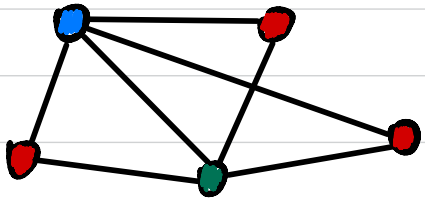
CSCI 1515 Applied Cryptography

This Lecture:

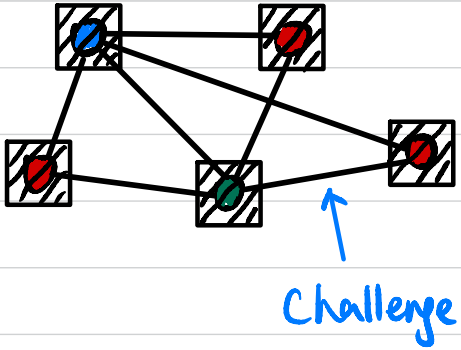
- Zero-Knowledge Proofs for All NP
- Succinct Non-Interactive Arguments (SNARGs)

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



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

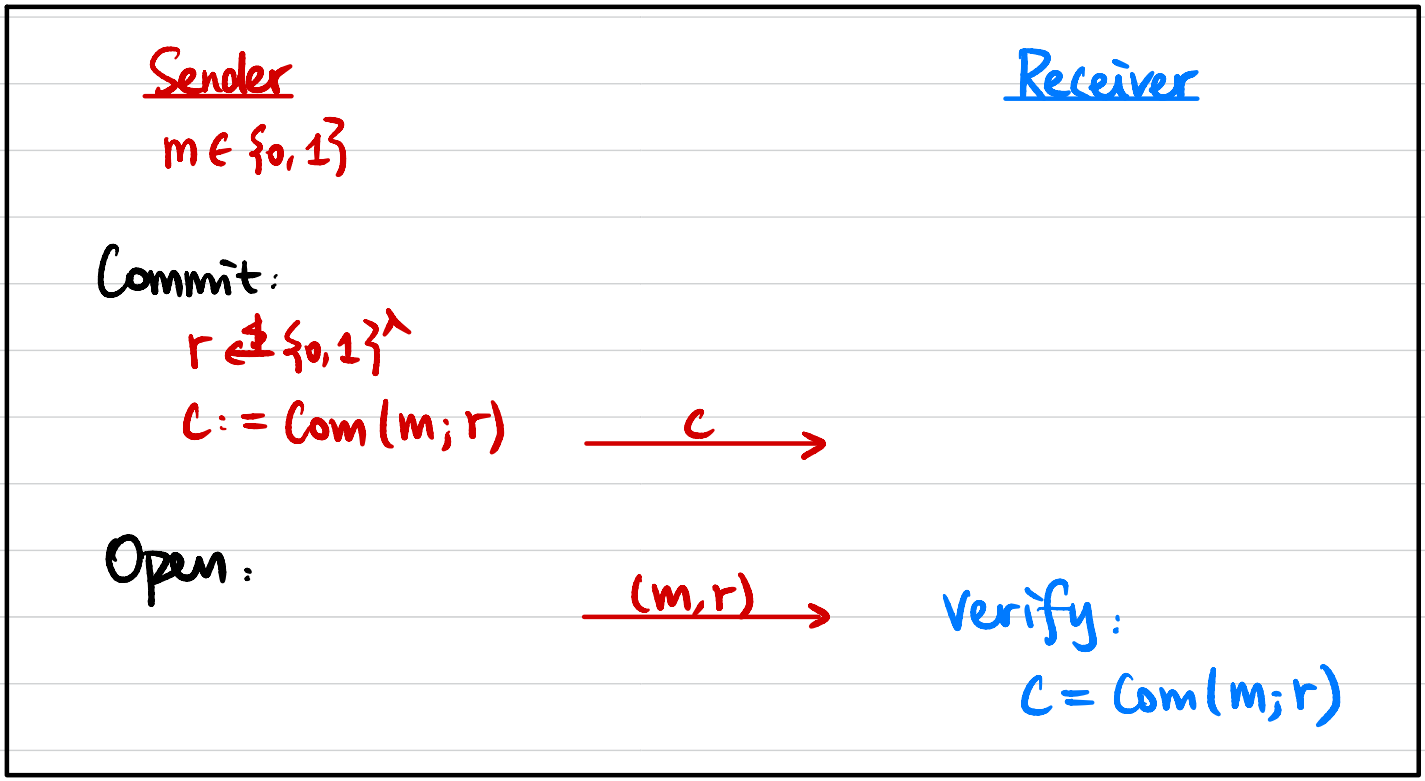
NP relation $R_L = \{ (G, 3COL) \}$



If $G \notin L$, $\Pr[P^* \text{ is caught}] \geq ?$

How to amplify soundness?

Commitment Scheme



Example: Pedersen Commitment

Cyclic group G of order q with generator g. $h \xleftarrow{\$} G$ ← can be generated by Receiver

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

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

Commitment Scheme

- **Hiding:** $\mathsf{Com}(0; r) \simeq \mathsf{Com}(1; s)$
  - **Perfectly hiding:** $\mathsf{Com}(0; r) \equiv \mathsf{Com}(1; s)$
  - **Computationally hiding:** $\mathsf{Com}(0; r) \overset{c}{\simeq} \mathsf{Com}(1; s)$

- **Binding:** Hard to find r, s s.t. $\mathsf{Com}(0; r) = \mathsf{Com}(1; s)$
  - **Perfectly binding:** $\forall r, s,\ \mathsf{Com}(0; r) \neq \mathsf{Com}(1; s)$
  - **Computationally binding:** Any PPT sender cannot find r, s s.t. $\mathsf{Com}(0; r) = \mathsf{Com}(1; s)$

What does Pedersen commitment scheme satisfy?

Can a commitment scheme be both perfectly hiding & perfectly binding?

Zero-Knowledge Proof for Graph 3-Coloring

Input: $G = (V, E)$

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

Given a computationally hiding, perfectly binding commitment scheme.

Prover

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

$\forall v \in V$, $r_v \xleftarrow{R} \{0,1\}^\lambda$, $c_v := \mathrm{Com}(\pi(\phi(v)); r_v)$

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

Verifier

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

$\xleftarrow{(u,v)}$

Prover

Open commitments c_u & c_v

$\xrightarrow{\alpha = \pi(\phi(u)),\ r_u \quad \beta = \pi(\phi(v)),\ r_v}$

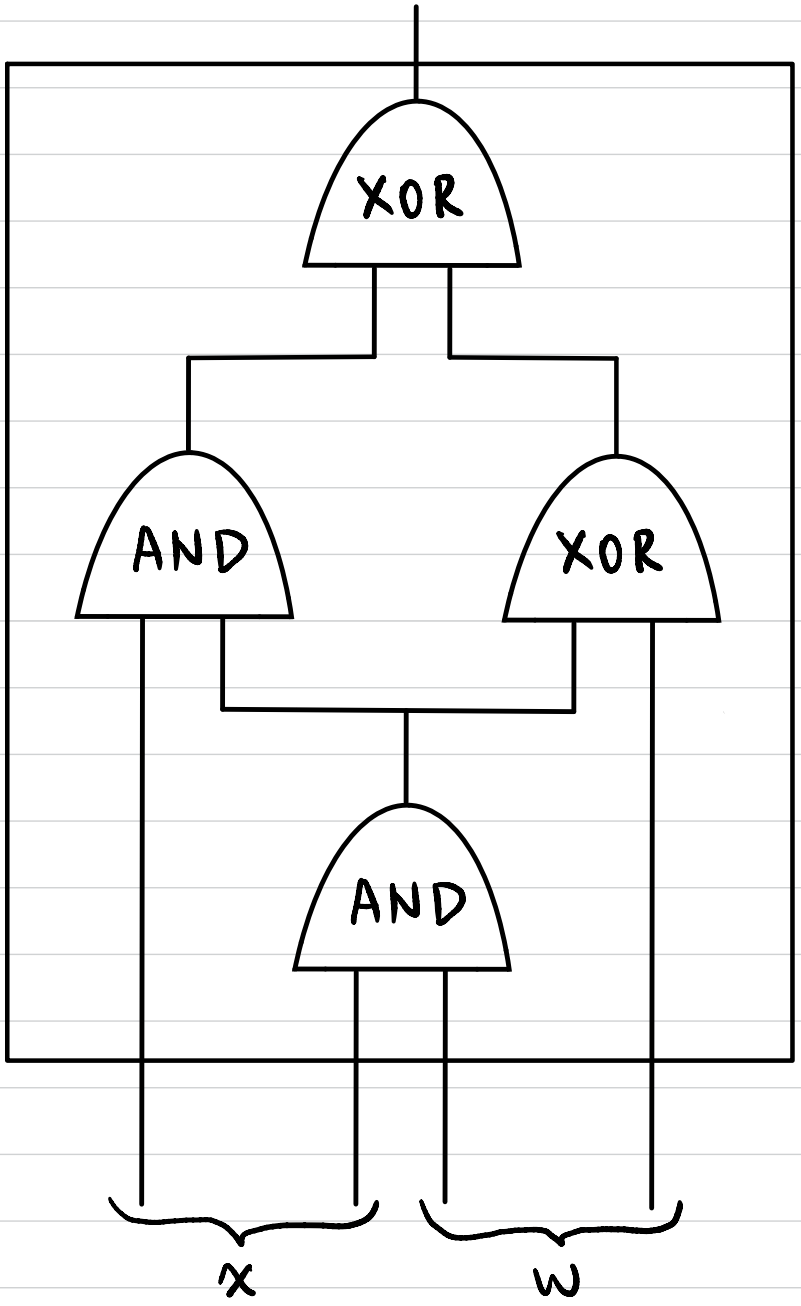
Verifier

Verify: $c_u = \mathrm{Com}(\alpha; r_u)$

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

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

Circuit Satisfiability (NP Complete)



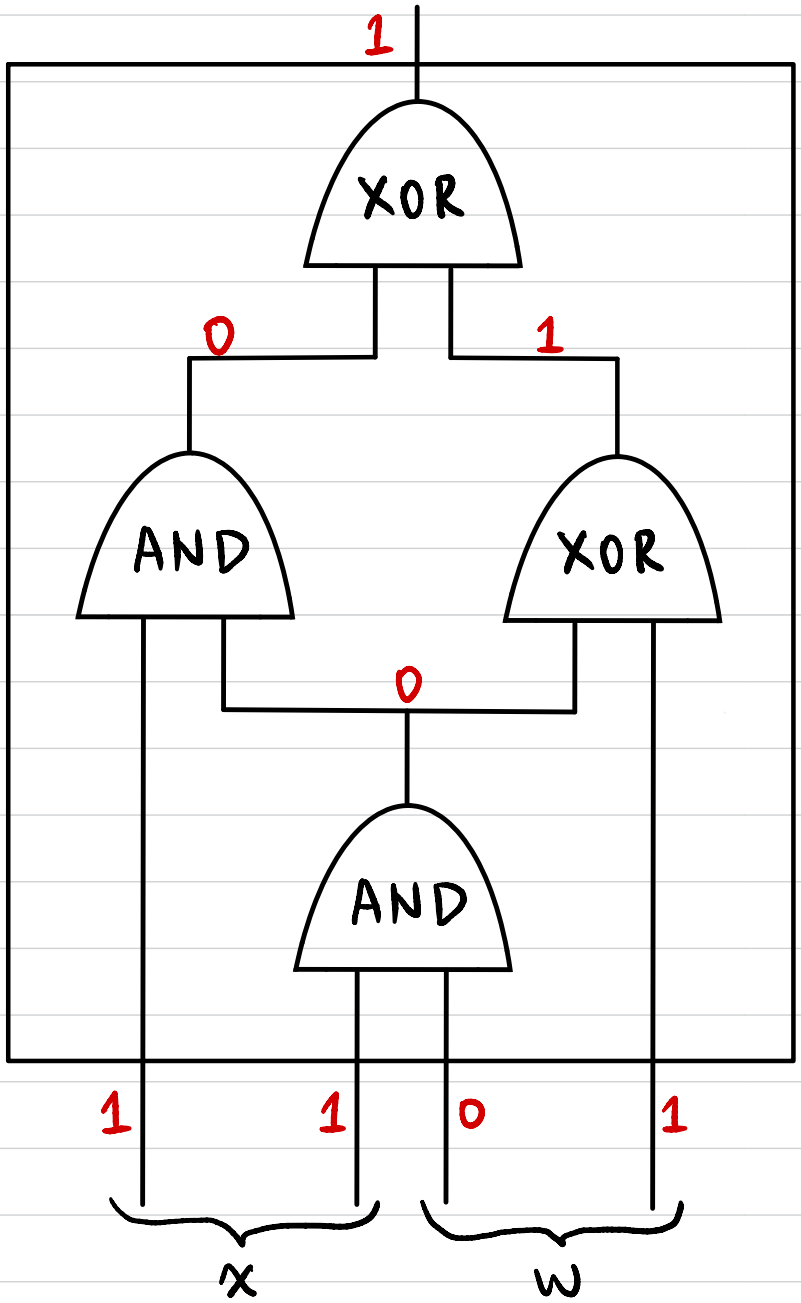
NP language $L_C = \{x \in \{0,1\}^n : \exists w \in \{0,1\}^m \text{ s.t. } C(x,w) = 1\}$

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

Example: pre-image of hash function

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

ZKP for Circuit Satisfiability



Proof Systems for Circuit Satisfiability

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

	NP	Σ-Protocol	(Fiat-Shamir) NIZK
	$P(x, w) \xrightarrow{w} V(x)$	$P(x, w) \rightleftarrows V(x)$	$P(x, w) \xrightarrow{\pi} V(x)$
Zero-Knowledge	NO	YES	YES
Non-Interactive	YES	NO	YES
Communication	$O(\lvert w \rvert)$		
V's computation			

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

Succinct Non-Interactive Argument (SNARG)

$\forall P^*$ $\forall PPT\ P^*$ (in soundness)

Def A non-interactive proof/argument system is succint if

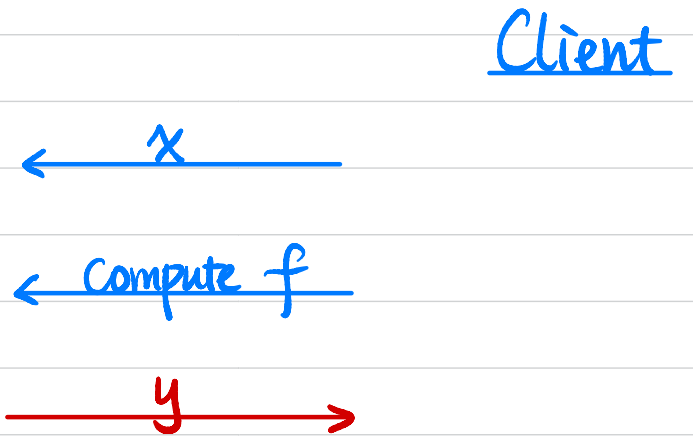
- The proof π is of length $|\pi| = poly(\lambda, \log|C|)$
- The verifier runs in time $poly(\lambda, |x|, \log|C|)$

- SNARK: Succinct Non-Interactive Argument of Knowledge
- zk-SNARG/zk-SNARK: SNARG/SNARK + zero-knowledge

Why Succinct Proofs?

Is it possible?

Verifiable Computation



Anonymous Transactions on Blockchain

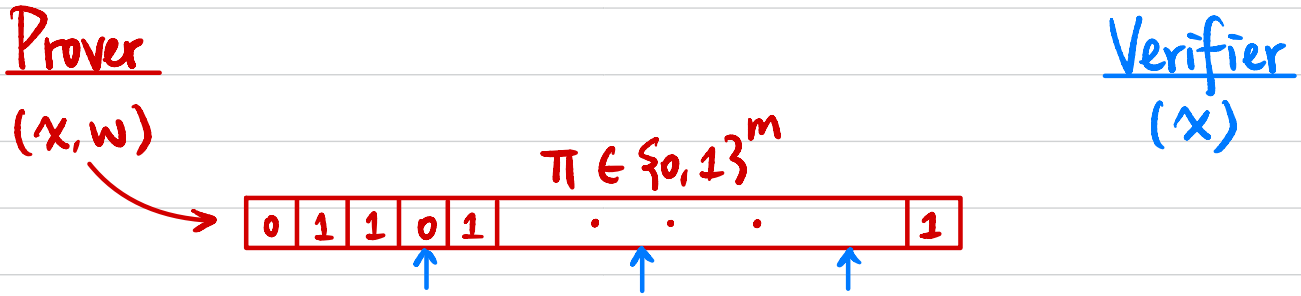
Transaction: $\boxed{vk_A, vk_B, 2BTC}$, $\sigma = Sign_{sk_A}(\cdot)$

Anonymous Transaction:

$$Com\left(\boxed{vk_A, vk_B, 2BTC}, \sigma = Sign_{sk_A}(\cdot)\right)$$

NIZk: valid transaction

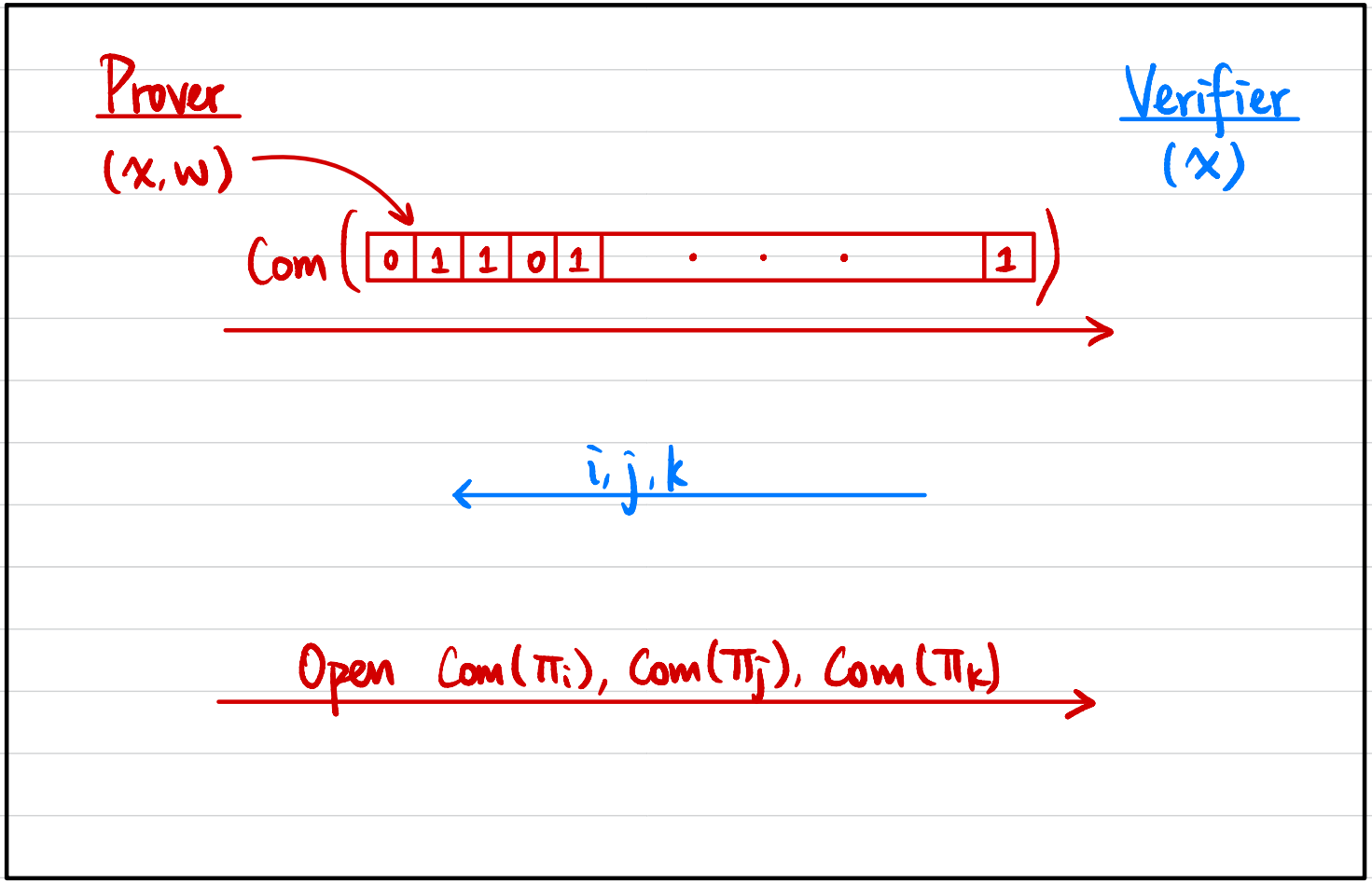
Probabilistically Checkable Proof (PCP)



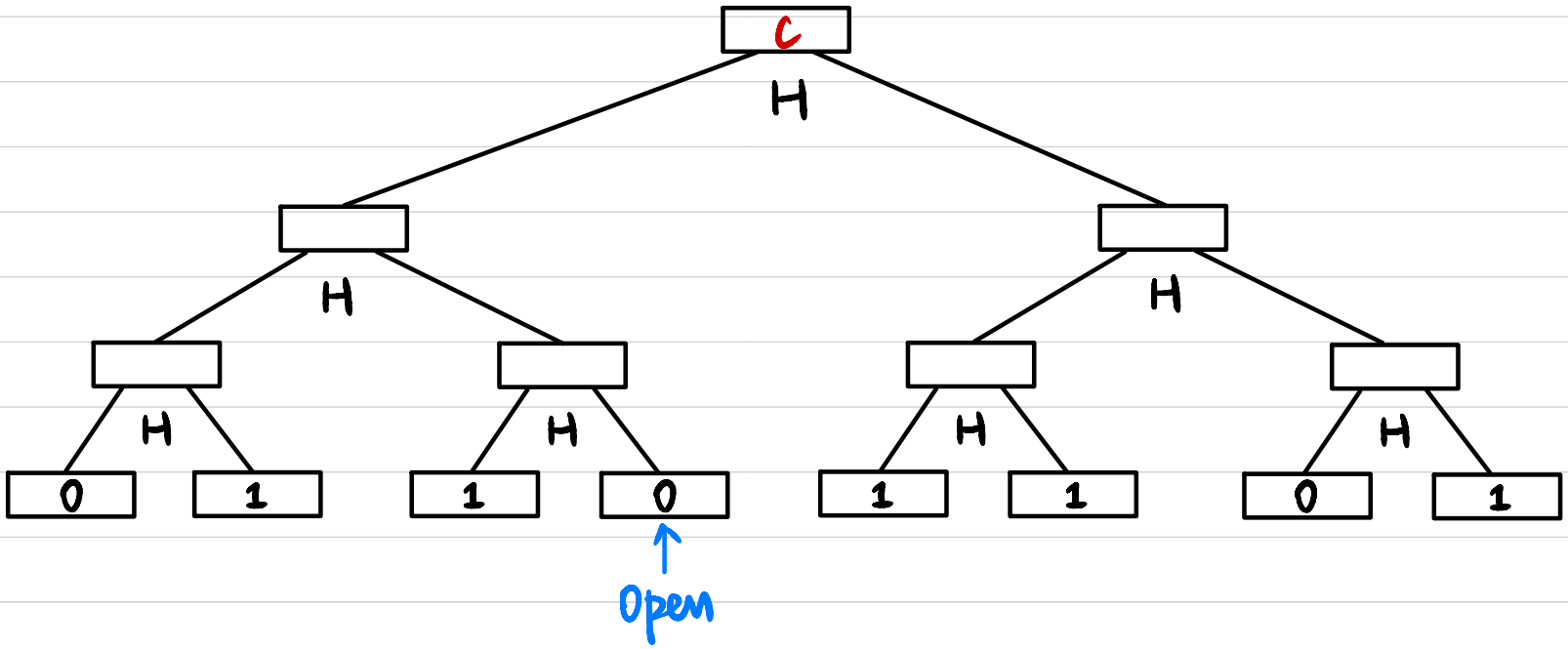
PCP Theorem (Informal):

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

First Attempt



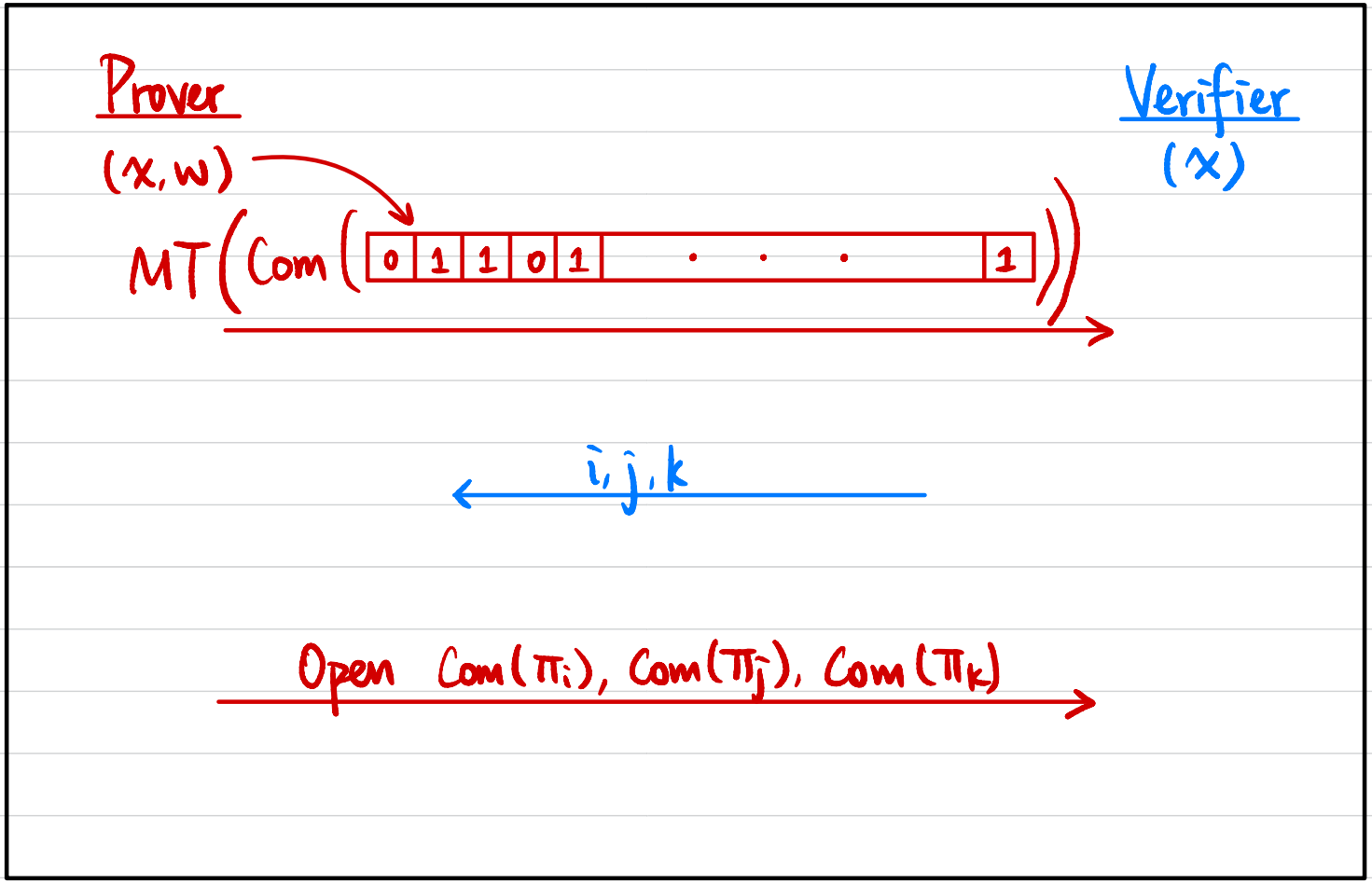
Merkle Tree



Why (computationally) binding ?

Can we make it hiding ?

Is it ZK?


Prover
(x, w)
MT(Com(0 1 1 0 1 . . . 1))
Verifier
(x)
i, j, k
Open Com(π_i), Com(π_j), Com(π_k)