Interactive Proofs (IP) and Zero Knowledge (ZK)
Lost Time: Pairings

- $e: G_1 \times G_2 \rightarrow G_{T}$

- 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: \( L = \{0,1\}^* \)

Statements have form \( x \in L \)

Examples

"15 is bi-prime"

\[ 15 \in \{pq : \text{primes } p,q\} \]
"Pythagoras' Theorem is true."

PYTHAG ∈ \{ true theorems \}

" \( \phi \) is a satisfiable boolean formula."

\[ \phi \in \{ \text{satisfiable formulas} \} \]

\( \phi \in \text{SAT} \) \( \phi = a \land b \land \overline{c} \)

" \( \phi \) is an unsatisfiable boolean formula."

\( \phi \in \text{coSAT} \) \( \phi = a \land \overline{b} \land c \)

Observation: some statements (e.g. \( \phi \in \text{SAT} \)) are easy to prove; others (e.g. \( \phi \in \text{coSAT} \)) seem hard...
Short, conventional proofs: "NP"

**Defn.**

\[
\text{Prover} (x) \quad \text{Verifier}(x)
\]

\[
\pi \rightarrow \{0,1\}^k
\]

1. It may be hard to find.
2. It must be easy to check!
   \((\text{poly-time, deterministic verifier, poly-length})\)

Complexity class "NP":

\(L \in \text{NP} \text{ if } \exists V \text{ such that}\)

- **Completeness**:
  \(x \in L \rightarrow V(x, \pi) = 1\)
  for some \(\pi\)

- **Soundness**:
  \(x \notin L \rightarrow V(x, \pi) = 1\)
  for no \(\pi\)
More formally:
\[ L \in \text{NP} \iff \exists \text{ deterministic, poly-time } V. \]

\[ \forall x \in L \iff \exists \pi \in \{0,1\}^{\text{poly}(|x|)} V(x,\pi) = 1 \]

Example:

a. for SAT, \( \pi \) is the assignment.

b. we believe \( \text{coSAT} \notin \text{NP} \) (\( \text{coNP} \neq \text{NP} \) assumption)
Interactive Proofs (IP) \( [ \text{Micali, Goldwasser} ] \)

With interaction? \( \frac{P}{V} \)

\( \Rightarrow \) 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:
\[
\forall x \in L \quad \Pr_{P, V} \left[ \langle P, V \rangle(x) = 1 \right] \geq \frac{2}{3}
\]

Soundness:
\[
\forall x \notin L \quad \forall P^* \quad \Pr_{V} \left[ \langle P, V \rangle(x) = 1 \right] \leq \frac{1}{3}
\]

"Soundness error" repeat to boost e.g. \( \frac{1}{3} \)
Which languages are in IP?

[Shamir '92][Shen '92]

=> all of PSPACE!
Zero Knowledge Proofs

- IP where $U$ learns $x \in L$ and nothing else

Examples:
- Prove a graph is 3-colorable without revealing the coloring
- Prove a formula is SAT without revealing the assignment
- Prove you know an unspent coin's id without revealing which coin ($\Rightarrow z\text{cash}$)
Formalizing ZK

Idea: the “how was school?” principle?

Dad: “How was school”
Kid: “fine” ← Dad could have guessed this

→ if $\mathcal{V}$ can fake the transcript, protocol is ZK.

Defn: $(P, \mathcal{V})$ is ZK if for all efficient $\mathcal{V}'$, there exists an efficient Sim

\[
\{ \text{View}_v, [P, \mathcal{V}'](x) \} \approx \{ \text{Sim}(x) \}
\]

Tip: relax this defn by giving Sim more inputs.

$\implies$ We'll show all $\mathbf{L \in NP}$ have a ZK proof system!
HAHCYCLE

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

Vertices \( V = \{1, 2, \ldots, n\} \)

edges represented by adjacency matrix:

\[
G_{ij} = \begin{cases} 
1 & \text{if } i \neq j \\
0 & \text{otherwise}
\end{cases}
\]

ham cycle is an \( e \in \mathbb{N}^n \) without repeats, such that \( \forall i \in \{1, 2, \ldots, n-1\} \quad G_{e_i, e_{i+1}} = 1 \)
HAMCYCLE ∈ NP:

\[
\frac{P(G)}{V(G)}
\]

\[e \Leftarrow ? \quad e \rightarrow \text{checks } e\]

\[\text{? not a ZK-proof unless } P = NP\]

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.
2K Proof for HAMCYCLE

\[ \begin{align*}
\text{PC}(G, e) & \quad \text{V}(G) \\
\sigma \in \text{permutations}(V) & \\
G' & \leftarrow \sigma(G) \\
C_{ij} & \leftarrow \text{Commit}(G'_{ij}) \\
d_i & \leftarrow \text{Commit}(\sigma(i)) \\
b & \leftarrow \{0, 1\}
\end{align*} \]

if \( b = 0 \):
- open all commits
- check all openings
- if \( b = 0 \):
  - check \( \sigma \) is a permutations
  - if \( b = 1 \):
    - check that openings form a HAMCYCLE

if \( b = 1 \):
- open the commits of \( G' \) which show the cycle \( \sigma(e) \)
Analysis

Completeness:
1. $\sigma$ is always a permutation
2. $h$ is always a cycle
3. Commitments are always legit

Soundness:
If $G \notin \text{HAMCYCLE}$, no permutation of it has a HAMCYCLE either
so the permutation is invalid
or the cycle is invalid

$\Rightarrow$ 50% chance of getting caught

$\Rightarrow$ repeat to improve
Zero-knowledge:

\[ \text{Sim}(G): \]
\[ b' \leftarrow \{0,1\} \]
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 \( b \neq b' \):
  \( - \) fixes distribution for \( V^* \) which does not choose \( b \& b' \)
  restart
if \( b = 0 \):
  open commits
if \( b = 1 \):
  open cycle commitments
Need to show
\[ \{ \text{View vr } [ (P, U) \xi ] \} \simeq \{ \text{Sim}(G) \} \]
\[ D \simeq D' \]
\[ \{ (G, (c_1, \ldots, c_{n, n}), (d_1, \ldots, d_n), b, \text{openings}) \} \]

- these are all \( \simeq \) in \( D, D' \)
  (conditioned on prior entries)
- need to show these are
  \( \simeq \) in \( D, D' \)
  
  \( \rightarrow \) use commitment hiding
  & \( n^2 + n \) hybrids
  
  \( \rightarrow \) each hybrid replaces
  one commitment
Recap:

1. NP-proofs
2. Interactive Proofs
3. IP: Zero knowledge
4. ZK for all of NP (via HAMCYCLE + commitments)

Rest of unit: other IP properties

Tues: Proof of knowledge
Thurs: Non-interactivity
Tues+Thurs: Succinctness