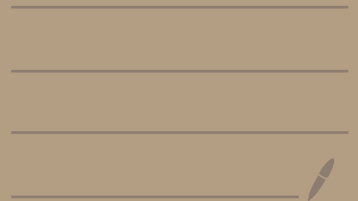


ZK for NP (w/ hardness)

- 0. Recap: ZK
- 1. Why do ZK for NP
- 2. HVZK for HamPath
- 3. ZK for HamPath



0 Last time: ZK and ZK for GI.

• ZK: $\forall$ PPT $V^*, \exists$ PPT Sim, $\forall x \in \mathcal{L}$,

$$\{\text{Sim}(x)\} \approx_c \{\text{view}_V[\langle P, V \rangle(x)]\}$$

• HVZK: fix $V^* = V$.

• ZK for GI:

$$P(G_0, G_1, \pi)$$

$$V(G_0, G_1)$$

$$\sigma \xleftarrow{\$} \text{Perms}[\mathcal{E}] \xrightarrow{H \leftarrow \sigma(G_0)} b \xleftarrow{\$} \{0,1\}$$

$$G_0 \approx H \cong G_1$$

$$\begin{array}{c} \xleftarrow{b} \\ \xrightarrow{P} H \stackrel{?}{=} P(G_b) \end{array}$$

• protocol is interactive

• for HVZK: Sim is out-of-order

• for ZK: Sim_{ZK} is more complex

• rejection sampling

• no computational assumptions

• Today: more general ZKPs, w/ assumptions

□ Motivation: ZK for NP:

- Recall our problem from last time: Private ID

$$\underline{P}(\text{id}, \text{pk}_{\text{GA}}, \sigma) \quad \underline{V}(\underline{\text{pk}_{\text{GA}}})$$

photo, age
→
claim: $\begin{cases} \text{public} \\ \text{secret} \end{cases}$

$$\left[\begin{array}{l} \exists \underline{\text{id}}, \underline{\sigma}, \text{SigVer}(\underline{\text{id}}, \underline{\sigma}, \underline{\text{pk}_{\text{GA}}}) \\ \text{secret} \wedge (\text{photo}, \text{age}) \in \underline{\text{id}} \end{array} \right] \phi(x, w)$$

- How can we prove claims like this? Lets abstract...
- public x ("instance"): photo, age, pk_{GA}
- secret w ("witness"): id, σ
- relation $\phi(x, w)$:
 - could evaluate ϕ in $\text{poly}(\phi)$

- Observation:

- This claim is in NP.

- Why? This trivial proof is not ZK, but is sound / complete:

$$\begin{array}{ccc} P(x, \omega) & & V(x) \\ & \xrightarrow{\omega} & \phi(x, \omega) \stackrel{?}{=} 1 \end{array}$$

- So, we it suffices to build a ZKP for any NP-hard language $\mathcal{L}$.

- Then we could do the following:

- Write claim as circuit C

- Reduce $\exists \omega, C(x, \omega) = 1$ to $\mathcal{L}$

- Prove $\mathcal{L}$, (unrestricted)

- Today: a ZKP for Hamiltonian Path

HCW:

3-coloring

- Hamiltonian Path:

- Let $G \in \{0, 1\}^{n \times n}$ be a graph

- adjacency matrix: $G_{ij} = 1 \Leftrightarrow i \rightarrow j$ in G .

- $p \in [n]^n$ is a hamiltonian path $\text{Ham}(G, p)$:

- no duplicates

- $\forall i \in [n-1] \quad G_{p_i, p_{i+1}} = 1$.

- For $\sigma \in \text{Perms}([n])$, $G' \leftarrow \sigma(G)$ permutes rows + columns:

$$G'_{\sigma(i), \sigma(j)} = G_{i, j}$$

- $G \in \text{HamPath}$ if a hamiltonian path exists.

② ZK for HamPath

Let $\text{Com}(m \in [n], r \in R) \Rightarrow c$ be perfectly binding and computationally hiding.

$P(G, p)$ s.t. HamPath

$V(h)$

$\sigma \xleftarrow{\$} \text{Perms}[n]$

$G' \leftarrow \sigma(G)$

$\forall i, j \in [n]^2:$

$r_{i,j} \xleftarrow{\$} R$

$c_{i,j} \leftarrow \text{Com}(G_{i,j}, r_{i,j})$

$\forall i \in [n]:$

$s_i \xleftarrow{\$} R$

$d_i \leftarrow \text{Com}(\sigma(i), s_i)$

$\xrightarrow{c, d} \text{see } G', \sigma$
or see $\sigma(p)$?

if $b = 0$,
send σ, r, s

$\xleftarrow{b} b \xleftarrow{\$} \{0, 1\}$

if $b = 1$,
send $p' \leftarrow \sigma(p), (r_{p'_i}, p'_{i,m})$
 $\forall i \in [n-1]$

if $b = 0$:
check all commitments
 $\wedge G' = \sigma(G)$

if $b = 1$:
 $\forall i \in [n-1],$
 $C_{p'_i, p'_{i,m}} = \text{Com}(1,$
 $r_{p'_i}, r_{p'_{i,m}})$

Example:

Start with

$$G: \begin{array}{cc} 1 \rightarrow 2 \\ \swarrow \downarrow \\ 4 \leftarrow 3 \end{array} \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad C: (1, 2, 3, 4)$$

P samples

$$\sigma: 1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 4, 4 \mapsto 1$$

P computes

$$G' \quad \begin{array}{cc} 3 \rightarrow 2 \\ \swarrow \downarrow \\ 1 \leftarrow 4 \end{array} \quad \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad C': (3, 2, 4, 1) \\ (3, 2), (2, 4), (4, 1)$$

P commits to G', σ .

If $b=0$, P opens all (p stays hidden)

If $b=1$, P opens c' and the blue entries

• We'll prove soundness + ZK.

• The soundness error is $1/2$ (so, repeat once). Pf:

• Fix $G \notin \text{Ham}$ and P^*

• Consider P^* 's first message: commitments.

• Since Com is perfectly binding, P^* 's commitments can be opened to at most one $\tilde{G}', \tilde{\sigma}$.

• We now bound P^* 's success probability in the rest of the protocol, by cases:

- $\tilde{G}'$ doesn't exist $\Rightarrow$ P fails when $b=0$ (prob. $1/2$)
(can't open c_i)
- $\tilde{\sigma}$ doesn't exist $\Rightarrow$ same
(can't open d_i)
- $\tilde{G}' \neq \tilde{\sigma}(G)$ $\Rightarrow$ some
($\forall$ checks $\hat{G}' \neq \tilde{\sigma}(h)$)
- in the remaining case
 $\tilde{G}' = \tilde{\sigma}(G)$
 $\Rightarrow \tilde{G}' \cong G$ (by $\tilde{\sigma}$)
 $\Rightarrow \tilde{G}' \notin \text{HomPath}$ (by $\cong$, $G \notin \text{Hom}$)
 $\Rightarrow$ P fails when $b=1$. (no such p') (prob. $1/2$)

• Now, HVZK.

• as usual, Sim is out-of-order

• $\text{Sim}(G)$:

$b \leftarrow \{0, 1\}$

if $b=0$:

• run protocol using $\underline{b}$ (and output transcript)

• (p , which Sim does not know, is unused when $b=0$)

if $b=1$:

• $G' \leftarrow \mathcal{G}$ (all 1 s), $\sigma \leftarrow \mathcal{H}$, $p' \leftarrow \text{Perms}[\mathbb{E}n]$

• run protocol w/ G', σ, p', b

• (p' is used - not p)

• Must show $\{\text{Sim}(G)\} \approx_c \{\text{view}_P[\langle P, V \rangle(G)]\}$

D_S

D_H

• 1st, $b \leftarrow \{0, 1\}$, so condition on b :

• case $b=0$ (easy)

• $D_{\text{sim}} = D_V$ (Sim runs protocol)

Π means protocol

• case $b=1$ (hard)

- transcript has: $c, d, b, p', (r_{p_i, p_{i+1}})_i$
- some components are uniform and independent of b :
 $p', (r_{p_i, p_{i+1}})_i$ so condition on their values:
 $\uparrow \quad \quad \quad \uparrow \quad \quad \quad \uparrow$
 $\quad \quad \quad \leftarrow \leftarrow \leftarrow R \text{ in both} \quad \quad \quad \sigma \sim \text{Perms}[n]$
 $\quad \quad \quad \text{in } \text{Sim}: p' \leftarrow \text{Perm}[n], \text{ in } \Pi: p' \leftarrow \sigma(p)$
- some commitments are determined by values above
 $(C_{p_i, p_{i+1}})_i$, so condition on their values

- collect the rest of c, d into c'
 r, s into r'
 G, σ into m'

• length: $(n^2 - n) + (n) = n^2$

• claim:

$$\{C's, \text{rest}\} \approx_c \{C'n, \text{rest}\}$$

$$\{(Com(1, r'_{s,i}))_i, \text{rest}\} \approx_c \{(Com(m'_n, r'_{n,i}))_i, \text{rest}\}$$

D_{n^2} D_0

fix PPT A .

Define hybrids:

D_i : first i messages in D_0 changed to 1.

For each i , define hiding adversary B_i :

- gets a commitment $\tilde{c}$ to 1 or $m_{n,i}$
- builds a D_{i+1} or D_i sample
 - by plugging in $1 / m_{n,j}, j \leq i$ and rest
- so $\text{Distadv}[A, D_i, D_{i+1}] \leq \text{Hidadv}[B_i, \text{Com}] \leq \text{negl}$.
- so $\text{Distadv}[A, D_0, D_n] \leq n^2 \text{negl} \leq \text{negl}$.
- so $D_0 \approx_c D_{n^2}$
- so $\{\text{Sim}(G)\} \approx_c \{\text{view}_v[(P, v)(G)]\}$



- ⑬ ZK for HamPath: Same protocol, let's prove ZK
- This is much more tedious. We'll just sketch it. It's not on HW.
 - Looking ahead: we'll soon have a generic HVZK $\rightarrow$ ZK transform, so true ZK won't matter much.
 - Define $\text{Sim}_{\text{ZK}}(G)$: via rejection sampling
 - $tr \leftarrow \text{Sim}(G)$
 - $(c, d, b, \dots) \leftarrow tr$
 - $b' \leftarrow V^*(c, d)$
 - if $b' = b$:
 - output tr
 - else:
 - rewind, or abort after λ tries.
 - Claim 1: Each c, d in Sim_{ZK} is $\approx_c$ c, d in Π
 - proof sketch: Commitment-hiding hybrids
 - Claim 2: $\Pr[b' = b] \geq 1/2 - \text{negl}$
 - proof sketch: use •
 - $\Pr[V^*(c_s, d_s) = b_s] \geq \Pr[V^*(c_\Pi, d_\Pi) = b_s] - \text{negl}$ (by $\approx_c$)
 $= 1/2 - \text{negl}$ (by $\perp_{b_s}$)
 - Therefore: $\Pr[\text{abort}] \leq (1/2)^\lambda + \text{negl}$
 - Claim 3: the opening messages in Sim_{ZK} and Π are $\approx_c$.
 - proof sketch:
 - $b=0$ case: both are openings of commitments
 - $b=1$ case: both are openings of random path.

Recap: