Zero-Knowledge Proof

Recap:

- Interactive proof: Prover, Verifier, L, x
  - Completeness: $x \in L$ gives $\langle P, V\rangle(x) \to \pi$ such that $V(x, \pi) = 1$
  - Soundness: $x \in L$, $\forall$ prover P, $\langle P, V\rangle(x) \to \pi$, and $\Pr[V(x, \pi) = 1] \leq \frac{1}{2}$
- What if a verifier is malicious and wants to learn more information?

Informal Definition (Zero-Knowledge)

- $View(P, V)$: Messages between P and V
- There exists a simulator S, such that

$$View(P, V) \approx_C S(x, \text{The statement is true}) \tag{1}$$

(**Honest-Verifier**: verifier really follows the protocol)

Proof System for Graph Isomorphism

- A prover P wants to prove $G_1 \cong G_2$ to a verifier V
- The prover P knows a permutation π that $\pi(G_1) = G_2$.
- P pick a permutation $\sigma \leftarrow S_{|V|}$ and send $G' = \sigma(G_1)$ to V
- The verifier V pick a random b from $\{1, 2\}$, and ask the prover to give a permutation from $\sigma(G_1)$ to G_b
- P outputs $\tau = \sigma$ if $b = 1$, $\tau = \sigma\pi^{-1}$ if $b = 2$.
- **Completeness, Soundness** holds for this scheme
- **Zero-Knowledge:**
  - Construct a simulator S: $b' \leftarrow \{1, 2\}$
  - $\sigma' \leftarrow S_{|V|}$, outputs $\sigma'(G'_b)$, b' and then σ'
  - $(G', b, \tau) \approx_C (\sigma'(G'_b), b', \sigma')$

Malicious Verifier Zero Knowledge Proof

- For all verifiers V^*, there exists a simulator S, such that

$$View(P, V) \approx_C S(x, V^*, \text{The statement is true}) \tag{2}$$

- which means we give the verifier to simulator as an oracle.

Construct another simulator for GI proof system for malicious verifiers:

- $b' \leftarrow \{1, 2\}$
- $\sigma' \leftarrow S_{|V|}$
- $\tilde{G} = \sigma'(G_{b'})$
- Query the verifier $\tilde{b} = V^*(\tilde{G})$

- If $b' = \tilde{b}$, outputs σ. Otherwise resample b' and do this again.
- Since $\sigma'(G_1)$ is identically distributed with $\sigma'(G_2)$, we succeed with 1/2 probability each time. Hence we can simulate this in polynomial trail.