Today:

- Zero-knowledge proofs (a.k.a. proofs of knowledge)
  - Interactive proofs
    - 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
\[ P \xleftarrow{\text{common input}} V \]

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

\( P \) may be powerful
\( V \) is probabilistic polynomial time.

\( x \) is typically an \textit{NP} statement:
\[ (\exists w) \quad \text{s.t.} \quad R(x, w) = 1 \]
\[ \text{poly-time} \]
\[ \text{poly-size} \]
\[ \text{witness} \]

\[ \exists x : (\exists w) \quad \text{s.t.} \quad y = g^w \pmod{p} \]

Maybe \( P \) does not want to reveal \( w \)!
\( P \) wants to reveal \textit{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

\[ \text{prob} > \text{const} > 0. \]

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

An iterative 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:

\[ P \xrightarrow{\text{commit}} V \]

\[ \xleftarrow{\text{Challenge}} \]

\[ \text{response} \]
Recall: Commitment scheme: \((\text{commit, open})\)

\[ C = \text{commit}(v, r) \] 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 (i.e., to one \(v\)).

\[ \text{Eg., Pedersen Commitment:} \]

\[ C = g^v h^r \]

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.

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 $c_1, \ldots, c_n \in \{\text{blue, red, green}\}$

\[
P \xrightarrow{\text{commit}(c_1), \ldots, \text{commit}(c_n)} \xleftarrow{i, j} \text{choose random adjacent vertices } i, j
\]

\[
\text{open}(c_i), \text{open}(c_j)
\]

accept if $c_i \neq c_j$ and $c_i, c_j \in \{\text{blue, red, green}\}$
Graph isomorphism:

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

$\pi^*: H \to G$

Choose random permutation $\pi: [n] \to [n]$

$J = \pi(G)$

if $b=0$ send $\pi$
if $b=1$ send $\pi^* \pi$

$J = \pi(G)$

if $b=0$ check
$J = \pi(G)$
if $b=1$ check
$J = \pi^* \pi^*(H)$

Hamiltonian Cycle - A cycle that visits every vertex exactly once

choose at random $b \in \{0, 1\}$

if $b=0$ send $\pi$
if $b=1$ send Hamiltonian cycle in $J$
Thm: Every NP statement has ZK proof.  

Cryptographic 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
- $g$ divides $p-1$, $g$ prime
- $g \in \mathbb{Z}_p$ s.t. $|<g>| = q$

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

PK: $y = g^x \text{ mod } p$

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

\[ A \quad \text{PK} = y = g^x \quad B \]

Choose $k \in \mathbb{Z}_q$  
$y = g^k$ ("commitment" to $x$)

\[ c \quad \text{"challenge"} \]

Choose $c \in \mathbb{Z}_q$

$r = cx + k$ ("response")

Check $y^c \cdot a^r = g^r$
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. $\geq \varepsilon$, then Alice "knows" $x$.

(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:

$$g^r = g^{ca+k} = yc \cdot a \checkmark$$

**Soundness & POK**:

Let $a$ be Alice's first msg.

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

$$\Rightarrow y^{c_1}a = g^{r_1}$$

$$\Rightarrow y^{c_2}a = g^{r_2}$$

$$\Rightarrow y^{c_1-c_2} = g^{r_1-r_2}$$

$$\Rightarrow x = \frac{r_1-r_2}{c_1-c_2} \mod g.$$

$\Rightarrow$ Alice "knows" $x$. 

Fiat-Shamir Paradigm

Any ID scheme (and in particular Schnorr’s protocol can be turned into a signature scheme by letting \( C = \text{hash}(a, m \_\text{msg}) \).

**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).

[2KPs that a high quality fissile material was destroyed (without revealing its design).]