ARIEL UNIVERSITY

אוניברסיטת אריאל בשומרון

Foundations of Modern Cryptography

Edward A. Hirsch

https://edwardahirsch.github.io/edwardahirsch

Neapolis University Pafos

Lecture 8: December 5, 2024

Lecture Plan

- Zero-knowledge proofs.

If the screen seems frozen and I do not respond,
please call me in Telegram.

Task: Zero-Knowledge Proof

Alice

x, proof that $x \in L$

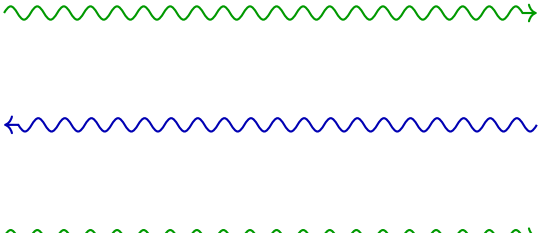
Bob

x

Task: Zero-Knowledge Proof

Alice

x, proof that $x \in L$



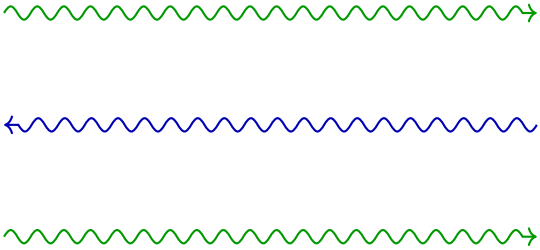
Bob

x

Task: Zero-Knowledge Proof

Alice

x, proof that $x \in L$



Bob

x

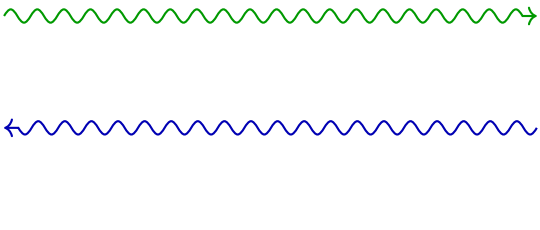
convinced that $x \in L$

Pictures courtesy AI Emojis Generator

Task: Zero-Knowledge Proof

Alice

x, proof that $x \in L$



Bob

x

convinced that $x \in L$

Bob gets convinced iff $x \in L$ (with certain probability of error).

Bob does not learn from this protocol about Alice's proof more than the fact $x \in L$.

Pictures courtesy AI Emojis Generator

Task: Zero-Knowledge Proof

Alice

x, proof that $x \in L$

Bob

x

convinced that $x \in L$

Bob gets convinced iff $x \in L$ (with certain probability of error).
Bob does not learn from this protocol about Alice's proof more than the fact $x \in L$.

Strong ZK: Bob also gets convinced that Alice indeed knows some proof that Bob can verify.

Pictures courtesy AI Emojis Generator

Zero-Knowledge Proofs: Definition

Definition

Language L has a computational zero-knowledge proof ($L \in \mathbf{CZK}$) if there is a protocol between prover $P(x)$ and polynomial-time bounded randomized verifier $V(x)$ s.t.

(Completeness) There are specific P, V such that $(P, \boldsymbol{V})(x)$ always accepts $x \in L$,

Zero-Knowledge Proofs: Definition

Definition

Language L has a computational zero-knowledge proof ($L \in \mathbf{CZK}$) if there is a protocol between prover $P(x)$ and polynomial-time bounded randomized verifier $V(x)$ s.t.

(Completeness) There are specific P, V such that $(P, \boldsymbol{V})(x)$ always accepts $x \in L$,

(Soundness) This V accepts $x \notin L$ with prob. $< \frac{1}{2}$ (for any P'),

Zero-Knowledge Proofs: Definition

Definition

Language L has a computational zero-knowledge proof ($L \in \mathbf{CZK}$) if there is a protocol between prover $P(x)$ and polynomial-time bounded randomized verifier $V(x)$ s.t.

(Completeness) There are specific P, V such that $(P, \boldsymbol{V})(x)$ always accepts $x \in L$,

(Soundness) This V accepts $x \notin L$ with prob. $< \frac{1}{2}$ (for any P'),

(CZK) and for every p.-t. b.r. V' (outputting a lot!) there is an oblivious $\tilde{V}$ s.t. $\forall x \in L$ the distributions

$$\{V'_r(x, \text{protocol}(P, V'_r)(x))\}_{r \in U} \text{ and } \{\tilde{V}_t(x)\}_{t \in U}$$

are computationally indistinguishable.

Remark

We can replace the output of $V', \tilde{V}$ by the transcript of the protocol (as viewed by the verifier).

Zero-Knowledge Proofs: Definition

Definition

Language L has a computational zero-knowledge proof ($L \in \mathbf{CZK}$) if there is a protocol between prover $P(x)$ and polynomial-time bounded randomized verifier $V(x)$ s.t.

(Completeness) There are specific P, V such that $(P, \boldsymbol{V})(x)$ always accepts $x \in L$,

(Soundness) This V accepts $x \notin L$ with prob. $< \frac{1}{2}$ (for any P'),

(CZK) and for every p.-t. b.r. V' (outputting a lot!) there is an oblivious $\tilde{V}$ s.t. $\forall x \in L$ the distributions

$$\{V'_r(x, \text{protocol}(P, V'_r)(x))\}_{r \in U} \text{ and } \{\tilde{V}_t(x)\}_{t \in U}$$

are computationally indistinguishable.

Remark

We can replace the output of $V', \tilde{V}$ by the transcript of the protocol (as viewed by the verifier).

Remark

There are also other classes: *statistical* and *perfect* zero-knowledge. We don't need them.

Zero-knowledge proofs for **NP**

Theorem

If one-way functions exist, then **NP** $\subseteq$ **CZK**.

- Consider graph G, assume that P knows its proper 3-coloring.

Zero-knowledge proofs for **NP**

Theorem

If one-way functions exist, then **NP** $\subseteq$ **CZK**.

- Consider graph G, assume that P knows its proper 3-coloring.
- P randomly permuts the colors and, for every vertex v, sends its commitment to color c_v to V.

Zero-knowledge proofs for **NP**

Theorem

If one-way functions exist, then $\mathbf{NP} \subseteq \mathbf{CZK}$.

- Consider graph G, assume that P knows its proper 3-coloring.
- P randomly permuts the colors and, for every vertex v, sends its commitment to color c_v to V.
- V randomly selects an edge (u, w) and sends it to P.

Zero-knowledge proofs for **NP**

Theorem

If one-way functions exist, then **NP** $\subseteq$ **CZK**.

- Consider graph G, assume that P knows its proper 3-coloring.
- P randomly permuts the colors and, for every vertex v, sends its commitment to color c_v to V.
- V randomly selects an edge (u, w) and sends it to P.
- P sends the keys for c_u and c_w to V.

Zero-knowledge proofs for **NP**

Theorem

If one-way functions exist, then **NP** $\subseteq$ **CZK**.

- Consider graph G, assume that P knows its proper 3-coloring.
- P randomly permuts the colors and, for every vertex v, sends its commitment to color c_v to V.
- V randomly selects an edge (u, w) and sends it to P.
- P sends the keys for c_u and c_w to V.
- V accepts iff $c_u \neq c_w$ and the commitment protocol succeeds.

Zero-knowledge proofs for **NP**

Theorem

If one-way functions exist, then **NP** $\subseteq$ **CZK**.

- Consider graph G, assume that P knows its proper 3-coloring.
- P randomly permuts the colors and, for every vertex v, sends its commitment to color c_v to V.
- V randomly selects an edge (u, w) and sends it to P.
- P sends the keys for c_u and c_w to V.
- V accepts iff $c_u \neq c_w$ and the commitment protocol succeeds.

Exercise

This protocol's success (reject G if it's not 3-colorable) is $\geqslant 1/|E|$. If we want to reduce the probability of error from $1 - 1/|E|$ to $1/2$ or even $1/2^n$, we can repeat it many times (both P and V use new randomness). Prove that still no knowledge is leaked.

Zero-knowledge proofs for **NP**

Theorem

If one-way functions exist, then $\mathbf{NP} \subseteq \mathbf{CZK}$.

- Consider graph G, assume that P knows its proper 3-coloring.
- P randomly permuts the colors and, for every vertex v, sends its commitment to color c_v to V.
- V randomly selects an edge (u, w) and sends it to P.
- P sends the keys for c_u and c_w to V.
- V accepts iff $c_u \neq c_w$ and the commitment protocol succeeds.

Exercise

This protocol's success (reject G if it's not 3-colorable) is $\geqslant 1/|E|$. If we want to reduce the probability of error from $1 - 1/|E|$ to $1/2$ or even $1/2^n$, we can repeat it many times (both P and V use new randomness). Prove that still no knowledge is leaked.

Remark

It is also a strong CZK proof: given access to P (for fixed G, c) as an oracle, one can reconstruct (some) coloring in polynomial time, thus P "knows" a coloring.

CZK protocol for 3-coloring: Why it works?

- The oblivious verifier $\tilde{V}$ behaves as V' and simulates P by itself using a random coloring c'.

CZK protocol for 3-coloring: Why it works?

- The oblivious verifier $\tilde{V}$ behaves as V' and simulates P by itself using a random coloring c'.
- The probability that it fails because of wrong coloring is $\frac{1}{3}$.

CZK protocol for 3-coloring: Why it works?

- The oblivious verifier $\tilde{V}$ behaves as V' and simulates P by itself using a random coloring c'.
- The probability that it fails because of wrong coloring is $\frac{1}{3} \leqslant \frac{1}{2}$.

CZK protocol for 3-coloring: Why it works?

- The oblivious verifier $\tilde{V}$ behaves as V' and simulates P by itself using a random coloring c'.
- The probability that it fails because of wrong coloring is $\frac{1}{3} \leqslant \frac{1}{2}$.
  - For specific (u, w), the prob. to output it changes by $\leqslant \frac{1}{2|E|}$.

CZK protocol for 3-coloring: Why it works?

- The oblivious verifier $\tilde{V}$ behaves as V' and simulates P by itself using a random coloring c'.
- The probability that it fails because of wrong coloring is $\frac{1}{3} \leqslant \frac{1}{2}$.
  - For specific (u, w), the prob. to output it changes by $\leqslant \frac{1}{2|E|}$.
  - Otherwise we distinguish the commitments for two different sequences.

CZK protocol for 3-coloring: Why it works?

- The oblivious verifier $\tilde{V}$ behaves as V' and simulates P by itself using a random coloring c'.
- The probability that it fails because of wrong coloring is $\frac{1}{3} \leqslant \frac{1}{2}$.
  - For specific (u, w), the prob. to output it changes by $\leqslant \frac{1}{2|E|}$.
  - Otherwise we distinguish the commitments for two different sequences.
  - For specific (u, w) consider the 3^{n-1} random colorings c' with $c'(u) = c'(w)$.

CZK protocol for 3-coloring: Why it works?

- The oblivious verifier $\tilde{V}$ behaves as V' and simulates P by itself using a random coloring c'.
- The probability that it fails because of wrong coloring is $\frac{1}{3} \leqslant \frac{1}{2}$.
  - For specific (u, w), the prob. to output it changes by $\leqslant \frac{1}{2|E|}$.
  - Otherwise we distinguish the commitments for two different sequences.
  - For specific (u, w) consider the 3^{n-1} random colorings c' with $c'(u) = c'(w)$.
  - The prob. to choose (u, w) for a specific c' is like for $V' \quad + \frac{1}{2|E|}$.

CZK protocol for 3-coloring: Why it works?

- The oblivious verifier $\tilde{V}$ behaves as V' and simulates P by itself using a random coloring c'.
- The probability that it fails because of wrong coloring is $\frac{1}{3} \leqslant \frac{1}{2}$.
  - For specific (u, w), the prob. to output it changes by $\leqslant \frac{1}{2|E|}$.
  - Otherwise we distinguish the commitments for two different sequences.
  - For specific (u, w) consider the 3^{n-1} random colorings c' with $c'(u) = c'(w)$.
  - The prob. to choose (u, w) for a specific c' is like for V' $+ \frac{1}{2|E|}$.
  - Total: $\frac{1}{3}$ for fail in V' and $\frac{1}{6} = \frac{1}{2|E|} \times 3^{n-1} \times |E| \times \frac{1}{3^n}$ for a different choice of the edge.

CZK protocol for 3-coloring: Why it works?

- The oblivious verifier $\tilde{V}$ behaves as V' and simulates P by itself using a random coloring c'.
- The probability that it fails because of wrong coloring is $\frac{1}{3} \leqslant \frac{1}{2}$.
  - For specific (u, w), the prob. to output it changes by $\leqslant \frac{1}{2|E|}$.
  - Otherwise we distinguish the commitments for two different sequences.
  - For specific (u, w) consider the 3^{n-1} random colorings c' with $c'(u) = c'(w)$.
  - The prob. to choose (u, w) for a specific c' is like for $V' \quad + \frac{1}{2|E|}$.
  - Total: $\frac{1}{3}$ for fail in V' and $\frac{1}{6} = \frac{1}{2|E|} \times 3^{n-1} \times |E| \times \frac{1}{3^n}$ for a different choice of the edge.
- If it does not fail, it's results (even transcripts) are indistinguishable from that of V'.
  - Intuitively clear, and you don't want to see the formal proof.

Takeout

- $\mathbf{NP} \subseteq \mathbf{CZK}$.

Takeout

- **NP** $\subseteq$ **CZK**.

Coming next:

- *How ZK helps to force malicious participants to be semi-honest.*
- *(maybe) Exercises and Repeat.*
- *Blockchains.*