CIS 5560

Cryptography
Lecture 21

Course website:
pratyushmishra.com/classes/cis-5560-s24/

Slides adapted from Dan Boneh and Vinod Vaikuntanathan

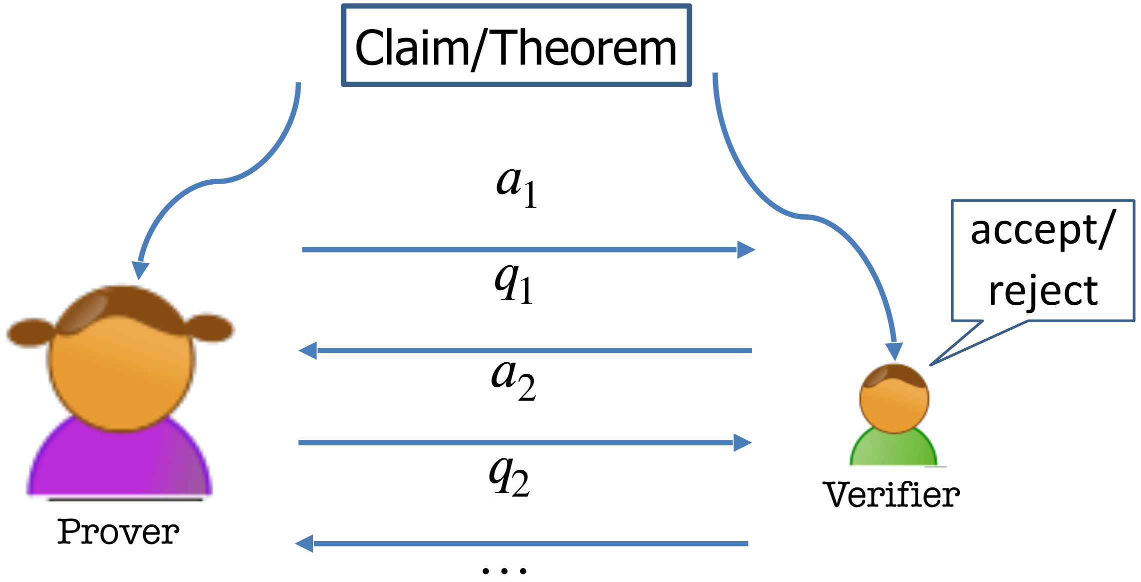
Announcements

- **HW 9 out**
  - Due **Wednesday Apr 17** at 11:59PM on Gradescope
  - Covers
    - One-time signatures
    - RSA-based signatures

Recap of last lecture

- What is a proof?
- Interactive Proofs
- *Zero-knowledge* interactive proofs

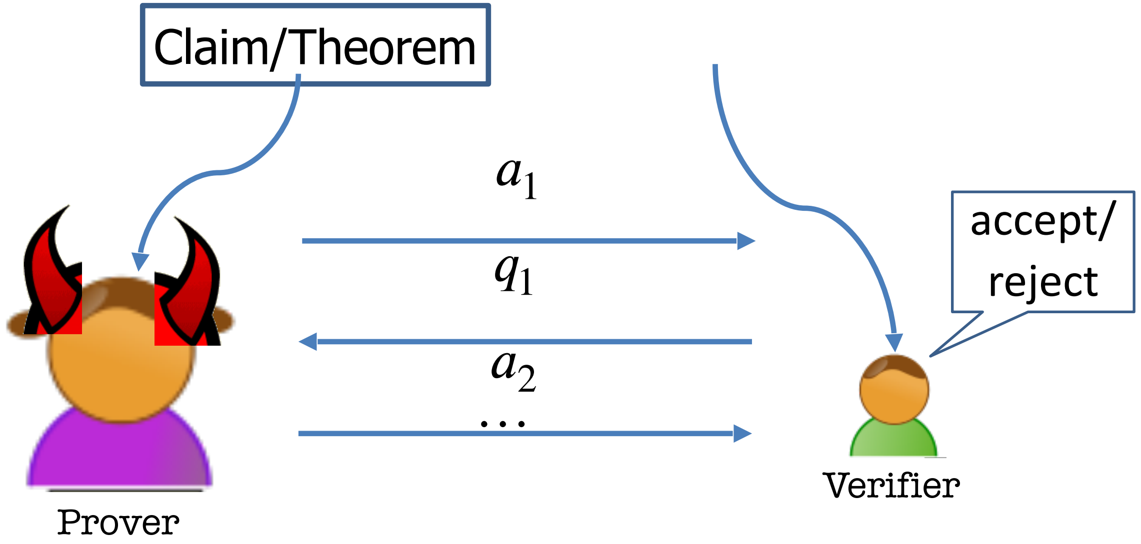
Interactive Proofs for a Language $\mathscr{L}$



Comp. Unbounded

Probabilistic
Polynomial-time

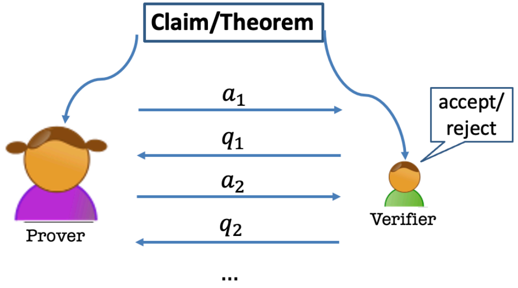
Interactive Proofs for a Language $\mathscr{L}$



Def: $\mathscr{L}$ is an IP-language if there is a unbounded P and **probabilistic poly-time** verifier V where

- **Completeness**: If $x \in \mathscr{L}$, V always accepts.
- **Soundness:** If $x \notin \mathscr{L}$, regardless of the cheating prover strategy, V accepts with negligible probability.

Interactive Proofs for a Language $\mathscr{L}$



Def: $\mathscr{L}$ is an IP-language if there is a **probabilistic poly-time** verifier V where

- **Completeness: If** $x \in \mathscr{L}$**,**

$$\Pr\left[(\mathrm{P}, V)(x) = accept\right] = 1.$$

- **Soundness: If** $x \notin \mathscr{L}$, **there is a negligible function** negl **s.t. for every** P^*,

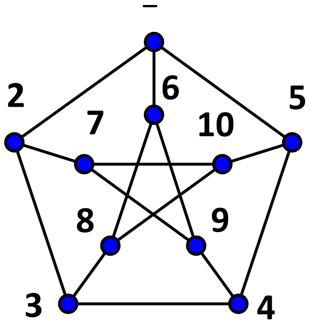
$$\Pr\left[\left(P^*, V\right)(x) = accept\right] = \mathrm{negl}(\lambda).$$

Today’s Lecture

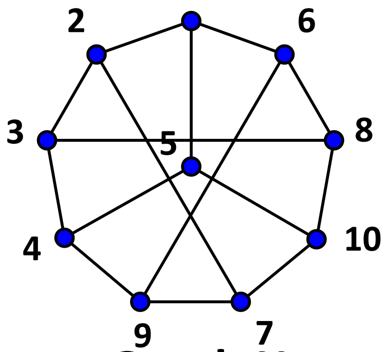
- Recap of GNI proof
- Look at “zero-knowledge” interactive proof for Graph Isomorphism
- Definition of Zero Knowledge
- Commitment Schemes
    - Pedersen Commitment Scheme

Recapping proof of GNI

ZK Proof for Graph Isomorphism



Graph G



Graph H

$\mathbf{H} = \pi(G)$

$K = \rho(G)$ →

where ρ is a random permutation

Prover

← random challenge bit b

Verifier

$b = 0$: send π_0 s.t. $\mathrm{K} = \pi_0(G)$ →

$b = 1$: send π_1 s.t. $\mathrm{H} = \pi_1(K)$

ZK Proof for Graph Isomorphism

Completeness?

$\mathbf{H} = \pi(G)$

Prover

$K = \rho(G)$ →

where ρ is a random permutation

← random challenge bit b

$b = 0$: send $\pi_0 = \rho$ →

$b = 1$: send $\pi_1 = \pi \circ \rho^{-1}$

Verifier

ZK Proof for Graph Isomorphism

Soundness: Suppose G and H are non-isomorphic, and a prover could answer both the verifier challenges. Then,

$\mathrm{K} = \pi_0(G)$ and $\mathrm{H} = \pi_1(K)$.

In other words, $\mathrm{H} = \pi_1 \circ \pi_0(G)$, a contradiction!

$\mathbf{H} = \pi(G)$

Prover

$K = \rho(G)$

where ρ is a random permutation

random challenge bit b

Verifier

$b = 0$: send $\pi_0 = \rho$

$b = 1$: send $\pi_1 = \pi \circ \rho^{-1}$

ZK Proof for Graph Isomorphism

Zero Knowledge?

$\mathbf{H} = \pi(G)$

Prover

$K = \rho(G)$ →

where ρ is a random permutation

Verifier

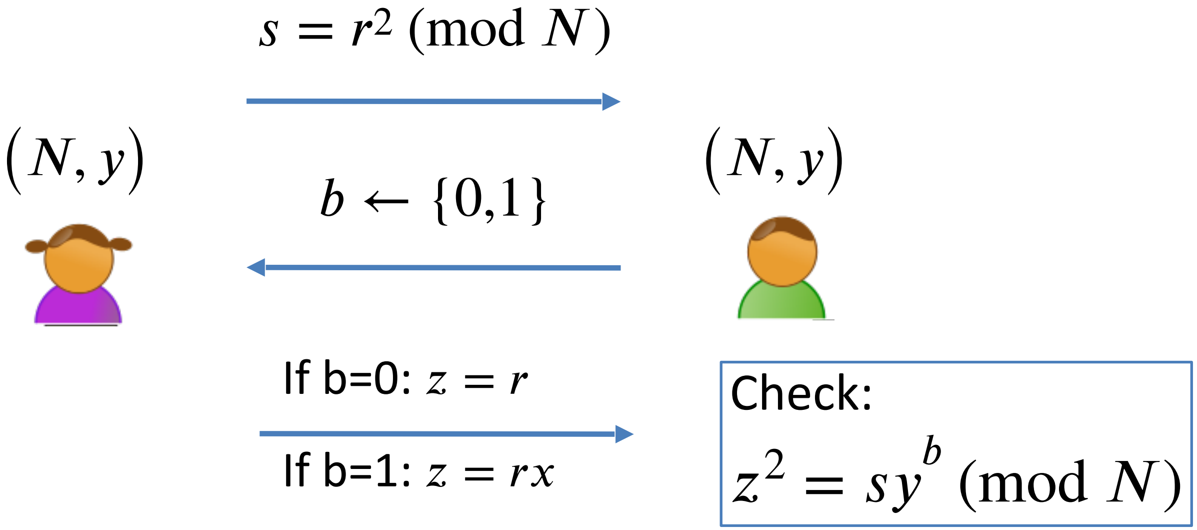
← random challenge bit b

$b = 0$: send $\pi_0 = \rho$ →

$b = 1$: send $\pi_1 = \pi \circ \rho^{-1}$

Interactive Proof for QR

$$\mathcal{L} = \{(N, y) \mid \exists x \in \mathbb{Z}_N, y = x^2 \mod N\}.$$



Completeness

Claim: If $(N, y) \in L,$ then the verifier accepts the proof with probability 1.

Proof:

$$z^2 = (rx^b)^2 = r^2(x^2)^b = sy^b \pmod{N}$$

So, the verifier's check passes and he accepts.

Soundness

Claim: If $(N, y) \notin L$, then for every cheating prover P^*, the verifier accepts with probability at most 1/2.

Proof: Suppose the verifier accepts with probability > 1/2.

Then, there is some $s \in Z_N^*$ s.t. the prover produces

$$z_0 : z_0^2 = s \pmod N$$

$$z_1 : z_1^2 = sy \pmod N$$

This means $(z_1/z_0)^2 = y \pmod N$, which tells us that $(N, y) \in L$.

This is Zero-Knowledge.

But what does that mean?

$$s = r^2 \pmod{N}$$

→

(N, y)

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

←

(N, y)

If b=0: $z = r$

→

If b=1: $z = rx$

Check:

$z^2 = sy^b \pmod{N}$

How to Define Zero-Knowledge?

After the interaction, V knows:

- The theorem is true; and
- A **view** of the interaction
  (= transcript + randomness of V)

P gives zero knowledge to V:

When the theorem is true, the view gives V nothing that he couldn't have obtained on his own without interacting with P.

How to Define Zero-Knowledge?

(P, V) is zero-knowledge if V can generate his **VIEW** of the interaction **all by himself** in **probabilistic polynomial time**.

How to Define Zero-Knowledge?

(P, V) is zero-knowledge if V can "simulate" his **VIEW** of the interaction **all by himself** in **probabilistic polynomial time**.

The Simulation Paradigm

n_S:

$b, z)$

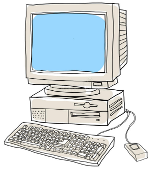
$view_V(P, V)$:

Transcript = (s, b, z),

(s, b, z)

Coins = b

PPT "simulator" S



(N, y)

$s = r^2 \pmod N$

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

(N, y)

If b=0: $z = r$

If b=1: $z = rx$

Check:
$z^2 = sy^b \pmod N$

Zero Knowledge: Definition

An Interactive Protocol (P,V) is zero-knowledge for a language L if there exists a **PPT** algorithm S (a simulator) such that **for every $x \in L$**, the following two distributions are indistinguishable:

1. $view_V(P, V)$

2. $S(x, 1^\lambda)$

(P,V) is a zero-knowledge interactive protocol if it is complete, sound and zero-knowledge.

Perfect Zero Knowledge: Definition

An Interactive Protocol (P,V) is **perfect zero-knowledge** for a language L if there exists a PPT algorithm S (a simulator) such that for every $x \in L$, the following two distributions are **identical**:

1. $view_V(P, V)$

2. $S(x, 1^\lambda)$

(P,V) is a zero-knowledge interactive protocol if it is complete, sound and zero-knowledge.

Computational Zero Knowledge: Definition

An Interactive Protocol (P,V) is **computational zero-knowledge** for a language L if there exists a PPT algorithm S (a simulator) such that for every $x \in L$, the following two distributions are **computationally indistinguishable**:

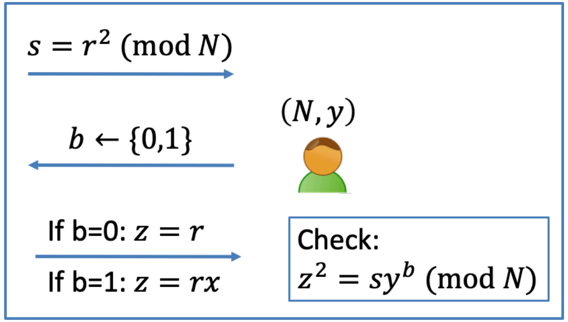
1. $view_V(P, V)$

2. $S(x, 1^\lambda)$

(P,V) is a zero-knowledge interactive protocol if it is complete, sound and zero-knowledge.

Zero Knowledge

Claim: The QR protocol is zero knowledge.



$view_V(P, V)$:
(s, b, z)

Simulator S works as follows:

1. First pick a random bit b.
2. pick a random $z \in Z_N^*$.
3. compute $\mathrm{s} = z^2/y^b$.
4. output $(\mathrm{s}, \mathrm{b}, \mathrm{z})$.

Exercise: The simulated transcript is identically distributed as the real transcript in the interaction (P,V).