Interactive Proof



P

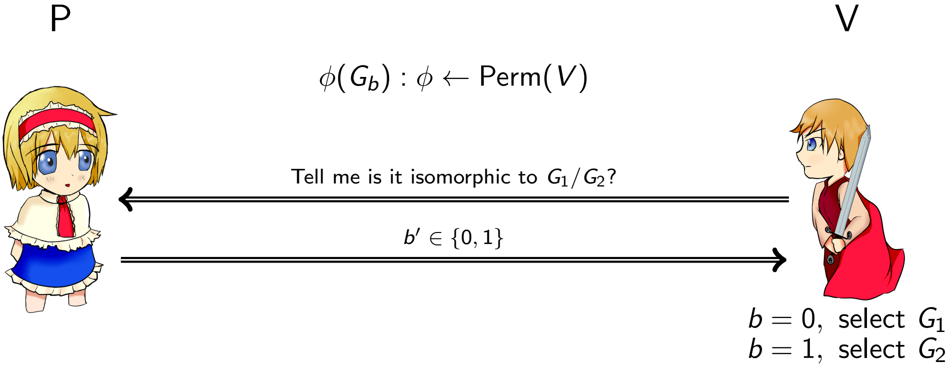
V

$\phi(G_b) : \phi \leftarrow \mathsf{Perm}(V)$

Tell me is it isomorphic to G_1/G_2?

$b = 0$, select G_1
$b = 1$, select G_2

GNI has an Interactive Proof



P

V

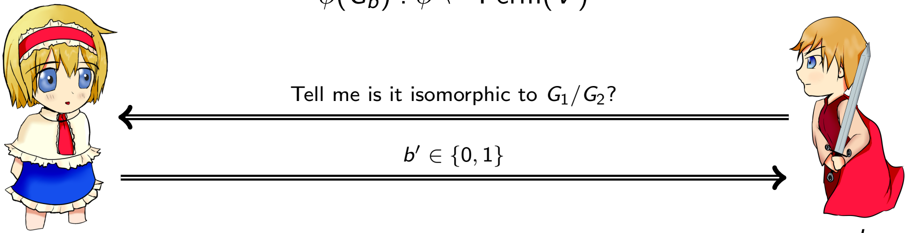
$\phi(G_b) : \phi \leftarrow \text{Perm}(V)$

Tell me is it isomorphic to G_1/G_2?

$b' \in \{0,1\}$

$b = 0$, select G_1
$b = 1$, select G_2

GNI has an Interactive Proof



P

V

$\phi(G_b) : \phi \leftarrow \mathrm{Perm}(V)$

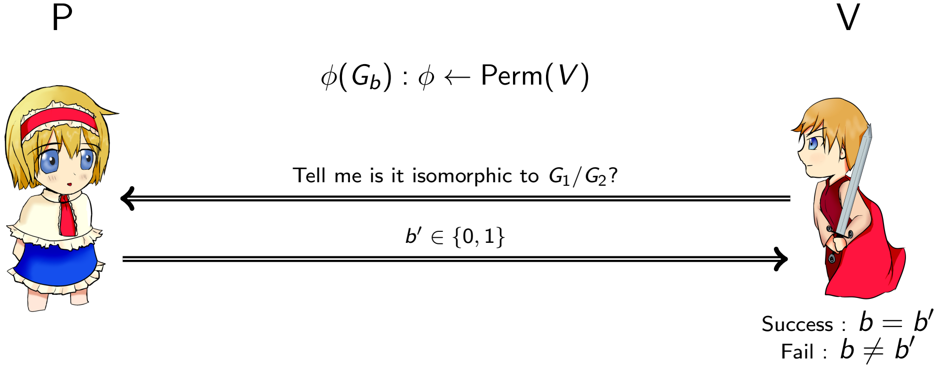
Tell me is it isomorphic to G_1/G_2?

$b' \in \{0,1\}$

Success : $b = b'$

Fail : $b \neq b'$

GNI has an Interactive Proof



P

V

$\phi(G_b) : \phi \leftarrow \mathrm{Perm}(V)$

Tell me is it isomorphic to G_1/G_2?

$b' \in \{0, 1\}$

Success : $b = b'$

Fail : $b \neq b'$

- Completeness holds.
- Repeat the experiment for t times, Soundness error 2^{-t}.

II. (Zero) Knowledge

The Notion of Knowledge

What is Knowledge ?

The Notion of Knowledge

What is Knowledge ?

Knowledge is the ability to complete a new task – Rafael Pass and Abhi Shelat

The Notion of Knowledge

What is Knowledge ?

Knowledge is the ability to complete a new task – Rafael Pass and Abhi Shelat

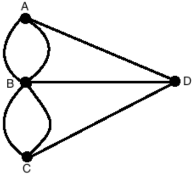
A conversation between two parties conveys knowledge when it allows the recipient to complete a “new” task that she could not complete before

The Notion of Zero Knowledge

The Notion of Zero Knowledge

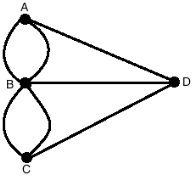
We can't but we can define Zero-Knowledge.

The Notion of Knowledge– An Example



“I know this figure can not be drawn in a paper without lifting the pen”

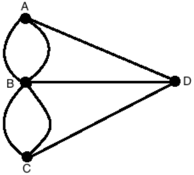
The Notion of Knowledge– An Example



“I know this figure can not be drawn in a paper without lifting the pen”

Does the message convey any knowledge ?

The Notion of Knowledge– An Example

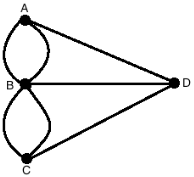


“I know this figure can not be drawn in a paper without lifting the pen”

Does the message convey any knowledge ?

No! I can very well compute whether the graph is “eulerian” or not.

The Notion of Knowledge– An Example

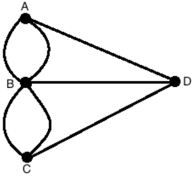


“I know this figure can not be drawn in a paper without lifting the pen”

Does the message convey any knowledge ?

No! I can very well compute whether the graph is “eulerian” or not. – (**Zero-Knowledge**)

The Notion of Knowledge– An Example



“I know this figure can not be drawn in a paper without lifting the pen”

Information which conveys no knowledge is called **zero knowledge**

III. (I) + (II) ⇒ Zero Knowledge Proof.

Notion of Zero Knowledge Proof (ZKP)

Can a classical proof system be a zero knowledge proof system ?

Notion of Zero Knowledge Proof (ZKP)

Can a classical proof system be a zero knowledge proof system ?

It must be an interactive proof system

- Efficient - Verification of the proof should be simple
- Completeness - A prover should be able to prove a valid statement.
- Soundness - A dishonest prover should not be able to prove an invalid statement.

Notion of Zero Knowledge Proof (ZKP)

Can a classical proof system be a zero knowledge proof system ?

It must be an interactive proof system

- Efficient - Verification of the proof should be simple
- Completeness - A prover should be able to prove a valid statement.
- Soundness - A dishonest prover should not be able to prove an invalid statement.

How do we model the proof system does not convey any knowledge ?

Modeling Zero Knowledge

Notion of Simulator

The verifier can produce a transcript that “looks similar” to the transcript that results from the interaction between the honest prover and the verifier.

Modeling Zero Knowledge

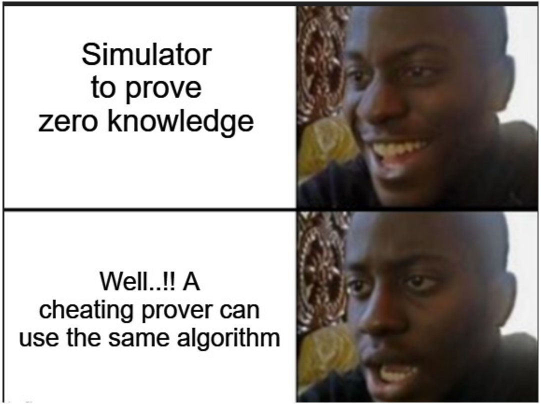
Notion of Simulator

The verifier can produce a transcript that “looks similar” to the transcript that results from the interaction between the honest prover and the verifier.

Rationale of Simulator

- It postulates that whatever a party can do “efficiently” by itself cannot be considered a gain from interaction with the outside.
- What matters is that any “real gain” can NOT occur whenever we are able to present a simulation.

Modeling Zero Knowledge


Simulator to prove zero knowledge
Well..!! A cheating prover can use the same algorithm

Modeling Zero Knowledge

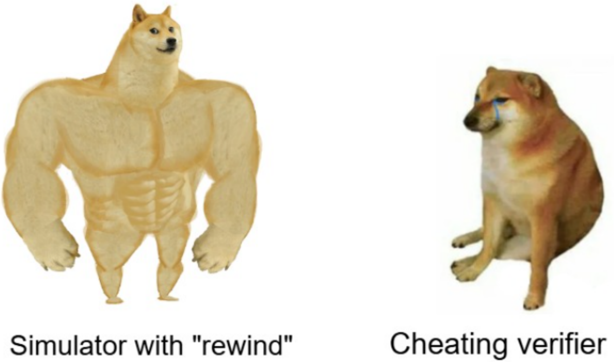
There must be something that the simulator can do but a cheating prover can not..!!

Modeling Zero Knowledge

There must be something that the simulator can do but a cheating prover can not..!!

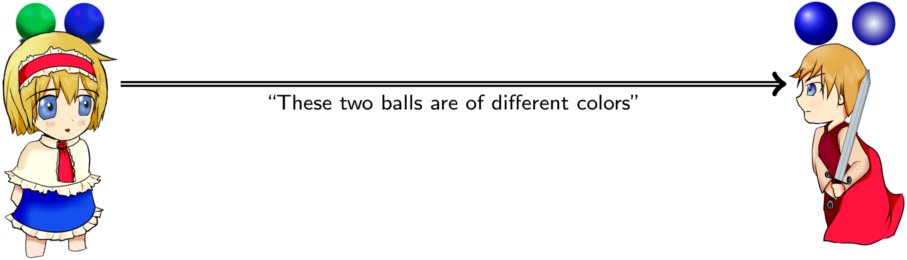
- The simulator can rewind the interaction.
- In fact, one should be able to construct simulators corresponding to a cheating verifier as well.

Modeling Zero Knowledge



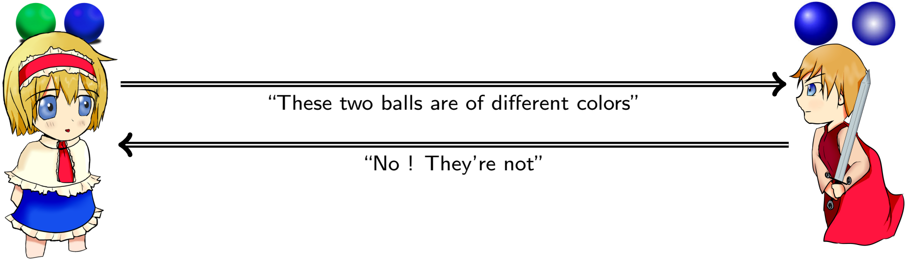
A Simple Example

Examples of ZKP : Two Balls and the Color-Blind Friend



“These two balls are of different colors”

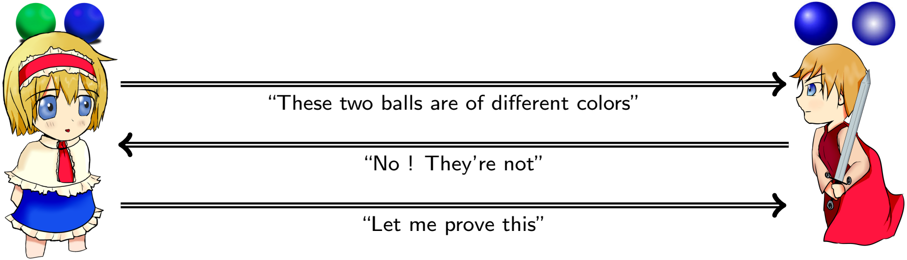
Examples of ZKP : Two Balls and the Color-Blind Friend



“These two balls are of different colors”

“No ! They’re not”

Examples of ZKP : Two Balls and the Color-Blind Friend

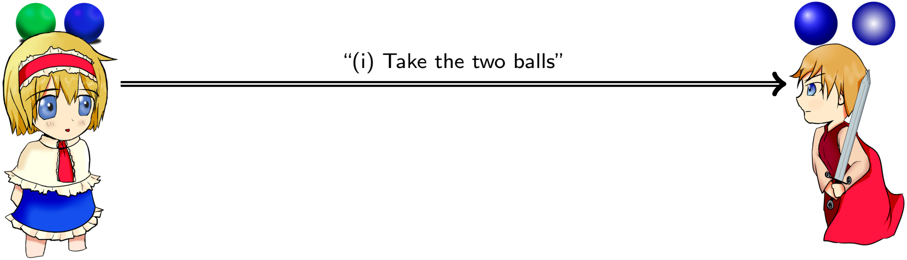


“These two balls are of different colors”

“No ! They’re not”

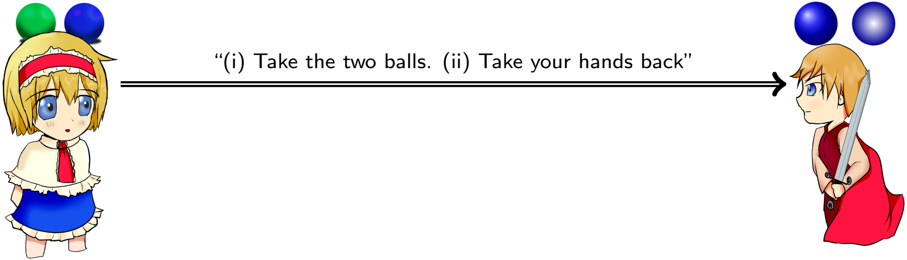
“Let me prove this”

Examples of ZKP : Two Balls and the Color-Blind Friend



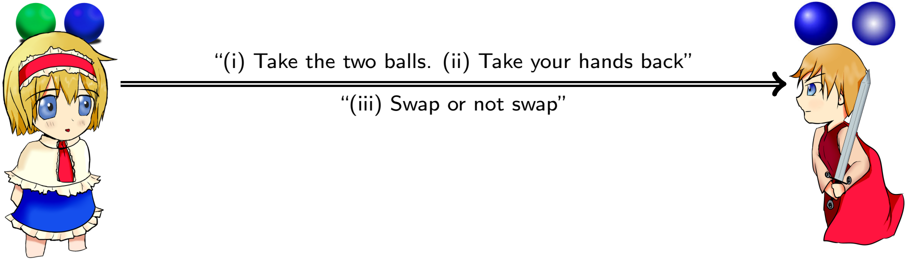
“(i) Take the two balls”

Examples of ZKP : Two Balls and the Color-Blind Friend



“(i) Take the two balls. (ii) Take your hands back”

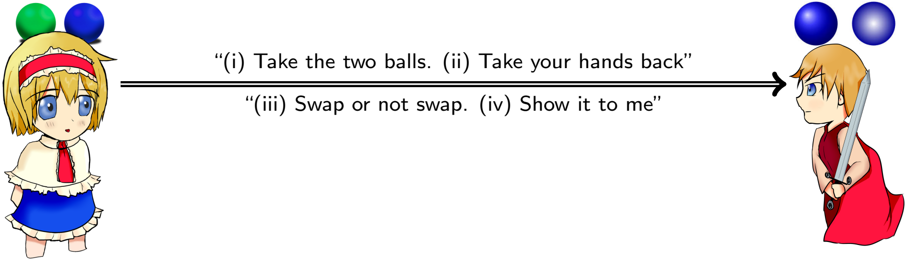
Examples of ZKP : Two Balls and the Color-Blind Friend



“(i) Take the two balls. (ii) Take your hands back”

“(iii) Swap or not swap”

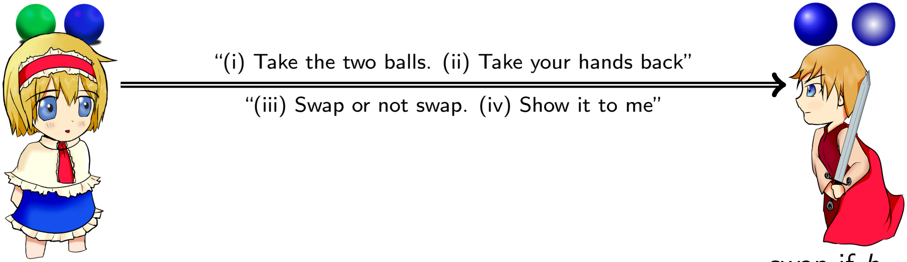
Examples of ZKP : Two Balls and the Color-Blind Friend



“(i) Take the two balls. (ii) Take your hands back”

“(iii) Swap or not swap. (iv) Show it to me”

Examples of ZKP : Two Balls and the Color-Blind Friend

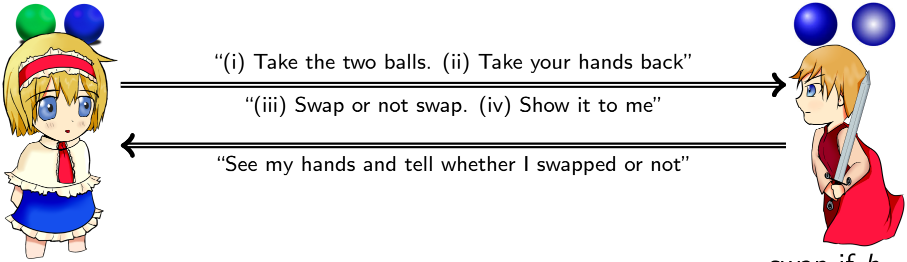


“(i) Take the two balls. (ii) Take your hands back”

“(iii) Swap or not swap. (iv) Show it to me”

swap if $b = 0$
not swap if $b = 1$

Examples of ZKP : Two Balls and the Color-Blind Friend



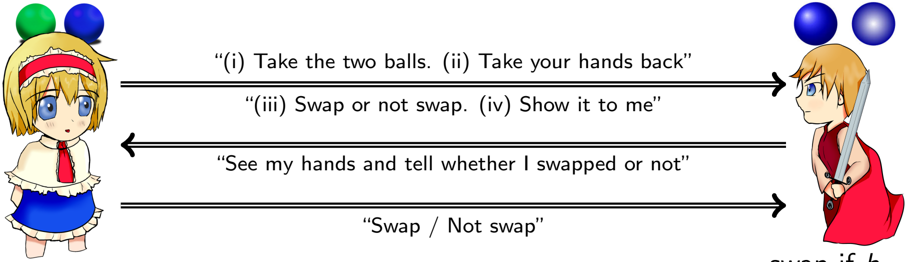
"(i) Take the two balls. (ii) Take your hands back"

"(iii) Swap or not swap. (iv) Show it to me"

"See my hands and tell whether I swapped or not"

swap if $b = 0$
not swap if $b = 1$

Examples of ZKP : Two Balls and the Color-Blind Friend



“(i) Take the two balls. (ii) Take your hands back”

“(iii) Swap or not swap. (iv) Show it to me”

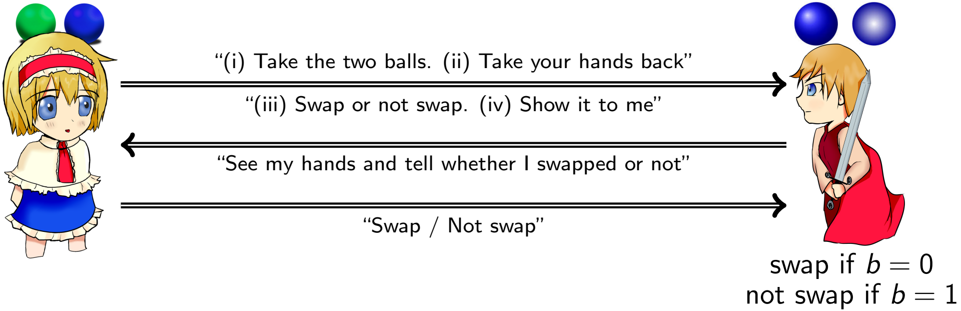
“See my hands and tell whether I swapped or not”

“Swap / Not swap”

swap if $b = 0$
not swap if $b = 1$

- If Alice really knows the balls are distinguishable, then she always wins – (**Complete**)

Examples of ZKP : Two Balls and the Color-Blind Friend



"(i) Take the two balls. (ii) Take your hands back"

"(iii) Swap or not swap. (iv) Show it to me"

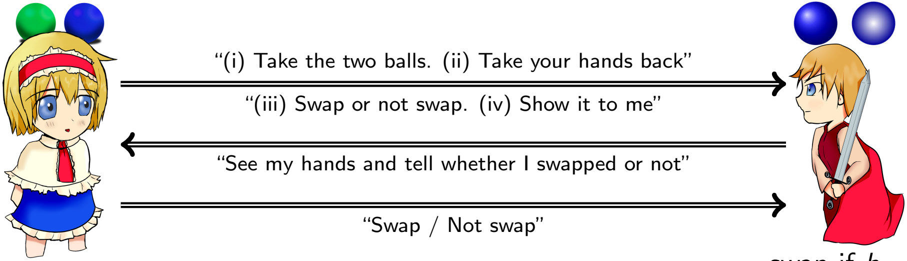
"See my hands and tell whether I swapped or not"

"Swap / Not swap"

swap if $b = 0$
not swap if $b = 1$

- If Alice really knows the balls are distinguishable, then she always wins – (**Complete**)
- If Alice does not know then she fails with probability 2^{-t} after $'t'$ many repetitions – (**Soundness error**)

Examples of ZKP : Two Balls and the Color-Blind Friend



"(i) Take the two balls. (ii) Take your hands back"

"(iii) Swap or not swap. (iv) Show it to me"

"See my hands and tell whether I swapped or not"

"Swap / Not swap"

swap if $b = 0$
not swap if $b = 1$

After the experiment, Bob does not know which ball is of which color – (**Zero Knowledge**)

A Cryptographic Example

Example of ZKP: Cryptographic Protocol

Discrete Logarithm Problem

- Take any large prime p, and consider $\mathbb{Z}_p^\star = \{1, 2, \ldots, p-1\}$
- Let g be a generator of $\mathbb{Z}_p^\star$, primitive element modulo p:

$$\langle g \rangle = \mathbb{Z}_p^\star = \{1, g, g^2, \ldots, g^{p-2}\} \bmod p.$$

- Given g and x, it is easy to calculate $g^x \bmod p$.
- However, given g and y, it is hard to find x in the range of 0 to $p-2$ that satisfies

$$g^x \equiv y \bmod p.$$

Use of Discrete Logarithm Problem in Locker Access

$$\langle g \rangle = \mathbb{Z}_p^*$$

$$x \in \mathbb{Z}_p^*, y \leftarrow g^x \mod p$$

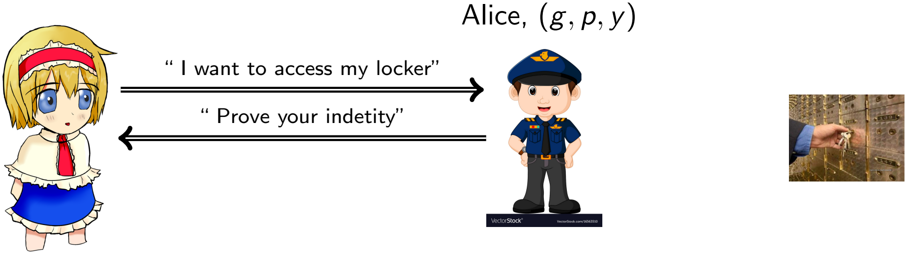
$$\xRightarrow{(g, p, y)}$$

Use of Discrete Logarithm Problem in Locker Access

“ I want to access my locker”

Alice, (g, p, y)

Use of Discrete Logarithm Problem in Locker Access

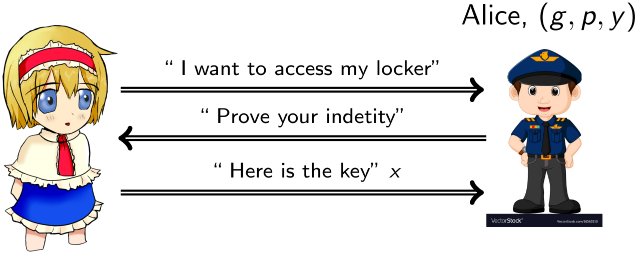


Alice, (g, p, y)

" I want to access my locker"

" Prove your indetity"

Use of Discrete Logarithm Problem in Locker Access



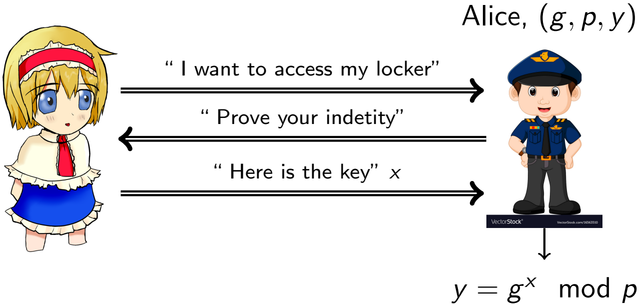
Alice, (g, p, y)

" I want to access my locker"

" Prove your indetity"

" Here is the key" x

Use of Discrete Logarithm Problem in Locker Access



Alice, (g, p, y)

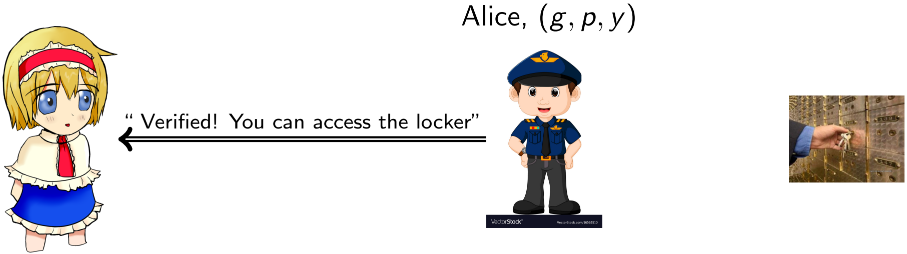
“ I want to access my locker”

“ Prove your indetity”

“ Here is the key” x

$$y = g^x \mod p$$

Use of Discrete Logarithm Problem in Locker Access



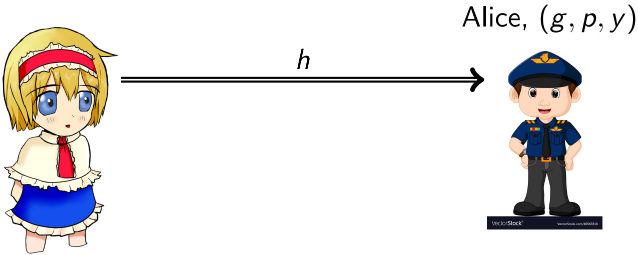
Alice, (g, p, y)

“ Verified! You can access the locker”

Use of Discrete Logarithm Problem in Locker Access

Use of ZKP of Discrete Logarithm Problem in Locker Access

$r \leftarrow \mathbb{Z}_p^*, h \leftarrow g^r \mod p$



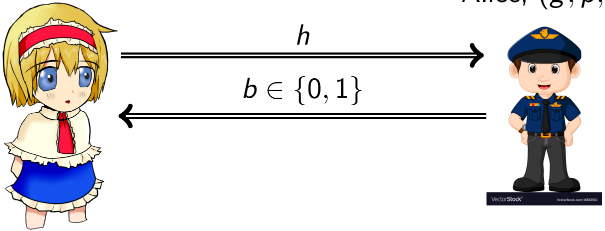
Alice, (g, p, y)

h

Use of ZKP of Discrete Logarithm Problem in Locker Access

$r \leftarrow \mathbb{Z}_p^*, h \leftarrow g^r \mod p$

Alice, (g, p, y)

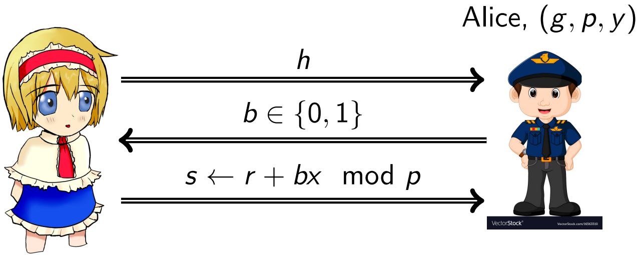


h

$b \in \{0, 1\}$

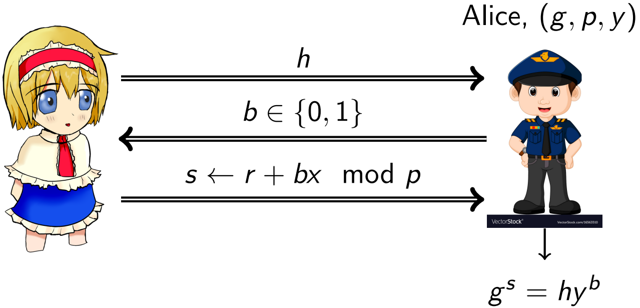
Use of ZKP of Discrete Logarithm Problem in Locker Access

$r \leftarrow \mathbb{Z}_p^*, h \leftarrow g^r \mod p$



Use of ZKP of Discrete Logarithm Problem in Locker Access

$r \leftarrow \mathbb{Z}_p^*, h \leftarrow g^r \mod p$



Alice, (g, p, y)

h

$b \in \{0, 1\}$

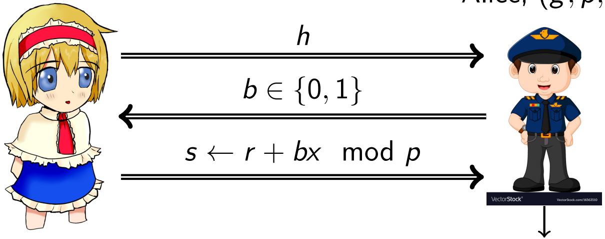
$s \leftarrow r + bx \mod p$

$g^s = hy^b$

Use of ZKP of Discrete Logarithm Problem in Locker Access

$r \leftarrow \mathbb{Z}_p^*, h \leftarrow g^r \mod p$

Alice, (g, p, y)



h

$b \in \{0, 1\}$

$s \leftarrow r + bx \mod p$

$g^s = hy^b$

Repeat the game for t times

Use of ZKP of Discrete Logarithm Problem in Locker Access

Completeness

If Alice knows the secret x, then she will always win the game by computing the s following the protocol.

Soundness

- If Alice cheats, then the probability of winning the game in a trial is $1/2$. (Can you show that?)
- Repeating the experiment t times: Soundness error: 2^{-t}

Use of ZKP of Discrete Logarithm Problem in Locker Access

Completeness

If Alice knows the secret x, then she will always win the game by computing the s following the protocol.

Soundness

- If Alice cheats, then the probability of winning the game in a trial is $1/2$. (Can you show that?)
- Repeating the experiment t times: Soundness error: 2^{-t}

Note: Repeating experiment means the randomness is generated freshly.

ZKP of Discrete Logarithm Problem

View of the interaction: $\text{view}_{\text{guard}^*}^{\text{Alice}}(g, p, y) = (h, b, s)$

ZKP of Discrete Logarithm Problem

View of the interaction: $\text{view}^{\text{Alice}}_{\text{guard}^*}(g, p, y) = (h, b, s)$

Simulator for DL Problem

1. Pick $b' \xleftarrow{\$} \{0,1\}$, $s \xleftarrow{\$} \mathbb{Z}_p^*$
2. Compute $h = \frac{g^s}{y^b} \bmod p$ and send it to the verifier
3. Verifier replies with b. If $b \neq b'$, rewind and execute step 1 again.
4. Transcript of the simulator: $M^*(g, p, y) = (h, b, s)$.

ZKP of Discrete Logarithm Problem

View of the interaction: $\text{view}_{\text{guard}^*}^{\text{Alice}}(g, p, y) = (h, b, s)$

Simulator for DL Problem

1. Pick $b' \xleftarrow{\$} \{0, 1\}$, $s \xleftarrow{\$} \mathbb{Z}_p^*$
2. Compute $h = \frac{g^s}{y^b} \bmod p$ and send it to the verifier
3. Verifier replies with b. If $b \neq b'$, rewind and execute step 1 again.
4. Transcript of the simulator: $M^*(g, p, y) = (h, b, s)$.

Observe that $\text{view}_{\text{guard}^*}^{\text{Alice}}(g, p, y) \cong M^*(g, p, y)$

ZKP of Discrete Logarithm Problem

View of the interaction: $\text{view}_{\text{guard}^*}^{\text{Alice}}(g, p, y) = (h, b, s)$

Simulator for DL Problem

- Pick $b \xleftarrow{\$} \{0, 1\}$
- Pick $s \xleftarrow{\$} \mathbb{Z}_p^*$
- Compute $h = \frac{g^s}{y^b} \bmod p$
- Transcript of the simulator: $M^*(g, p, y) = (h, b, s)$.

Can a cheating prover generate the view?

ZKP of Discrete Logarithm Problem

View of the interaction: $\text{view}^{\text{Alice}}_{\text{guard}^*}(g, p, y) = (h, b, s)$

Simulator for DL Problem

- Pick $b \xleftarrow{\$} \{0, 1\}$
- Pick $s \xleftarrow{\$} \mathbb{Z}_p^*$
- Compute $h = \frac{g^s}{y^b} \mod p$
- Transcript of the simulator: $M^*(g, p, y) = (h, b, s)$.

Can a cheating prover generate the view? No, it receives b only after sharing h.

ZKP for all Problems in $\mathcal{NP}$

Zero Knowledge Proofs for $\mathcal{NP}$

The Class $\mathcal{NP}$

A language L is in $\mathcal{NP}$ if given a witness it can be verified in polynomial time.

$\mathcal{NP}$-Completeness

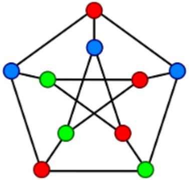
A language L is $\mathcal{NP}$-Complete if

- $L \in \mathcal{NP}$, and
- Each $L' \in \mathcal{NP}$ is polynomially reducible to L.

Examples: 3-COL, 3-SAT, CLIQUE, Vertex Cover.

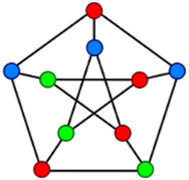
3-COL Problem

A graph G is 3-colorable if the vertices of a given graph can be colored with only three colors, such that no two vertices of the same color are connected by an edge. Given a graph can you make it 3-colorable?



3-COL Problem

A graph G is 3-colorable if the vertices of a given graph can be colored with only three colors, such that no two vertices of the same color are connected by an edge. Given a graph can you make it 3-colorable?



3-COL problem is an $\mathcal{NP}$-complete Problem

Zero Knowledge Proofs for $\mathcal{NP}$

The Basic Idea

- 3-COL is $\mathcal{NP}$-complete
- Any problem in $\mathcal{NP}$ can be reduced to the 3-COL problem
- We will show a Zero Knowledge Proof for 3-COL problem

ZK Proof of Graph 3-Colorability

- Common Input: A 3-colorable graph $G(V, E)$, $|V| = n$.
- Auxiliary Input (Prover): A 3-coloring $\phi : V \rightarrow \{1, 2, 3\}$

Interactive Protocol

- P1: Execute the following:
  - $\pi \leftarrow_{\$} \{1, 2, 3\}$, sets $\psi(i) = \pi(\phi(i))$, $\forall i = 1(1)n$.
  - Choose $s_1, \ldots, s_n \leftarrow_{\$} \{0, 1\}^n$.
  - Computes $c_i = C_{s_i}(\psi(i))$ and sends $c_1, \ldots, c_n$.

ZK Proof of Graph 3-Colorability

- Common Input: A 3-colorable graph $G(V, E)$, $|V| = n$.
- Auxiliary Input (Prover): A 3-coloring $\phi : V \rightarrow \{1, 2, 3\}$

Interactive Protocol

- P1: Execute the following:
  - $\pi \leftarrow_{\$} \{1, 2, 3\}$, sets $\psi(i) = \pi(\phi(i))$, $\forall i = 1(1)n$.
  - Choose $s_1, \ldots, s_n \leftarrow_{\$} \{0, 1\}^n$.
  - Computes $c_i = C_{s_i}(\psi(i))$ and sends $c_1, \ldots, c_n$.
- V1: $(u, v) \leftarrow_{\$} E$ and sends to P.

ZK Proof of Graph 3-Colorability

- Common Input: A 3-colorable graph $G(V, E)$, $|V| = n$.
- Auxiliary Input (Prover): A 3-coloring $\phi : V \to \{1, 2, 3\}$

Interactive Protocol

- P1: Execute the following:
  - $\pi \leftarrow_{\$} \{1, 2, 3\}$, sets $\psi(i) = \pi(\phi(i))$, $\forall i = 1(1)n$.
  - Choose $s_1, \ldots, s_n \leftarrow_{\$} \{0, 1\}^n$.
  - Computes $c_i = C_{s_i}(\psi(i))$ and sends $c_1, \ldots, c_n$.
- V1: $(u, v) \leftarrow_{\$} E$ and sends to P.
- P2: Upon receiving $e = (u, v) \in E$, reveals $(s_u, \psi(u))$ and $(s_v, \psi(v))$.

ZK Proof of Graph 3-Colorability

- Common Input: A 3-colorable graph $G(V, E)$, $|V| = n$.
- Auxiliary Input (Prover): A 3-coloring $\phi : V \to \{1, 2, 3\}$

Interactive Protocol

- P1: Execute the following:
  - $\pi \leftarrow_\$ \{1, 2, 3\}$, sets $\psi(i) = \pi(\phi(i))$, $\forall i = 1(1)n$.
  - Choose $s_1, \ldots, s_n \leftarrow_\$ \{0, 1\}^n$.
  - Computes $c_i = C_{s_i}(\psi(i))$ and sends $c_1, \ldots, c_n$.
- V1: $(u, v) \leftarrow_\$ E$ and sends to P.
- P2: Upon receiving $e = (u, v) \in E$, reveals $(s_u, \psi(u))$ and $(s_v, \psi(v))$.
- V2: Upon receiving (s, σ) and (s', σ'), verifies $c_u = C_s(\sigma)$, $c_v = C_{s'}(\sigma')$ and $\sigma \neq \sigma'$. If all the conditions hold, accept; otherwise, reject.

ZK Proof of Graph 3-Colorability

Main Result

If the commitment scheme satistisfies the hiding and the binding requirements, then the construction constitutes an auxiliary-input zero-knowledge interactive proof for G3C.

Properties

- Completeness bound: 1.
- Soundness bound: $1/|E|$.

Some Real Life Applications

Use of ZKP in e-Auction Protocol

- Fairness: All bids should remain confidential, no bidder should be able to modify the committed bid, lowest bid must win.
- Confidentiality: Except the winning bid all the other bids must remain confidential
- Anonymity: Information about the identity of the bidders (except the winner) must be confidential.

Use of ZKP in e-Auction Protocol

- The auction repository stores all committed bids, not their openings.
- The bidders commit their bids by submitting the cryptographic commitments of their bid value.
- After the commitment phase is finished, the auctioneer opens all commitments.
- It is generated one proof for each losing bid. This proof demonstrate that the difference between the losing value and winning value is positive.
- Each proof can be publicly verified by any interested party

Use of ZKP in e-Voting

- A voter can cast his/her vote to 0 or 1 in an encrypted way.
- The authority gets all the encrypted votes, add all ballots using the scheme's add algorithm, decrypts the sum.
- A voter can encrypt an invalid vote and the authority would decrypt the sum incorrectly.
- Any one can verify that no votes have been modified, added, or deleted during the process.
- No one should be able to find your casted vote.

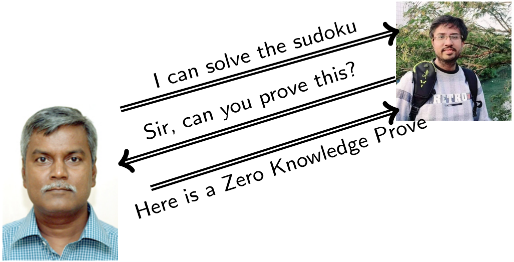
Applications of ZKP in Crypto currencies

- Sending private blockchain transactions should not reveal
  - source of the actual money,
  - how much money was sent, or
  - the identity of the final recipient.
- Traitional methods may reveal some relevant information.

Now-a-days, ZKP is widely used in several cryptocurrencies: ZCASH, Monero, PIVX, Zerocoin.

Revisiting the Sudoku Problem

Solving the Sudoku



I can solve the sudoku

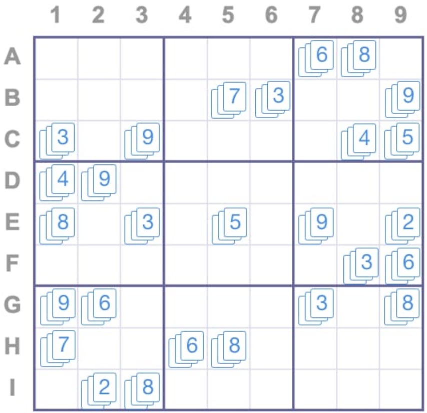
Sir, can you prove this?

Here is a Zero Knowledge Prove

Zero Knowledge Proof for Sudoku

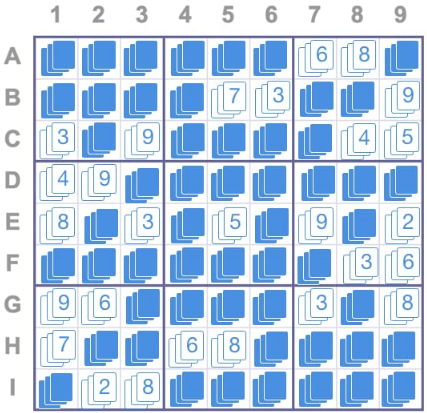
	1	2	3	4	5	6	7	8	9
A							6	8	
B					7	3			9
C	3		9					4	5
D	4	9							
E	8		3		5		9		2
F								3	6
G	9	6					3		8
H	7			6	8				
I		2	8						

Zero Knowledge Proof for Sudoku



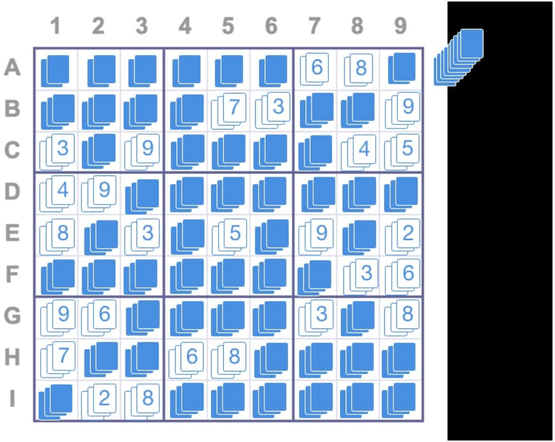
	1	2	3	4	5	6	7	8	9
A							6	8	
B					7	3			9
C	3		9					4	5
D	4	9							
E	8		3		5		9		2
F								3	6
G	9	6					3		8
H	7			6	8				
I		2	8						

Zero Knowledge Proof for Sudoku



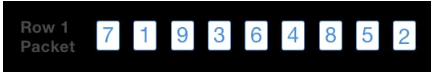
	1	2	3	4	5	6	7	8	9
A							6	8	
B					7	3			9
C	3		9					4	5
D	4	9							
E	8		3		5		9		2
F								3	6
G	9	6					3		8
H	7			6	8				
I		2	8						

Zero Knowledge Proof for Sudoku



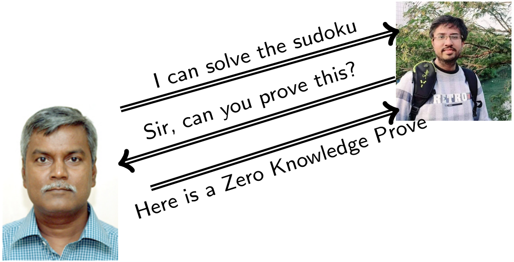
	1	2	3	4	5	6	7	8	9
A							6	8	
B					7	3			9
C	3		9					4	5
D	4	9							
E	8		3		5		9		2
F								3	6
G	9	6					3		8
H	7			6	8				
I		2	8						

Zero Knowledge Proof for Sudoku



All the cards are shuffled: Zero Knowledge.

Solving the Sudoku



I can solve the sudoku

Sir, can you prove this?

Here is a Zero Knowledge Prove

World Sudoku Championship

Effect of ZKP

Thank You

Hope you have gained some knowledge about "Zero Knowledge"..!!