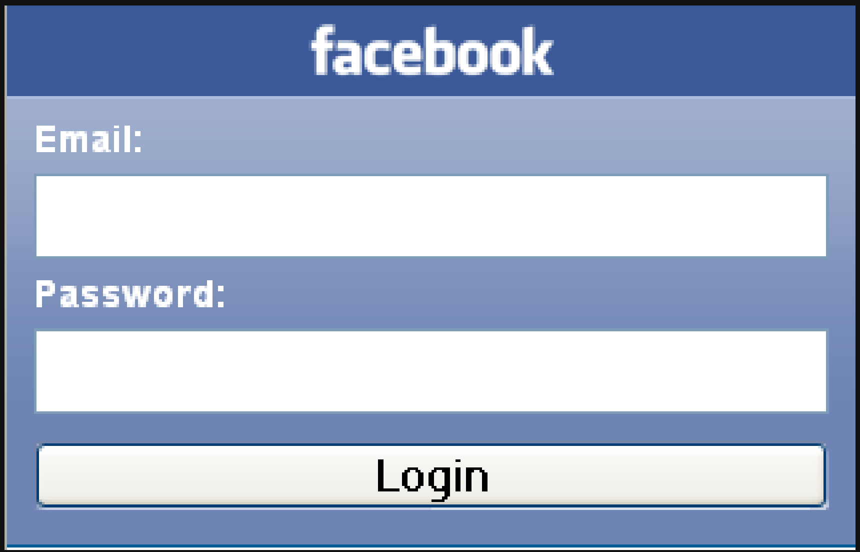
Zero Knowledge

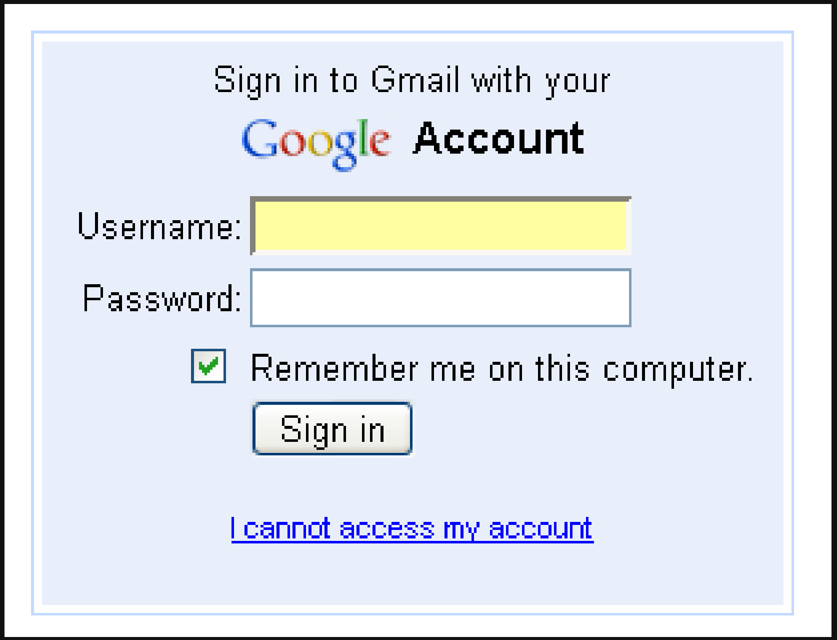
Anupam Datta

CMU

Fall 2014

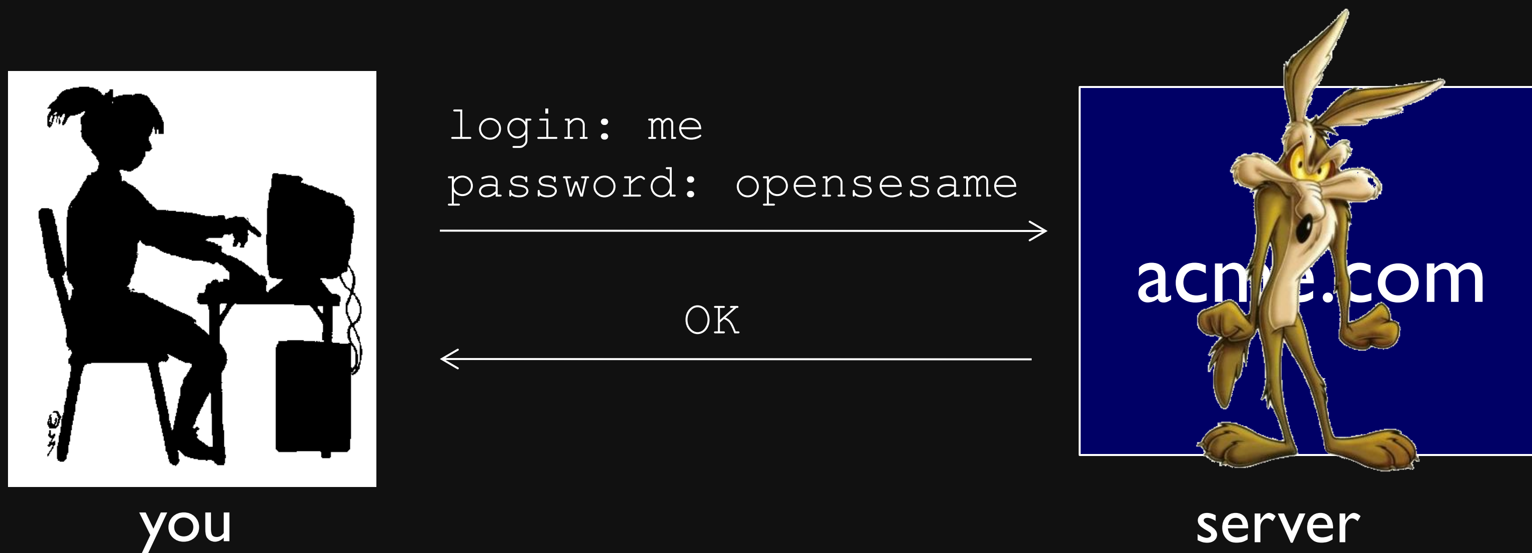
Authentication





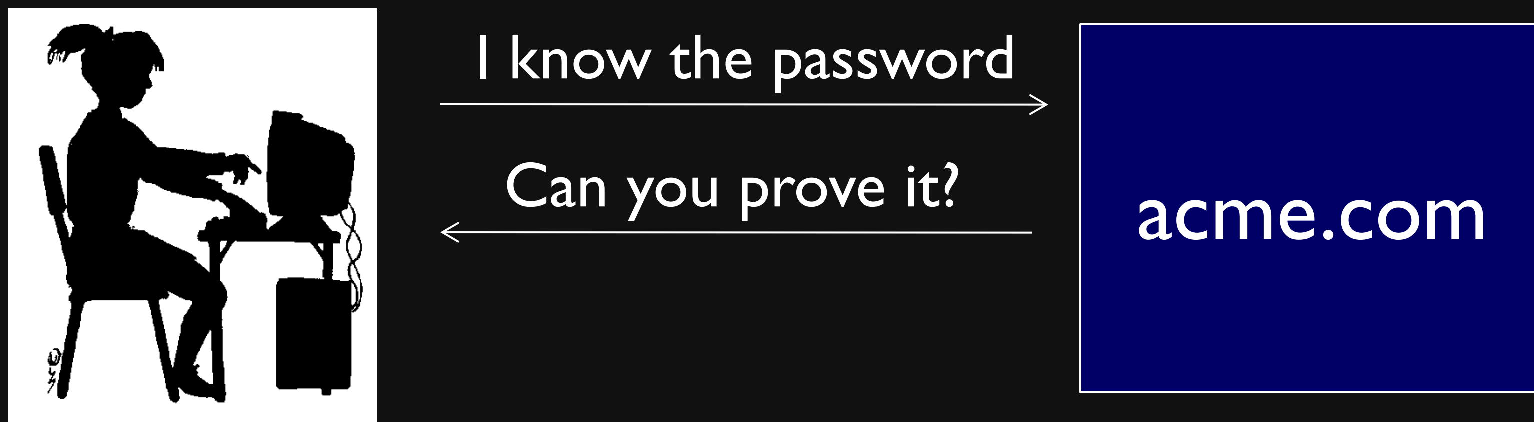
What happens when you type in your password?

Naïve authentication



- The server knows your password
- So they can impersonate you at other web sites where you use the same password

“Zero-knowledge” authentication



Can you convince the server that you know your password, without revealing it (or any other information)?

What is knowledge?

What is ignorance?

(lack of knowledge)

- Example 1: Tomorrow's lottery numbers

2 31 12 7 28 11

We are ignorant of them because they are random

What is ignorance?

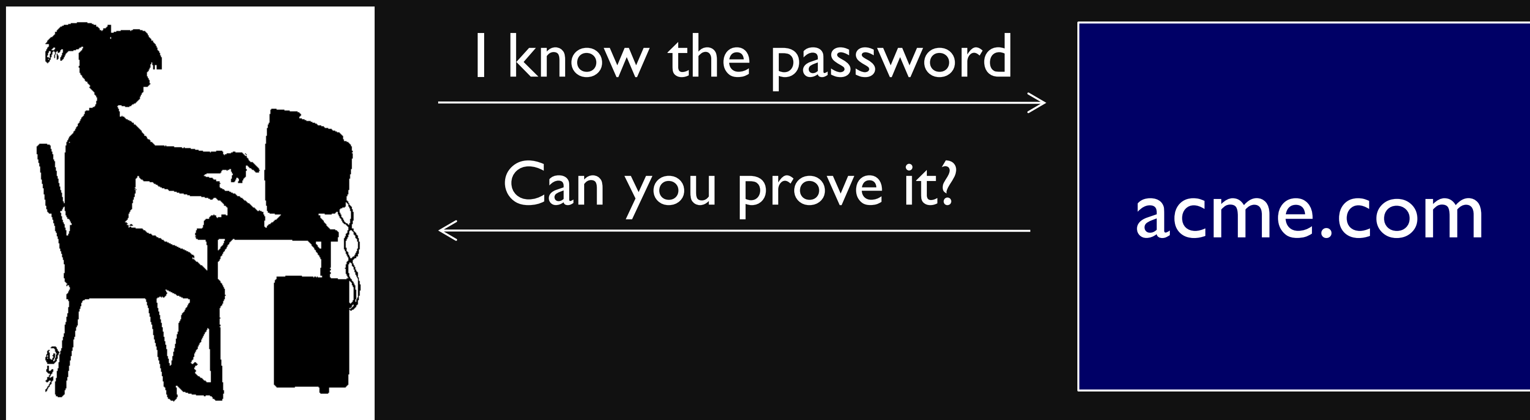
- Example 2: A difficult math problem

Prove that $\mathrm{P} \neq \mathrm{NP}$

We are ignorant because it takes a lot of work to figure out the answer

- Questions of this type include
  - Finding satisfying assignments to Boolean formulas
  - Finding cliques in graphs
  - All NP-hard problems

Using ignorance to our advantage



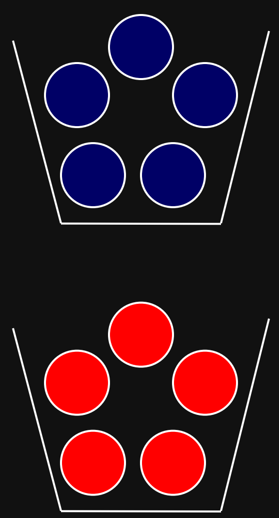
We want to convince the server that we know the password, while keeping it ignorant of the password itself

The server is convinced, but gains zero-knowledge!

An Interactive Protocol

A protocol for “non-color-blindness”

- You (the prover) want to convince me (the verifier) that you are not color-blind



I pull at random either a red ball or a blue ball and show it to you

You say “red” or “blue”

We repeat this 10 times

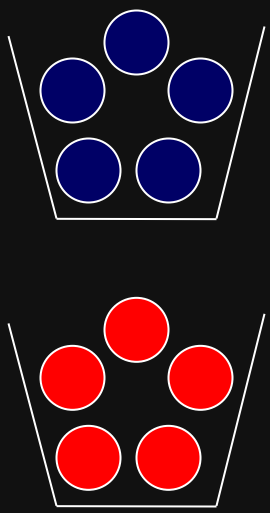
If you got all the answers right,
I am convinced you know red from blue

Properties

- Soundness
  - If Verifier accepts then the property (Prover is not color blind) holds with high probability
- Completeness
  - If property (Prover is not color blind) holds then the Verifier always accepts

Interaction and knowledge

- What knowledge did I gain from this interaction?



I learned that you can tell blue from red

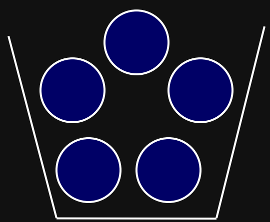
But I also learned the colors of the balls in each glass

Suppose I was color-blind

Then I used you to gain some knowledge!

An Interactive Protocol that is Zero Knowledge

A different protocol

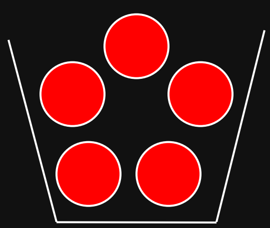


box 1

I pull at random either two balls from same box or one ball from box 1 and one from box 2

You say “same color” or “different color”

We repeat 10 times



box 2

If you got all the answers right,
I am convinced you know red from blue

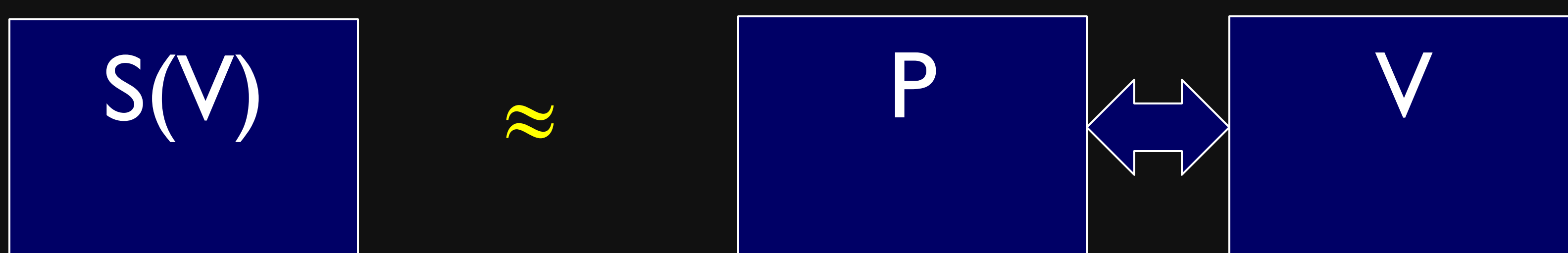
But I did not gain any other knowledge!

Zero-knowledge

- Suppose I am color-blind but you are not
- In the first protocol, I cannot predict your answer ahead of time
- In the second protocol, I know what you will say, so I do not gain knowledge when you say it

Zero-knowledge

The verifier's view of the interaction with the prover can be efficiently simulated without interacting with the prover



Probability distributions on transcripts are indistinguishable

ZK Proof Outline for Non-Color Blindness

- Verifier V*'s view in interaction with Prover P
  1. wp *p*: draw two balls from same box; Prover says "same color"
  2. wp *(1-p)*: draw one ball from box 1 and one ball from box

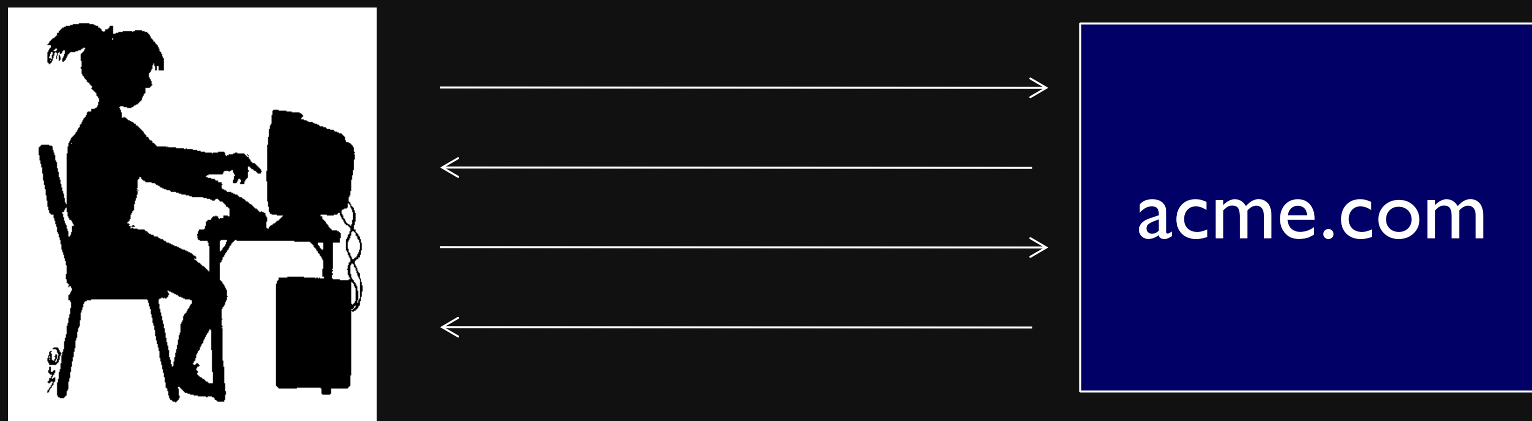
(P,V*) interaction transcript ≈ S(V*) transcript

-
  1. When V* says "draw two balls from same box" it does so and says "same color" to simulate P (wp *p*)
  2. When V* says "draw one ball from box 1 and one ball from box 2" it does so and says "different color" to simulate P (wp *1-p*)

Comments

- Verifier is polynomial time
- Prover has unbounded computation power
- ZK property has to hold for all verifiers V* (not just the honest verifer V)

Zero-knowledge password authentication

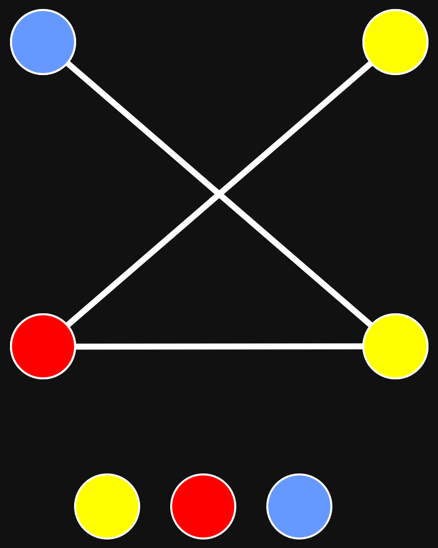



Oded Goldreich


Silvio Micali


Avi Wigderson

Graph coloring



Task: Assign one of 3 colors to the vertices so that no edge has both endpoints of same color

$3\text{COL} = \{G\text{: } G$ has a valid 3-coloring$\}$

- Theorem

3COL is NP-complete

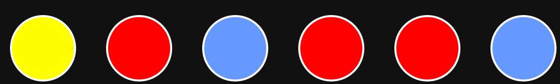
Password authentication via 3-coloring

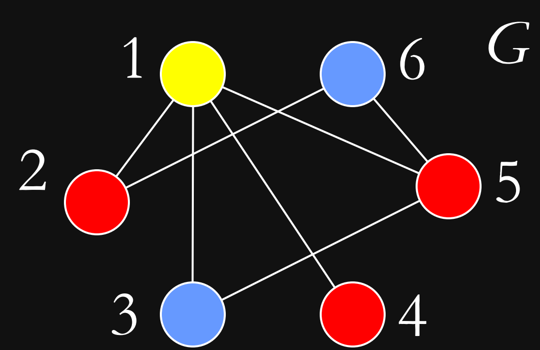
- Step 0: When you register for the web service,

registration

acme.com

choose your password to be a valid 3-coloring of some (suitable) graph

`password:` 



Password authentication via 3-coloring

- When the server asks for your password

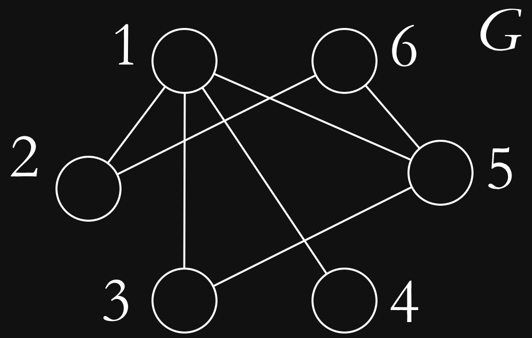
password?

G

acme.com

do not send the password, but send the graph G instead (without the colors)

password: 

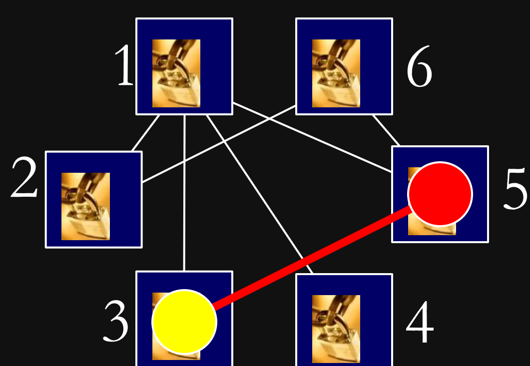


Intuition about registration phase

- Because 3-coloring is hard, the server will not be able to figure out your password (coloring) from G
- Later, when you try to log in, you will convince the server that you know how to color G, without revealing the coloring itself
- The server will be convinced you know your password but remain ignorant about what it is

The login phase

password:



You randomly permute the colors

You lock each of the colors in a box and send the boxes to the server

The server chooses an edge at random and asks for the keys to the boxes at the endpoints

You send the requested keys

The server unlocks the two boxes and checks the colors are different

---

Repeat this 1000 times. Login succeeds if colors always different

Analysis in the login phase

- Soundness: If you are an impostor, you won't know how to color the graph, so at least one of the edges will have endpoints of the same color, and the server is likely to catch this

- Completeness: If you know the coloring then you will always successfully convince the server

- ZK: If you are honest, the server remains ignorant about your password because all he sees are two random different colors

ZK Proof Outline for 3-COL

- Simulator S
  - Internally select random edge (i, j) and random permutation

1. P→V*: Generate coloring s.t. color(i) not equal color(j);

(P,V*) interaction transcript ≈ S(V*) transcript

are not equal)

Note: If V* is not honest, use V* as a blackbox to output edge e in step 2; rewind if e not equal to (i,j)

Acknowledgment

- Slides are from Andrej Bogdanov except slides 10, 15, 16, 24

Seminal Results

- IP and ZK defined [GMR'85]
- ZK for all NP languages [GMW'86]
  - Assuming one way functions exist
- ZK for all of IP [BGGHKMR'88]
  - Everything that can be proven can be proven in ZK assuming one way functions exist