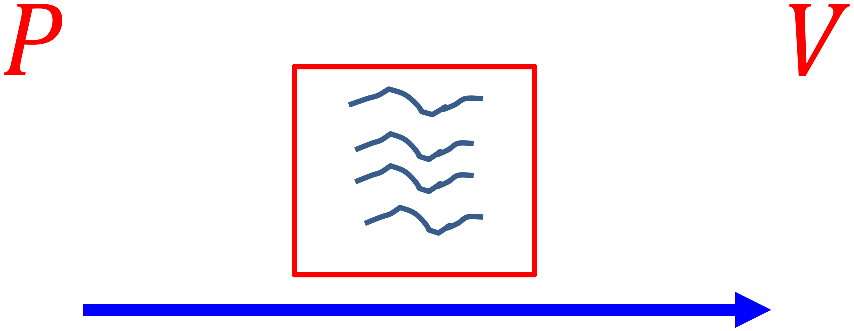
The Evolution of Proofs in Computer Science:

Zero-Knowledge Proofs

6.857

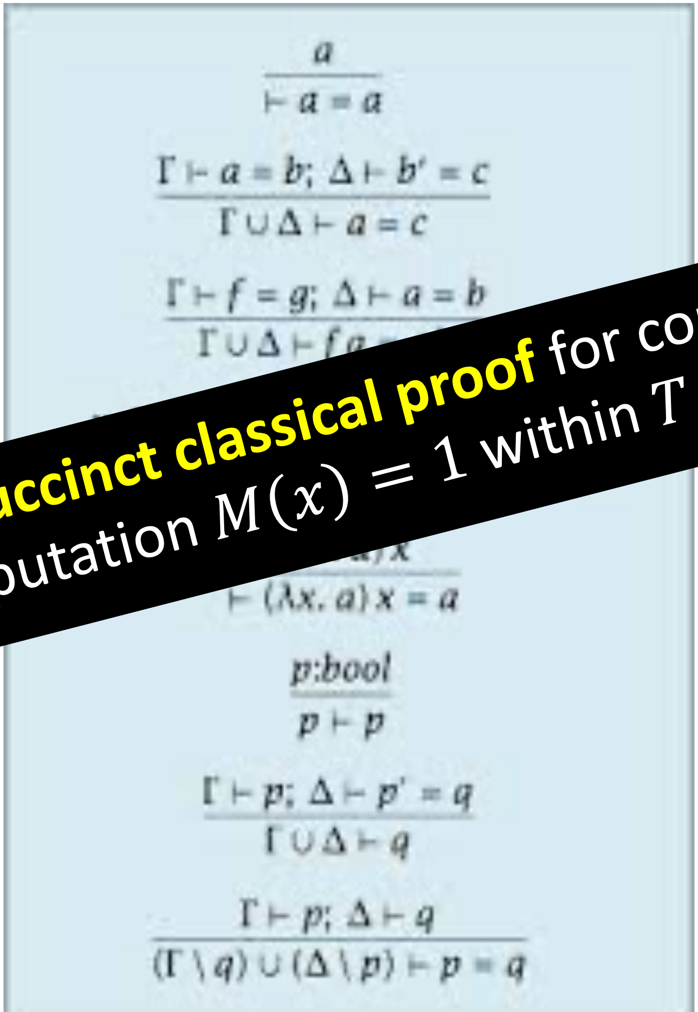
Lecture 13

Classical Proofs



Classical Proofs

P



$$\frac{a}{\vdash a = a}$$

$$\frac{\Gamma \vdash a = b;\ \Delta \vdash b' = c}{\Gamma \cup \Delta \vdash a = c}$$

$$\frac{\Gamma \vdash f = g;\ \Delta \vdash a = b}{\Gamma \cup \Delta \vdash fa}$$

$$\vdash (\lambda x.\, a)x = a$$

$$\frac{p{:}bool}{p \vdash p}$$

$$\frac{\Gamma \vdash p;\ \Delta \vdash p' = q}{\Gamma \cup \Delta \vdash q}$$

$$\frac{\Gamma \vdash p;\ \Delta \vdash q}{(\Gamma \setminus q) \cup (\Delta \setminus p) \vdash p = q}$$

V

Conjecture: $\nexists$ **succinct classical proof** for correctness of any computation $M(x) = 1$ within T steps

Zero-Knowledge Proofs

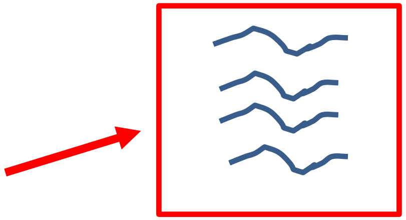
[Goldwasser-Micali-Rackoff85]

Proofs that **reveal no information** beyond the validity of the statement

Zero-Knowledge Proofs

[Goldwasser-Micali-Rackoff85]

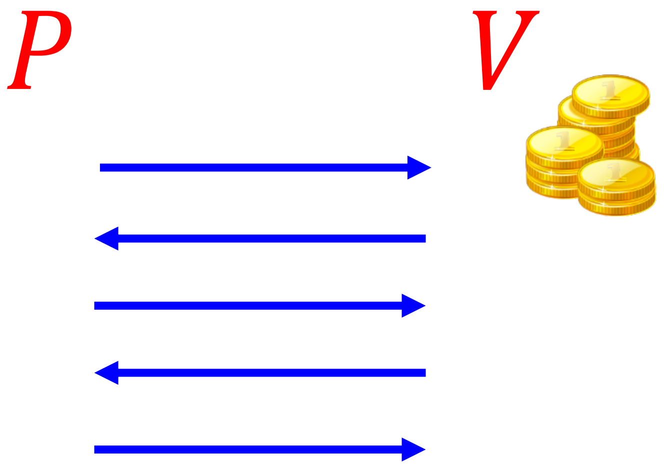
Impossible!



This is information!

Interactive Proofs

[Goldwasser-Micali-Rackoff85]



Completeness: $\forall x \in L \;\; \Pr[(P,V)(x)=1] \geq 2/3$

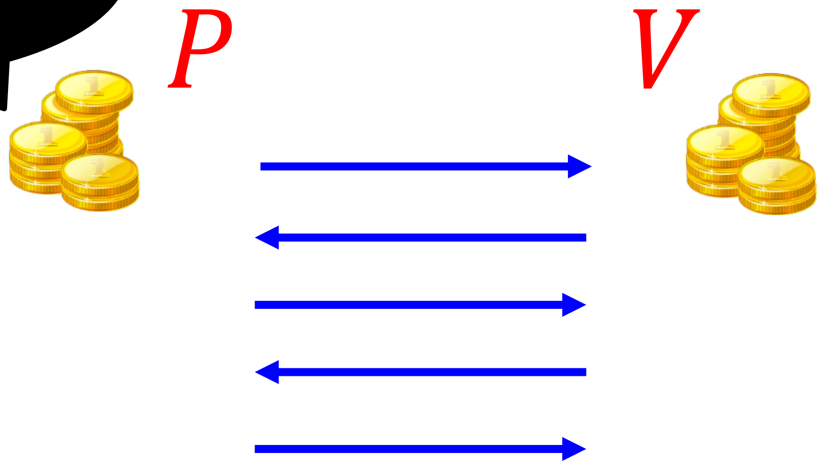
Soundness: $\forall x \notin L, \forall P^* \;\; \Pr[(P^*,V)(x)=1] \leq 1/3$

Note: By repetition, we can get completeness $1-2^{-k}$, and soundness 2^{-k}

Interactive Proofs

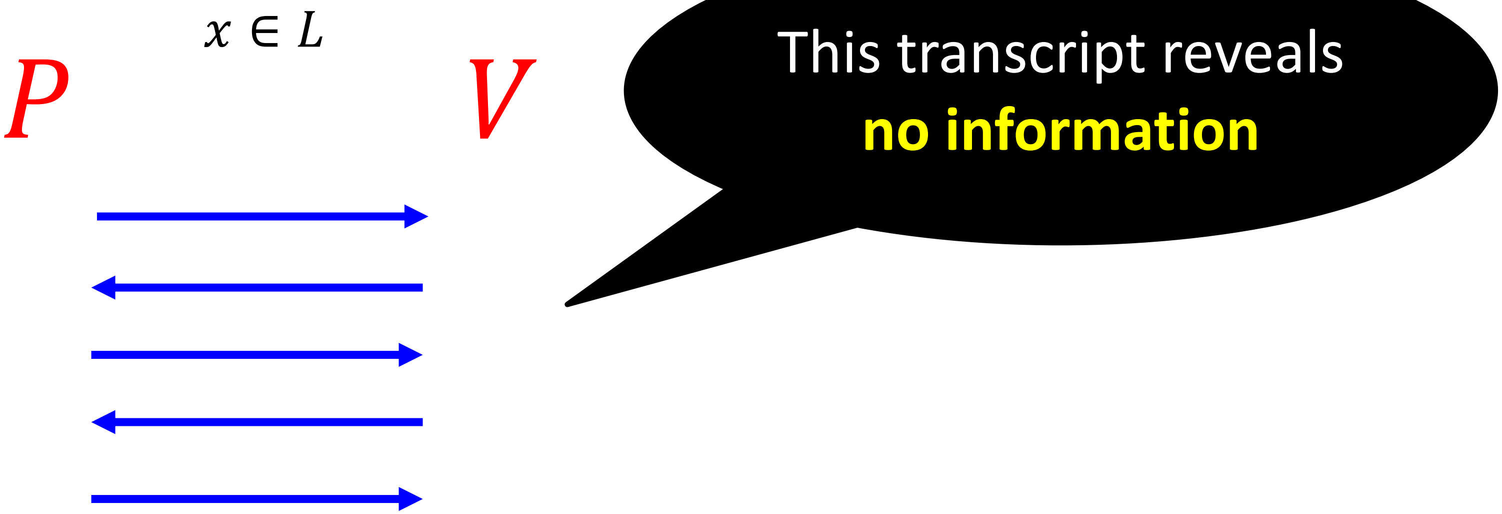
[Goldwasser-Micali-Rackoff85]

For ZK the prover
needs to be
randomized



[Goldreich-Micali-Wigderson87]: Every statement that has a classical proof has **zero-knowledge (ZK)** interactive proof, assuming one-way functions exist

Defining Zero-Knowledge


$x \in L$

P

V

This transcript reveals **no information**

Formally: There exists a PPT algorithm S (called a simulator), such that for every $x \in L$:

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

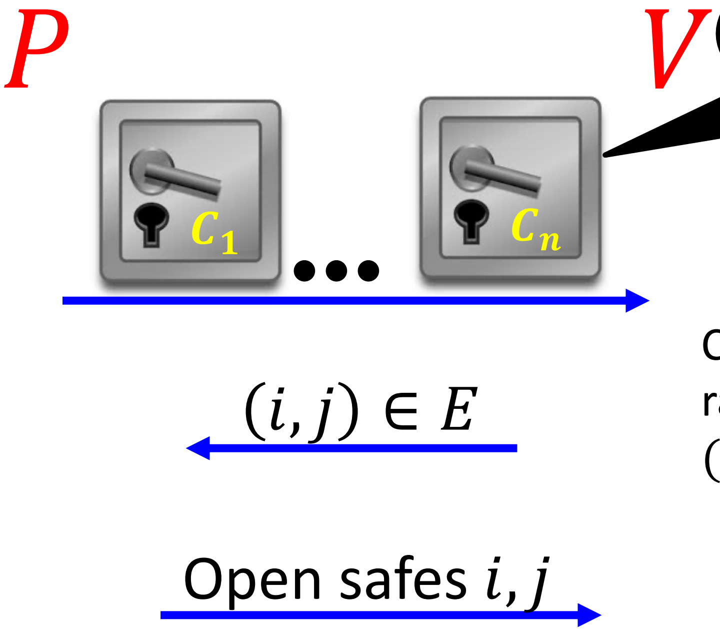
Denotes the transcript

ZK Proofs for NP

Graphs for which vertices can be colored by {1,2,3} s.t. no two adjacent vertices are colored by the same color

For the NP-complete language of all 3-colorable graphs

$G = (V, E)$



Locked safe, reveals no information about its content

Randomly permute the coloring, to obtain valid coloring $(c_1, \dots, c_n)$

$(i, j) \in E$

Choose a random edge $(i, j) \in E$

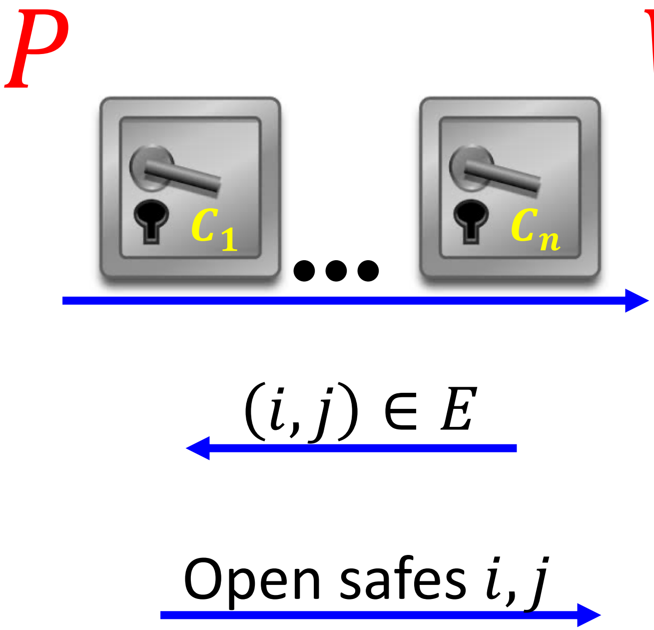
Open safes i, j

Soundness: Only $1 - \frac{1}{|E|}$ but can be amplified via repetition.

ZK Proofs for NP

For the NP-complete language of all 3-colorable graphs

$G = (V, E)$



P V

…

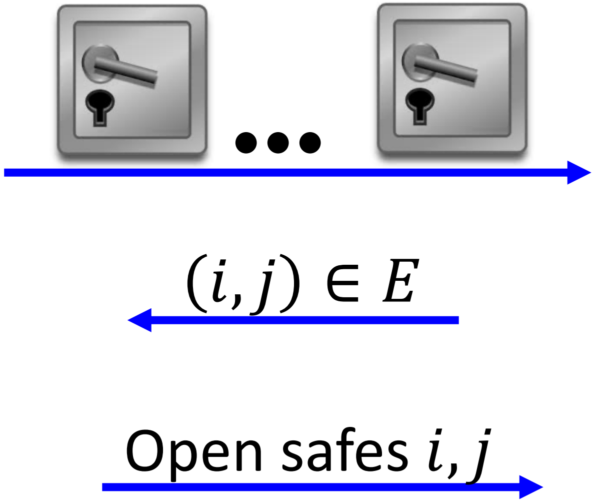
$(i, j) \in E$

Open safes i, j

$S(V, E)$:

1. Choose a random $(i, j) \in E$
2. Choose random distin
   colors c_i, c_j
3. The simulated transc

safes
i, j have
values c_i, c_j



…

$(i, j) \in E$

Open safes i, j

Implementing Digital Safes: Commitment Scheme

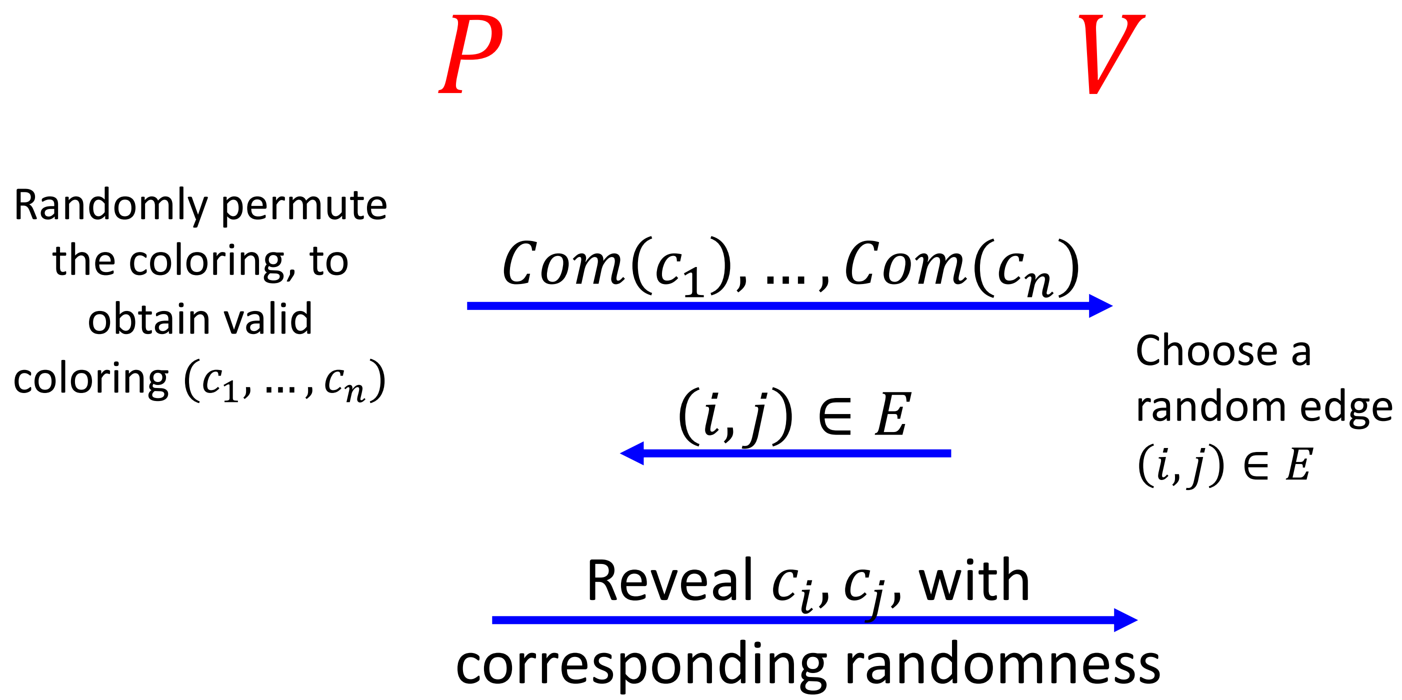
A **commitment scheme** is a randomized algorithm Com s.t.:

- **Hiding:** $\forall m, m' \;\; Com(m; r) \approx Com(m'; r')$.
- **Binding:** $\nexists (m, r), (m', r')$ s.t. $m \neq m'$ and $$Com(m; r) = Com(m'; r')$$

Using Commitments to Construct ZK Proofs

For the NP-complete language of all 3-colorable graphs

$$G = (V, E)$$



P

V

Randomly permute the coloring, to obtain valid coloring $(c_1, \ldots, c_n)$

$Com(c_1), \ldots, Com(c_n)$

Choose a random edge $(i, j) \in E$

$(i, j) \in E$

Reveal c_i, c_j, with corresponding randomness

Constructing a Commitment Scheme

Construction 1:

Let $f: \{0,1\}^* \to \{0,1\}^*$ be an injective OWF.

$$\boldsymbol{Com(b;(r,s)) = (f(r), s, (\bigoplus r_i\, s_i) \oplus b)}$$

Binding: Follows from the fact that f is injective

Hiding: Relies on the fact that if $\boldsymbol{f}$ **is one-way** then:

$$(f(r), s, \bigoplus r_i s_i) \approx (f(r), s), U)$$

Known as a **hard-core predicate**

[Goldreich-Levin89]

Constructing a Commitment Scheme

Construction 2:

Let G be a group of prime order p, let $g \in G$ be any generator, and h be a random group element.

$$\boldsymbol{Com_{g,h}(m,r) = g^m h^r}$$

Hiding: Information theoretically!

Binding: Follows from the Discrete Log assumption.

If $\exists PPT$ alg A s.t.

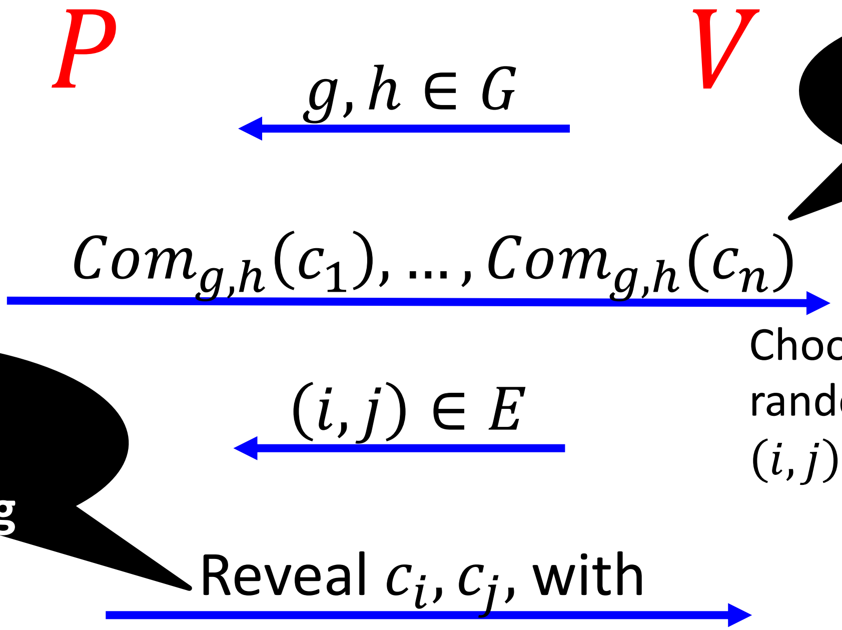
$A(g,h) = (m_1, m_2, r_1, r_2)$ where $g^{m_1}h^{r_1} = g^{m_2}h^{r_2}$ then

$m_1 + sr_1 = m_2 + sr_2$ mod p,

which implies that $s = \frac{m_1 - m_2}{r_2 - r_1}$ mod p

Constructin dge Proofs

This is **perfect ZK!**
But only
computationally sound



Perfectly hiding

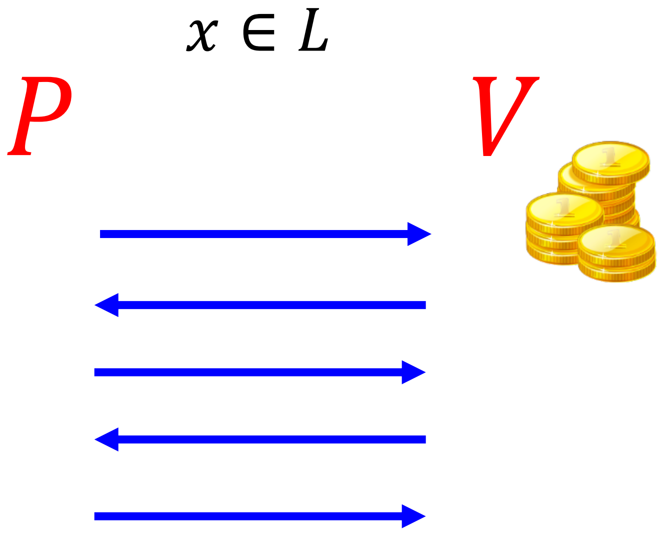
Randomly permute the coloring, to obtain valid col

All powerful prover can break binding

Choose a random edge $(i, j) \in E$

Interactive Computationally Sound Proofs (a.k.a. Arguments)

[Brassard-Chaum-Creapeau88]



$x \in L$

P V

Completeness: $\forall x \in L \;\; \Pr[(P,V)(x) = 1] \geq 2/3$

Soundness: $\forall x \notin L, \forall \boldsymbol{PPT}\; P^* \;\; \Pr[(P^*,V)(x) = 1] \leq 1/3$

So Far…

- **Constructed ZK proofs for all of NP**
  - using commitment schemes

- **Constructed commitment scheme**
  - Based on injective OWF:

    computationally hiding, perfectly binding

    Computational ZK proofs

  - Based on Discrete Log:

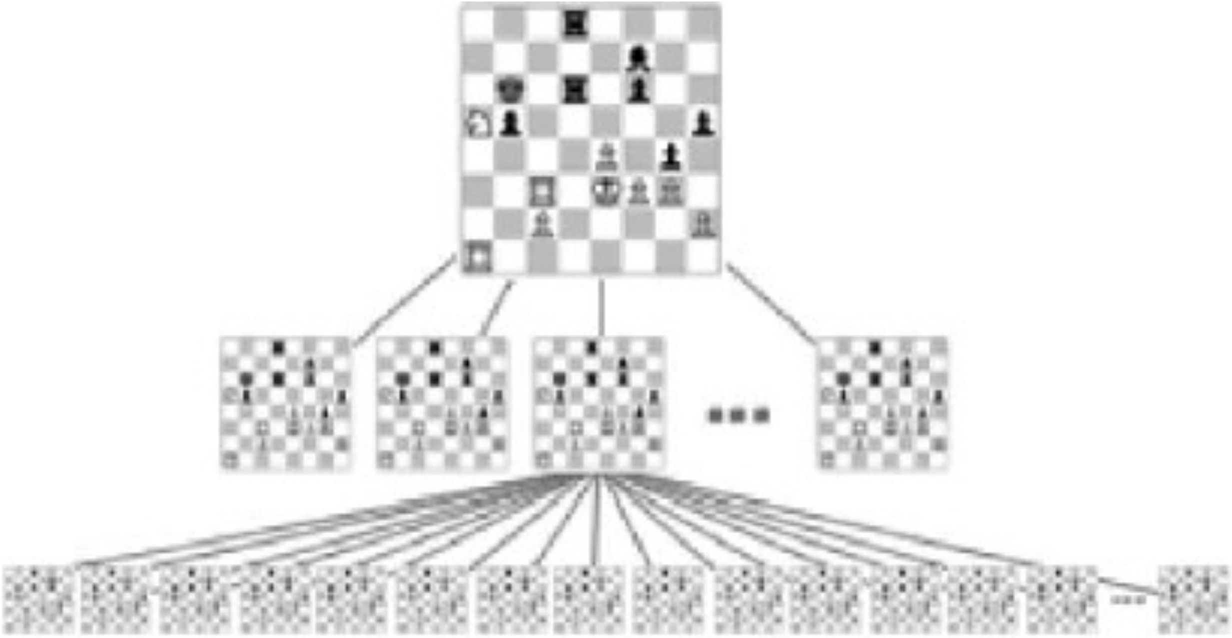
    perfectly hiding, computationally binding

    Perfect ZK arguments

Interactive Proofs are More Efficient!

[Lund-Fortnow-Karloff-Nissan90, Shamir90]

Example: Chess



Interactive Proofs are More Efficient!

[Lund-Fortnow-Karloff-Nissan90, Shamir90]

correctness of any computation can be proved:

Time to verify

$\approx$

Space required to do the computation

Interactive Proof

$$\boldsymbol{IP = PSPACE}$$

Interactive Proofs are More Efficient!

[Lund-Fortnow-Karloff-Nissan90, Shamir90]

correctness of any computation can be proved:

Time to verify

$\approx$

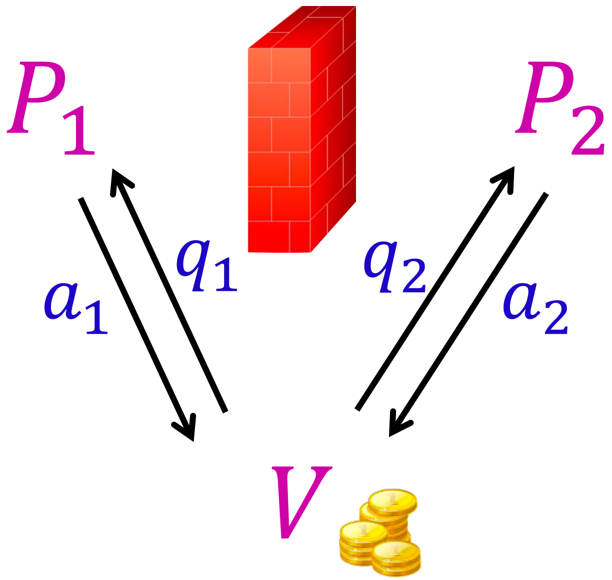
Space required to do the computation

Succinct space → succinct interactive proof

Multi-Prover Interactive Proofs

[BenOr-Goldwasser-Kilian-Wigderson88]

motivated by constructing **perfect ZK proofs**



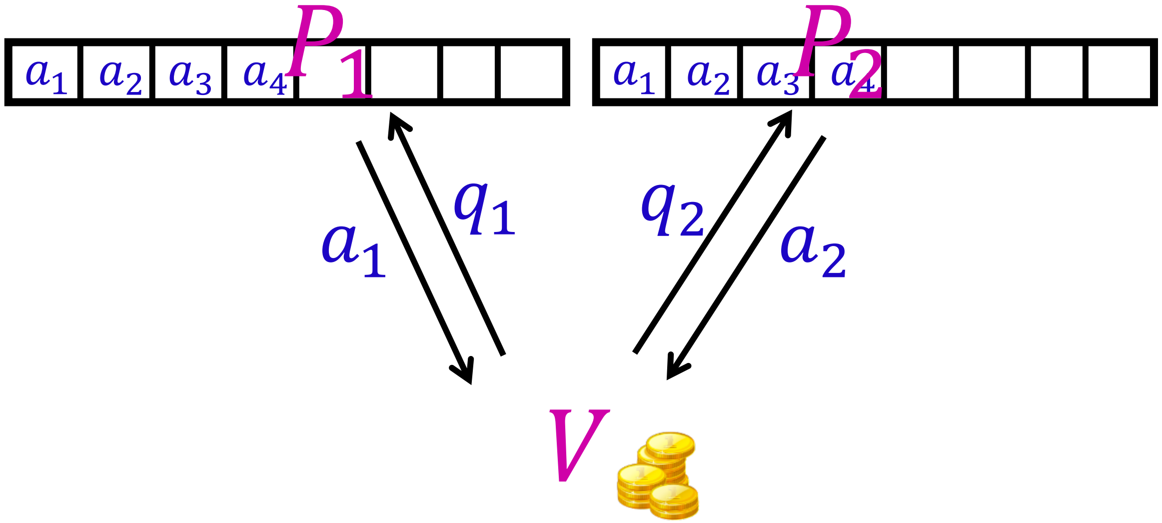
$\forall f$ computable in time T:

2-provers can convince verifier that $f(x) = y$,

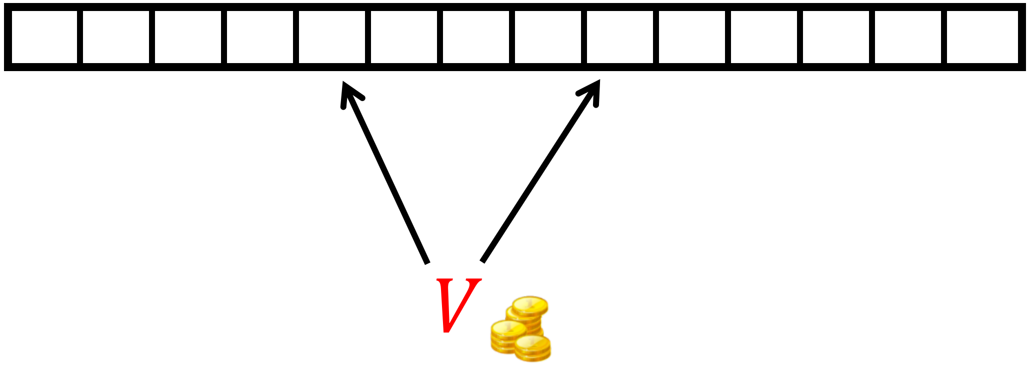
where the **runtime** of the **verifier** is only $|x| \cdot polylog(T)$

and the **communication** is $polylog(T)$

[Fortnow-Rompel-Sipser88]:



Probabilistically Checkable Proofs



[Feige-Goldwasser-Lovasz-Safra-Szegedy91, Babai-Fortnow-Levin-Szegedy91, Arora-Safra92, Arora-Lund-Mutwani-Sudan-Szegedy92]

Read only **3 bits** of the proof, and obtain soundness 1/8

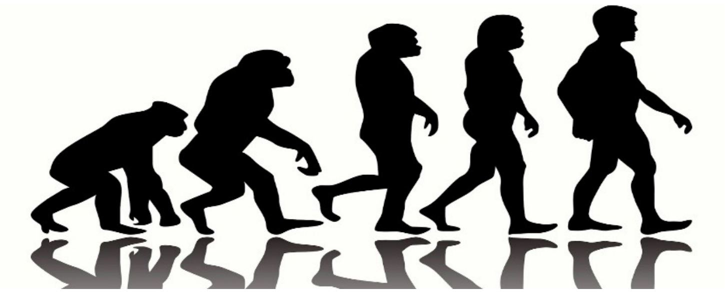
Classical proofs

(Zero-knowledge)
Interactive proofs

Multi-prover
interactive proofs

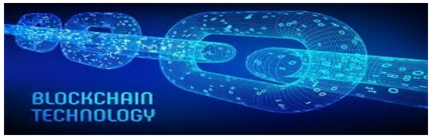
Probabilistically
checkable proofs (PCPs)

Interactive PCP/
Interactive oracle proofs



Fiat-Shamir paradigm

SNARGs




THANK
YOU