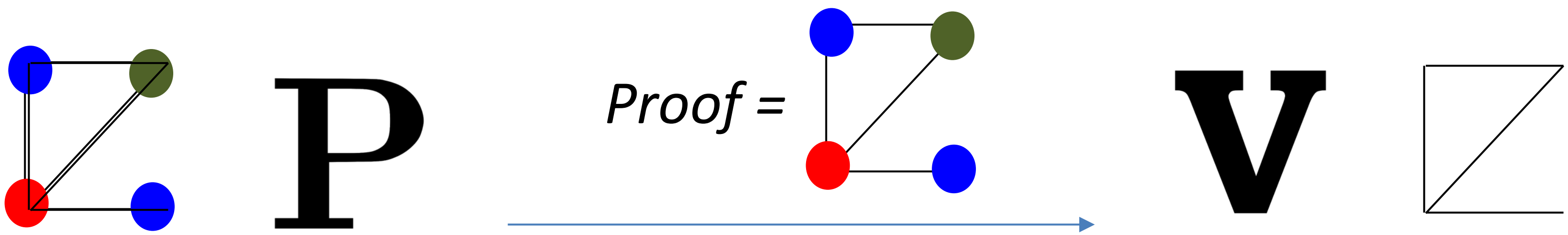
MIT 6.875

Foundations of Cryptography
Lecture 16

NP Proofs

For the NP-complete problem of graph 3-coloring

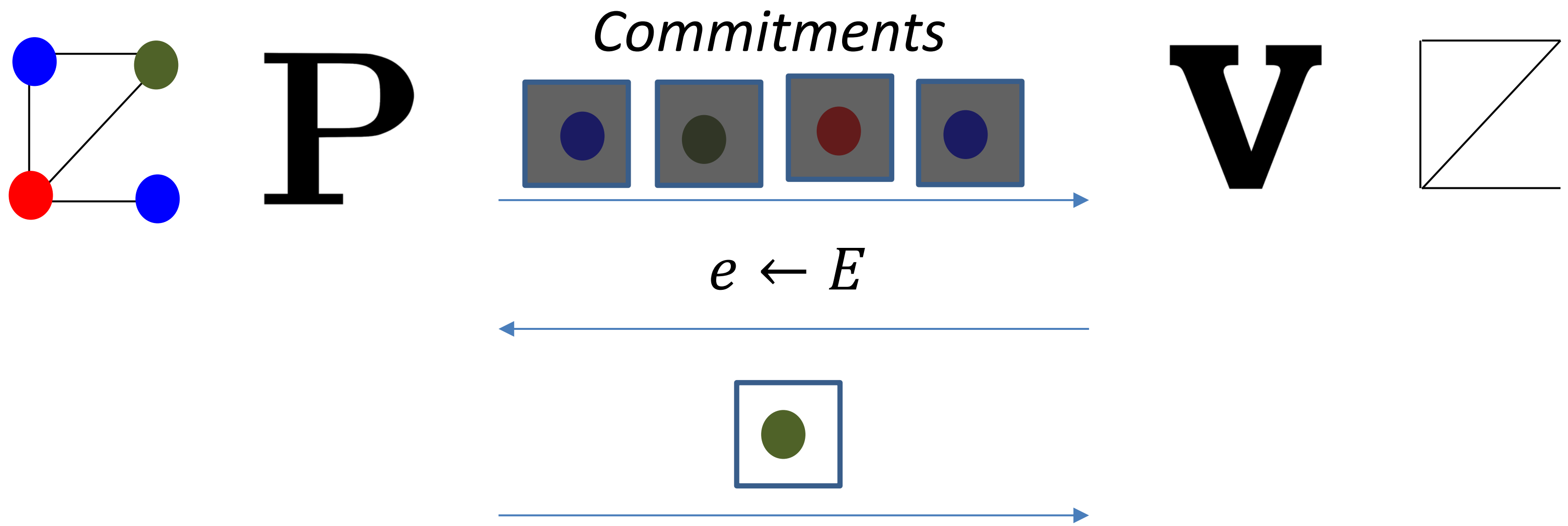


Prover P has a witness, the 3-coloring of G

Verifier V checks:
(a) only 3 colors are used &
(b) any two vertices connected by an edge are colored differently.

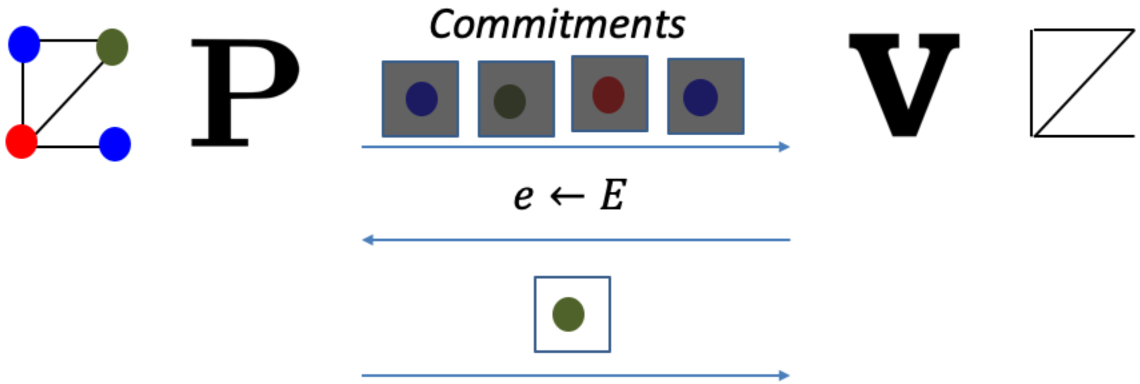
Zero-Knowledge (Interactive) Proof

Because NP proofs reveal too much



Zero-Knowledge (Interactive) Proof

Because NP proofs reveal too much



1. Completeness: For every G ∈ 3COL, V accepts P's proof.

2. Soundness: For every G ∉ 3COL and any cheating P^*, V rejects P^*'s proof with probability $\geq 1 - \mathrm{neg}(n)$

3. Zero Knowledge: For every cheating V^*, there is a PPT simulator S such that for every G ∈ 3COL, S ***simulates the view*** of V^*.

Zero Knowledge Proofs

Theorem [Goldreich-Micali-Wigderson’87] Assuming one-way functions exist, all of NP has computational zero-knowledge proofs.


zkproof.org
Error
ZKPROOF
HOME
ABOUT
EVENTS
RESOURCES
FORUM
GALLERY
BLOG
5TH WORKSHOP
ZKProof Standards
A global movement to standardize and mainstream advanced cryptography by building a community-driven trust ecosystem
UPCOMING EVENT
5th ZKProof Workshop
November 15-17, 2022 • Tel-Aviv
TELL ME MORE!
View past events >

Topic 1:

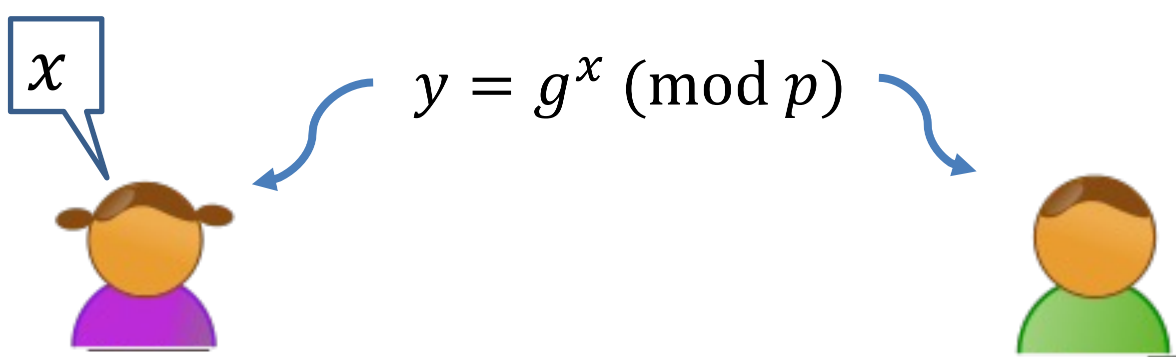
Proofs of Knowledge

So far: Decision Problems

$y \in L$ or $y \notin L$

(e.g. y is a quadratic residue mod N or it is not)

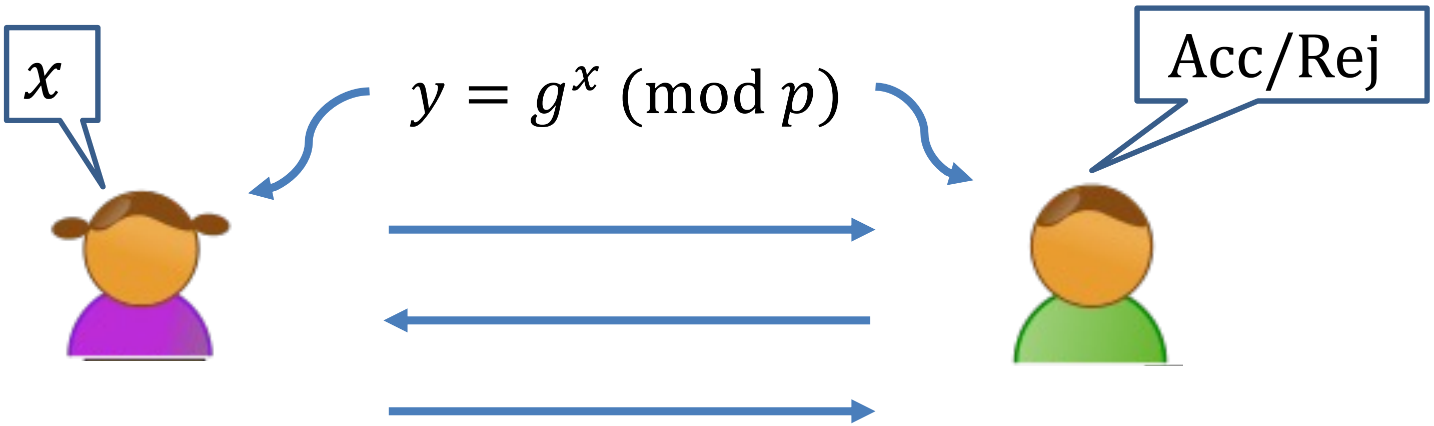
Here is a different scenario:



Discrete log of y always exists (assuming g is a generator)…

Alice wants to convince Bob that ***she knows a solution*** to a problem, e.g. that she knows the discrete log of y

So far: Decision Problems

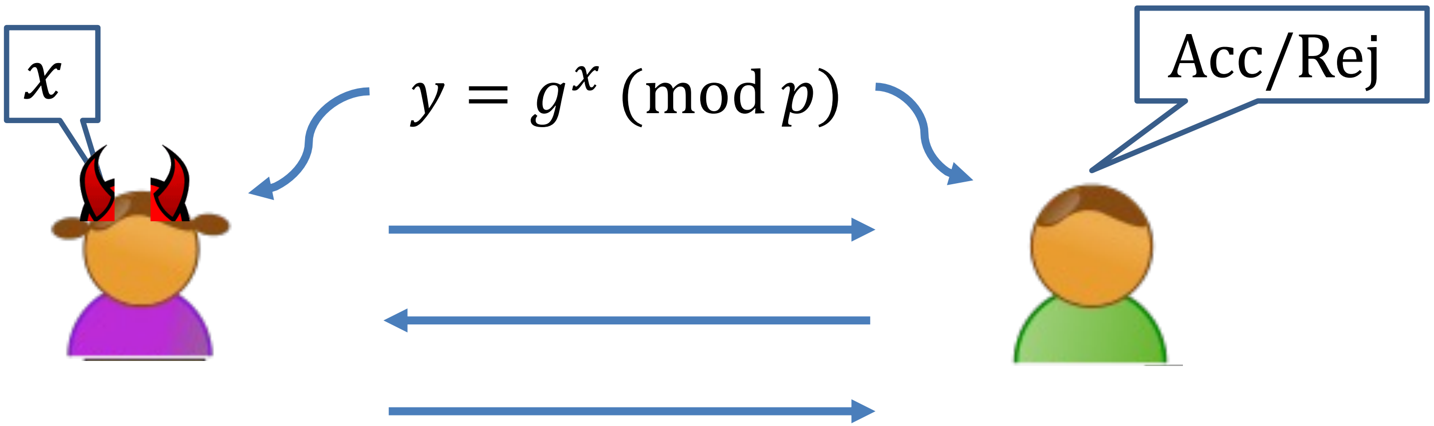


Completeness: When Alice and Bob run the protocol where Alice has input x, Bob outputs *accept*.

Soundness? How to define it?

Zero Knowledge: There is a simulator that, given only y, outputs a view of Bob that is indistinguishable from his view in an interaction with Alice.

Proof of Knowledge



If Alice knows x, there must be a way to "extract it from her".

I will not define an extractor formally but will show you an example (see Goldreich's book for more)

ZK Proof of Knowledge of Discrete Log

$p = 2q + 1$

x

$y = g^x \pmod{p}$

Acc/Rej

$z = g^r \pmod{p}$ $\longrightarrow$

$c \leftarrow \{0,1\}$ $\longleftarrow$

$s = r + cx \pmod{q}$ $\longrightarrow$

Accept iff $g^s = z \cdot y^c$

Completeness and Zero Knowledge: Exercise.

Proof of Knowledge: Extractor

$y = g^x \pmod p$

P^*

$z = g^r \pmod p$

$c = 0$ $c = 1$

s_0 s_1

Assume P^* convinces the verifier with prob. $> \frac{1}{2} + 1/poly$

Extractor runs P^* to get a z.

Runs P^* with $c = 0$ and gets s_0

Rewinds P^* to the first message.

Runs P^* with $c = 1$ and gets s_1

$g^{s_0} = z$ and $g^{s_1} = zy$ w.p. $1/poly$

$g^{s_1 - s_0} = y$.
So, $s_1 - s_0$ is the discrete log of y.

Zero Knowledge vs. Proof of Knowledge

Zero knowledge is a property of the prover against malicious verifiers. A prover P reveals zero knowledge if for all V^* …

Soundness and Proof of knowledge are properties of the verifier against malicious provers. A verifier V is sound (resp. satisfied PoK) if for all P^* …

Zero Knowledge Proofs of Knowledge

Theorem [Goldreich-Micali-Wigderson’87] Assuming one-way functions exist, all of NP has computational zero-knowledge proofs of knowledge.

Topic 2:

The Round-Complexity of ZK

Reducing Soundness Error

The 3COL protocol has a large soundness error of $1 - 1/|E|$

(probability that V accepts even though $G \notin 3COL$)

Theorem: Sequential Repetition reduces soundness error for interactive proofs (and preserves the ZK property.)

Problem: Lots of rounds

Theorem: Parallel Repetition reduces soundness error for interactive proofs. It is also honest-verifier ZK.

Theorem [Goldreich-Krawczyk'90] There exist ZK proofs whose parallel repetition is NOT (malicious verifier) zero knowledge.

But the GK 90 counterexample is quite contrived. How about "natural protocols", e.g. the GMW 3-coloring protocol from the last lecture?

Theorem [Goldreich-Krawczyk'90] There exist ZK proofs whose parallel repetition is NOT (malicious verifier) zero knowledge.

Theorem [Holmgren-Lombardi-Rothblum'21] Parallel Repetition of the (Goldreich-Micali-Wigderson) 3COL protocol is ***not*** zero-knowledge.

Fiat-Shamir via List-Recoverable Codes (or: Parallel Repetition of GMW is not Zero-Knowledge)

Justin Holmgren* Alex Lombardi† Ron D. Rothblum‡

March 6, 2021

Abstract

Shortly after the introduction of zero-knowledge proofs, Goldreich, Micali and Wigderson (CRYPTO '86) demonstrated their wide applicability by constructing zero-knowledge proofs for the NP-complete problem of graph 3-coloring. A long-standing open question has been whether parallel repetition of their protocol preserves zero knowledge. In this work, we answer this question in the negative, assuming a standard cryptographic assumption (i.e., the hardness of learning with errors (LWE)).

Leveraging a connection observed by Dwork, Naor, Reingold, and Stockmeyer (FOCS '99), our negative result is obtained by making *positive* progress on a related fundamental problem in cryptography: securely instantiating the Fiat-Shamir heuristic for eliminating interaction in public-coin interactive protocols. A recent line of works has shown how to instantiate the heuristic securely, albeit only for a limited class of protocols.

Our main result shows how to instantiate Fiat-Shamir for parallel repetitions of much more general interactive proofs. In particular, we construct hash functions that, assuming LWE,

Reducing Soundness Error

Fortunately, we have:

Theorem [Goldreich-Kahan'95] There is a constant-round ZK proof system for 3COL (with exponentially small soundness error), assuming discrete logarithms are hard (more generally, assuming the existence of collision-resistant hash functions).

Topic 3:

Can we make proofs non-interactive again?

Why?

1. *V does not need to be online during the proof process.*
2. *Proofs are not ephemeral, can stay into the future.*

Topic 3:

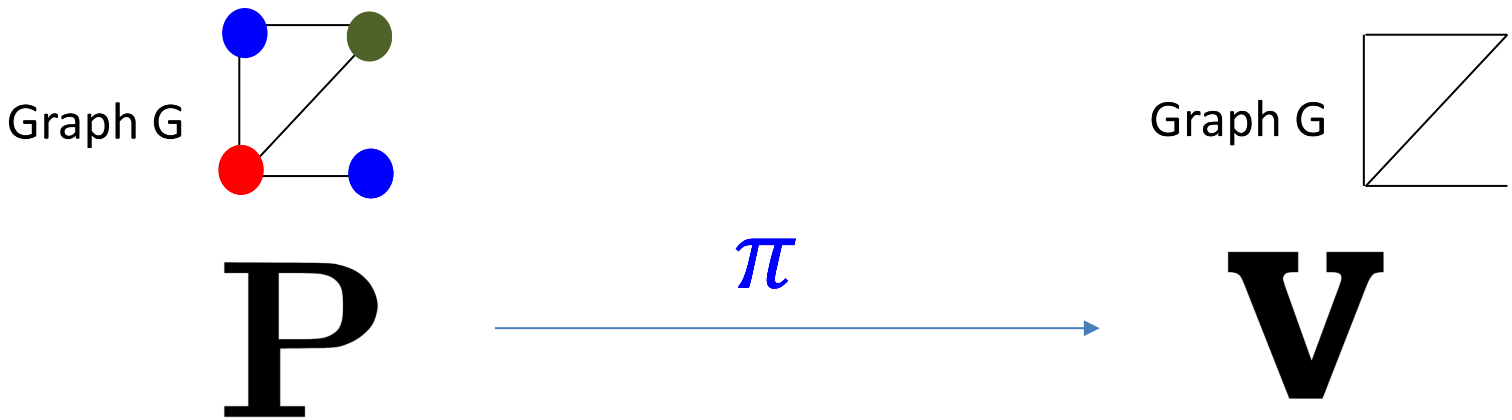
Can we make proofs non-interactive again?

YES, WE CAN!

NO!

Non-Interactive ZK is Impossible

Suppose there *were* an NIZK proof system for 3COL.

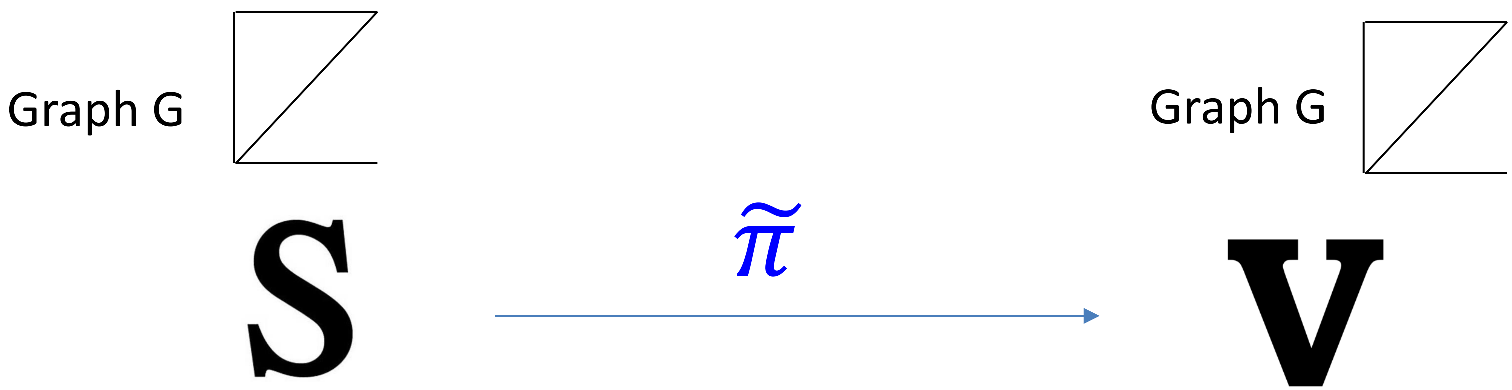


Step 1. When G is in 3COL, V accepts the proof π.

(Completeness)

Non-Interactive ZK is Impossible

Suppose there *were* an NIZK proof system for 3COL.

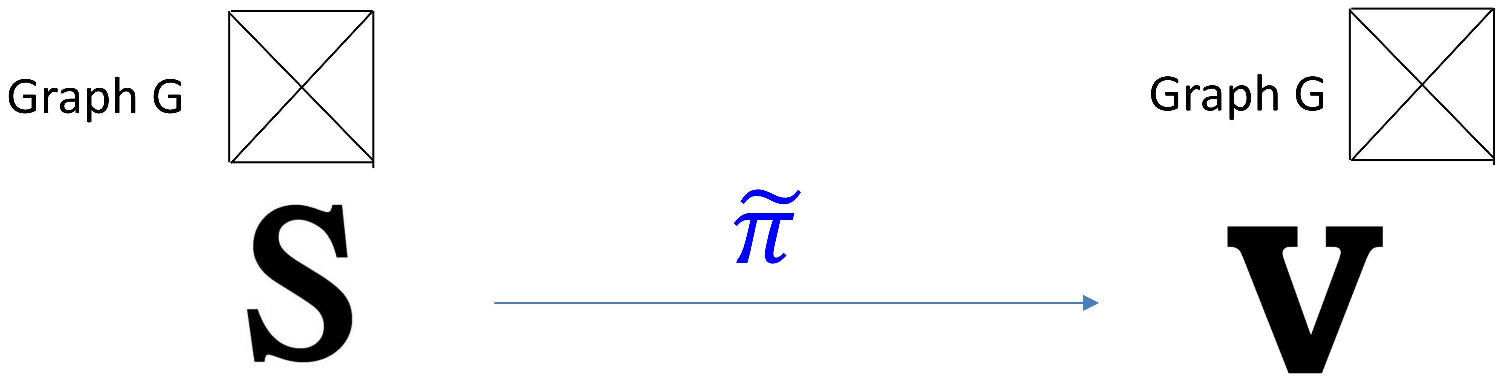


Step 2. **PPT** Simulator S, **given only G in 3COL**, produces an indistinguishable proof $\tilde{\pi}$ (Zero Knowledge).

In particular, V accepts $\tilde{\pi}$.

Non-Interactive ZK is Impossible

Suppose there *were* an NIZK proof system for 3COL.

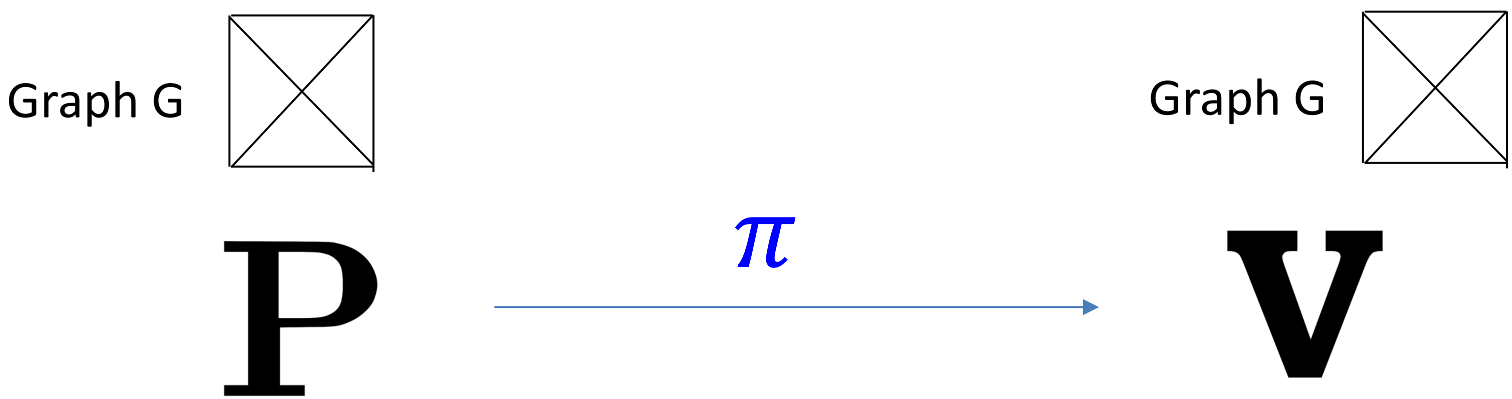


Step 3. Imagine running the Simulator S on a $G \notin$ 3COL. It produces a proof $\tilde{\pi}$ which the verifier still accepts!

(WHY?! Because S and V are PPT. They together cannot tell if the input graph is 3COL or not)

Non-Interactive ZK is Impossible

Suppose there *were* an NIZK proof system for 3COL.



Step 4. **Therefore, S is a cheating prover!**

Produces a proof for a $G \notin$ 3COL that the verifier nevertheless accepts.

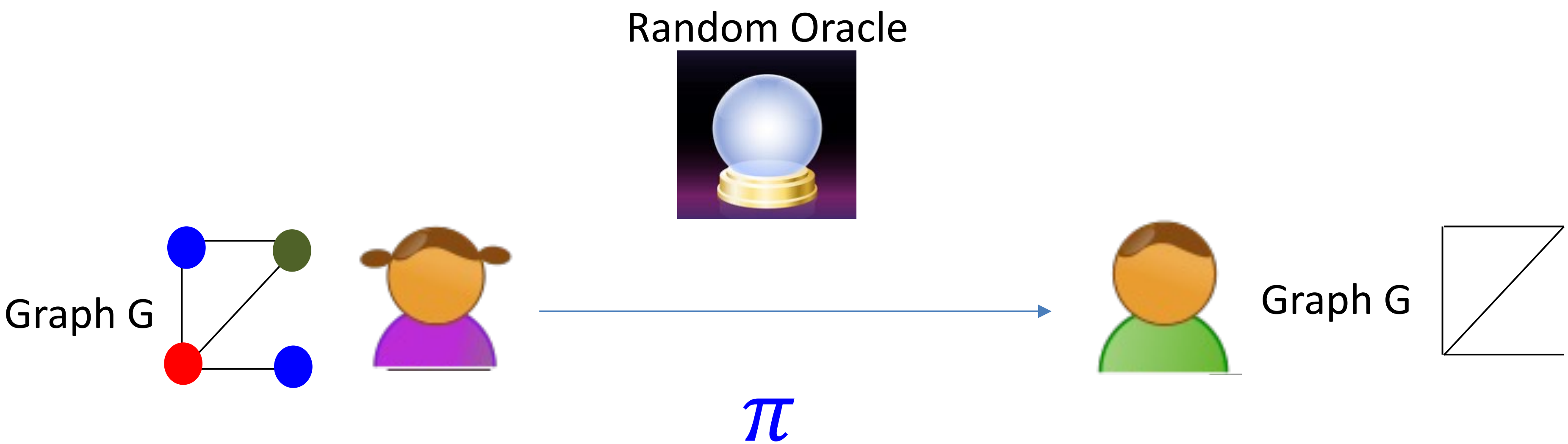
Ergo, the proof system is NOT SOUND!

THE END

Or, is it?

Two Roads to Non-Interactive ZK (NIZK)

1. Random Oracle Model & Fiat-Shamir Transform.



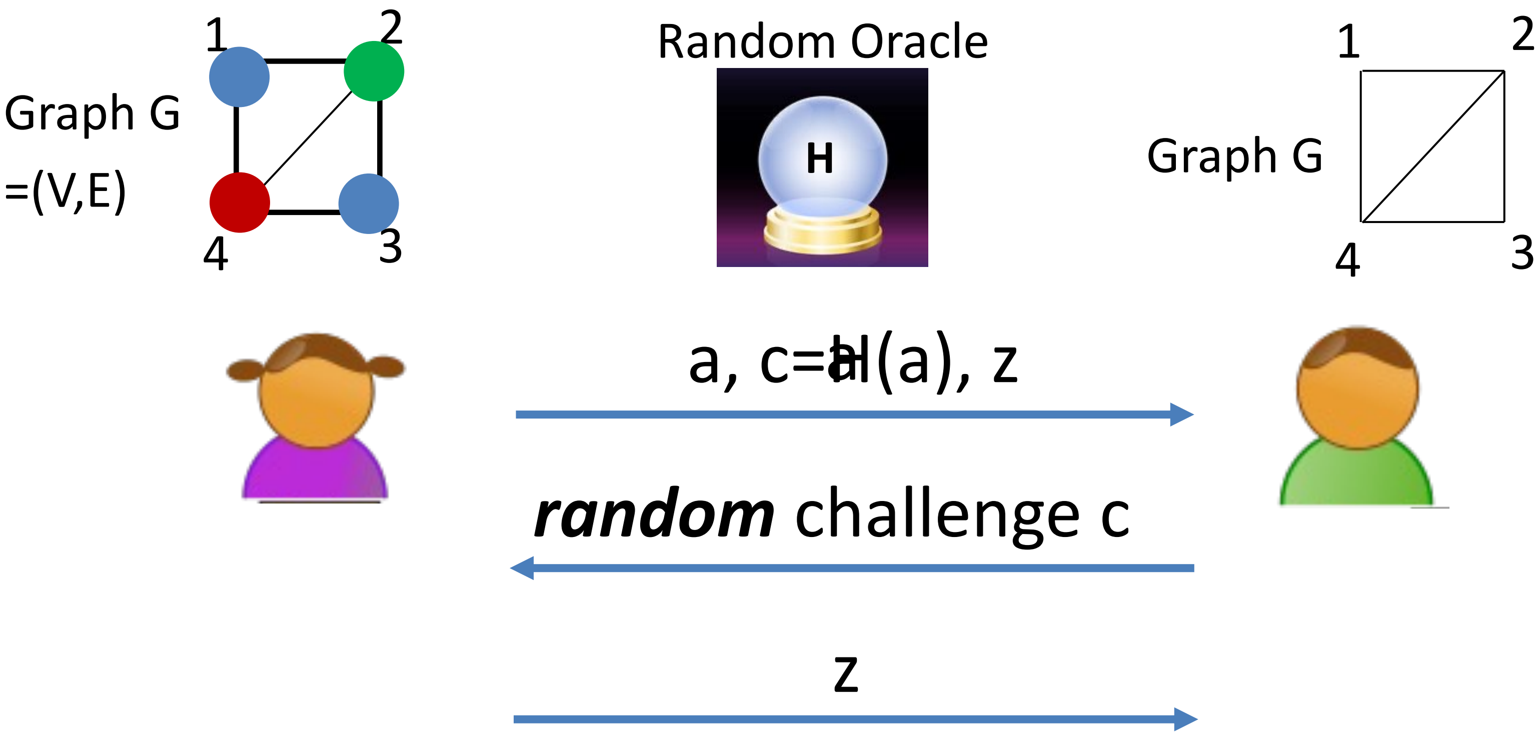
2. Common Random String Model (We won't go into this in the course, but if you are curious, see L16 slides from Fall 2021.)

NIZK Proof for 3COL

Start with the parallel repetition of the 3COL protocol.

Recall: it is complete, has exponentially small soundness error, and is HVZK.

NIZK Proof for 3COL



Fiat and Shamir 1986: Let c = H(a). Now the prover can compute the challenge herself!

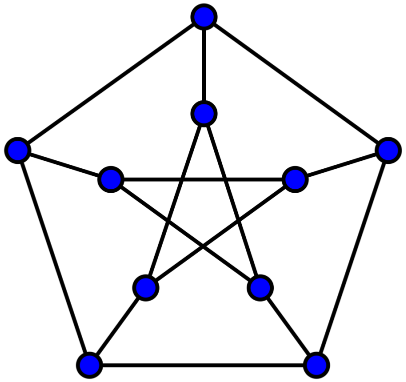
Potentially harmful for soundness. But in the random oracle model for H, can prove soundness.

Topic 4:

The Power of Interactive Proofs

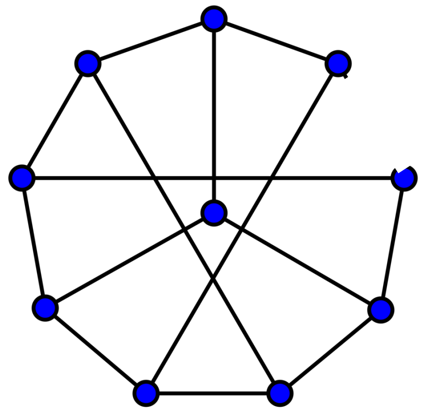
What can we prove with interaction?

Interactive Proof for Graph **Non**-Isomorphism



Graph G_0

$\ncong$



Graph G_1

Completely unclear how to prove in NP.

Prover

Verifier

Pick a random bit b and a random permutation ρ

$$\xleftarrow{\quad \rho(G_b) \quad}$$

$$\xrightarrow{\quad b' \quad}$$

Accept if $b = b'$.

A window into a promised land…

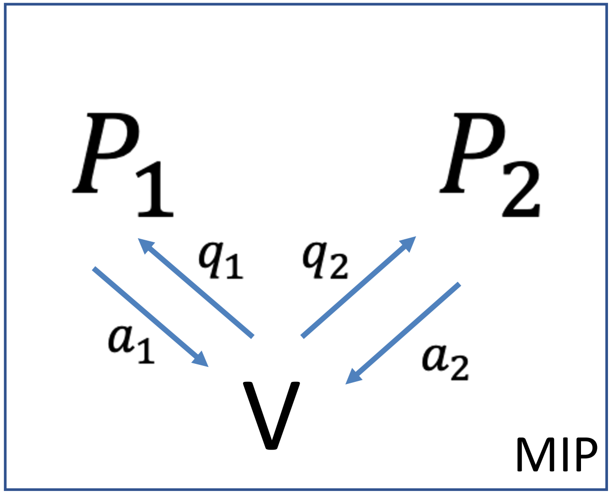
The Power of Interactive Proofs

Theorem [Nisan'90, Lund-Fornow-Karloff-Nisan'90] There is an interactive proof for the statement that the number of satisfying assignments to a formula is a given number (this complexity class is called $\#P$).

Theorem [Shamir'90] $IP = PSPACE$.

The Power of Interactive Proofs

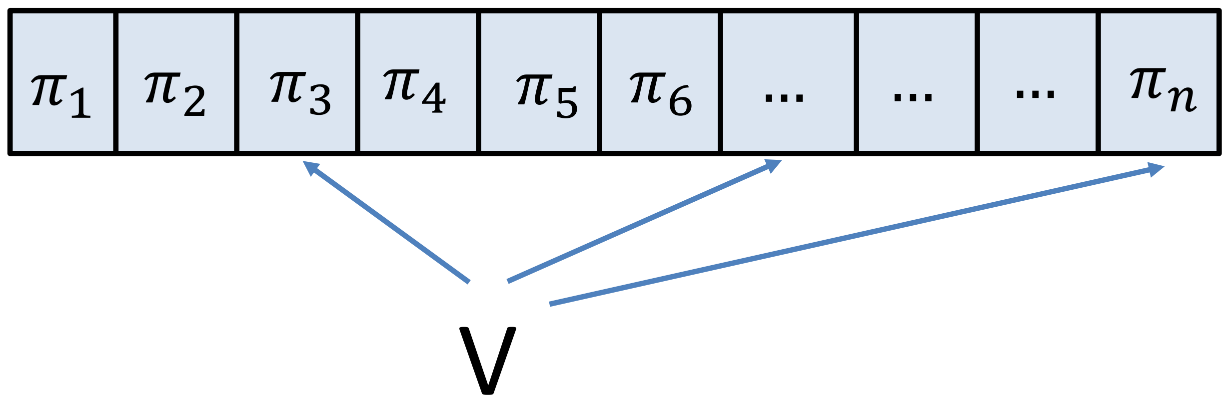
Definition of multi-prover interactive proofs [BenOr-Goldwasser-Kilian-Wigderson'88]



Theorem [Babai-Fornow-Lund'90] $\mathrm{M}IP = NEXP$.

The Power of Interactive Proofs

Definition of probabilistically checkable proofs [Arora-Safra'92, Feige-Goldwasser-Lovasz-Safra-Szegedy'91]



Theorem [Arora-Lund-Motwani-Sudan-Szegedy'92]

$$\mathrm{PCP}(3) = NP.$$

E-mail and the unexpected power of interaction

László Babai *
Eötvös University, Budapest
and
The University of Chicago

Abstract

This is a true fable about Merlin, the infinitely intelligent but never trusted magician; and Arthur, the reasonable but impatient sovereign with an occasional unorthodox request; about the concept of an efficient proof; about polynomials and interpolation, electronic mail, coin flipping, and the *incredible power of interaction*.

About MIP, IP, $\#P$, $PSPACE$, $NEXPTIME$, and new techniques that do not relativize. About fast progress, fierce competition, and e-mail ethics.

1 How did Merlin end up in the cave?

In the court of King Arthur[1] there lived 150 knights and 150 ladies. "Why not 150 married couples," the King contemplated one rainy afternoon, and action followed the thought. He asked the Royal Secret Agent (RSA) to draw up a diagram with all the 300 names, indicating bonds of mutual interest between lady and knight by a red line; and the lack thereof, by

Of course not even a tiny fraction could fit in the throne room, but Arthur wouldn't even wait till the room filled up. He dismissed Merlin's procedure ("obviously, you overlooked a case") and ordered him to come back with a solution the next day. Arthur's diaries reveal another thought that was on his mind: "The lifetime of the universe wouldn't suffice to check all that crud. That's how the old fox wants to fool me."

Merlin *knew* that he was right, and he knew also that Arthur was reasonable. All Merlin had to do was to convince him, *in five minutes*, that there was no solution.

Fortuitously, in the cafeteria he bumped into an unassuming character dressed in brand new blue jeans. An East Bloc visitor, the man humbly introduced himself as Dénes König, number one expert on perfect matchings. "Frobenius also claims this title," he added without bitterness. "Are you perhaps interested in my mini-max theory?" Having, at last, found a willing listener, the visiting scholar forgot his French fries and the free ketchup, and began a passionate lecture about bipartite graphs, maximum matchings

A history of the PCP Theorem   By Ryan O’Donnell

(This is a brief illustrated take on the history of the PCP Theorem, as inferred by the author, Ryan O’Donnell. My main sources were Babai’s article Email and the unexpected power of interaction*, Goldreich’s article* A taxonomy of proof systems*, and the original sources. Likely there are several inaccuracies and omissions, and I apologize for these and ask for corrections in advance. Since this note was prepared for a class at the University of Washington, a few details relating to UW have also been emphasized.)*

With the exciting new proof of the PCP Theorem by Irit Dinur (April 2005), a course on the PCP Theorem

Irit Dinur

no longer needs to get into many — if any — of the details involved in the original proof. But this original proof and the seven years of work leading up to it form an interesting history that is certainly worth hearing.

The story of the PCP Theorem begins at MIT in the early 1980s, with a paper that would win the first ever Gödel Prize: *The Knowledge Complexity of Interactive Proof Systems*, by Goldwasser, Micali, and Rackoff. This paper was first published in STOC ’85. However drafts of it are said to have existed as early

Shafi Goldwasser

Silvio Micali

Charlie Rackoff

Next Lecture:

Succinct Interactive Proofs:*

SNARGs, SNARKs and other beasts of the crypto zoo

<u>Vitalik Buterin, founder of Ethereum</u>: “I expect zk-SNARKs to be a significant revolution as they permeate the mainstream world over the next 10-20 years.”