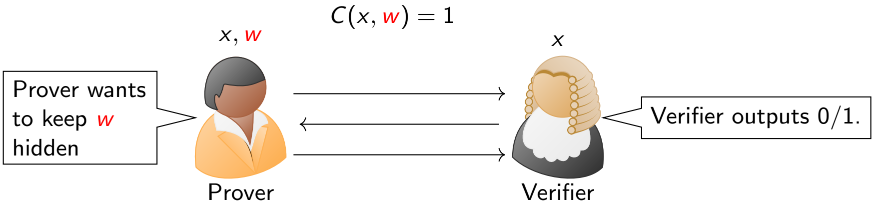
CS171: Cryptography

Lecture 20

Sanjam Garg

Zero-Knowledge Proof System



- Syntax: Two algorithms, $P(1^n, x, w)$ and $V(1^n, x)$.
- Completeness: Honest prover convinces an honest verifier with *overwhelming* probability.

$$\Pr[V \text{ outputs 1 in the interaction } P(1^n, x, w) \leftrightarrow V(1^n, x)] = 1 - \text{neg}(n)$$

- Soundness: A PPT cheating prover P^* cannot make a Verifier accept a false statement. For all PPT P^*, x such that $\forall w, C(x, w) = 0$then we have that

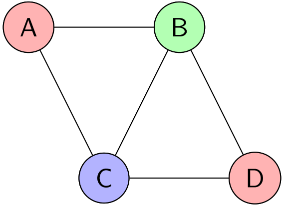
$$\Pr[V \text{ outputs 1 in the interaction } P^*(1^n, x) \leftrightarrow V(1^n, x)] = \text{neg}(n)$$

- Zero-Knowledge: The proof doesn't leak any information about the witness w. $\exists$ a PPT simulator $\mathcal{S}$ that for all PPT V^*, x, w such that $C(x, w) = 1$, we have that $\forall$ PPT D:

$$\left| \Pr[D(V^*\text{'s view in } P(1^n, x, w) \leftrightarrow V^*(1^n, x)) = 1] - \Pr[D(\mathcal{S}^{V^*}(1^n, x)) = 1] \right| \leq \text{neg}(n)$$

Graph Three Coloring Problem

- Graph $G = (V, E)$.
- Task: Show a coloring function $c : V \to \{R, B, G\}$ such that such that $\forall (u, v) \in E$, we have that $c(u) \neq c(v)$.



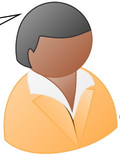
- Not every graph is three-colorable. Figuring out whether a graph is three-colorable is believed to be computationally hard.

Zero-Knowledge Proof System for Graph Three Coloring Problem

$$\forall (u, v) \in E, c(u) \neq c(v)$$

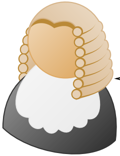
$G = (V, E), c$

Samples uniform $\forall v \in V, r_v$ and permutation $\pi : \{R, G, B\} \to \{R, G, B\}$



Prover

$G = (V, E)$



Verifier

Sample uniform $e = (u, v) \leftarrow E$.

$\xrightarrow{\forall v \in V, com_v = \mathrm{Com}(\pi(c(v)); r_v)}$

$\xleftarrow{\text{Challenge } e = (u, v)}$

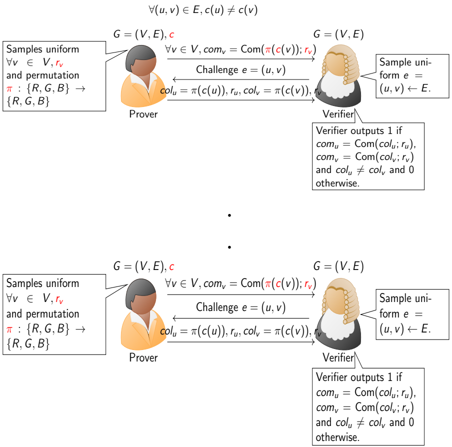
$\xrightarrow{col_u = \pi(c(u)), r_u, col_v = \pi(c(v)), r_v}$

Verifier outputs 1 if $com_u = \mathrm{Com}(col_u; r_u)$, $com_v = \mathrm{Com}(col_v; r_v)$ and $col_u \neq col_v$ and 0 otherwise.

Completeness: Note $c(u) \neq c(v)$. Thus, $\pi(c(u)) \neq \pi(c(v))$ and verifier accepts.

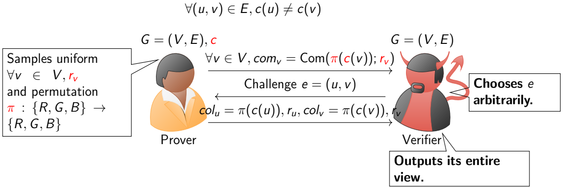
Soundness: Let $com_v = \mathrm{Com}(col_v; r_v)$. Since the graph is not three colorable $\exists e = (u, v) \in E$ such that $col_u = col_v$. Verifier challenges on this edge e with probability $1/|E|$. Thus, rejects with probability at least $\frac{1}{|E|}$

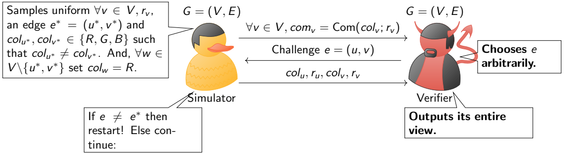
Soundness Amplification



- Repeat the protocol $n|E|$ times.
- A malicious prover succeeds in the i^{th} execution with probability $\leq (1 - \frac{1}{|E|})$.
- A malicious prover succeds in all $n|E|$ execution with probability $\leq \left(1 - \frac{1}{|E|}\right)^{n|E|} \approx e^{-n}$ which is negligible in n.

Zero Knowledge (Simulator)



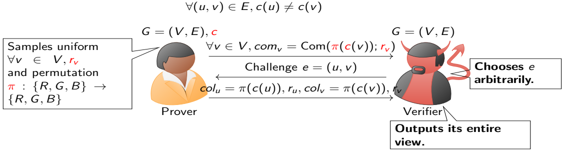


- The verifier is now malicious and can have arbitrary behavior and output.
- Simulator attempts to generate an indistinguishable output — without the witness's knowledge.
- $\Pr[e = e^*] = 1/|E|$. Furthermore, when this happens, the output of the adversary is indistinguishable from the case with an honest prover. (Note that commitment is hiding.)
- Simulator runs the malicious verifier roughly $|E|$ times to get an output.

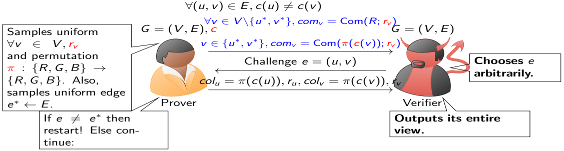
Zero Knowledge - Simulation by Cropping Undesirable Parts

- Great skill?
- Took 156 attempts.
- Hard to distinguish.

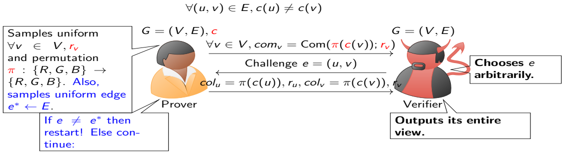
Zero Knowledge — Simulator output is Indistingusiable



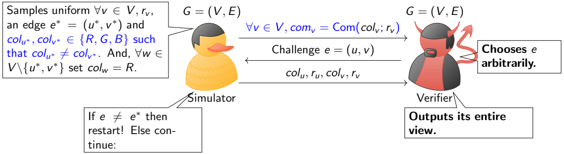
Hybrid H_0.



Hybrid H_2. (Indistinguishable from H_1 using the hiding property of the commitment scheme.)



Hybrid H_1.(Information theoretically indistinguishable from H_0. Cropping Argument.)



Hybrid H_3. (Only renaming things from H_3. Not using c anymore.)

Thank You!