Zero Knowledge - Session 3

Elahe Sadeghi

October 2020

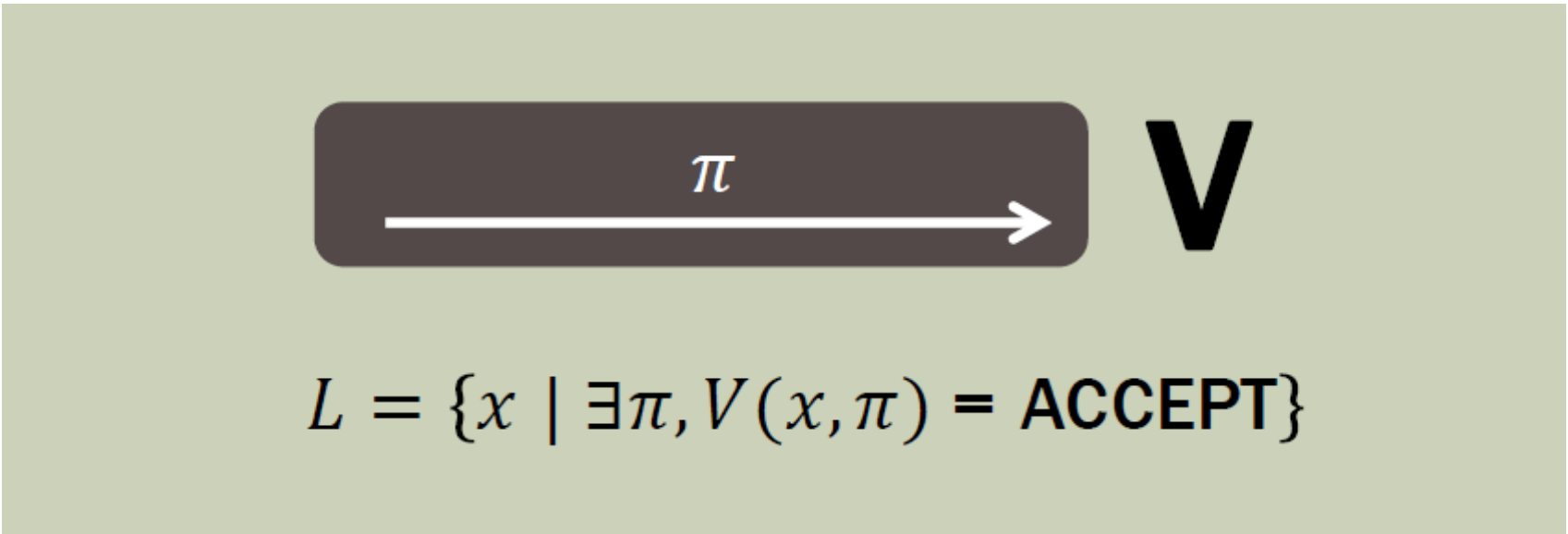
Proof Systems

Proof System

A proof system for membership in L is an algorithm V such that $\forall x$:

- **Completeness**: If $x \in L$, then $\exists \pi, V(x, \pi) = 1$.
- **Soundness**: If $x \notin L$, then $\forall \pi, V(x, \pi) = 0$.

- Suppose we want to prove $x \in L$ for some language L



Proof Systems

NP Proof System

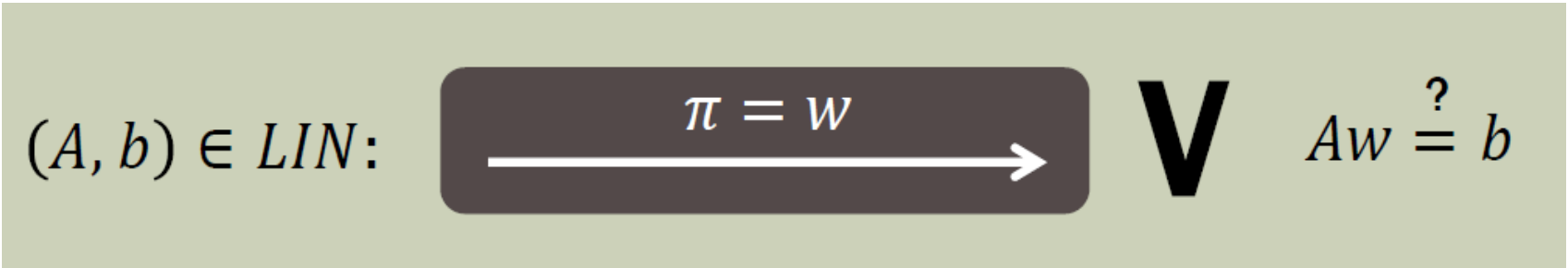
An NP proof system for membership in L is an algorithm V such that $\forall x$:

- **Completeness**: If $x \in L$, then $\exists \pi, V(x, \pi) = 1$.
- **Soundness**: If $x \notin L$, then $\forall \pi, V(x, \pi) = 0$.
- **Efficiency**: $V(x, \pi)$ halts after at most $poly(|x|)$ steps.

- Note that $poly(|x|) = |x|^c$ for some constant c.

Proof Systems

- **Example:** Consider $LIN = \{(A, b) \mid Aw = b \text{ has a solution}\}$.



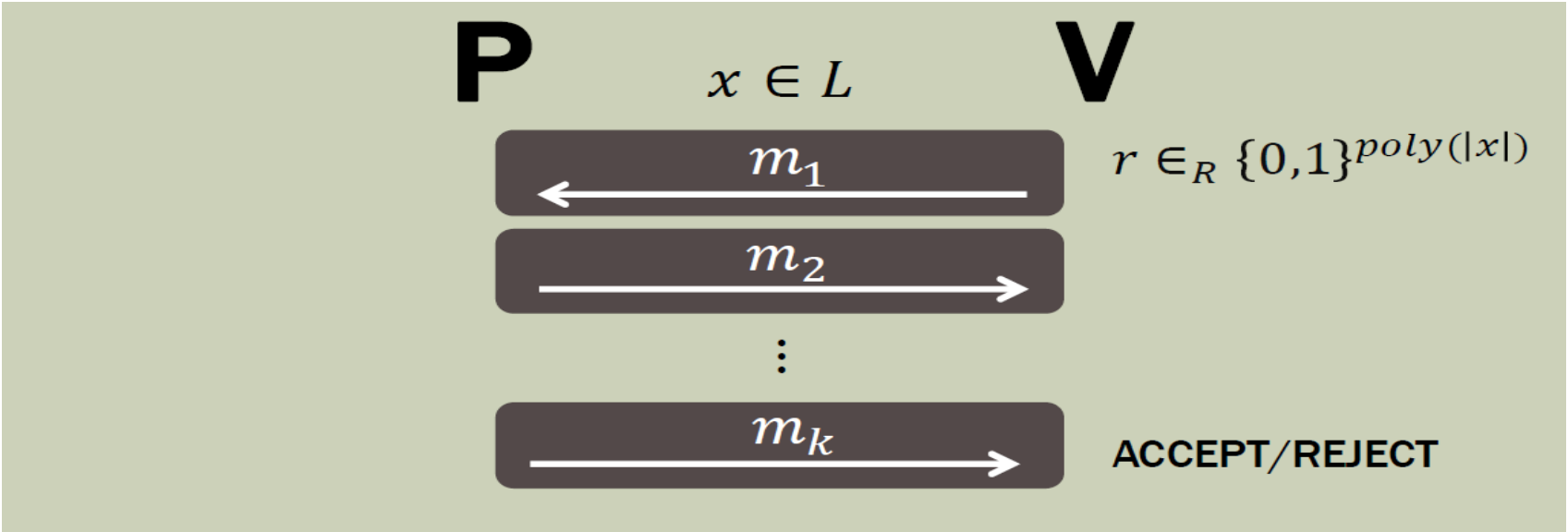
Interactive Proof Systems

Interactive Proof System

An interactive proof system for L is a PPT algorithm V and a function P such that $\forall x$:

- **Completeness**: If $x \in L$, then $\Pr[(P, V) \textit{ accepts } x] \geq 2/3$.
- **Soundness**: If $x \notin L$, then $\forall P^*, \Pr[(P^*, V) \textit{ accepts } x] \leq 1/3$.

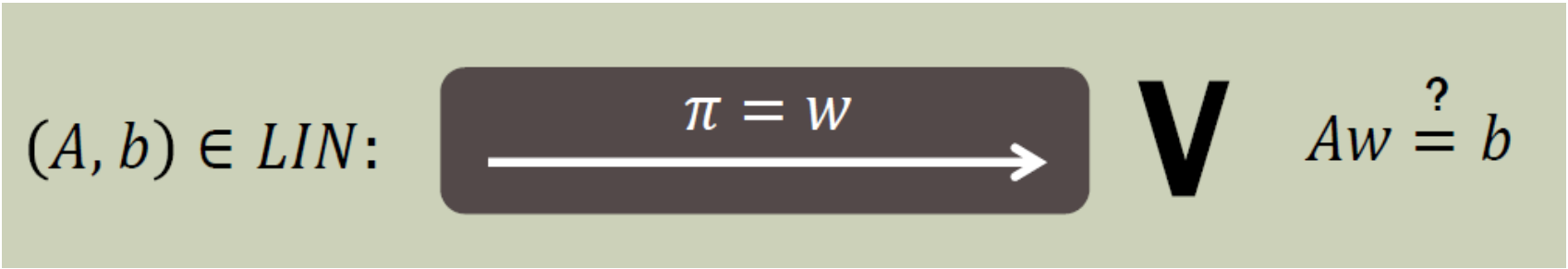
Interactive Proof Systems



- V is probabilistic polynomial-time (PPT)
- For any common input x, let:

$$\Pr[(P, V) \textit{ accepts } x] \equiv \Pr_r[(P, V)(x, r) = 1]$$

Zero-Knowledge



- V **got something for free** from seeing π.
- V may have not been able to find w on his own!

Zero-Knowledge

- When would we say that V did learn something?
  If following the interaction V could compute something he could have not computed without it!

Zero-Knowledge

Whatever is computed following interaction could have been computed without it.

Zero-Knowledge

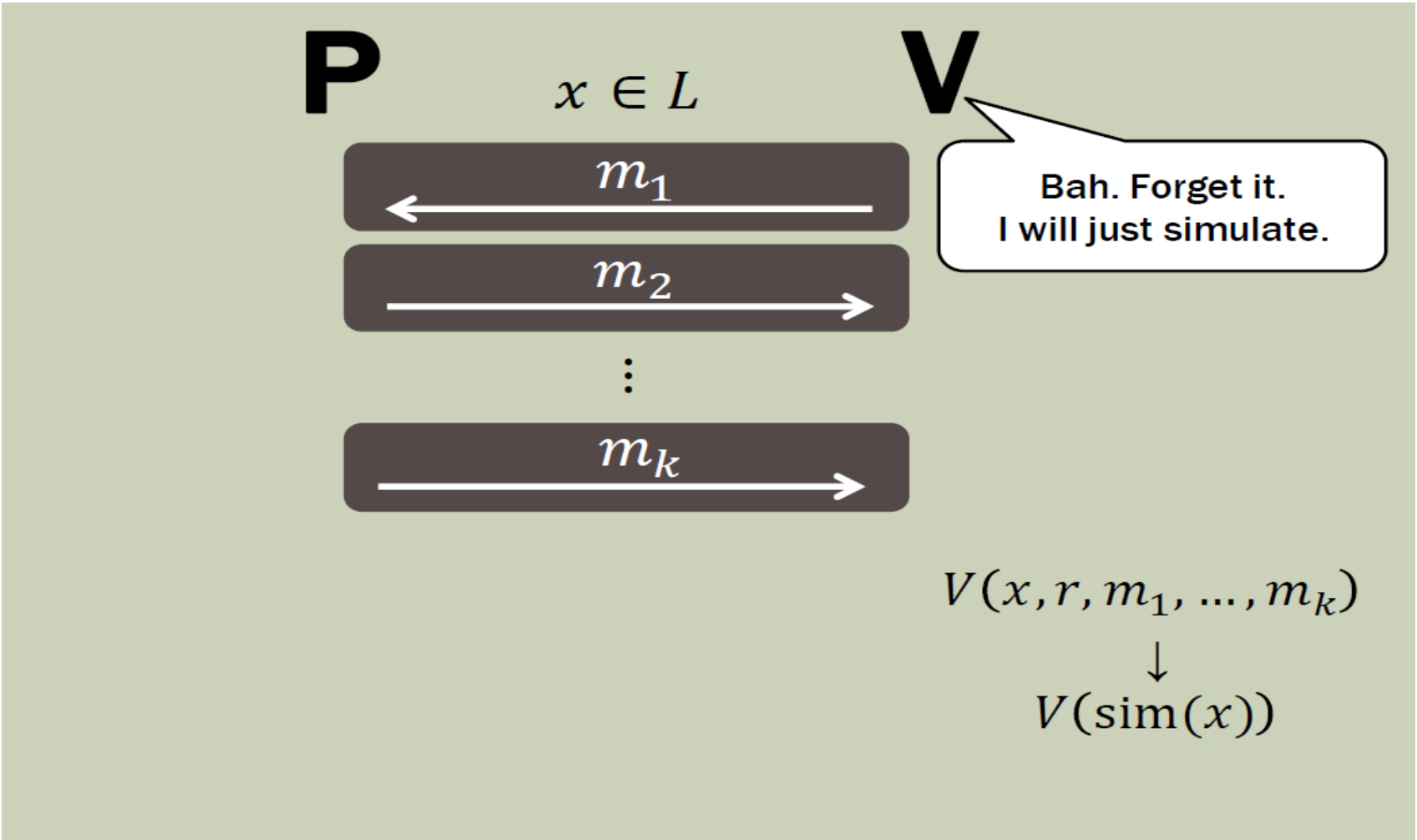
$\rightarrow$ V's view $=$ V's random coins and messages it receives.

$\Rightarrow$ $\forall x \in L$, V's view can be efficiently **simulated**.

$$V(view) \approxeq V(simulation)$$

Whatever V could compute following the interaction, he could have computed even without talking to P, **by running the simulator on his own**.

Zero-Knowledge



Zero-Knowledge

(Honest Verifier) Zero-Knowledge

An interactive proof (P, V) for L is (honest verifier) zero-knowledge if $\exists PPT\, S, \forall x \in L$:

$$S(x) \approx (P, V)(x)$$

- $(P, V)(x)$ denotes V's view.

$\Rightarrow$ V's view distribution can be simulated in polynomial-time.

Zero-Knowledge

Perfect Zero-Knowledge

An interactive proof (P, V) for L is perfect zero-knowledge (PKZ) if $\forall PPT\, V^* \exists PPT\, S, \forall x \in L$:

$$S(x) \approxeq (P, V^*)(x)$$

- $(P, V)(x)$ denotes V's view.

$\Rightarrow$ V's view distribution can be simulated in polynomial-time.

– Let X and Y be random variables taking values in a set Ω.
  - **perfect indistinguishability** ($X \approx Y$): $\forall T \subseteq \Omega$:

$$\Pr_X[X \in T] = \Pr_Y[Y \in T]$$

  - ϵ-**indistinguishability** ($X \approx_S Y$): $\forall T \subseteq \Omega$:

$$|\Pr[X \in T] - \Pr[Y \in T]| \leq \epsilon$$

→ If

- X, Y are ϵ_1-indistinguishable **and**
- Y, Z are ϵ_2-indistinguishable **then**
- X, Z are $(\epsilon_1 + \epsilon_2)$-indistinguishable

→ If

- X, Y are ϵ-indistinguishable **then**
- X^q, Y^q are $q\epsilon$-indistinguishable

Statistical Zero-Knowledge

Statistical Zero-Knowledge (SZK)

$\forall PPT\, V^* \exists PPT\, S, \forall x \in L$:

$$S(x) \approx_S (P, V^*)(x)$$

– Let X and Y be random variables taking values in a set Ω.
  - ϵ-**indistinguishability** ($X \approx_S Y$): $\forall T \subseteq \Omega$:

$$|\Pr[X \in T] - \Pr[Y \in T]| \leq \epsilon$$

  - (t, ϵ)-**indistinguishability** ($X \approx_C Y$): $\forall T \subseteq \Omega$ that are decidable in time t:

$$|\Pr[X \in T] - \Pr[Y \in T]| \leq \epsilon$$

∗ $T \subseteq A$ is decidable in time t if $\exists$time-t D such that $\forall x \in A$:

$$x \in T \leftrightarrow D(x) = 1$$

→ If

- X, Y are (t_1, ϵ_1)-indistinguishable **and**
- Y, Z are (t_2, ϵ_2)-indistinguishable **then**
- X, Z are $(\min\{t_1, t_2\}, \epsilon_1 + \epsilon_2)$-indistinguishable

→ If

- X, Y are (t, ϵ)-indistinguishable **then**
- X^q, Y^q are $(t, q\epsilon)$-indistinguishable

Computational Zero-Knowledge

Computational Zero-Knowledge (CZK)

$\forall PPT\, V^* \exists PPT\, S, \forall x \in L$:

$$S(x) \approx_C (P, V^*)(x)$$

$$PZK \subseteq SZK \subseteq CZK$$

- **Theorem**: Suppose one-way functions exists. Then $NP \subseteq CZK$

One-Way Functions

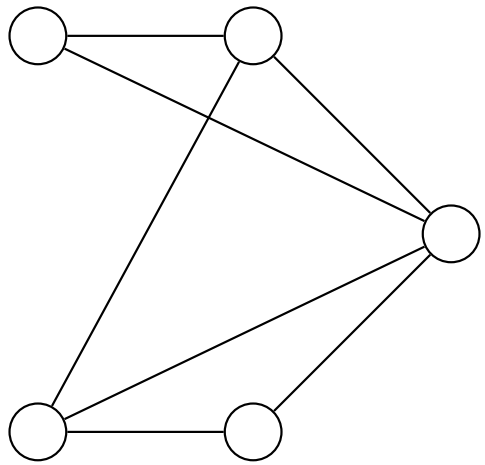
One-Way Function (OWF)

$f : \{0,1\}^* \to \{0,1\}^*$ is (t, ϵ)-one-way if $\forall$time-t A:

$$\Pr_X[A \text{ inverts } f(X)] \leq \epsilon$$

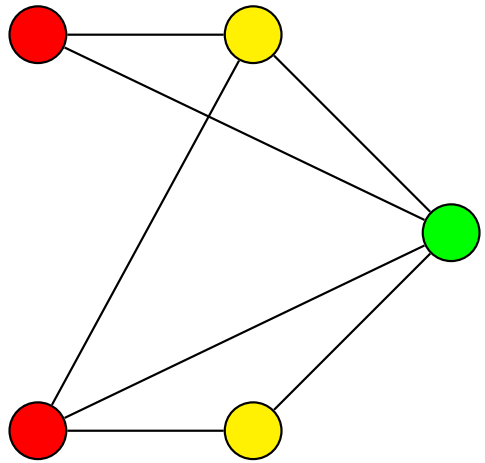
- Some candidates for OWF:
  - Rabin/RSA: $x^2 \bmod N$ $x^e \bmod N$
  - Discrete Exponentiation: $g^x \bmod P$
  - SIS/LWE: $Ax \bmod q$ $Ax + e \bmod q$
  - SHA: $H(x)$

We show this theorem for $\mathcal{NP}$ languages. So, it suffices to construct a zero-knowledge proof system for a "$\mathcal{NP}$-complete" language.
Consider the language of **graph 3-colorability**: Given a graph G, can you color the vertices such that no adjacent nodes have the same color?

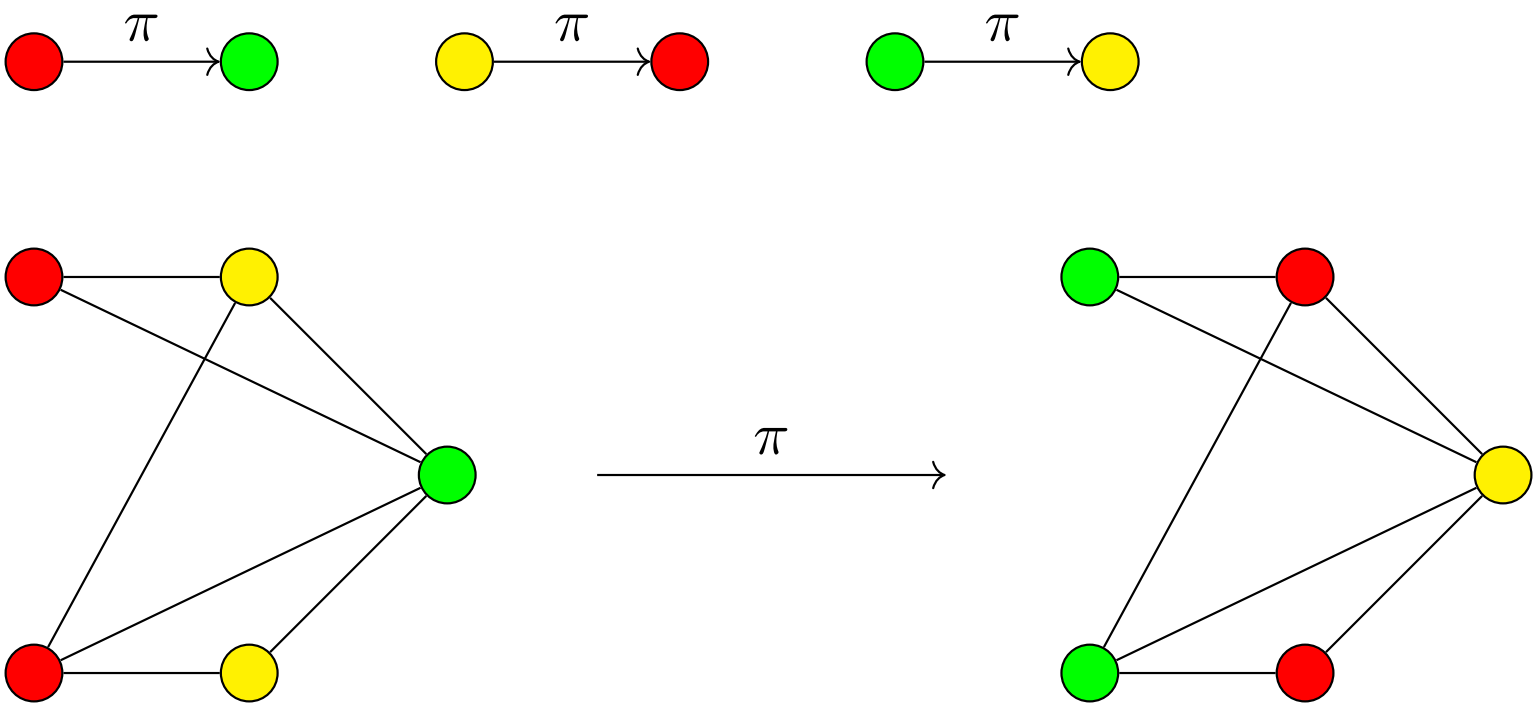


Alice wants to prove that a given graph G is 3-colorable.

- let $K = \{K_i \in \{0, 1, 2\}\}_{i \in V}$ be a 3-coloring of G.

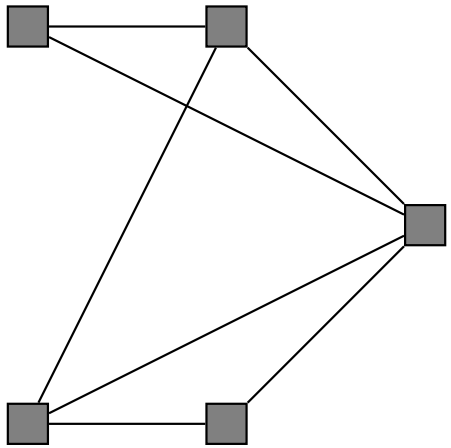


- Alice choose a random permutation $\pi \leftarrow Perm[\{0, 1, 2\}]$.

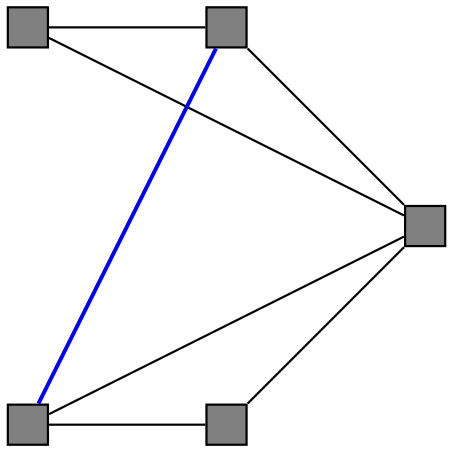


Alice Commits to color of each node and sends commitments to Bob.

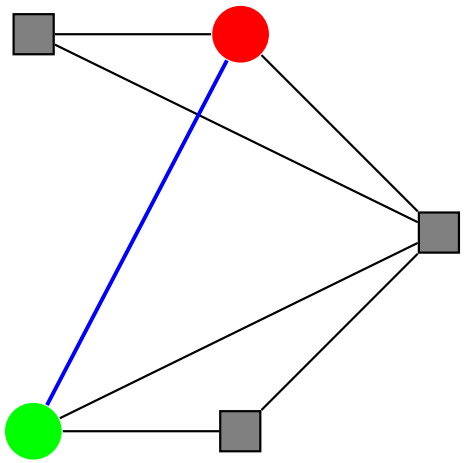
- $c_i \leftarrow \text{Commit}(K_i; r_i)$ for random r_i.



Bob challenges Alice to reveal coloring of a single edge.

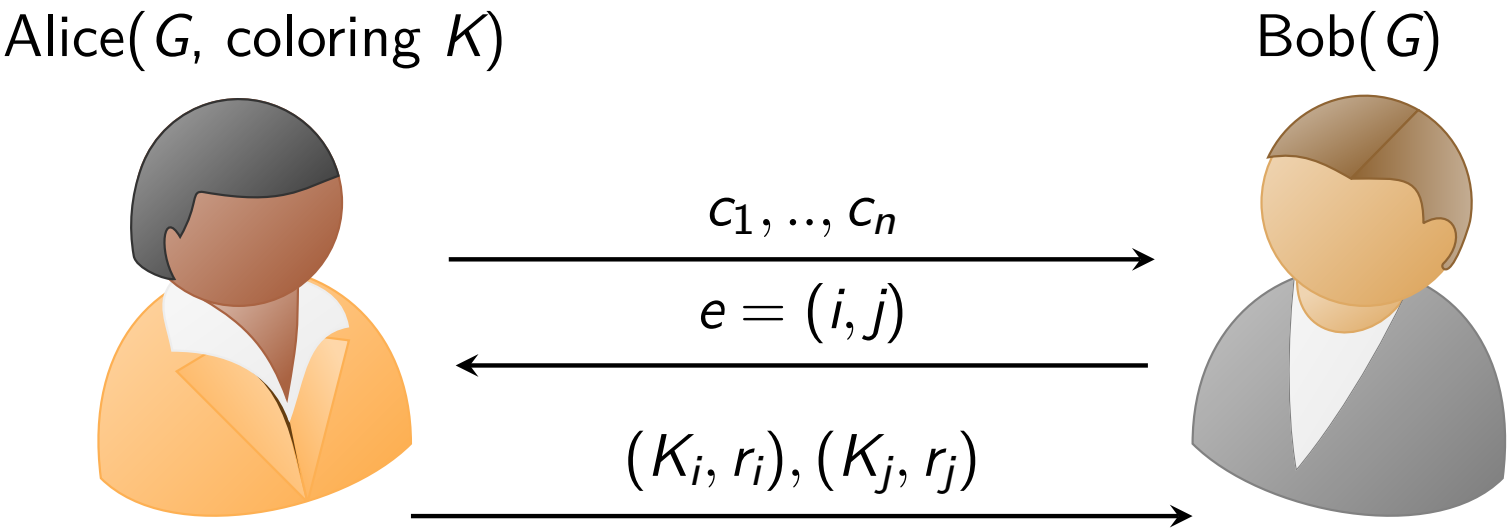


Alice reveals the coloring on the chosen edge and opens the entries in the commitment.



So why is it a zero-knowledge proof?!

So our ZK proof for graph 3-coloring will be as following:



- Bob accepts if $K_i \neq K_j$ and $K_i, K_j \in \{0, 1, 2\}$ and $\text{Verify}(K_i, c_i, r_i) = 1 = \text{Verify}(K_j, c_j, r_j)$, reject otherwise.

- **Completeness**: if coloring is valid, Alice can always answer the challenge properly.
- **Soundness**: Suppose G is not 3-colorable. Let $K_1, .., K_n$ be the coloring the prover committed to. If the commitment scheme is perfectly binding, $c_1, .., c_n$ uniquely determine $K_1, .., K_n$. Since G is not 3-colorable, there is an edge $(i, j) \in E$ where $K_i = K_j$ or $i, j \notin \{0, 1, 2\}$. Bob will choose this edge with probability of $\frac{1}{|E|}$. So $\Pr[\textit{Bob rejects}] \geq \frac{1}{|E|}$.
  With repeating this protocol, we can reduce this soundness error to $e^{-|E|}$.

- **Zero-Knowledge**: We need to construct a simulator that outputs a valid transcript given only the graph G as an input.
  Let V^* be the verifier. Construct simulator S as follows:
  1. Choose $K_i \leftarrow \{0, 1, 2\}$ for all $i \in [n]$.
     Let $c_i \leftarrow \text{Commit}(K_i; r_i)$
     Give $(c_1, .., c_n)$ to V^*.
  2. V^* outputs an edge $(i, j) \in E$
  3. If $K_i \neq K_j$,then S outputs $(K_i, K_j r_i, r_j)$.
     Otherwise, restart and try again.

  Simulator succeeds with probability of $\frac{2}{3}$. So it produces a valid transcript with probability $1 - \frac{1}{3^\lambda} = 1 - negl(\lambda)$ after λ attempts.

Since graph 3-colorability is NP-complete, we have the following two theorems:

- **Theorem**: Suppose one-way functions exists. Then $NP \subseteq CZK$.
- **Theorem**: If statistically-binding commitments exist, then $NP \subseteq CZK$.

$$BPP \subseteq PZK \subseteq SZK \subseteq CZK = IP$$

Thank you!