CIS 5560

Cryptography
Lecture 21

Course website:

pratyushmishra.com/classes/cis-5560-s24/

Slides adapted from Dan Boneh and Vinod Vaikuntanathan

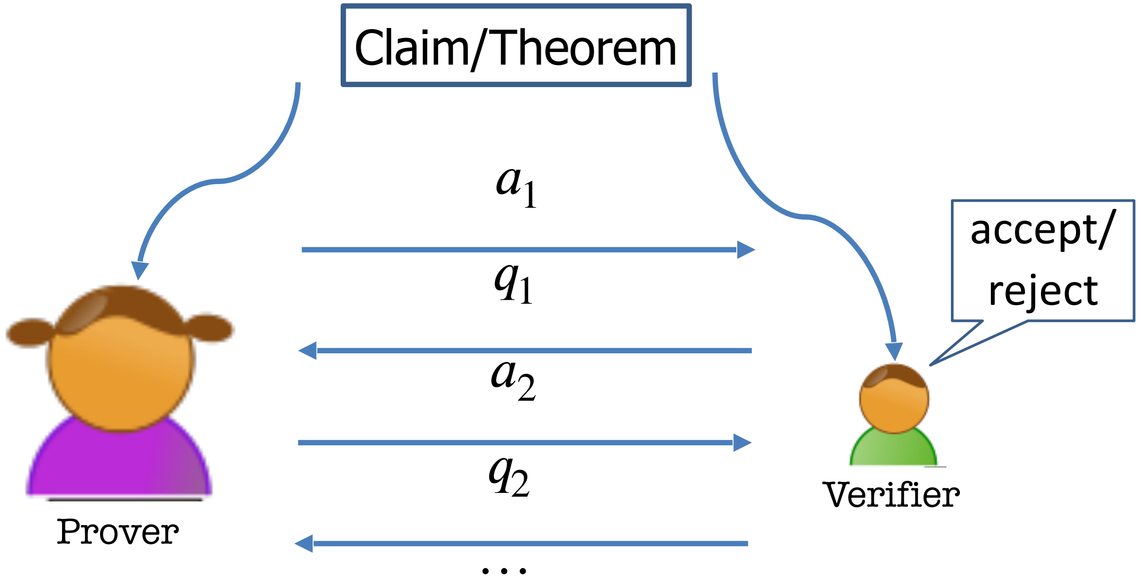
Announcements

- **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 $\mathscr{L}$



Claim/Theorem

a_1

q_1

a_2

q_2

$\dots$

Prover

Verifier

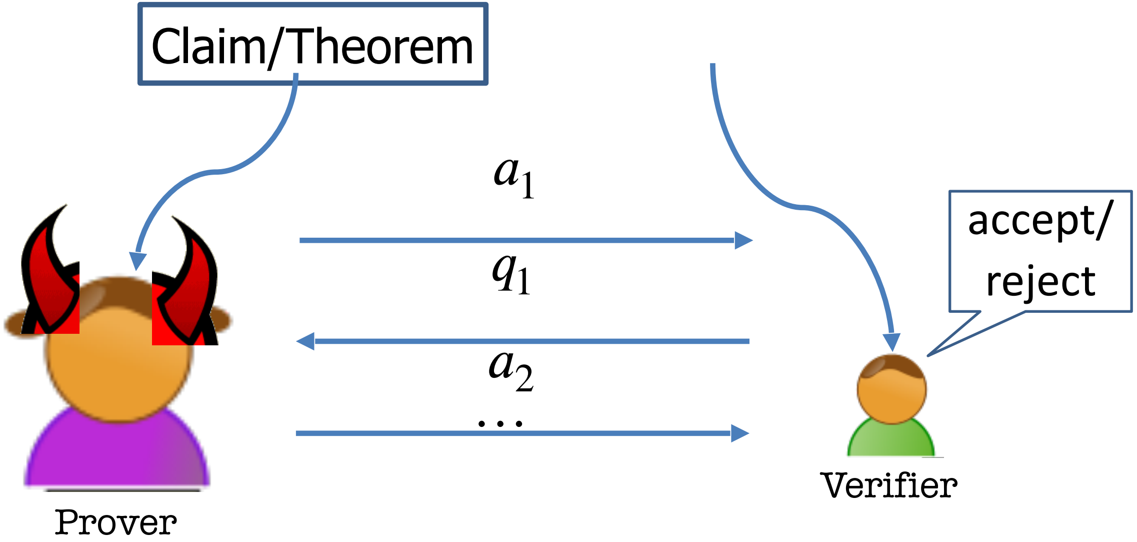
accept/ reject

Comp. Unbounded

Probabilistic

Polynomial-time

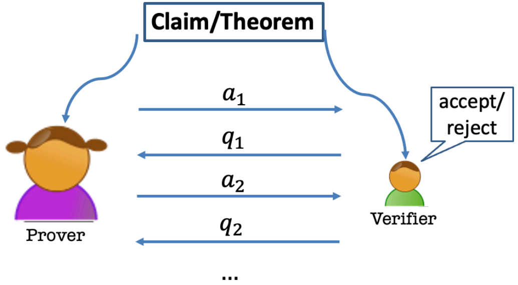
Interactive Proofs for a Language $\mathscr{L}$



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** $\mathrm{x} \in \mathscr{L}$**,**

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

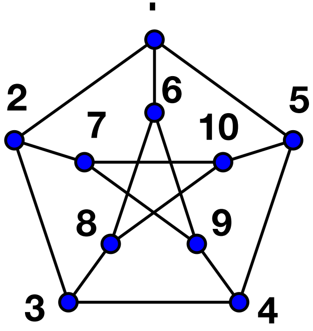
- **Soundness: If** $\mathrm{x} \notin \mathscr{L}$, **there is a negligible function** negl **s.t. for every** P^*,

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

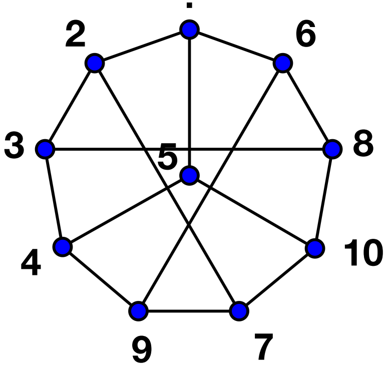
Today’s Lecture

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

IP for Graph *Non*-Isomorphism



Graph G



Graph H

Prover

Verifier

Sample random permutation ρ

Sample bit b

Set $K_0 = \rho(G)$ and $K_1 = \rho(H)$

K_b

Figure out which graph K_b is isomorphic to.

b'

Accept if $b = b'$

IP for Graph Non-Isomorphism

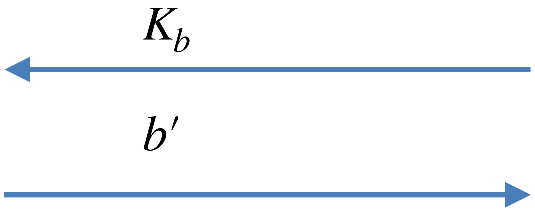
Completeness?

Prover

Verifier

Sample random permutation ρ
Sample bit b
Set $K_0 = \rho(G)$ and $K_1 = \rho(H)$

Figure out which graph K_b is isomorphic to.

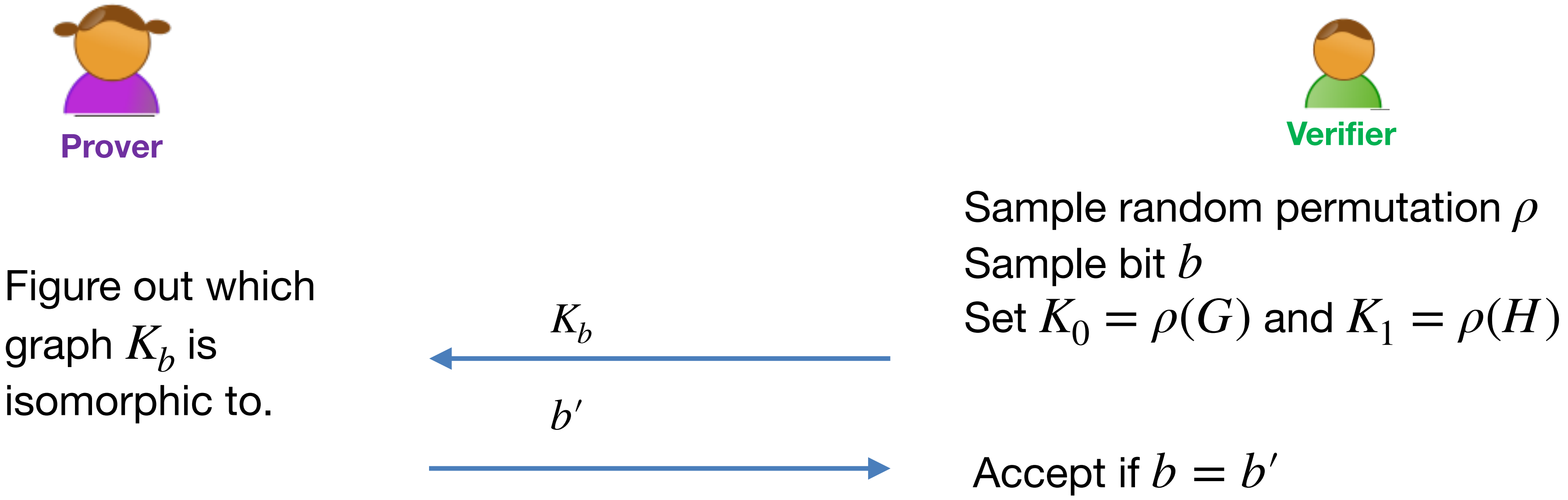

K_b

b'

Accept if $b = b'$

IP for Graph Non-Isomorphism

Soundness: Suppose G and H are isomorphic.
Then K_b is isomorphic to *both graphs.* Prover can't figure out which one it is isomorphic to
So best it can do is guess!



Prover

Verifier

Sample random permutation ρ
Sample bit b
Set $K_0 = \rho(G)$ and $K_1 = \rho(H)$

K_b

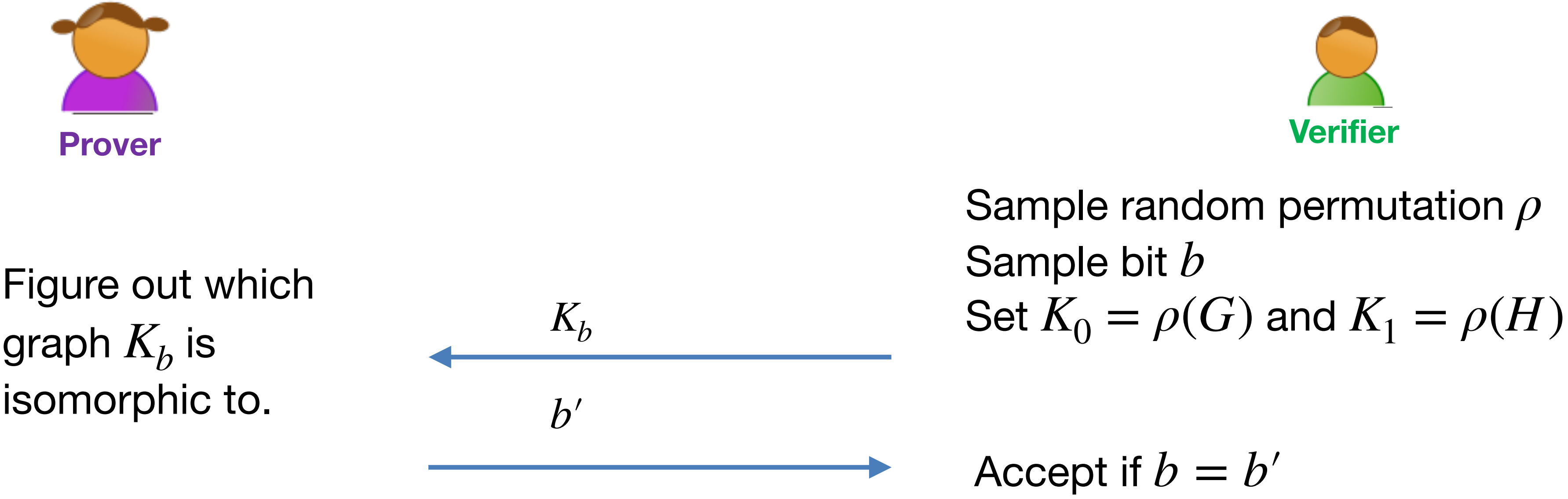
Figure out which graph K_b is isomorphic to.

b'

Accept if $b = b'$

IP for Graph Non-Isomorphism

What else does the verifier learn?



Sample random permutation ρ

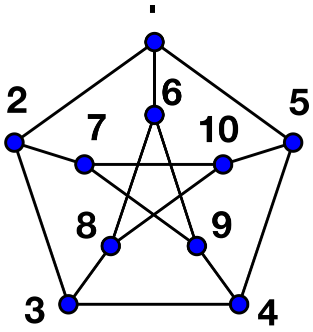
Sample bit b

Set $K_0 = \rho(G)$ and $K_1 = \rho(H)$

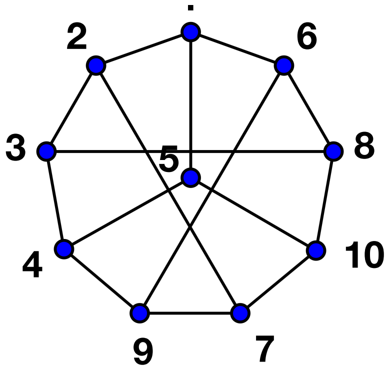
Figure out which graph K_b is isomorphic to.

Accept if $b = b'$

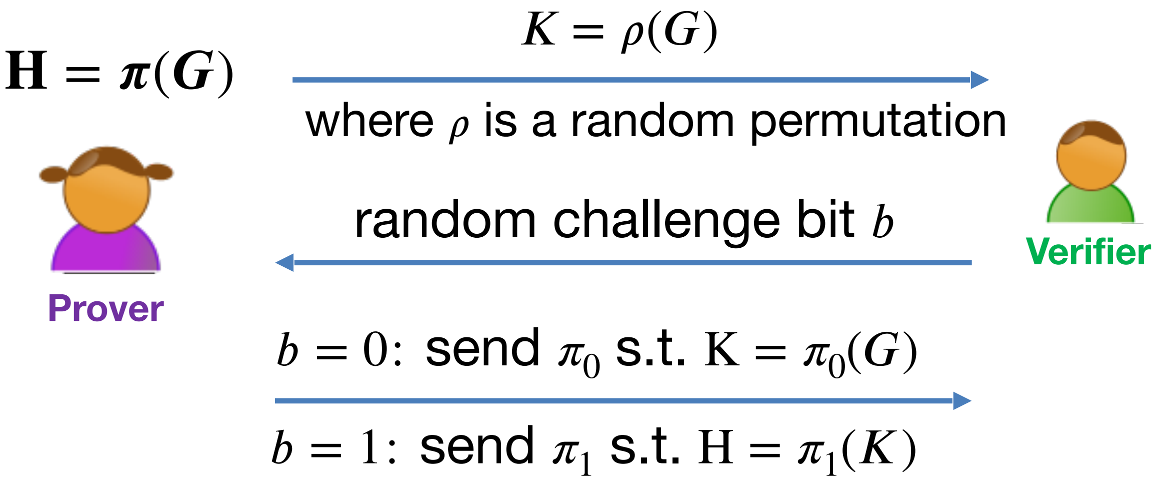
IP for Graph Isomorphism



Graph G



Graph H



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

$K = \rho(G)$

where ρ is a random permutation

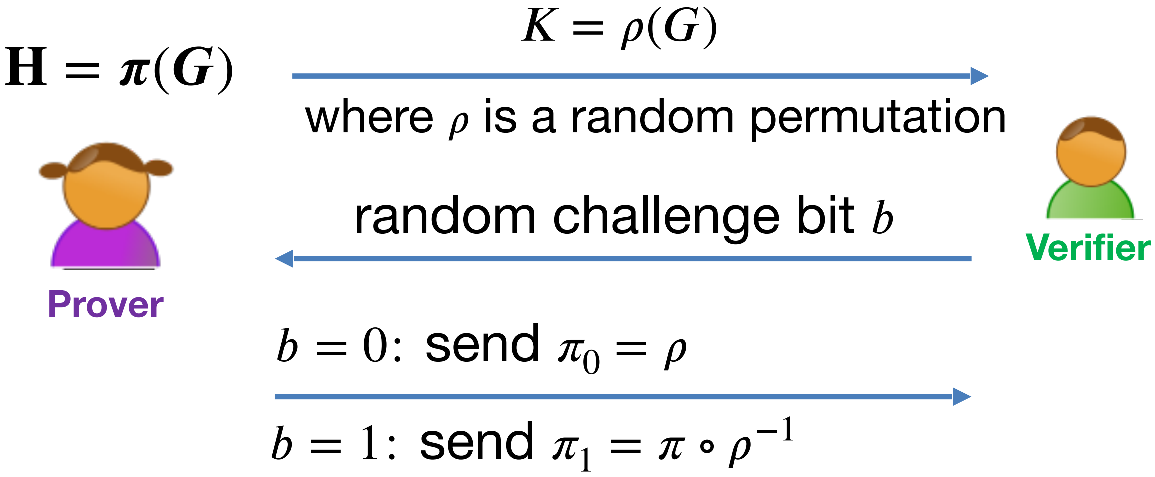
random challenge bit b

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

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

IP for Graph Isomorphism

Completeness?



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

Prover

$K = \rho(G)$

where ρ is a random permutation

random challenge bit b

Verifier

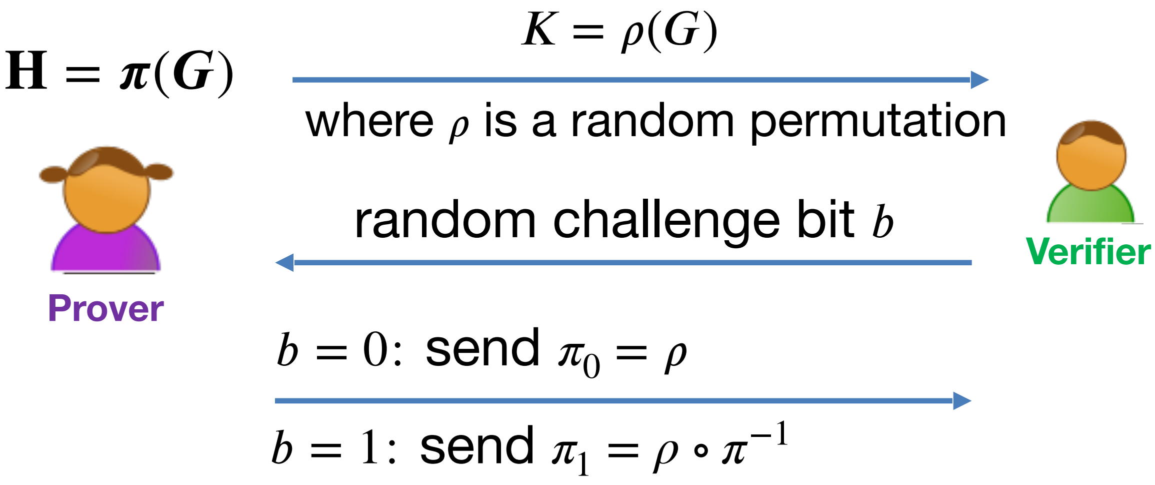
$b = 0:$ send $\pi_0 = \rho$

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

IP for Graph Isomorphism

Soundness: Suppose G and H are non-isomorphic, and a prover could answer both the verifier challenges. Then, $K = \pi_0(G)$ and $H = \pi_1(K)$

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



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

$K = \rho(G)$

where ρ is a random permutation

random challenge bit b

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

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

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?

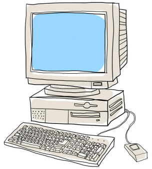
(P, V) is zero-knowledge if V can “simulate” his **VIEW** of the interaction **all by himself** in **probabilistic polynomial time**.

The Simulation Paradigm

sim S

(K, b, π')

PPT “simulator” S



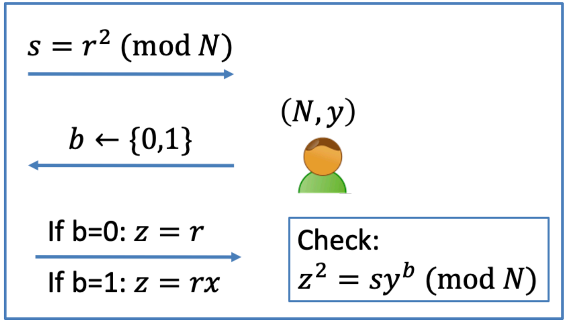
(G, H)

$view_V(P, V)$:

(K, b, π')

Transcript $= (K, b, \pi')$

Coins $= b$



$s = r^2 \pmod N$

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

(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-

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-

What if V is NOT HONEST.

OLD DEF

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

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

REAL DEF

An Interactive Protocol (P,V) is **perfect zero-knowledge** for a language L if **for every PPT V^***, there exists a (expected) poly time simulator S s.t. for every $x \in L$, the following two distributions are identical:

1. $view_{V^*}(P, V^*)$ 2. $S(x, 1^\lambda)$