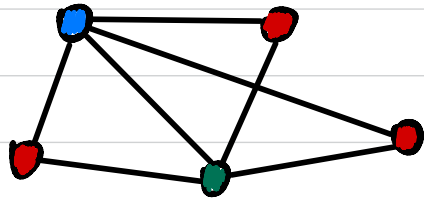


CSCI 1515 Applied Cryptography

This Lecture:

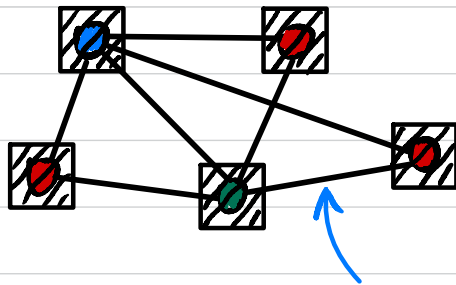
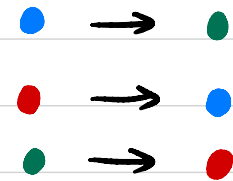
- Zero-Knowledge Proofs for All NP (Continued)
- Succinct Non-Interactive Arguments (SNARGs)
- SNARGs from PCP

Zero-Knowledge Proof for Graph 3-Coloring (All NP)

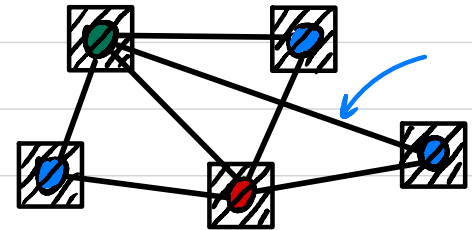


NP language $L = \{ G : G \text{ has 3-coloring} \}$

NP relation $R_L = \{ (G, \text{3COL}) \}$



New Coloring:



If $G \notin L$, $\Pr[P^* \text{ is caught}] \geq \frac{1}{|E|}$

How to amplify soundness? Repeat k times, $k = \lambda \cdot |E|$

$$\Pr[P^* \text{ isn't caught}] \leq \left(1 - \frac{1}{|E|}\right)^k = \left(1 - \frac{1}{|E|}\right)^{|E| \cdot \lambda} \approx \left(\frac{1}{e}\right)^\lambda \quad \left(1 - \frac{1}{n}\right)^n \approx \frac{1}{e}$$

$$\Pr[P^* \text{ is caught at least once}] \geq 1 - \left(\frac{1}{e}\right)^\lambda$$

Commitment Scheme

<u>Sender</u> $m \in \{0, 1\}$	<u>Receiver</u>
Commit: $r \in \{0, 1\}^\lambda$ $c := \text{Com}(m; r) \xrightarrow{c}$	
Open: $\xrightarrow{(m, r)}$	Verify: $c = \text{Com}(m; r)$

- **Hiding:** $\text{Com}(0; r) \cong \text{Com}(1; s)$
- **Binding:** Hard to find r, s st. $\text{Com}(0; r) = \text{Com}(1; s)$

Commitment Scheme

Example 1: Hash-based Commitment

$$r \leftarrow \{0,1\}^\lambda$$

$$\text{Com}(m; r) := H(r \parallel m)$$

↑
Random Oracle

Example 2: Pedersen Commitment

Cyclic group G of order q with generator g . $h \leftarrow G$

$$r \leftarrow \mathbb{Z}_q$$

$$\text{Com}(m; r) = g^m \cdot h^r$$

↑
can be generated by Receiver

$$h = g^x, x \text{ hidden to Sender}$$

Why are the schemes hiding & binding?

Zero-Knowledge Proof for Graph 3-Coloring

Input: $G = (V, E)$

Witness: $\phi: V \rightarrow \{0, 1, 2\}$

Prover

Randomly sample $\pi: \{0, 1, 2\} \rightarrow \{0, 1, 2\}$

$\forall v \in V, r_v \leftarrow \{0, 1\}^k, c_v := \text{Com}(\pi(\phi(v)), r_v)$

$\{c_v\}_{v \in V}$

→

(u, v)

←

Randomly pick an edge $(u, v) \in E$

Open commitments c_u & c_v

$\alpha = \pi(\phi(u)), r_u$

$\beta = \pi(\phi(v)), r_v$

→ Verify:

$c_u = \text{Com}(\alpha; r_u)$

$c_v = \text{Com}(\beta; r_v)$

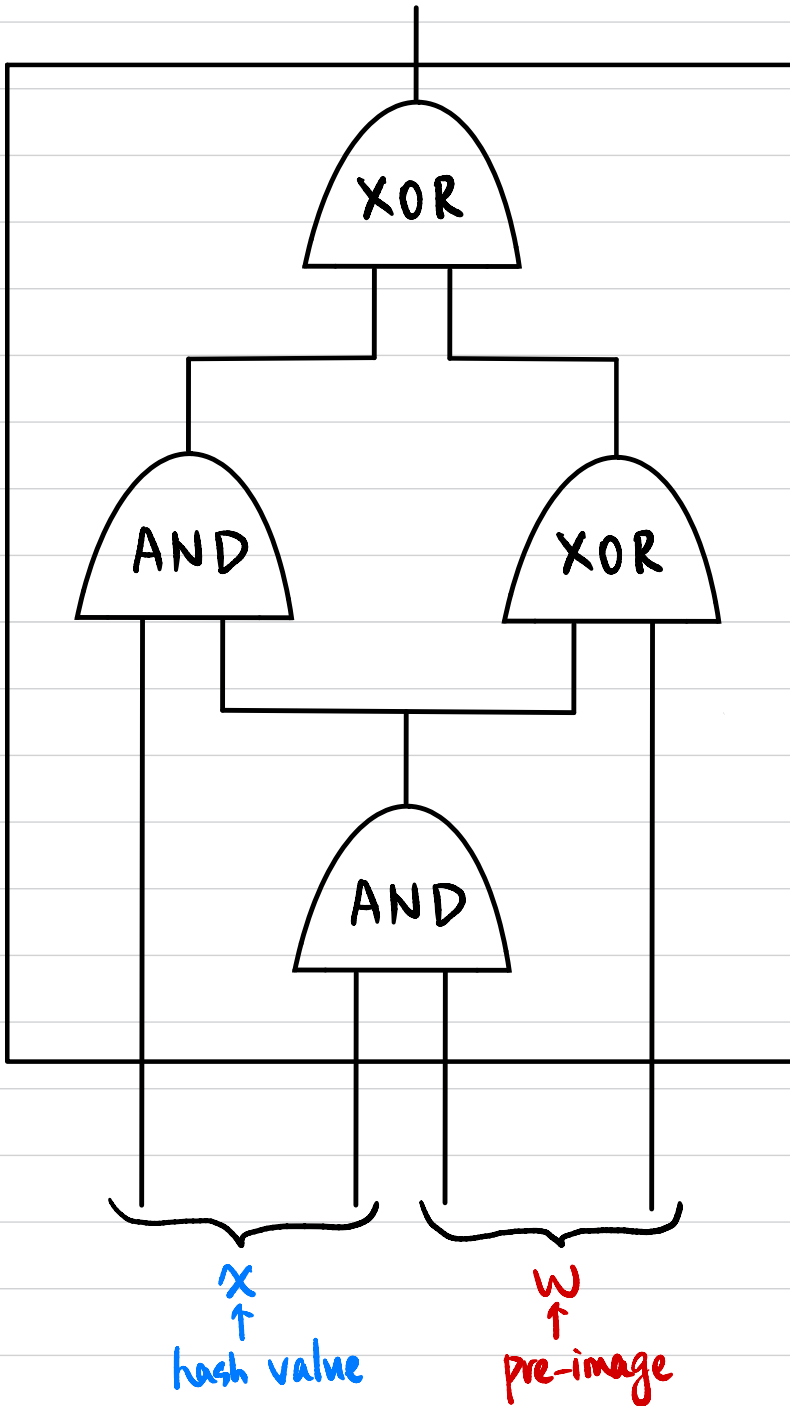
$\alpha, \beta \in \{0, 1, 2\}, \alpha \neq \beta$

Completeness?

Soundness?

Zero-Knowledge?

Circuit Satisfiability (NP Complete)



NP language $L_c = \{x \in \{0,1\}^n : \exists w \in \{0,1\}^m \text{ st. } C(x,w) = 1\}$

NP relation $R_L = \{ (x, w) : C(x, w) = 1 \}$

↑ ↑

(public) (secret)

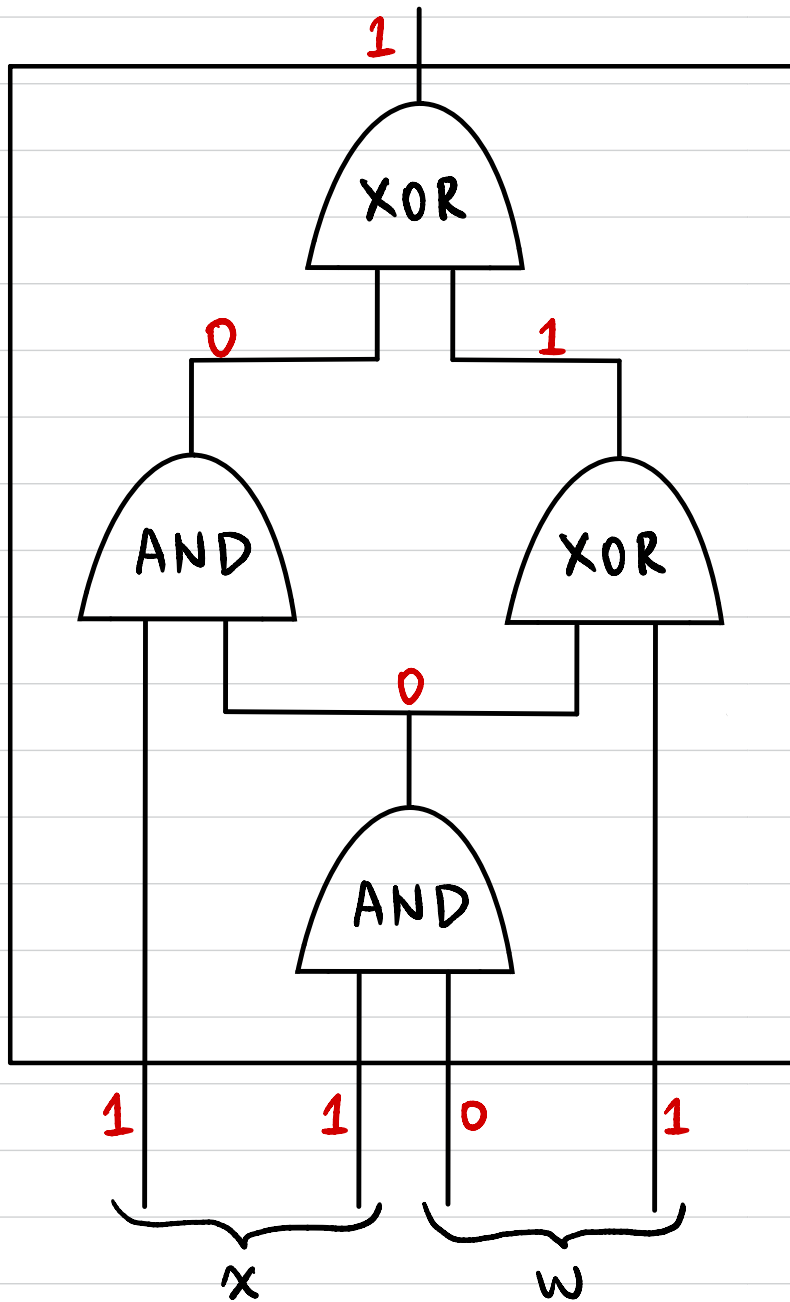
Statement Witness

Example: pre-image of hash function

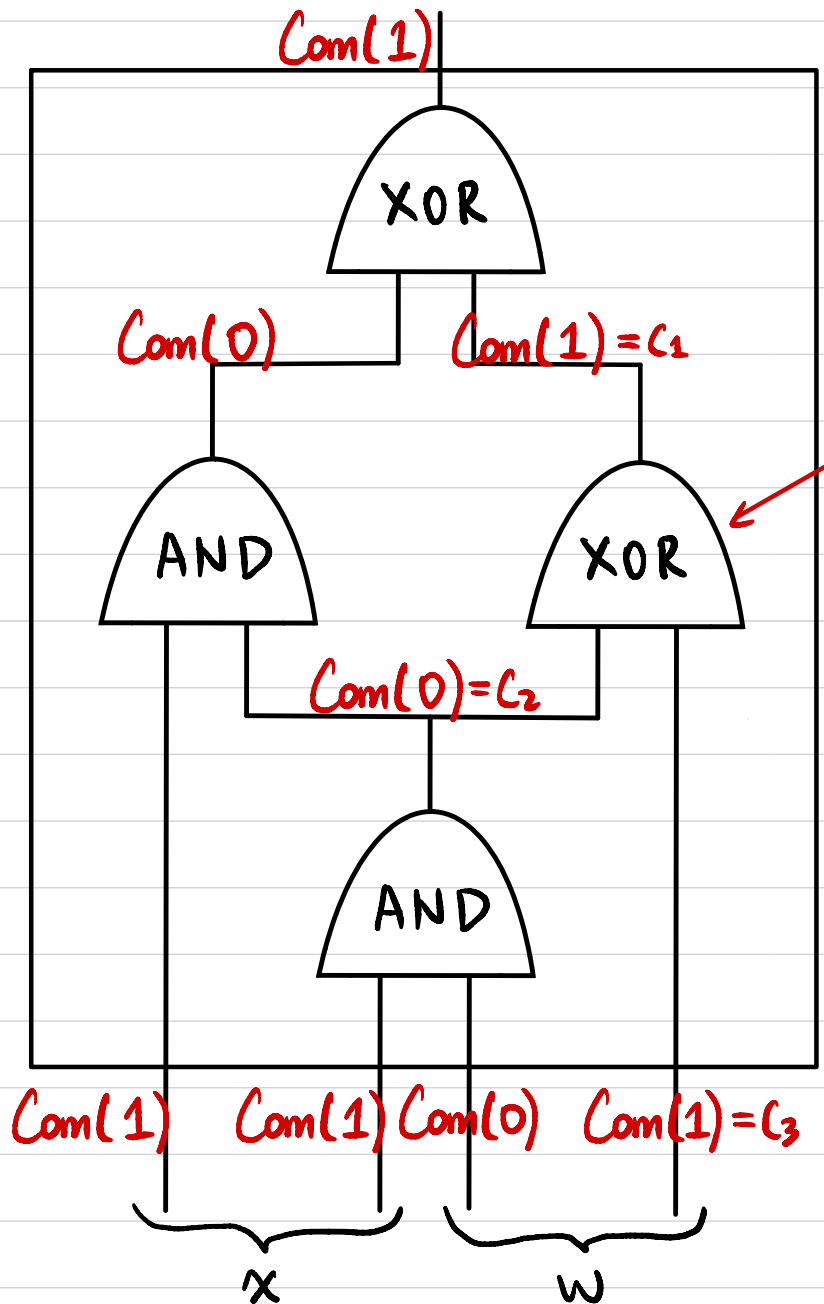
$$C(x, w) = H(w) - x + 1$$

$$H(w) = x$$

ZKP for Circuit Satisfiability



ZKP for Circuit Satisfiability



$$\begin{pmatrix} c_1 = \text{Com}(0) \\ c_2 = \text{Com}(0) \\ c_3 = \text{Com}(0) \end{pmatrix}$$

OR

$$\begin{pmatrix} c_1 = \text{Com}(1) \\ c_2 = \text{Com}(0) \\ c_3 = \text{Com}(1) \end{pmatrix}$$

OR

$$\begin{pmatrix} c_1 = \text{Com}(1) \\ c_2 = \text{Com}(1) \\ c_3 = \text{Com}(0) \end{pmatrix}$$

OR

$$\begin{pmatrix} c_1 = \text{Com}(0) \\ c_2 = \text{Com}(1) \\ c_3 = \text{Com}(1) \end{pmatrix}$$

Proof Systems for Circuit Satisfiability

NP relation $R_C = \{ (x, w) : C(x, w) = 1 \}$

	NP	Σ -Protocol	(Fiat-Shamir) NIZK
	$P(x, w) \xrightarrow{w} V(x)$	$P(x, w) \begin{matrix} \longrightarrow \\ \longleftarrow \\ \longrightarrow \end{matrix} V(x)$	$P(x, w) \xrightarrow{\pi} V(x)$
Zero-Knowledge	NO	YES	YES
Non-Interactive	YES	NO	YES
Communication	$O(w)$	?	?
V's computation	$O(C)$	?	?

Can we have communication complexity & verifier's computational complexity sublinear in $|C|$ & $|w|$?

Succinct Non-Interactive Argument



- **SNARG**: Succinct Non-Interactive Argument
- **SNARK**: Succinct Non-Interactive Argument of Knowledge
- **zk-SNARG / zk-SNARK**: SNARG / SNARK + Zero-Knowledge
- **Succinct**: $|\pi| = \text{poly}(\lambda, \log |C|)$
Verifier runtime $\text{poly}(\lambda, |x|, \log |C|)$
- **Argument**: In Soundness / Proof of Knowledge: $\forall \text{PPT } P^*$

Verifiable Computation

Server

Client

← x

← Compute f

→ y

$$y \stackrel{?}{=} f(x)$$

Anonymous Transactions on Blockchain

Alice's Account A $\xrightarrow{2\text{BTC}}$ Bob's Account B

VK_A (public)
 SK_A (private)

VK_B (public)
 SK_B (private)

Transaction: $[VK_A, VK_B, 2\text{BTC}]$, $\sigma = \text{Sign}_{SK_A}(\rightarrow)$

Anonymous Transaction:

$\text{Com}([VK_A, VK_B, 2\text{BTC}], \sigma = \text{Sign}_{SK_A}(\rightarrow))$

NIZK: valid transaction

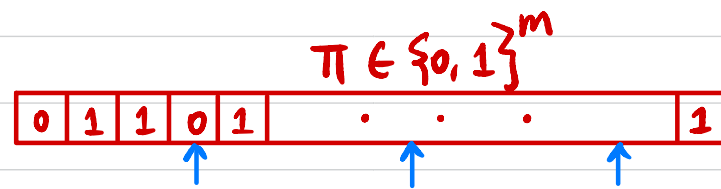
Probabilistically Checkable Proof (PCP)

Prover

(x, w)

Verifier

(x)



PCP Theorem (Informal):

Every NP language has a PCP where the verifier reads only a constant number of bits of the proof.

First Attempt

Prover

(x, w)

$\text{Com} \left(\begin{array}{|c|c|c|c|c|c|c|c|} \hline 0 & 1 & 1 & 0 & 1 & \cdot & \cdot & \cdot \\ \hline \end{array} \right)$

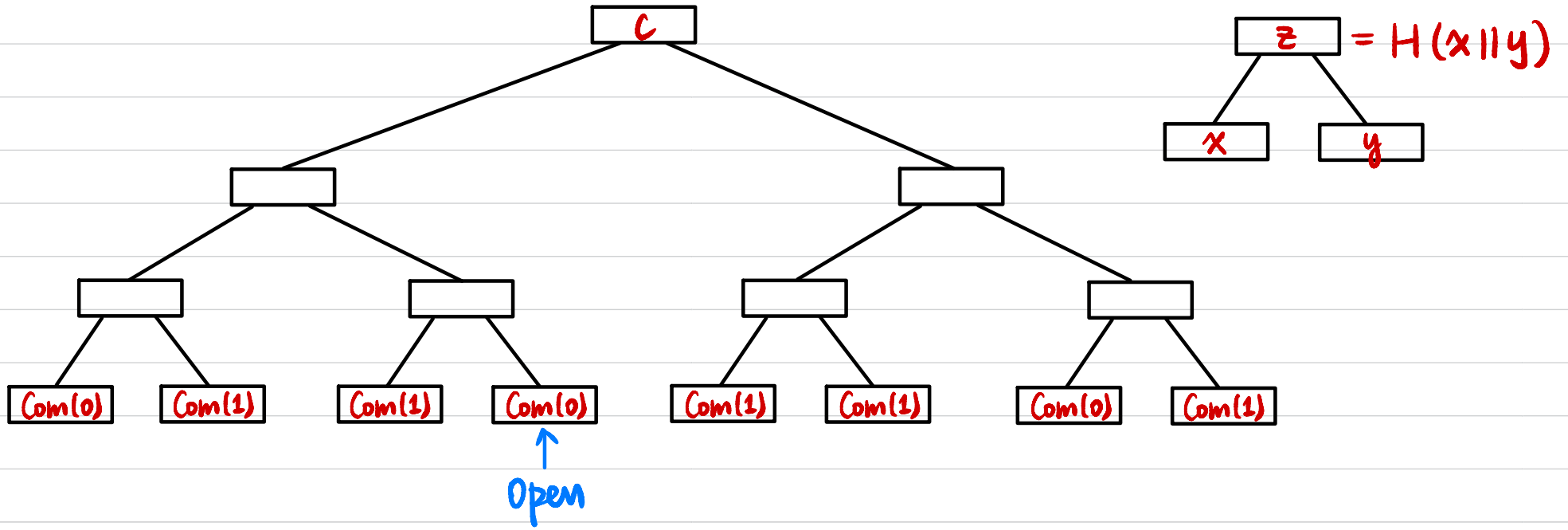
Verifier

(x)

$\leftarrow i, j, k$

$\text{Open } \text{Com}(\pi_i), \text{Com}(\pi_j), \text{Com}(\pi_k)$

Merkle Tree



How to open commitment?

Why hiding & binding?