Today: - Zero-knowledge (ZK) proofs
- Interactive proofs
- Every NP-statement has ZK proof.

Example: * Graph 3-colorability
* Graph Hamiltonicity

- ZK proofs of knowledge (PoK)

Application * Identification scheme (Schnorr)
* Signature Schemes via Fiat-Shamir paradigm

Zero-Knowledge Proofs [Goldwasser-Micali-Rackoff 85]

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

Is that possible? A proof is information!

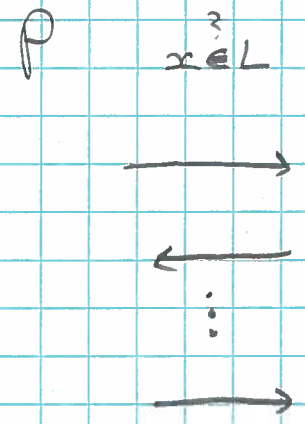
⇓

Impossible!

Idea: Change the model!

Interactive Proofs

Proofs that are interactive, and verifier uses randomness and a small probability of error is allowed.



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

* V runs in probabilistic poly-time.
* P may be powerful.

Def: An interactive proof for proving membership in a language L has the following two properties:

Completeness: $\forall x \in L \quad Pr[(P,V)(x) = 1] = 1$

Soundness: $\forall x \notin L \quad \forall$ (cheating) P^*

$$Pr[(P^*, V)(x) = 1] < \frac{1}{2}$$

Soundness amplification: Iterate the protocol sequentially t times to reduce the soundness error to 2^{-t}.

Def: An interactive proof is ZK if the verifier doesn't learn anything beyond the fact that $x \in L$.

(the verifier can simulate the conversation "in his head")

Thm [Goldwasser-Micali-Wigderson 88]:

Every NP language has a ZK proof,

assuming the existence of a commitment scheme

(w. hiding & binding properties,

which can be constructed from any OWF).

Suffices to show ZK proof for NP complete language.

We will show ZK proof for graph 3-coloring & graph Hamiltonicity (both which are NP complete)

Often ZK proofs have the following structure:

P V

commit →

← challenge

open →

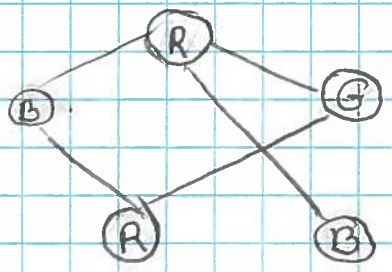
The prover commits to the "entire solution" (or "entire proof"), but reveals only to a small portion chosen randomly by the verifier.

The verifier checks the portion opened.

This portion is small enough not to reveal any information, but if accepted (with high prob) implies that (with "high" prob) the commitment can be opened consistently to other challenges as well, since the verifier does not know the challenge ahead of time.

Graph 3-Colorability

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



Idea: Prover will randomly permute the colors (Blue, Red, Green)

Denote the (permuted) coloring of the n vertices by

$c_1, \ldots c_n \in \{\text{Blue, Red, Green}\}$

P V

$com(c_1), \ldots, com(c_n)$ →

← i, j

Choose at random adjacent vertices i, j

$open(c_i), open(c_j)$ →

Accept iff $c_i \neq c_j$ and $c_i, c_j \in \{\text{Blue, Red, Green}\}$

Completeness: ✓

Soundness: Can cheat w.p. $1 - \frac{1}{m}$ (m = # of edges, at most)

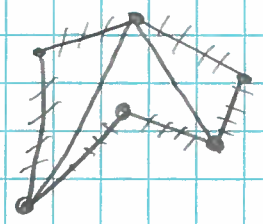
Repeat $m \cdot k$ times sequentially to get negl error (k = security parameter)

ZK: Can simulate this conversation by first choosing at random (i, j) and then choosing at random different colors c_i, c_j.

The rest of the colors can be arbitrary (eg. all blue), since these commitments won't be opened.

Also: ZK against malicious verifier.

Hamiltonian Cycle - A cycle that visits each vertex exactly once.



P by committing to each bit in the adjacency matrix

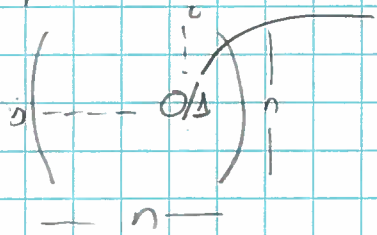
$com(G')$ ✓

$com(\pi)$ →

choose a random permutation π that permutes the vertices of G

Let $G' = \pi(G)$

Express G' as adjacency matrix

$G' =$ 

1 iff (i,j) is an edge in G'

← b

Choose at random $b \leftarrow \{0,1\}$

If $b=0$ open both commitments →

If $b=1$ open only a Hamiltonian cycle in G'

Completeness ✓

Soundness: A cheating prover can cheat w.p. $\leq \frac{1}{2}$

ZK: Can simulate this conversation by first choosing b. If $b=0$ then choose π, $G' = \pi(G)$ honestly, and open honestly. If $b=1$ then let G' be a random Hamiltonian cycle,

and commit to an arbitrary π (that has no connection to G' & G).

Note: Both ZK proofs we saw are a Proof of Knowledge, namely:

If a prover P^* convinces the verifier to accept $G \in L$ then P^* must "know" a witness for G (either a 3-col or Hamiltonian cycle).

In other words: If P^* convinces V then one can efficiently extract a witness from P^*.

This is done by rewinding P^*.

Application: Identification Schemes

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

Schnorr's ID scheme (DL-based)

Suppose: $PK = y = g^x \bmod p$, $SK = x$

where: $g \in \mathbb{Z}_p^*$ s.t. $q = |\langle g \rangle|$ is a large prime dividing $p-1$.

& x is randomly chosen in $\mathbb{Z}_q$.

[This is the distribution of keys in El-Gamal]

ID scheme

P		V
choose at random $k \leftarrow \mathbb{Z}_q$	$a = g^k$ ("commitment to k") →	
	← c ("challenge")	choose $c \leftarrow \mathbb{Z}_q$
$r = c \cdot x + k$	r ("response") →	check: $y^c \cdot a \stackrel{?}{=} g^r$

Thm: This protocol is:

Complete: (If the prover knows x & follows the protocol then he is accepted w.p. 1)

Soundness & PoK: If any P^* in convincing V to accept w.p. $\geq \underbrace{\varepsilon}_{\text{const}}$ then P^* "knows" x.

(I.e., there exists an efficient extractor alg, that extracts x from P^*)

ZK: V does not learn anything about x, beyond y if he follows the protocol

(known as honest verifier ZK)

HVZK

"Pf" of Soundness & PoK:

Fix any P^* that convinces V on input $PK=y$.

Denote by a its first message.

Suppose P^* successfully answers two different challenges c_1 & c_2 in $\mathbb{Z}_q$.

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

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

$\Rightarrow$ Can efficiently extract the secret x.

Fiat-Shamir Paradigm

Any ID scheme (with the above structure, where the verifier sends a random challenge) can be turned into a signature scheme, as follows.

Fix any hash function H, or choose a seeded hash function and append it to PK.

To sign a message m, generate an accepting transcript corresponding to the ID scheme, (a, c, r), where

$$c = H(PK, a)$$

(H: hash function; a: first msg.)

Thm [Pointcheval-Stern 96]: If the ID scheme is secure (complete PoK HVZK) then the corresponding signature scheme is secure.

ZK proofs are extremely useful!

ID schemes, sig schemes, electronic voting & auctions, cryptocurrencies, ..., nuclear disarmament.