ZERO-KNOWLEDGE PROOFS

A, B HONEST BUT CURIOUS

\[
C = \text{Enc}(\text{Pu}, x)
\]

PROOF THAT \(C\) IS AN ENC OF \(x\) UNDER \(P\).

PROOFS THAT REVEAL NOTHING EXCEPT THAT CLAIM IS TRUE.

GRAPH ISOMORPHISM

IS A BIJECTION \(\pi\) BETWEEN VERTICES THAT PRESERVES THE EDGES.

Alice

"I know \(\pi\)"

Bob
Graph Isomorphism Protocol

Alice knows $\Pi$ s.t. $\Pi(G_0) = G_1$.

1. Alice chooses a random permutation $\sigma$ of vertices and sends $\sigma(G_0) = G$ to Bob.
2. Bob sends a random bit $b$.
3. If $b = 0$, Alice reveals $\sigma$.
   If $b = 1$, Alice reveals $\Pi$.
4. Bob checks that $\phi(G_b) = G$.

Claim: If $G_0, G_1$ not isomorphic then Alice cannot handle both challenges.

Proof: Suppose she could.

$\rightarrow G \cong G_0$ and $G \cong G_1 \rightarrow G_0 \cong G_1$. 
Bob's view is \((G, b, \phi)\) \(\phi(G_b) = g\).

He can simulate by choosing \(b, \phi\) at random and setting \(G = \phi(G_b)\).

In particular, no info leaked about \(\Pi\).

---

**Two types of statements**

1. "\(G_0, G_1\) are isomorphic" **Proof of fact**
2. "I know an isomorphism \(\Pi\)" **Proof of knowledge**

**Proof relation** \(R(x, \Pi)\)

- statement \(x = (G_0, G_1)\), \(\Pi\) isomorphism \(G_0 \rightarrow G_1\), \(((G_0, G_1), \Pi) \in R\) if \(\forall x, y : (x, y)\) edge in \(G_0\), \((\Pi(x), \Pi(y))\) edge in \(G_1\).

**Proof system for \(R\) is a protocol**

**Between** \(P(x, \Pi)\) and \(V(x)\):

- **Completeness**: if \((x, \Pi) \in R\) then \(V(x)\) accepts with prob. 1.
- **Soundness**: if \((x, \Pi) \notin R\) for all \(\Pi\) then \(V(x)\) rejects any \(P^*\) with probability \(\geq \frac{1}{2}\).
(P, V) is \textbf{Honest-verifier zero-knowledge} if \exists Sim \text{ s.t.} \forall (x, \Pi) \in \mathcal{E} \text{ the view of} \ V \text{ upon interacting with} \ P(x, \Pi) \text{ is indistinguishable from} \ Sim(x).

GI simulator is \( (\infty, 0) \)-HVZK.

\[
\begin{array}{c}
(60, 61) \\
(60, 61) \rightarrow (G_0, G_1) \\
(60, 61) \rightarrow (G_0, G_1) \\
\end{array}
\]

A cheating \( V^* \) could choose his challenge \( b^* \) to depend on \( G \) \( (b^* = b^*(G)) \).

(\( P, V \)) is \( (\delta, \varepsilon) \)-zero-knowledge if for every \( V^* \) of size \( \leq t \) and every \( (x, \Pi) \) \( \in \mathcal{E} \) there is a simulator \( Sim \text{ s.t.} Sim(x) \) outputs a ry that is \( (\delta, \varepsilon) \)-indistinguishable from \( (V^*(x) \leftrightarrow P(x, \Pi)) \).
SIMULATION OVERHEAD $oh(t) = \text{ EXTRA AMOUNT OF WORK Sim HAS TO DO.}$

$Sim$ FOR $G_1$:
• RANDOMLY GUESS $V^*$ CHALLENGE $b$.
• SIMULATE 1ST PROVER MESSAGE $G = \phi(G_b)$
• IF $V^*$ RESPONSE $b^* = b$, OUTPUT $\phi$.

1. $Sim(G_0, G_1)$ LOOKS LIKE $P(x, b) \leftrightarrow V^*(x)$
2. $P(b^* = b)$ IS REASONABLE

VIEW $|b^* = b| : G$, $b$, $\phi$ s.t. $\phi(G_b) = 6$
IDENTICAL TO SIMULATED RANDOM VIEW.

$G = \phi(G_b)$ w/lp 1/2
$\phi(G)$ w/lp 1/2 $\Rightarrow V^*$

IDENTICALLY DISTRIBUTED
$\leftarrow$ IND. OF $b$ $\rightarrow$ $P(b^* = b) = \frac{1}{2}$.

$oh(t)$: CONSISTS OF SAMPLING $\phi_b$ AND COMPUTING $\phi(G_b) \rightarrow O(n^2 + \log n)$ EFFICIENT

$\frac{1}{2} \rightarrow \frac{1}{2^{100}} \rightarrow \text{REPEAT 100 TIMES}$
EG. ZKP STATEMENT \( \exists X, Y \) s.t. \( h = g^x \), \( h' = g^y \), \( h'' = g^{xy} \)

PROOF \( X, Y \)

ZERO-KNOWLEDGE PROOFS FOR ANY FACT

COMMITMENTS

RECALL OF PROTOCOL

\[ \begin{array}{c}
X_0, X_1 \\
A & \begin{array}{c}
\text{AND}(x_0, b) \\
\text{AND}(x_1, b)
\end{array} & B
\end{array} \]

REFER TO SAME \( b \).

COMMITMENT SCHEME IS A 2-PHASE PROTOCOL BETWEEN SENDER AND RECEIVER

COMMITMENT \( S \)

\[ C = \text{Com}(M) \]

\( R \)

DISCLOSURE

\[ M \]

PROOF THAT \( M \) IS "DETERMINED" BY \( C \)
(Com, Rev) is \((\infty, 0)\) - binding

Hiding: Sim outputs ind. random \((h, h', h'')\) ~ \((g^x, g^y, g^e)\)

Assume \((s, \varepsilon)\)-DDH, \((g^x, g^y, g^e)\)
\((s-tx, \varepsilon)\) - ind. from \((g^x, g^y, g^x \cdot M)\).

\[ S \quad \text{Com}: \quad (h, h', h'') = (g^x, g^y, g^{xy} \cdot M) \to R \]

Rev: \[ M, X, Y \]

Check that \(h = g^x, h' = g^y, h'' = g^{xy} \cdot M\)

Uniquely determines

Hiding: Commitments are \((s, \varepsilon)\)-simulatable without knowing \(M\).

Binding: No \(S^*\) of size \(\leq S\) can decommit to two different \(M \neq M'\) with prob. \(\geq \varepsilon\)
A 3-coloring of a graph $G$ is an assignment of colors $\{R,G,B\}$ to vertices so that no edge has both endpoints of same color.

$G$ is 3-colorable if there exists a valid 3-coloring.

\[
\begin{array}{c}
\text{ Valid 3-coloring } \\
\text{ \quad \quad IT = RBRBG } \\
\end{array}
\]

\[
\begin{array}{c}
\text{ Not valid } \\
\end{array}
\]

\[
\begin{array}{c}
\text{ Not valid } \\
\text{ Not 3-colorable } \\
\end{array}
\]

3col proof relation

\[(G, \pi) : \pi \text{ is a valid 3col of } G.\]
\( \text{EG.} \quad A \leftarrow (h, h', h'') \rightarrow B \)

\[
\begin{align*}
(x, y) & \quad \text{PROOF} \\
\text{π} & \quad \text{COLORING} \\
\text{G} & \quad \text{GRAPH} \\
\text{π} \text{ IS A 3COL OF G}
\end{align*}
\]

• If \((x, y)\) are DDH exponents \(h = g^x, h' = g^y, h'' = g^{xy}\), then \(\text{π}\) is a 3-col of \(G\).
• If \((h, h', h'')\) is not a DDH triple, then \(G\) is not 3-colorable.

**GoLDREICH-MICALI-WIGDERSON PROTOCOL**

\[ P(G, \pi) \quad V(G) \]

Randomly permute colors

\[ C_1 = \text{Com}(\pi), \ldots, C_n = \text{Com}(\pi) \]

Random edge \((u, v)\) in \(G\)

Discloses \(\pi_u, \pi_v\)

Accept if \(\pi_u \neq \pi_v\) and disclosures validate
**Completeness**: $V(G)$ accepts $P(G, T)$ with prob. 1 if $T$ is a 3col of $G$.

**Soundness**: $G$ not 3-colorable $\rightarrow$ $P^*$'s commitment must contain pair $(u^*_v, v^*_v)$ s.t. $C_u^*$ and $C_v^*$ decommit to same color $\rightarrow (u, v) = (u^*_v, v^*_v)$ w/p $\geq \frac{1}{m}$

So $P(P^* \text{ passes}) \leq 1 - \frac{1}{m}$.

Repeat $\frac{1}{k}$ times $\rightarrow (1 - \frac{1}{m})^{m/k} \leq e^{-k}$.

---

**Zero Knowledge**

**Model**: $V$ observes only two random distinct colors

- **Issue 1**: $C_m$ is not perfectly hiding
- **Issue 2**: $V^*$ can choose $(u^*_v, v^*_v)$ as a function of $(G, \ldots, C_n)$. 

---
Simulator for $V^*$:

- **Guess** $(u,v)$ at random
- **Simulate** commitments except for $(u,v)$ where $C_u = \text{Com}(X)$, $C_v = \text{Com}(X')$ for two random distinct colors.
- **If** $u^* = u$ and $v^* = v$, **output** $(V^*$'s randomness, $C_1,...,C_n, X, X'$).
- **If not**, **repeat**.

$$\begin{align*}
P & \quad (\text{Com}(\Pi_1), \ldots, \text{Com}(\Pi_n)) \xrightarrow{V^*} (u^*, v^*) \\
& \quad \text{REAL INTERACTION} \\
\text{Sim} & \quad (\text{Sim}_1, \ldots, \text{Com}(X), \ldots, \text{Com}(X'), \ldots, \text{Sim}_n) \\
& \quad (u^*, v^*) \xrightarrow{\text{MAY DEPEND ON } u, v} \\
& \quad \text{SIMULATED INTERACTION} \\
& \quad (\text{Sim}_1, \ldots, \text{Sim}_u, \ldots, \text{Sim}_v, \ldots, \text{Sim}_n) \\
& \quad (u^*, v^*) \xrightarrow{\text{STATISTICALLY IND OF } u, v} \\
& \quad P[(u^*, v^*) = (u, v)] = \frac{1}{\omega} \quad \rightarrow \quad P[(u^*, v^*) = (u, v)] \geq \frac{1}{\omega} - 2\epsilon \\
& \quad \text{IN SIMULATED INTERACTED}
\end{align*}$$