Zero-Knowledge Proofs - II

CS 601.642/442 Modern Cryptography

Fall 2018
If one-way permutations exist, then every language in $\text{NP}$ has a zero-knowledge interactive proof.

- The assumption can in fact be relaxed to just one-way functions
- Think: How to prove the theorem?
- Construct ZK proof for every $\text{NP}$ language?
- Not efficient!
Proof Strategy:

**Step 1:** Construct a ZK proof for an \textbf{NP}-complete language. We will consider \textit{Graph 3-Coloring}: language of all graphs whose vertices can be colored using only three colors s.t. no two connected vertices have the same color.

**Step 2:** To construct ZK proof for any \textbf{NP} language \( L \), do the following:

- Given instance \( x \) and witness \( w \), \( P \) and \( V \) reduce \( x \) into an instance \( x' \) of Graph 3-coloring using Cook’s (deterministic) reduction.
- \( P \) also applies the reduction to witness \( w \) to obtain witness \( w' \) for \( x' \).
- Now, \( P \) and \( V \) can run the ZK proof from Step 1 on common input \( x' \).
Consider graph \( G = (V, E) \). Let \( C \) be a 3-coloring of \( V \) given to \( P \).

\( P \) picks a random permutation \( \pi \) over colors \( \{1, 2, 3\} \) and colors \( G \) according to \( \pi(C) \). It hides each vertex in \( V \) inside a locked box.

\( V \) picks a random edge \((u, v)\) in \( E \).

\( P \) opens the boxes corresponding to \( u, v \). \( V \) accepts if \( u \) and \( v \) have different colors, and rejects otherwise.

The above process is repeated \( n|E| \) times.

**Intuition for Soundness:** In each iteration, cheating prover is caught with probability \( \frac{1}{|E|} \).

**Intuition for ZK:** In each iteration, \( V \) only sees something it knew before – two random (but different) colors.
Towards ZK Proof for Graph 3-Coloring

- To “digitze” 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 Schemes

- Digital analogue of locked boxes

- Two phases:
  - **Commit phase**: Sender locks a value $v$ inside a box
  - **Open phase**: Sender unlocks the box and reveals $v$

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

Definition (Commitment)

A randomized polynomial-time algorithm $\text{Com}$ is called a commitment scheme for $n$-bit strings if it satisfies the following properties:

- **Binding:** For all $v_0, v_1 \in \{0, 1\}^n$ and $r_0, r_1 \in \{0, 1\}^n$, it holds that $\text{Com}(v_0; r_0) \neq \text{Com}(v_1; r_1)$

- **Hiding:** For every non-uniform PPT distinguisher $D$, there exists a negligible function $\nu(\cdot)$ s.t. for every $v_0, v_1 \in \{0, 1\}^n$, $D$ distinguishes between the following distributions with probability at most $\nu(n)$
  
  - $\{ r \leftarrow \{0, 1\}^n : \text{Com}(v_0; r) \}$
  - $\{ r \leftarrow \{0, 1\}^n : \text{Com}(v_1; r) \}$
Commitment Schemes: Remarks

- The previous definition only guarantees hiding for one commitment

- **Multi-value Hiding:** Just like encryption, we can define multi-value hiding property for commitment schemes

- Using hybrid argument (as for public-key encryption), we can prove that any commitment scheme satisfies multi-value hiding

- **Corollary:** One-bit commitment implies string commitment
Construction of Bit Commitments

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

**Commit phase:** Sender computes $\text{Com}(b; r) = f(r), b \oplus h(r)$. Let $C$ denote the commitment.

**Open phase:** Sender reveals $(b, r)$. Receiver accepts if $C = (f(r), b \oplus h(r))$, and rejects otherwise.

**Security:**

- Binding follows from construction since $f$ is a permutation.
- Hiding follows in the same manner as IND-CPA security of public-key encryption scheme constructed from trapdoor permutations.
ZK Proof for Graph 3-Coloring

Common Input: $G = (V, E)$, where $|V| = n$

$P$’s witness: Colors $\text{color}_1, \ldots, \text{color}_n \in \{1, 2, 3\}$

Protocol $(P, V)$: Repeat the following procedure $n|E|$ times using fresh randomness

$P \rightarrow V$: $P$ chooses a random permutation $\pi$ over $\{1, 2, 3\}$. For every $i \in [n]$, it computes $C_i = \text{Com}(\widetilde{\text{color}}_i)$ where $\widetilde{\text{color}}_i = \pi(\text{color}_i)$. It sends $(C_1, \ldots, C_n)$ to $V$

$V \rightarrow P$: $V$ chooses a random edge $(i, j) \in E$ and sends it to $P$

$P \rightarrow V$: Prover opens $C_i$ and $C_j$ to reveal $(\widetilde{\text{color}}_i, \widetilde{\text{color}}_j)$

$V$: If the openings of $C_i, C_j$ are valid and $\widetilde{\text{color}}_i \neq \widetilde{\text{color}}_j$, then $V$ accepts the proof. Otherwise, it rejects.
Proof of Soundness

- If $G$ is not 3-colorable, then for any coloring $\text{color}_1, \ldots, \text{color}_n$, there exists at least one edge which has the same colors on both endpoints.

- From the binding property of $\text{Com}$, it follows that $C_1, \ldots, C_n$ have unique openings $\tilde{\text{color}}_1, \ldots, \tilde{\text{color}}_n$.

- Combining the above, let $(i^*, j^*) \in E$ be s.t. $\tilde{\text{color}}_{i^*} = \tilde{\text{color}}_{j^*}$.

- Then, with probability $\frac{1}{|E|}$, $V$ chooses $i = i^*, j = j^*$ and catches $P$.

- In $n|E|$ independent repetitions, $P$ successfully cheats in all repetitions with probability at most:

$$
\left(1 - \frac{1}{|E|}\right)^{n|E|} \approx e^{-n}
$$
Proving Zero Knowledge: Strategy

- Will prove that a single iteration of \((P, V)\) is zero knowledge
- For the full protocol, use the following (read proof online):

**Theorem**

Sequential repetition of any ZK protocol is also ZK

- To prove that a single iteration of \((P, V)\) is ZK, we need to do the following:
  - Construct a Simulator \(S\) for every PPT \(V^*\)
  - Prove that expected runtime of \(S\) is polynomial
  - Prove that the output distribution of \(S\) is correct (i.e., indistinguishable from real execution)
- Intuition for proving ZK for a single iteration: \(V\) only sees two random colors. Hiding property of Com guarantees that everything else remains hidden from \(V\).
Proving Zero Knowledge: Simulator

**Simulator** \( S(x = G, z) \):

- Choose a random edge \((i', j') \leftarrow E\) and pick random colors \(\text{color}_{i'}, \text{color}_{j'} \leftarrow \{1, 2, 3\}\) s.t. \(\text{color}_{i'} \neq \text{color}_{j'}\). For every other \(k \in [n] \setminus \{i', j'\}\), set \(\text{color}_k = 1\).
- For every \(\ell \in [n]\), compute \(C_\ell = \text{Com}(\text{color}_\ell)\).
- Emulate execution of \(V^*(x, z)\) by feeding it \((C_1, \ldots, C_n)\). Let \((i, j)\) denote its response.
- If \((i, j) = (i', j')\), then feed the openings of \(C_i, C_j\) to \(V^*\) and output its view. Otherwise, restart the above procedure, at most \(n|E|\) times.
- If simulation has not succeeded after \(n|E|\) attempts, then output \(\text{fail}\).
Correctness of Simulation

Hybrid Experiments:

- $H_0$: Real execution
- $H_1$: Hybrid simulator $S'$ that acts like the real prover (using witness $\text{color}_1, \ldots, \text{color}_n$), except that it also chooses $(i', j') \leftarrow E$ at random and if $(i', j') \neq (i, j)$, then it outputs fail
- $H_2$: Simulator $S$
Correctness of Simulation (contd.)

- \( H_0 \approx H_1 \): If \( S' \) does not output \texttt{fail}, then \( H_0 \) and \( H_1 \) are identical. Since \((i,j)\) and \((i',j')\) are independently chosen, \( S' \) fails with probability at most:
  \[
  \left(1 - \frac{1}{|E|}\right)^{|E|} \approx e^{-n}
  \]
  Therefore, \( H_0 \) and \( H_1 \) are statistically indistinguishable

- \( H_1 \approx H_2 \): The only difference between \( H_1 \) and \( H_2 \) is that for all \( k \in [n] \setminus \{i', j'\} \), \( C_k \) is a commitment to \( \pi(\text{color}_k) \) in \( H_1 \) and a commitment to \( 1 \) in \( H_2 \). Then, from the multi-value hiding property of \( \text{Com} \), it follows that \( H_1 \approx H_2 \)
Additional Reading

- Zero-knowledge Proofs for Nuclear Disarmament [Glaser-Barak-Goldston’14]
- Non-black-box Simulation [Barak’01]
- Concurrent Composition of Zero-Knowledge Proofs [Dwork-Naor-Sahai’98, Richardson-Kilian’99, Kilian-Petrunk’01, Prabhakaran-Rosen-Sahai’02]
- Non-malleable Commitments and ZK Proofs [Dolev-Dwork-Naor’91]