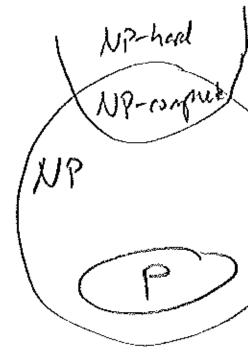
CIS 700 Lecture 21: Zero-Knowledge Proofs



NP: Class of decision problems w/ poly-time verifiable proofs
"witness"

$L = \{x \in \{0,1\}^n : \exists w \in \{0,1\}^n \ V(x,w) = 1\}$

$P_{\text{prover}} \xrightarrow{w} V_{\text{verifier}}$

Def "proof system" for lang. L:
Poly-time "verifier" alg. s.t.

- completeness "true assertions have proofs"
  $x \in L \Rightarrow \exists w \quad |w| \le poly(|x|) \quad V(x, w) = accept$
- soundness "false assertions have no proofs"
  $x \in L \Rightarrow \forall w' \quad V(x, w') = reject$

3 Coloring:

3-COL: $\{G : G \text{ is 3-colorable}\}$ 3-colorable graph: $\exists$ coloring of vertices s.t. $\forall$ edge (u,v) color$(u) \neq$ color(v)

3-COL $\in$ NP:

$P \xrightarrow[\text{coloring}]{\{v_i \to c_i\}} V$

Interactive Probabilistic Proofs

NP $\subseteq$ IP
IP = PSPACE

- completeness
  $x \in L \Rightarrow \Pr[P(x,w) \overset{?}{\leftrightarrows} V(x) = 1] \ge 1 - \varepsilon(n)$
- soundness
  $x \notin L \Rightarrow \forall w' \ \Pr[P(x,w') \overset{?}{\leftrightarrows} V(x) = 1] \le \varepsilon(n)$

IP for 3COL:

$P(G, w) \xrightarrow{\text{commit}(c(v_1)) \ \text{commit}(c(v_2)) \ldots}$

$\xleftarrow{e = (v_i, v_j)} V(G)$

$\xrightarrow{\text{open}(\text{commit}(c(v_i)))}$
open(commit$(c(v_j))$)

G n vertices
m edges

check $c(v_i) \neq c(v_j)$

$\downarrow$ 100m trys

w.h.p. reveal all of $c(v_i)$

- Complete: w 3-coloring
  $\Rightarrow c(v_i) \neq c(v_j)$
  $\forall$ edges (v_i, v_j)
- Soundness: G not 3-colorable
  $\Rightarrow \exists$ edge (v_i, v_j)
  s.t. $c(v_i) = c(v_j)$

$\Pr(\text{check fails}) \ge \frac{1}{m}$

$\Pr(\text{never fail check}) = \left(1 - \frac{1}{m}\right)^{100m}$

$\sim e^{-100}$

Zero Knowledge Interactive Proof

$$\begin{array}{ccc} P & \xrightarrow{p_1} & V \\ X, \omega & \xleftarrow{v_1} & X \\ r_p \text{ coin} & \xrightarrow{p_2} & r_V \text{ coins} \\ & \xleftarrow{v_2} & \\ & \vdots & \end{array}$$

<u>Def</u> (P,V) (honest-verifier) zero-knowledge if

$$\exists S \text{ s.t. } \forall x \in L \quad \underbrace{\text{View}_V}_{\text{transcript } V \text{ sees of proof}}(P(x,\omega) \rightleftarrows V(x)) \underbrace{\approx}_{\text{computationally indistinguishable}} S(x)$$

(P,V) zero-knowledge

$$\forall V' \; \exists S' \; \forall x \in L \quad \text{View}_{V'}(P(x,\omega) \rightleftarrows V'(x)) \sim S'(x)$$

V might try to cheat $\Rightarrow$ simulator S depends on V

ZKP for 3COL:

$$\begin{array}{ccc} P(G,\omega) & \xrightarrow{\text{commit}(\pi(c(v_1))),\ \text{commit}(\pi(c(v_2)))\ldots} & V(G) \\ \pi \text{ random permutation of colors} & \xleftarrow{e = (v_i, v_j)} & \\ & \xrightarrow{\text{open}(\pi(c(v_i)))\ \text{open}(\pi(c(v_j)))} & \text{check } \pi(c(v_i)) \neq \pi(c(v_j)) \\ & & \text{repeat } 100m \text{ times} \end{array}$$

- completeness: same as before
- soundness: same as before
- zero knowledge:
  - simulate: Guess edge $e = (v_i, v_j)$ that will be queried by V
    - If correct, check passes $\Rightarrow$ include in transcript
    - incorrect, rewind (don't include in transcript

$\Pr(S$ guesses correct edge $= \frac{1}{m}) \Rightarrow 100m^2$ rounds until simulated protocol

3

Graph Isomorphism

$L = \{(G,H) : \exists \pi \; H = \pi(G)\}$

$$P(G,H,\omega) \xrightarrow{G' = \sigma(G)} V(G,H)$$

$$\xleftarrow{c \in_R \{0,1\}}$$

$$\xrightarrow[c=1:\ \sigma \circ \pi^{-1}]{\text{if } c=0:\ \sigma}$$

if $c=0$:
verify $G' = \gamma G$

if $c=1$:
verify $G' = \gamma H$

repeat 100x

completeness:
G, H isomorphic: check always succeeds

soundness:
G, H not isomorphic:
check only succeeds if $c = 0$
$\Rightarrow \Pr(\text{success}) = \frac{1}{2}$

Zero-knowledge:
Simulator:

$$S(G,H) \xrightarrow{G' = \begin{cases} \gamma G & \text{if } c'=0 \\ \gamma H & \text{if } c'=1 \end{cases}} V^*(G,H)$$

$$\xleftarrow{c}$$

$$\xleftrightarrow[\text{else } \sigma]{\text{if } c \neq c' \text{ rewind}}$$

$\Pr(\text{success}) = \frac{1}{2} \Rightarrow \sim 2 \cdot 100$ steps to transcript

Thm Every NP-language has ZKIP

Pf 3-coloring is NP-complete.
Given x construct G s.t. G 3-colorable $\Leftrightarrow x \in L$,
Prove G 3-colorable

Zero-Knowledge Proof of Knowledge for Discrete Log (Schnorr)

"Proof of knowledge": P "knows" a witness (replaces soundness)

Def "knowledge soundness w/ error δ"

$\forall$ prover P' $\forall x$

If P' satisfies $\Pr[\mathrm{View}_V(P', V(x,r)) = \text{accept}] > \delta + \rho$

$\exists$ algorithm $\mathcal{E}$ (knowledge extractor) running in time poly in $\frac{1}{\rho}$

$\mathcal{E}(x) = w$ w.p. $\geq \frac{1}{2}$

Schnorr proof of knowledge for discrete log

G of order q g generator

$h = g^x$

P		V
x, (g,h)	$\xrightarrow{a = g^r}$	(g,h)
$r \in \mathbb{Z}_q$	$\xleftarrow{b}$	$b \in_R \mathbb{Z}_q$
	$\xrightarrow{c = r + xb}$	$ah^b \overset{?}{=} g^c$

completeness: ✓

proof of knowledge: P runs protocol twice w/ same a (rewinding)

$(a,b,c), (a,b',c')$

$b \neq b'$ $c \neq c'$

$ah^b = g^c$ $ah^{b'} = g^{c'}$

$h^{b-b'} = g^{c-c'}$ $x = \frac{c-c'}{b-b'} \bmod q$

honest-verifier zero knowledge:

simulator: $b, c \in_R \mathbb{Z}_q$

set $a = h^{-b} g^c$

Application: Identification scheme:

Observer learns nothing about secret x