Lec16.a
4/10/17

Today: • Zero-knowledge proofs (& proofs of knowledge)

• Interactive proofs

Examples
- Graph 3-colorability
- Graph isomorphism
- Hamiltonian graph

• Any NP problem has a ZK proof.

Cryptographic applications
• Identification scheme (Schnorr)
• Fiat-Shamir paradigm.

Zero Knowledge Proofs [Goldwasser-Micali-Rackoff]

These are proofs that reveal no information beyond the validity of the statement.

Is that possible? Every proof is information!

Interactive Proofs

Proofs that are interactive use randomness common input (statement to be proved)

$P \qquad x \qquad V$

$\longrightarrow$

$\longleftarrow$

$\longrightarrow$

$$(P, V)(x) = 0/1 \quad (\text{reject}/\text{accept}).$$

P may be powerful

V is probabilistic polynomial time.

x is typically an NP statement:

$$(\exists w) \text{ s.t. } R(x, w) = 1$$

poly-size witness. poly time

Ex: $(\exists w)$ s.t. $y = g^{w} \pmod{p}$

Maybe P does not want to reveal w!

P wants to reveal no information about w (beyond $y = g^{w}$)

Interactive proof (for statement x) has the following properties:

Completeness: If x is true then V accepts.

Soundness: If x is false then V rejects with prob $\geq \underset{\varepsilon}{\underset{\shortparallel}{\text{const}}} > 0$.

Soundness amplification: Iterate the protocol t times to reduce soundness error: Prover cheats w.p. $\leq (1-\varepsilon)^t$

An iteractive proof is zero-knowledge if the verifier learns nothing else except whether x is true.

Proof-of-Knowledge: Verifier becomes convinced that P actually knows a solution.

Zero-Knowledge Interactive Proofs

Often have the following structure:

$$P \qquad\qquad\qquad V$$

$$\xrightarrow{\text{commit}}$$

$$\xleftarrow{\text{challenge}}$$

$$\xrightarrow{\text{response}}$$

Recall: Commitment scheme: (commit, open)

$c = \text{commit}(v, r)$ commit to v using randomness r

$\text{open}(c) \rightarrow (v, r)$ reveal or open commitment

hiding: seeing c gives no information about v.

binding: c can only be opened one way (ie., to one v).

Eg, Pedersen Commitment:

$$c = g^v h^r$$

g, h are known generators (DL of h base g is hard

r random.

Perfect hiding ✓

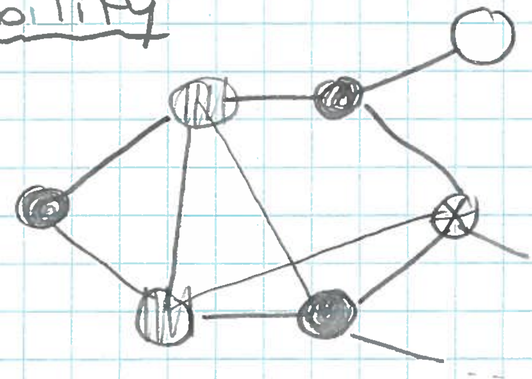
Computational binding (assuming DLP is hard)

In ZKP prover will commit to the "entire solution" but reveal only some portion chosen randomly by the verifier. ✓

$$P \xrightarrow{\text{commit}}$$
$$\xleftarrow{\text{challenge}}$$
$$\xrightarrow{\text{open}}$$

Verifier will check the portion opened

Graph 3-colorability



How can I convince you that I know a 3-coloring of vertices, without telling you **anything** about the coloring I know?

Idea: Prover will randomly permute the colors (blue, red, green).

Denote the coloring of the n vertices by $c_1, \ldots, c_n \in \{\text{blue}, \text{red}, \text{green}\}$

P $\qquad\qquad\qquad\qquad\qquad\qquad$ V

$$\xrightarrow{\text{commit}(c_1), \ldots, \text{commit}(c_n)}$$

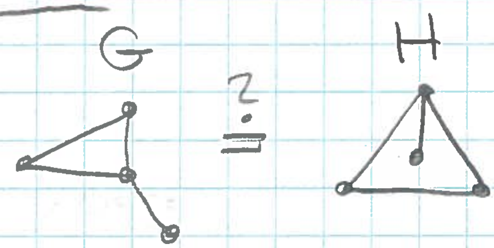
$$\xleftarrow{\;i, j\;}$$

choose random adjacent vertices i, j

$$\xrightarrow{\text{open}(c_i),\ \text{open}(c_j)}$$

accept iff $c_i \neq c_j$ and $c_i, c_j \in \{\text{blue}, \text{red}, \text{green}\}$

Graph isomorphism:



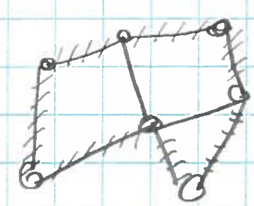
How can I prove to you that G & H are isomorphic without revealing the isomorphism?

$\pi^*: H \to G$

P		V
Choose random permutation $\pi: [n] \to [n]$	$\xrightarrow{J = \pi(G)}$
	$\xleftarrow{b}$	choose at random $b \in \{0,1\}$
	$\xrightarrow{\text{if } b=0 \text{ send } \pi}$	if $b=0$ check $J = \pi(G)$
	if $b=1$ send $\pi \circ \pi^*$	if $b=1$ check $J = \pi \circ \pi^*(H)$

Hamiltonian Cycle

\- A cycle that visits every vertex exactly once

G = 

P		V
	$\xrightarrow{J = \pi(G)}$
	$\xleftarrow{b}$	choose at random $b \in \{0,1\}$
	$\xrightarrow{\text{if } b=0 \text{ send } \pi}$
	if $b=1$ send Hamiltonian cycle in J.

Thm: Every NP statement has ZK proof.

Cryptograpic Applications: Identification Schemes

Goal: Alice wants to prove to Bob that she is the owner of a PK (i.e., knows corresponding SK) without revealing any information about SK (beyond PK).

Schnorr's ID scheme (DL-based).

p large prime

q divides $p-1$, q prime

$g \in \mathbb{Z}_p^*$ s.t. $|\langle g \rangle| = q$

SK: $x \leftarrow \mathbb{Z}_q$

PK: $y = g^x \bmod p$.

How can Alice prove to Bob that she knows x in ZK?

$$A \qquad PK = y = g^x \qquad B$$

Choose $k \leftarrow \mathbb{Z}_q$ $\quad \xrightarrow[\text{("commitment" to } k)]{a = g^k}$

$\xleftarrow[\text{"challenge"}]{c}$ $\quad$ Choose $c \leftarrow \mathbb{Z}_q$

$r = cx + k$ $\quad \xrightarrow[\text{"response"}]{r}$ $\quad$ Check $y^c \cdot a \stackrel{?}{=} g^r$

Thm: The protocol is

- Complete (If Alice knows x, and follows the protocol then Bob always accepts ✓

- Soundness & POK: If Alice succeeds in convincing Bob to accept w.p. $> \varepsilon$ then Alice "knows" x
  constant

(Equivalently, if Alice does not know x, she will be rejected w.p. $> 1-\varepsilon$)

- ZK: Bob does not learn anything about x (if he follows the protocol)

"Pf": Completeness:

$$g^r = g^{cx+k} = y^c \cdot a \quad ✓$$

Soundness & POK

Let a be Alice's first msg

Suppose Alice succeeds for c_1 & $c_2 \neq c_1$

$$\Rightarrow \begin{array}{l} y^{c_1} \cdot a = g^{r_1} \\ y^{c_2} \cdot a = g^{r_2} \end{array} \Rightarrow y^{c_1-c_2} = g^{r_1-r_2}$$

$$\Rightarrow x = \frac{r_1-r_2}{c_1-c_2} \bmod q.$$

$\Rightarrow$ Alice "knows" x.

Fiat-Shamir Paradigm

Any ID scheme (and in particular Schnorr's protocol) can be turned into a signature scheme by letting $c = \text{hash}(a, \underset{\text{msg}}{m})$

Thm: If the ID scheme is secure then the corresponding signature scheme is secure in the ROM.

ZK proofs extremely useful!

- ID schemes ✓
- signature schemes ✓
- Electronic voting
- Electronic auctions

  ⋮

- Nuclear disarmament. (Physical ZK).

[ZKP that a high quality fissile material was destroyed (without revealing its design).]