Zero Knowledge Proofs

What is a ZK proof?

- Proof that something is true without revealing anything else

(P) $\xrightarrow{c}$ (V)

sk

c = ciphertext

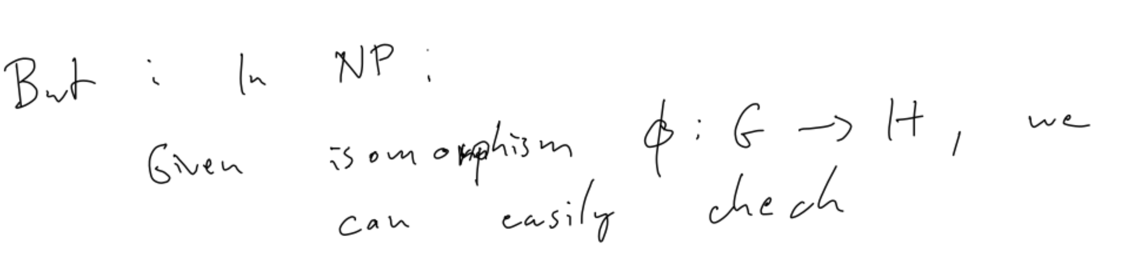
Knows: c decrypts to valid XML

$\xrightarrow{\text{Proves: c contains valid XML}}$

Why?

- Make protocol parties adhere to protocol (passive to active sec "compiler")

Graph Isomorphism



Deciding whether two given graphs are isom is hard (somewhat)

But: In NP:

Given isomorphism $\phi: G \to H$, we can easily check

ZK proof for GI

Statement: $x = (G_1, G_2)$ // known to P, V

Witness: $\phi: G_1 \to G_2$ // known to P

(P) $\xrightarrow{H}$ (V)

Pick permut of vertices randomly

$H := \psi_1(G_1)$

$i \xleftarrow{\$} \{1,2\}$

$\psi_2 := H \circ \phi^{-1}$

$\xrightarrow{\psi_i : G_i \to H}$ Check: $\psi_i : G_i \to H$ is isom.

$\boxed{\psi_2 : G_2 \xrightarrow{\phi^{-1}} G_1 \xrightarrow{\psi_1} H}$

- If prover + verifier honest, proof succeeds ("completeness")
- Soundness: This actually "proves" that G_1, G_2 are isom.

Intuition: Assume $G_1 \not\cong G_2 \Rightarrow H \not\cong G_1$ or $H \not\cong G_2$

$\Rightarrow$ with prob $\geq \frac{1}{2}$, $H \not\cong G_i$

$\Rightarrow$ with prob $\geq \frac{1}{2}$, V rejects

Have "soundness" with soundness error $1/2$

- ZK: Why doesn't this reveal anything?

$\rightarrow$ V just sees a random graph H isom. to G_i + isom. $\psi_i : G_i \to H$

$\rightarrow$ V could have computed that on their own.

$\Rightarrow$ V does not learn anything.

Defs: Completeness: All works (omitted)

Soundness: For any unlimited malicious prover, if x is not valid statement ($\nexists w$) then $\Pr[\text{success}] \leq \varepsilon$ (details omitted)

Zero-Knowledge: A pair (P, V) is statistical ZK iff $\forall$ poly-time V^*, exists poly-time S "simulator" and negl μ s.t. $\forall (x,w) \in R$, $\forall z \in \{0,1\}^*$; auxiliary input

$SD(\underbrace{\langle P(x,w), V^*(x,z) \rangle}_{V^*\text{'s output}}, S(x,z)) \leq \mu(|x|)$

all valid statement/witness pairs

Thm: GI has completeness.

Thm: GI has $\frac{1}{2}$-soundness.

Thm: GI has statistical ZK

Proof sketch: Fix V^*. Need to construct: S

First step: Simulator S_1 that may fail

$\boxed{S_1}$ (P) ① Guess $i^* \xleftarrow{\$} \{1,2\}$ (V^*)

$\xrightarrow{H}$

ψ_{i^*} random

$H := \psi_{i^*}(G_{i^*})$

$\xleftarrow{i}$

if $i \neq i^*$: abort

$\xrightarrow{\psi_i : G_i \to H}$ $\psi_i = \psi_{i^*}$

accept $\rightarrow S_1$ outputs V^*'s output

After somewhat more careful analysis of distribs:

$S_1(x,z) \mid \text{not abort} \equiv \langle P(x,w), V^*(x,z) \rangle$

$\Pr[\text{abort}] = 1/2$

$\boxed{S}$ - Run $y \leftarrow S_1(x,z)$

- If not abort: Output y
- Else: restart (max |x| iterations)

$\Pr[\text{no success}] \leq 2^{-|x|}$

$S \overset{2^{-|x|}}{\approx} S \mid \text{succ} \equiv S_1 \mid \text{succ} \equiv \langle P, V^* \rangle$

$\Rightarrow SD(\langle P, V^* \rangle, S) \leq 2^{-|x|}$ negligible. ∎

Quantum setting

Is this proto secure against q. adversaries?

At first glance:

Since we never used that adv. is poly-time, sec. holds for all adv. incl. q.

Correct for soundness

For ZK: (P, V) is q. stat. ZK iff

$\forall$ quantum poly-time V^*, $\exists$ quantum poly-time S, negl μ s.t. $\forall (x,w) \in R$, $\forall \rho$

$TD(\langle P(x,w), V^*(x,\rho) \rangle, S(x,\rho)) \leq \mu(|x|)$

Proof attempt

Step 1: Construct $S_1(x,\rho)$

(P) Guess i^* (V) ρ

Then: $\underbrace{S_1(x,\rho) \mid \text{not abort}}_{\text{density op.}} = \underbrace{\langle P(x,w), V^*(x,\rho) \rangle}_{\text{density op}}$

Step 2: Construct $S(x, Z)$ where Z is the register containing ρ

- Run $S_1(x, Z) \to Y$ (output register)
- If success: Return Y
- Else: restart

Does not work! Need a copy of original Z for next loop.

$\rightarrow$ Cannot copy quantum states!

Example of rewinding:

- During execution (in a proof step) go back to earlier state

Classical: Easy

Quantum: Does not work that way

In some situations, q rewinding is poss., but not by copying but by (partial) uncomputing