Zero-knowledge proofs
• Goal: P proves to V that some statement is true
  • *Without* conveying additional information

• In general, probabilistic
  • Repeat a bunch of times as proof
Example 1: Hallway password

• Does Peggy have the password?

• Both stand in the entrance.
  • When Victor isn’t looking, Peggy picks one hall
  • Victor then yells “GREEN” or “ORANGE”
  • Peggy must come back via the chosen color

• Repeating many times “proves” Peggy has password
  • With high probability
Example 2: Two baseballs

- Peggy has two baseballs: One red, one green
  - Otherwise identical

- Victor is color-blind, thinks they are the same

- Peggy places them in Victor’s hands
  - Victor puts them behind his back, may switch
  - Peggy tells whether he switched
  - As before, repeat many times
Security properties

• Complete: Honest V will be convinced by honest P

• Sound: Honest V can’t* be convinced by cheating P

• Proves nothing to outside observers either way
  • Peggy and Victor can collude by precomputation

• Peggy could cheat with a time machine
  • Victor gets the same info either way
  • Implies that real protocol does not leak
Defining 3COL:

- $G=(V,E)$ is 3-colorable iff there exists a mapping $\Phi: V \to \{1,2,3\}$ so that $\Phi(u) \neq \Phi(v)$ for all $u, v \in E$ ($\Phi$ is called “a 3-coloring of $G$”).
- $3\text{COL} = \{ G: G \text{ is 3-colorable} \}$ (NP Complete)
ZK Protocol for 3COL

- Common input: Graph $G=(V,E)$
- $P$: knows a 3-coloring, wants to prove $G$ is 3-colorable
ZK Protocol for 3COL

• Common input: Graph G=(V,E)
• P: knows a 3-coloring, wants to prove G is 3-colorable
• P chooses a random color permutation
• P permutes colors accordingly
• Puts all the nodes in “envelops”....
• ....And sends them to verifier
ZK Protocol for 3COL

- Verifier gets envelopes $V_1, V_2, V_3, ...$
- Chooses a random edge, eg. $(V_2, V_3)$, and sends to prover
- Prover checks that the two nodes are indeed an edge...
- ...then opens the envelopes of to reveal colors
ZK Protocol for 3COL

- Verifier gets envelopes $V_1 \ V_2 \ V_3 \ ...$
- Chooses a random edge, eg. $(V_2, V_3)$, and sends to prover
- Prover checks that the two nodes are indeed an edge...
- ... then opens the envelops of to reveal colors
- Verifier accepts if colors are different

(We saw formal description in class last time, using commitments for envelops)
Theorem: If the protocol uses perfectly binding commitments, then this is a zero knowledge protocol with completeness 1 and soundness $1 - 1/|E|$

Proof sketch:

• **Completeness**: If $G$ is 3-colorable and both $P$ and $V$ follow the specified protocol, $V$ will always accept

• **Soundness**: Suppose $G$ is not 3-colorable. Then no matter what any cheating prover $P^*$ puts in the envelopes, there will be at least one edge $(u,v)$ in $E$ that is colored badly. That edge is picked by $V$ with probability $1/|E|$.  
  • Note: this uses the fact that the commitments are binding even against a computationally unbounded prover