Interactive Proofs (IP) and Zero Knowledge (ZK)

Last Time: Pairings

- $e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$
  - Properties
    1. Bilinear
    2. Efficient
    3. Non-trivial
  - Applications
    - signatures
    - 3-party key exchange
    - more! (see lecture 11)

This time:

1. Interactive Proofs
2. Zero Knowledge
3. ZK-proof for HAMCYCLE

What is a Proof?

Someone ("prover")

convinces someone else ("verifier")

that something ("a statement")

is true

formalizing statements:

define languages: $\mathcal{L} \subseteq \{0,1\}^*$

statements have form $x \in \mathcal{L}$

Examples

"15 is biprime"

$$15 \in \{pq : \text{primes } p, q\}$$

"Pythagoras' Theorem is true"

PYTHAG $\in$ {true theorems}

"ϕ is a satisfiable boolean formula"

$\phi \in$ {satisfiable formulas}

$\phi \in SAT$ $\quad \phi = a \wedge b \wedge \neg c$

"ϕ is an unsatisfiable boolean formula"

$\phi \in coSAT$ $\quad \phi = a \wedge \neg a$

Observation some statements (e.g. $\phi \in SAT$) are easy to prove others (e.g. $\phi \in coSAT$) seem hard...

Short, conventional proofs: "NP"

Defn.

Prover (x) $\xrightarrow{\pi}$ **Verifier(x)**

$\downarrow$

$\{0,1\}$

1. π may be hard to find.
2. It must be easy to check!

(poly-time, deterministic verifier, poly-length)

Complexity class "NP":

$\mathcal{L} \in NP$ if $\exists\ \mathcal{V}$ such that

completeness: $x \in L \rightarrow \mathcal{V}(x, \pi) = 1$ for some π

soundness: $x \notin L \rightarrow V(x, \pi) = 1$ for <u>no</u> π

More formally:

$\mathcal{L} \in NP \iff \exists$ deterministic, poly-time V.

$\forall x \quad x \in \mathcal{L} \iff$

$\exists \pi \in \{0,1\}^{poly(|x|)}$

$V(x, \pi) = 1$

Example:

a. for SAT, π is the <u>assignment</u>.

b. we believe $coSAT \notin NP$

($coNP \neq NP$ assumption)

Interactive Proofs (IP) [Micali Goldwasser]

$P \quad V$

$\longrightarrow$
$\longleftarrow$
$\longrightarrow$

With interaction?

$\Rightarrow$ Still NP (see HW)

With interaction + randomness?

- An IP, (P,V) is a pair of randomized machines
- V is efficient
- If $\langle P,V\rangle(x)$ denote's V's output

completeness:

$$\forall x \in L \quad \Pr_{P,V}[(P,V)(x)=1] \geq 2/3$$

"perfect" if ≥ 1

soundness:

$$\forall x \notin L \; \boxed{\forall P^*} \; \Pr_V[\langle P,V\rangle(x)=1] \leq \varepsilon$$

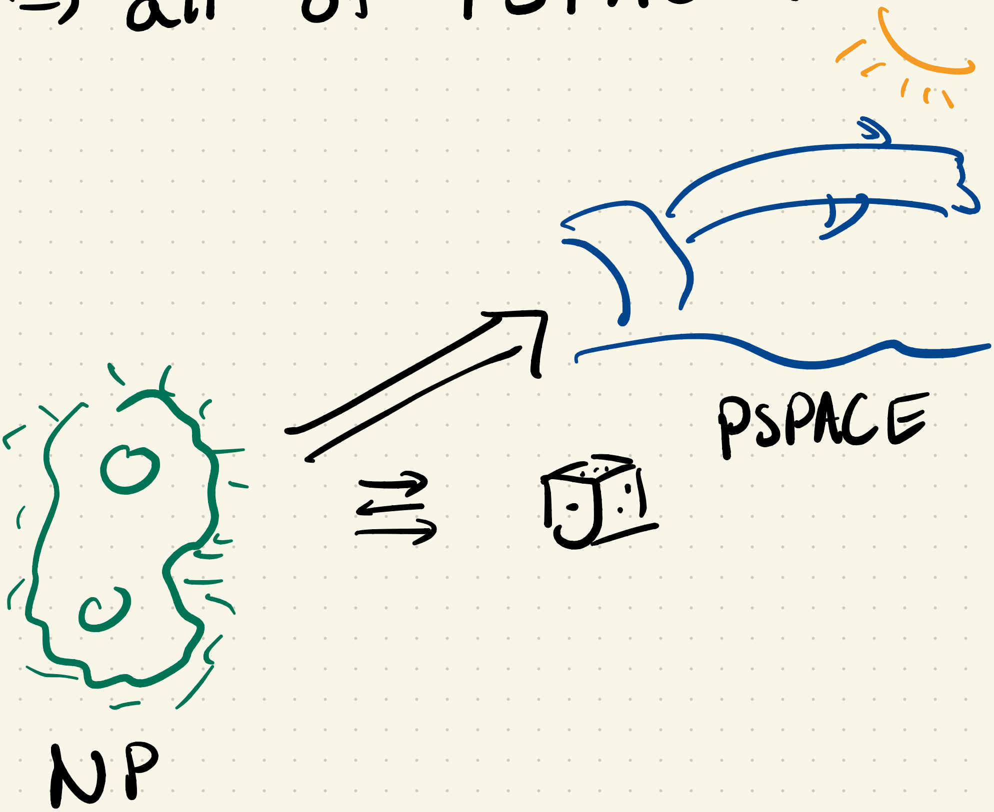
"soundness error" e.g. 1/3

repeat to boost

Which Languages are in IP?

[Shamir '92][Shen '92]

$\Rightarrow$ all of PSPACE!



Zero Knowledge Proofs

- IP where V learns $x \in \mathcal{L}$ and nothing else

Examples:

Prove a graph is 3-colorable without revealing the coloring

↖ today.

Prove a formula is SAT without revealing the assignment

Prove you know an unspent coin's id without revealing which coin ($\Rightarrow$ zcash)

Formalizing ZK

Idea: the "how was school?" principle?

Dad: "How was school"
Kid: "fine" ← Dad could have guessed this
→ if V can fake the transcript, protocol is ZK.

Defn: (P,V) is ZK if for all efficient V^*, there exists an effisient Sim

$$\{ \mathrm{View}_{V^*}[\langle P, V^* \rangle (x)] \} \approx \{ \mathrm{Sim}(x) \}$$

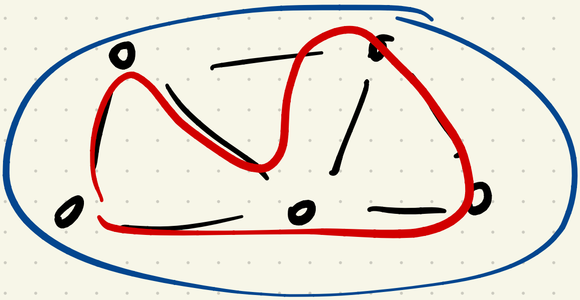
↑ statistically, computationally, perfectly

tip: relax this defn by giving sim more inputs.

⇒ We'll show all $\mathcal{L} \in NP$ have a ZK proof system!

HAMCYCLE

HAMCYCLE is the set of graphs with a hamiltonian cycle: a cycle that visits each vertex exactly once.



Vertices $V = \{1, 2, \ldots, n\}$

edeges represented by adjacency matrix:

$$G_{ij} = \begin{cases} 1 & i \sim j \\ 0 & \text{otherwise} \end{cases}$$

ham cycle is an $\ell \in \mathbb{N}^n$ without repeats, such that $\forall i \in \{1, 2, \ldots, n-1\}$ $G_{\ell_i, \ell_{i+1}} = 1$

HAMCYCLE ∈ NP:

P(G)

V(G)

ℓ ← ?

$\xrightarrow{\ell}$

checks ℓ

↑ not a ZK proof unless P=NP

HAMCYCLE is NP-hard [Karp '72]

HAMCYCLE → directed HAMCYCLE

→ vertex cover → clique

→ SAT

→ NP [Cook-Levin '71]

So a ZK-proof for HAMCYCLE can be extended to all of NP.

ZK Proof for HAMCYCLE

$P(G, \ell)$	$V(G)$

$\sigma \xleftarrow{\$} \text{permutations}(V)$

$G' \leftarrow \sigma(G)$

$c_{i,j} \leftarrow \text{Commit}(G'_{i,j})$

$d_i \leftarrow \text{Commit}(\sigma(i))$ $\longrightarrow$

show commits

$b \xleftarrow{\$} \{0, 1\}$

show cycle

$\xleftarrow{\quad b \quad}$

if $b = 0$:
open all commits

if $b = 1$:
open the commits of G' which show the cycle $\sigma(\ell)$ $\longrightarrow$

- check all openings
- if $b = 0$:
  check σ is a permutations

  if $b = 1$:
  check that openings form a HAMCYCLE

Analysis

completeness:

1. σ is always a permutation
2. ℓ is always a cycle
3. commitments are always legit

soundness:

if $G \notin$ HAMCYCLE, no permutation of it has a HAMCYCLE either

so the permutation is invalid
<u>or</u> the cycle is invalid

$\Rightarrow$ 50% chance of getting caught.

$\Rightarrow$ repeat to improve

Zero-Knowledge:

Sim(G):

$b' \xleftarrow{\$} \{0,1\}$

if $b=0$:

commit to random permutation of G

else:

commit to random permutation of an n-vertex cycle graph.

$b \leftarrow V^*(\text{commitments})$

if $b \neq b$:

restart ← fixes distribution for V^* which does not chose $b \xleftarrow{\$} \{0,1\}$

if $b=0$:

open commits

if $b=1$:

open cycle commitments

Need to show

$$\{ \text{View}_{V^*}[\langle P, V\rangle(x)] \} \approx_c \{ \text{Sim}(G) \}$$

$$D \approx D'$$

$$\{ (\underline{G}, \underline{(c_{1,1}, \ldots, c_{n,n})}, (\underline{d_1, \ldots, d_n}), \underline{b}, \underline{\text{openings}}) \}$$

- these are all $\equiv$ in D, D' (conditioned on prior entries)
- need to show these are $\approx$ in D, D'
  - $\rightarrow$ use commitment hiding & $n^2 + n$ hybrids.
    - $\rightarrow$ each hybrid replaces <u>one</u> commitment

Recap:

$\boxed{0}$ NP-proofs

$\boxed{1}$ Interactive Proofs

$\boxed{2}$ IP: zero knowledge

$\boxed{3}$ ZK for all of NP

(via HAMCYCLE
+ commitments)

Rest of unit: other IP properties

Tues: Proof of knowledge

Thurs: Non-interactivity

Tues + Thurs: Succinctness