

lec05: Zero knowledge (zk)

11 Finish sumcheck

12 zk

13 zk for GI

14 zk needs interaction

☐ Recall: IPs

Defⁿ an IP is (P, V)

- V is PPT, P need not be

- P convinces V $x \in \mathcal{L}$

- complete: $\forall x \in \mathcal{L}$,

$$\Pr[\langle P, V \rangle(x) = 0] \leq 1/3$$

- sound : $\forall x \notin \mathcal{L}, \forall P^*$

$$\Pr[\langle P^*, V \rangle(x) = 1] \leq 1/3$$

☐ Finish sumcheck:

- unroll it

- soundness proof

- (see last week's notes)

[2] Zero Knowledge

• Motivation: Private Credentials

- To enter a bar, I must show my ID:

• photo
• age
• name
• address
• DL #
• ...

these are necessary.
I'm willing to show them

these are not necessary
I would rather not show them...

- In Australia + soon the UK, you must age verify for social media...

- How could we do this privately?

- 3 steps:

1. State signs my (full) ID $\text{Sign}(sk, \text{data}) \rightarrow \sigma$
2. State gives me σ , data
3. I show the bar data subset and prove

$$\text{SigVerify}(pk, \text{data}, \sigma) = 1 \wedge \text{data subset} \subseteq \text{data}$$

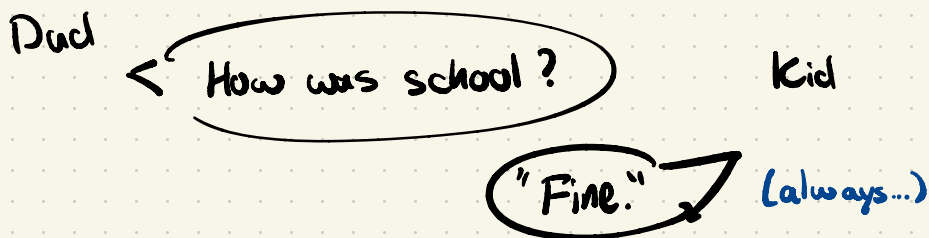
↑ revealed

not revealed

• Q: How to define that a protocol reveals some things, but "nothing else"?

• Inspiration for an answer:

Dad picks up kid from school



Dad could have simulated this transcript himself.
He didn't really learn anything

Principle: ZK as simulatability

In a IP, the transcript is the messages

If V can simulate the transcript,

the proof is zero knowledge.

Defⁿ (P, V) is honest-verifier ZK (HVZK) if there exists a PPT simulator Sim s.t.

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

$\uparrow$
 $\approx_s$ and $=$ give other HVZK variants

Defⁿ (P, V) is ZK if $\forall$ PPT V^* , $\exists$ a PPT Sim,

$$\forall x \in \mathcal{X}, \text{view}_V[\langle P, V^* \rangle(x)] \approx_c \text{Sim}(x)$$

interpretation: $\approx_c$ captures "same information"

info from protocol $\approx$,

info derived from x .

Later: HVZK $\rightarrow$ ZK

transformations.

Now, let's see an example of a ZKP for GI.

③ A ZKP for graph isomorphism.

Recall GI: for graphs G_0, G_1 on n nodes,
does there exist a $\pi \in \text{Perms}[n]$ s.t. $G_1 = \pi(G_0)$

Trivial IP for GI

$$\begin{array}{ccc} \underline{P(G_0, G_1, \pi)} & & \underline{V(G_0, G_1)} \\ & \xrightarrow{\pi} & \\ & & G_1 \stackrel{?}{=} \pi(G_0) \end{array}$$

Note: this protocol is non interactive.

It is clearly complete and sound.

Is it ZK?

Intuitively, no: V learns π .

Formally: only if GI $\in$ BPP.

If GI $\in$ BPP, then $\exists$ a PPT

$$\text{FindP}_i(G_0, G_1) \rightarrow \pi$$

So, $\text{Sim} \triangleq \text{FindP}_i$

But, we don't know that FindP_i exists...

problems
solvable
in randomized
polytime

So, we don't know that Sim exists...

So now we'll do a new protocol for GI that is provably ZK.

$P(G_0, G_1, \pi)$

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

if $b=0$:

$p \leftarrow \sigma$

if $b=1$:

$p \leftarrow \sigma \circ \pi$

$V(G_0, G_1)$

$H \leftarrow \sigma(G_0)$

we should have:

$G_0 \cong H \cong G_1$

b

"show $H \cong G_b$ "

p

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

$H \stackrel{?}{=} p(G_b)$

This is perfectly complete.

This is $1/2$ -sound.

- If $G_0 \not\cong G_1$, then $H \not\cong G_0$ or $H \not\cong G_1$.

- That is, $H \cong G_{b'}$, for some b'

- $\Pr[b=b'] = 1/2$.

- Repeat twice for soundness error $(1/2)^2 = 1/4 < 1/3$

This is also ZK!

First, let's prove HVZK.

The key insight is that Sim can build the transcript out of order.

Sim(G_0, G_1):

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

$p \leftarrow \text{Perms}[n]$

$H \leftarrow p(G_b)$

Claim: $\forall G_0 \cong G_1,$

$$\{\text{view}_V[\langle P, V \rangle(G_0, G_1)]\} = \{\text{Sim}(G_0, G_1)\}$$

$$\{(H_L, b_L, \rho_L)\} = \{(H_R, b_R, \rho_R)\}$$

$$1. \{b_L\} = \{b_R\} = \mathcal{U}(\{0, 1\})$$

2. Conditioned on b_L / b_R :

$$\{\rho_L\} = \{\rho_R\} = \mathcal{U}(\text{Perms}[\{n\}])$$

to see $\{\rho_L\} = \mathcal{U}(\text{Perms}[\{n\}])$, see that if $b=0$:

$$\rho_L = \sigma \sim \mathcal{U}(\text{Perms}[\{n\}]) \quad \checkmark$$

$$\text{if } b=1: \rho_L = \sigma \circ \pi^{-1}$$

$$\sigma \sim \mathcal{U}(\text{Perms}[\{n\}]) \quad \checkmark$$

3. Conditioned on $\rho_L / \rho_R, b_L / b_R$

$$\{H_L\} = \{H_R\}$$

$$H_L = \rho_L(G_{b_L})$$

$$H_R = \rho_R(G_{b_R})$$

Q: where did we use the fact that $G_0 \cong G_1$?

A: In assuming that π exists.

If it did not, $\text{view}[\langle P, V \rangle(G_0, G_1)]$ is different...

Reflection: How can an IP be sound + HVZK?

sound: the claim must be true to convince V

$\rightarrow P$ uses π to succeed.

HVZK: simulate transcript without π .

Answer: soundness is about in-order interactions, while ZK is about the transcript, which can be built

out-of-order.

That was HVZK.

Now, let's prove ZK.

• Why doesn't Sim show ZK?

• In Sim, $b \sim U(\{0,1\})$

• But, V^* might sample b differently...

• so in $\text{view}_V[\langle P, V^* \rangle(G_0, G_1)]$, b might not be 50/50

• b 's distribution might depend on H !!

• Fix: a new simulator

$\text{Sim}_{\text{ZK}}(G_0, G_1)$:

$b, \rho, H \leftarrow \text{Sim}(G_0, G_1)$

$b' \leftarrow V^*(G_0, G_1, H)$

if $b' \neq b$: rewind

or, abort after $\text{poly}(\lambda)$ tries.

• this is rejection sampling to ensure that the joint distribution (b, H, G_0, G_1) is correct.

• rejection sampling outputs the correct distribution when it completes

• we need to bound the probability of failure

• $\Pr[b' = b \text{ (in an iteration)}]$?

fact: $H \perp\!\!\!\perp b$ independent

Why? $G_0 \cong G_1$, so $\{p(G_0)\}_\rho = \{p(G_1)\}_\rho$

$\{H \mid b=0\} = \{H \mid b=1\}$

← Sim_{ZK} can run V^* ,
since Sim_{ZK} is
quantified after V^* .

thus, $b' \perp b$

(V^* compute b' from G_0, G_1, H)

so, $\Pr[b' = b] = 1/2$

$\Pr[\text{Sim}_{zk} \text{ aborts}] = (1/2)^{\text{poly}(\lambda)}$

so,

$$\{\text{view}_v[\langle P, V^* \rangle(G_0, G_1)]\} \approx_s \{\text{Sim}_{zk}(G_0, G_1)\}$$

↑
not perfect ($=$)
because of aborts

So, we've seen:

- the NP proof for GI is not provably Σ_k .
- the IP is.

This is not a coincidence:

[4] Non-interactive Zero Knowledge (NIZK)
is impossible for non-trivial languages.

Defⁿ an IP is non-interactive if it is one message $P \rightarrow V$.

Defⁿ a language L is trivial if it is in BPP.

Thm [NIZK impossibility, GO'94]:

If $\mathcal{L}$ has a NIZK, $\mathcal{L} \in \text{BPP}$.

Proof:

Since $\mathcal{L}$ is a NIZK, we have

$$\frac{P(x)}{\text{Prove}(x) \rightarrow \pi} \quad \frac{V(x)}{\underline{\quad}}$$

$\uparrow$
possibly
inefficient

$$\xrightarrow{\pi}$$

Verify(x, π)?

and we have PPT $\text{Sim}(x) \rightarrow \pi$;

$$\{\text{Sim}(x)\} \approx_c \{\text{Prove}(x)\}$$

we will build a PPT $D(x) \rightarrow b$ to decide $\mathcal{L}$.

on $x \in \mathcal{L}$, $D(x)$ must output 1 w.h.p.

on $x \notin \mathcal{L}$, $D(x)$ must output 0 w.h.p.

define $D(x) \triangleq \text{Verify}(\text{Sim}(x))$

if $x \notin \mathcal{L}$,

$$\Pr[D(x)=1]$$

$$= \Pr[\text{Verify}(\text{Sim}(x))=1] \text{ (def. of } D)$$

$$= \Pr[\langle P^*, V \rangle(x)=1] \text{ (for } P^* = \text{Sim})$$

$$\leq 1/3$$

(IP soundness)

if $x \in \mathcal{L}$

$$\Pr[D(x)=1]$$

$$= \Pr[\text{Verify}(\text{Sim}(x))=1] \text{ (def. of } D)$$

$$\geq \Pr[\text{Verify}(\text{Prove}(x))=1] - \epsilon \text{ (Sim is } \approx_c)$$

(for neg. ϵ)

$$= \Pr[\langle P, V \rangle(x)=1] - \epsilon \text{ (} P = \text{Prove)}$$

$$\geq 2/3 - \epsilon$$

(IP completeness)

Why?

Let

$$A = \Pr[\text{Verify}(\text{Sim}(x)) = 1]$$

$$B = \Pr[\text{Verify}(\text{Prove}(x)) = 1]$$

then,

$$|B - A| \leq \epsilon \quad (\text{acc.})$$

so

$$B - A \leq \epsilon$$

$$B - \epsilon \leq A$$

So, D is a PPT decider for $\mathcal{L}$
 $\Rightarrow \mathcal{L} \in \text{BPP}$.

Recap: we:

1. defined (HV) ZK proofs
2. saw a ZKP for GI that is interactive
3. saw that ZK requires interaction
(in the standard model)

Next time: ZK for every $\mathcal{L} \in \text{NP}$.