Lecture 15

Zero Knowledge II
Class NP

Prover \( x \in L? \) Verifier

\( \text{Works Hard} \) \( w \) \( \text{Polyomial Time} \)

Iff \( V(x,w) = 1 \) Then accept \( x \)

\( \text{NP} = \{ D \text{ s.t. } \exists \text{ polynomial time } V \text{ s.t. } \} \)

\( x \in D \text{ iff } \exists w \text{ of polynomial size s.t. } V(x,w) = 1 \} \)

Any statement which have Efficiently Verifiable Classical Proofs
Class IP

Prover P

Verifier V

\[ x \in L? \]

a_1 \rightarrow q_1 \rightarrow a_2

\text{Probabilistic Polynomial time algorithm}

Accepts / Rejects

\[ \text{IP} = \{ L \text{ s.t. } \exists (P,V) \text{ s.t.} \]

if \( x \in L \), then \( \text{prob}((P,V)[x] = \text{accepts}) \geq 2/3 \)

if \( x \notin L \), then \( \text{prob}((P,V)[x] = \text{accepts}) < 1/3 \)
Perfect Zero-Knowledge

For a given P and V on input x, define probability space $\text{View}_{(P,V)}(x) = \{(q_1,a_1,q_2,a_2,...,\text{coins})\}$ (over coins of V and P)

$(P,V)$ is **honest** verifier perfect zero-knowledge for L if:
$\exists \text{SIM an expected polynomial time randomized algorithm s.t. } \forall x \text{ in L, } \text{View}_{(P,V)}(x) = \text{SIM}(x)$

$(P,V)$ is **perfect zero-knowledge** for L if:
$\forall \text{PPT } V^* \exists \text{SIM an expected polynomial time randomized algorithm s.t. } \forall x \text{ in L, } \text{View}_{(P,V^*)}(x) = \text{SIM}(x)$
(P,V) is **statistical zero-knowledge** for L if:

\[ \forall V^* \exists \text{SIM expected polynomial time randomized algorithm} \]
\[ \text{s.t.} \forall x \in L \]
\[ | \sum_v | \text{prob}[v \in \text{View}_{(P,V^*)}(x)] - \text{prob}[v \in \text{SIM}(x)]| < \text{neg}(|x|) \]
Today

• Computational Zero Knowledge

• Every problem in NP has a Computational Zero Knowledge Interactive Proofs

• Is IP greater than NP?
  – Today: examples unknown to be in NP
  – Complexity class IP=PSPACE

• Applications
Computational Zero-Knowledge

(P,V) is **honest** verifier perfect zero-knowledge for L if:

\[ \exists \text{SIM an expected polynomial time randomized algorithm s.t. } \forall x \in L, \text{View}_{(P,V)}(x) \approx c \text{ SIM}(x) \]

Relax to “indistinguishable” by any observer who runs in probabilistic polynomial time

(P,V) is **computational zero-knowledge** for L if:

\[ \forall \text{PPT } V^* \exists \text{SIM an expected polynomial time randomized algorithm s.t. } \forall x \in L, \text{View}_{(P,V^*)}(x) \approx c \text{ SIM}(x) \]

Notation: \[ \text{View}_{V^*}(x) \approx_c \text{SIM}(x) \]
Prover Gives Perfect Zero Knowledge

- If: we can efficiently simulate the view of any verifier s.t. "Simulated views" `real verifier" are indistinguishable by any PPT distinguisher

The observer
Any Probabilistic Poly Time Algorithm
Zero Knowledge for all of NP

Theorem: If one-way permutations exist, then every problem in NP has a computational zero knowledge interactive proofs.

- The assumption can be relaxed to one-way functions.

Building Block: One Way Functions imply Commitments schemes.

- To prove the theorem, should we construct ZK proof for every NP language? Not efficient!
How can you prove something so general?

Idea: Show a zero knowledge interactive proof for Complete Problem for NP.

3COLOR = all graphs which can be colored with 3 colors s.t for for all edges (u,v) color(u) ≠ color(v)

NP Completeness [Cook-Levin-Karp]: Given L in NP.
Instances x is polynomial time reducible to $G_x$

$x \in L \implies G_x$ is 3 colorable
$x \notin L \implies G_x$ is not 3 colorable

Show a Zero-knowledge Proof for 3-coloring
Physical Intuition for Protocol

On common input graph $G = (V,E)$ and Provers private input coloring $\pi : V \rightarrow \{0,1,2\}$

- $P$ picks a random permutation $\sigma$ of the coloring $\pi$ & color the graph with coloring $\alpha = \sigma(\pi)$. It hides the color $\alpha(u)$ of each vertex inside a locked box.

- $V$ Select a random edge $(u,v)$
- $P$ opens boxes corresponding to $u$ and $v$

- $V$ accepts if and only if $\alpha(u) \neq \alpha(v)$ [colors are different]
Intuition for Completeness and Soundness

• **Completeness**: if prover uses a proper 3-coloring, the verifier will accept.

• **Soundness**: Let $k = |E|^2$
  If $G$ is not 3-colorable, then for all $P^*$
  $\text{Prob}[(P^*,V)(G) \text{ accepts}] < 1 - 1/|E|$

Repeat $k$ times.

  $\text{Soundness} \text{ Prob}[(P^*,V)(G) \text{ accepts}] < (1-1/|E|)^k < 1/e^{|E|}$
From Intuition to a Proof

To “digitize” the above proof, we need to implement locked boxes

Need two properties from digital locked boxes:

- **Hiding**: $V$ should not be able to see the content inside a locked box

- **Binding**: $P$ should not be able to modify the content inside a box once its locked
Commitment Scheme
(Digital analogue of locked boxes)

• An efficient two-stage protocol between a sender S and receiver R on input \((1^k)\) s.t.:

  • **commit stage**: S has private input \(b \in \{0, 1\}\); At the end of the commit stage
    – both parties hold output \(\text{com}\) (called the commitment)
    – S holds a private output \(\text{dec}\) (called the de-commitment)

  • **reveal stage**: S sends the pair \((\text{dec}, b)\) to R. R accepts or rejects
Properties of a Commitment Scheme

Completeness: \( R \) always accepts in an honest execution of \( S \).

Hiding: \( \forall R^*, \ b \neq b' \in \{0,1\}, \ \text{In commit stage} \)
\[
\{\text{View} \ (S(b),R^*)(1^k)\} \approx_c \{\text{View}(S(b'),R^*)(1^k)\}.
\]

Binding: Let \( com \) be output of commit stage \( \forall S^* \)

\[\text{Prob}[S^* \text{ can reveal two pairs } (\text{dec},b) \& (\text{dec}',b')]\]
\[\text{s.t. } R(\text{com}, \text{dec}, b) = \]
\[R(\text{com}, \text{dec}', b') = \text{Accept}] < \text{neg}(k)\]

Ex: \( c \in \text{Enc}(r,b) \) for semantically secure PK enc.
Comm=c, Dec=\{r,b\}
Commitment Schemes: Remarks

The previous definition only guarantees hiding for one bit and one commitment

Claim: One-bit commitment implies multiple string commitment (using hybrid argument as in encryption)
Commitment Schemes

Can be implemented using interactive protocols, but we will consider non-interactive case. Both commit and reveal phases will consist of single messages.

One-Way function based commitments require 2 rounds of interaction in commit stage.
Construction of Bit Commitments

**Construction:** Let $f$ be a OWP, $B$ be the hard core predicate for $f$

**Commit phase**($b$): Sender chooses $r$, sends $\text{Comm} = f(r), b \oplus B(r)$

**Reveal phase:** Sender reveals $(b, r)$. Receiver accepts

*If $\text{Comm} = (f(r), b \oplus B(r))$, and rejects otherwise*

**Security:**

- Binding follows from construction since $f$ is a permutation
- Hiding follows in the same manner as IND-CPA security
ZK interactive proof for G3COL

On common input graph $G = (V, E)$ and private prover input coloring $\pi: V \rightarrow \{0, 1, 2\}$

- $P \rightarrow V$: Pick a random permutation $\sigma$ of the coloring & color the graph with coloring $\alpha(\pi) = \sigma(\pi(v))$. Send commitments $Enc(r_v, \alpha(v)) \forall$ vertex $v$.
- $V \rightarrow P$: Select a random edge $(u, v)$ and send it.
- $P \rightarrow V$: reveal colors of $u$ and $v$ committed in $Enc(r_u, \alpha(u))$ and $Enc(r_v, \alpha(v))$ by releasing $r_u$ and $r_v$.
- If $\alpha(v) \neq \alpha(u) V \text{ rejects}$, otherwise repeat and $V \text{ accepts}$ after $k$ iterations.
Simulator S in input G=(V,E) : guess in advance the challenge (a,b) of the honest verifier V.

- Choose random edge (a,b) in G
- Choose $a_a, a_b$ in $\{0,1,2\}$ s.t $a_a \neq a_b$ at random and for all $v \neq a,b$ set $a_a = 2$.
- Output $\text{SIM} = (\text{Enc}(r_v, a_v), (a, b), r_a, r_b )$

Claim: $\text{SIM} \approx c \text{ View}_{(P,V)}(G)$
Computational ZK: Simulation for any Verifier $V^*$

Simulator $SIM$ on input $G$ and verifier $V^*$:

- Fix random tape $\omega$ for $V^*$
- For $i = 1$ to $|E|^2$
  - Choose random edge $(a, b)$ and generate vector $com = Enc(r_v, a_v)$ as in honest verifier simulation.
  - Run $V^*(com; \omega)$ to obtain challenge $(a^*, b^*)$;
    if $(a^*, b^*) = (a, b)$, then output transcript as in honest verifier case, transcript $= Enc(r_v, a_v), (a, b), r_a, r_b$

If all iterations fail, output $\perp$.

Theorem: If $Enc$ is semantically secure with respect to non-uniform adversaries, then

Claim 1: $\forall G, \pi$ (a true coloring) : $\text{prob}[\perp \text{ output}] = \text{neg}(|E|)$

Claim 2: if $\perp$ is not output, then simulated-view $\approx_c$ real-view
**Simulation for any Verifier V**

**Claim 1**: \( \forall G, \pi \) (a true coloring) : \( \text{prob}[\bot \text{ output}] = \text{neg}(|E|) \)

**Proof**: By Hybrid argument.

Hybrid 1 \((G)\): Fix random tape \( \omega \) for \( V^* \)

For \( i = 1 \) to \(|E|^2\):
1. Choose random edge \((a, b)\)
2. Let \( \text{com} = \text{vector of encrypted colored vertices s.t all vertices } v \text{ are colored by } \alpha(v) \text{ each with randomness } r_a(v) \) [as prover does in real protocol].
3. Run \( V^*(\text{com}) = (a^*, b^*) \). If \((a^*, b^*) = (a, b)\), output transcript \((\text{com}, (a^*, b^*), r_a, r_b)\)
   If all iterations fail, output \( \bot \).

**Lemma 1**: Hybrid 1 and View \((P, V^*) (G)\) are statistically close (chance of \( \bot \) is negligible)

**Lemma 2**: Hybrid 1 and SIM\((G,V^*)\) are computationally indistinguishable if Enc is semantically secure
Examples of NP-assertions

• graph G is 3-colorable

• graph G has a traveling salesman tour of cost C,

... 

• NP=Given encrypted inputs E(x) and program PROG, y=PROG(x)....
Many, Many Applications:

- Can prove properties about $m$ without ever revealing $m$, only $E(m)$

- Can prove relationships between $m_1$ and $m_2$ never revealing either one, only $E(m_1)$ and $E(m_2)$.

For example: $L = \{(C_1, C_2): \text{there exists } r_1, r_2, M \text{ s.t. } C_1 = E_1(r_1, M) \text{ and } C_2 = E_2(r_2, M) \}$ is in NP

Generally: A tool to enforce honest behavior without forcing to reveal information.
**General Cryptographic Importance**

- Proving correctness of protocols is complex even if users are honest; If users deviate from protocol in arbitrary ways, almost impossible in a case-by-case manner, need tools and framework to prove correctness.
- Proof of proper behavior is fundamental tool for design of secure protocols.
- **Zero Knowledge Proofs** enable automatic conversion of any protocol proven secure against honest-but-curious adversaries to protocol secure against deviating adversaries.
Today

• Computational Zero Knowledge

• Every problem in NP has a Computational Zero Knowledge Interactive Proofs

• Is IP greater than NP?
  – Today: examples unknown to be in NP
  – Complexity class IP=PSPACE

• Applications
Zero Knowledge Proof

Prove to color blind Bob that colors exist

Claim: there are 2 colors on this page, red top

Bob tosses coin
If Heads keep red on top.
Tails flip to green on top.

Bob color blind

Bob sends resulting page
Alice names color on top

Do It Again
Chance that Alice is correct twice = \( \frac{1}{4} \)

if Alice is wrong, Reject the claim

If Alice is correct
\( \frac{1}{2} \) chance that its just luck

Alice names color on top
Zero Knowledge Proof

Prove to color blind bob that colors exist

Claim: there are 2 colors on this page, red top

Completeness: if there are 2 colors, Bob will always accept

Soundness: if there is only 1 color, then Probability that after 100 iterations Bob will reject > $1-1/2^{100}$
Zero Knowledge Proof
Prove to color blind bob that colors exist

Bob tosses coin to decide if to flip page:
Heads keep red on top.
Tails flip to green on top.

Bob sends resulting page

Alice names color on top = \( \text{coin}_1 \)
Bob sends resulting page
Alice names color on top = \( \text{coin}_2 \)

Bob color blind

Claims there are 2 colors on this page

View of Bob = \(((\text{Page, coin})\)\)
Example: $G_1$ is NOT isomorphic to $G_2$

Shortest classical proof:
$\approx$ exponential $n!$
But can convince with an efficient interactive proof
Graph Non-Isomorphism (Non-ISO) in $IP$

**Prover**

if $H$ isomorphic to $G_0$
then $b = 0$, else $b = 1$

**Verifier**

flip coin $c \in \{0,1\}$; pick random $\gamma$

Output ACCEPT iff $b = c$

**Completeness:** if $(G_0, G_1) \in \text{Non-ISO}$, then $$\text{Prob}[(P, V)[(G_0, G_1)] = \text{accept}] = 1$$

**Soundness:** if $(G_0, G_1) \in \text{ISO}$, then $$\text{Prob}[(P, V)[(G_0, G_1)] = \text{accept}] \leq 1/2$$
GNI Interactive Proof

• completeness:
  – if $G_0$ not isomorphic to $G_1$ then $H$ is isomorphic to exactly one of $(G_0, G_1)$
  – prover will choose correct $b=c$

• soundness:
  if $G_0$ is isomorphic to $G_1$ then prover sees same distribution on $H$ for $c = 0$, $c = 1$
  which no information on $c$ ⇒
  $\Prob[\text{prover } P^\ast \text{ outputs } b=c] \leq 1/2$
Honest Verifier Zero Knowledge

This is obviously honest verifier zero-knowledge (when the graphs are isomorphic):
--All the verifier gets is the coin c he tossed.

But, is it zero-knowledge for all verifiers?
- No. V can use P to find out if H is isomorphic to $G_0$ or isomorphic to $G_1$.

- Instead, the Verifier proves in ZK that he knows $\gamma$ s.t either $H=\gamma(G_0)$ or $H=\gamma(G_1)$
Applications

✓ Preventing Identity Theft

• Secure Protocols

• Proving properties of secrets:
  – Commit + prove
Recent Uses of Zero Knowledge Proofs

2014  Zero Knowledge and Nuclear Disarmament: projects at Princeton and MIT [Barak et al]

2015 Zero Knowledge and Forensics [Naor et al]

Zero Cash, crypto currency which protects the privacy of transactions [BenSasson, Chiesa, Tromer et al]

2017 Proof of “compliance” of FISA with secret laws
Recent Uses of Zero Knowledge Proofs

2014 Zero Knowledge and Nuclear Disarmament: projects

2015 Zero Cash, crypto currency which protects the privacy of transactions

Tromer et al.

2016

2017 Proof of "compliance" of FISA with secret laws

The 1st ZKProof Standards Workshop
10-11th May, 2018

ZKProof

Zero Knowledge Proofs are a cutting edge cryptographic tool that is starting to see adoption. This breakthrough technology forms the basis of several cryptographic applications, improving the trade-offs between data privacy and integrity. Zero Knowledge Proofs allow a prover to convince a verifier that some computational statement is correct without revealing any information except the veracity of the statement.

ZKProof.org is an open initiative of industry and academia to standardize the use of zero knowledge proofs. We are planning several workshops to standardize the security, implementation, applications and all other related aspects of this technology. The first workshop will take place in Boston in mid May and will bring together for the first time academic and industry experts in the field.
**ZK Arguments**

Prover $P$

PPT

Verifier $V$

**Completeness:** there exists $P$ such that

if $x \in L$, then $\text{prob}((P,V)[x] = \text{accepts}) \geq 2/3$

**Soundness’:** if $x \notin L$, then for all probabilistic polynomial time provers $P^*$, $\text{Prob}((P,V)[x] = \text{accepts}) < 1/3$

**Theorem:** Perfect ZK Arguments exist for all NP if one way functions exist [OWF used for soundness’]
Basic Questions about Zero Knowledge(I)

• Q1: Sequential Compositions
• Q2: Parallel Compositions?
  - Not always (artificial counter example)
  - Known natural examples cannot be proved using black box simulation
  - A: Weaken definition of ZK to Witness Hiding [FeSh87]