EECS 575: Advanced Cryptography
Fall 2022
Lecture 21

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Zero knowledge
- Interactive proofs example: Coke vs. Pepsi
- Interactive proofs, formally
- Interactive proof for graph non-isomorphism

Agenda for this lecture

- Announcements
- Recap from last time
- Zero knowledge
- Interactive proofs example: Coke vs. Pepsi
- Interactive proofs, formally
- Interactive proof for graph non-isomorphism

Announcements

- HW5 online, due 11/21 this Monday
- My OH are after class

Agenda for this lecture

- Announcements
- Recap from last time
- Zero knowledge
- Interactive proofs example: Coke vs. Pepsi
- Interactive proofs, formally
- Interactive proof for graph non-isomorphism

Digital signatures

- PKI
  - → revocation: what happens if priv. key stolen?
    - OCSP: servers argue non-revocation
  - → mis-issuance of certs
    - DigiNotar
    - Certificate transparency
      - log of issued certificates
        - → "blockchain"
- split signing key: threshold signature
- anonymize signer: ring signatures (Monero)
- Group Sigs, designated-verifier, aggregate, undeniable

Agenda for this lecture

- Announcements
- Recap from last time
- Zero knowledge
- Interactive proofs example: Coke vs. Pepsi
- Interactive proofs, formally
- Interactive proof for graph non-isomorphism

Zero Knowledge

IND-CPA : can't tell which message was encrypted

ROR-CPA : encryptions "look" random

quantity (ciphertext) "reveals information" about other quantity (message)

X reveals no info. about Y

$\Leftrightarrow$ X, Y indep.

How to define "no computational info" ?

Zero Knowledge

X can be determined by Y!

X ↓ g^{ab}

Y ↓ (g, g^a, g^b)

CDH implies can't compute g^{ab}

DDH implies g^{ab} "looks" random

$\Rightarrow$ Simulation

Y reveals no info about X when

Y can be simulated without knowing X

Zero Knowledge

(Gen, Enc, Dec) is "zero knowledge" if

$\exists$ efficient simulator S s.t. $\forall m$,

$$\{k \leftarrow Gen : Enc_k(m)\} \approx_c \{c \leftarrow S(1^n)\}$$

what is this "saying"?

→ Ciphertexts reveal no knowledge of plaintext

↳ "zero"

Exercise:

one-time ind. $\Leftarrow$ zero knowledge

Zero Knowledge

- why do we care?

→ Simulation is flexible/powerful!

useful paradigm for defining security

Agenda for this lecture

- Announcements
- Recap from last time
- Zero knowledge
- Interactive proofs example: Coke vs. Pepsi
- Interactive proofs, formally
- Interactive proof for graph non-isomorphism

Coke vs. Pepsi

What is a proof?

- systematic series of steps to go from truth to truth
- whatever peer reviewers believe?

Proofs are static, fixed strings

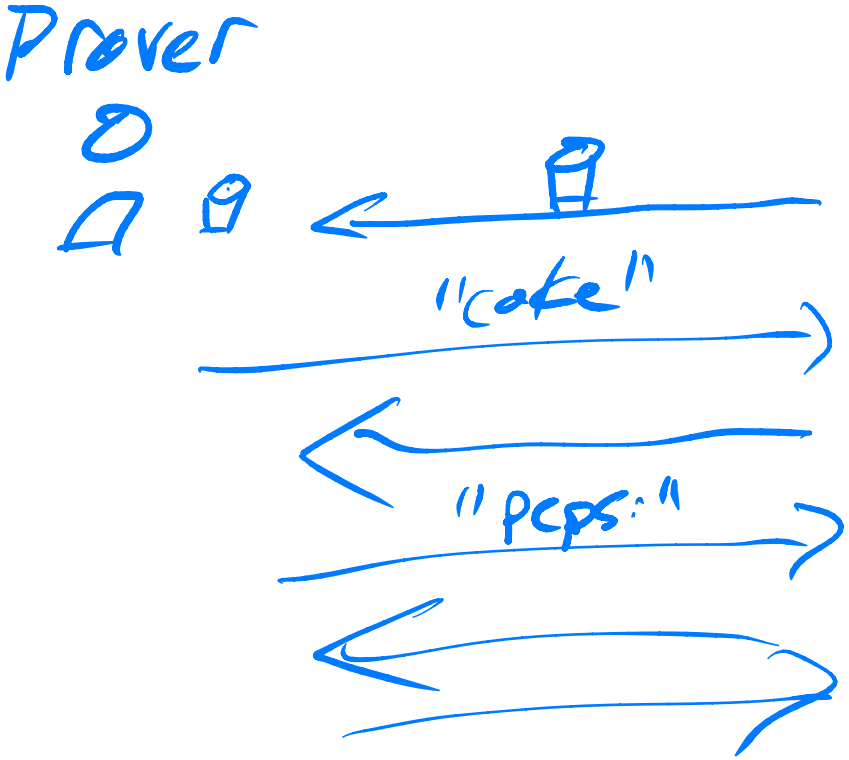
"proof" is interaction b/w prover and verifier multiple rounds. Math can be randomized.

Coke vs. Pepsi

Thm: Coke and Pepsi are different.

"static" proof: publish recipes

"interactive" proof:



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

If true:
verif always convinced

If false:
verif not convinced,
except w. negl prob

Agenda for this lecture

- Announcements
- Recap from last time
- Zero knowledge
- Interactive proofs example: Coke vs. Pepsi
- Interactive proofs, formally
- Interactive proof for graph non-isomorphism

Syntax of interactive proofs (IPs)

IP is pair of algos (P, V) (ITM)

- each is randomized, can communicate

- $P(\cdot) \leftrightarrow V(\cdot)$

- $\text{out}_V[P(\cdot) \leftrightarrow V(\cdot)]$
  - often $b = 0/1$

- Language $L \subseteq \{0,1\}^*$
  - membership proof $x \in \{0,1\}^*$
    P proves $x \in L$

Security of IPs

IP system w/ soundness error $\leq$ for $L \in \{0,1\}^*$ is pair of algos (P, V) s.t.

- Completeness:
  $\forall x \in L$, $\text{out}_V[P(x) \leftrightarrow V(x)] = 1$ w.p. 1

- Soundness:
  $\forall P^*$ (even unbounded), $\forall x \notin L$,
  $\Pr[\text{out}_V[P^*(x) \leftrightarrow V(x)] = 1] \leq s$

- Note: V is ppt or nuppt.
  P can be unbounded

Agenda for this lecture

- Announcements
- Recap from last time
- Zero knowledge
- Interactive proofs example: Coke vs. Pepsi
- Interactive proofs, formally
- Interactive proof for graph non-isomorphism

IP for graph non-isomorphism

Graph $G = (V, E)$ is:
- vertex set $[n]$
- edge set $E \subseteq V \times V$

G_0 and G_1 are isomorphic if

$\exists$ bijection $p : V_0 \to V_1$

s.t. $e_0 \in E_0$ iff

(u_0, u_1) $p(e_0)$ is in E_1

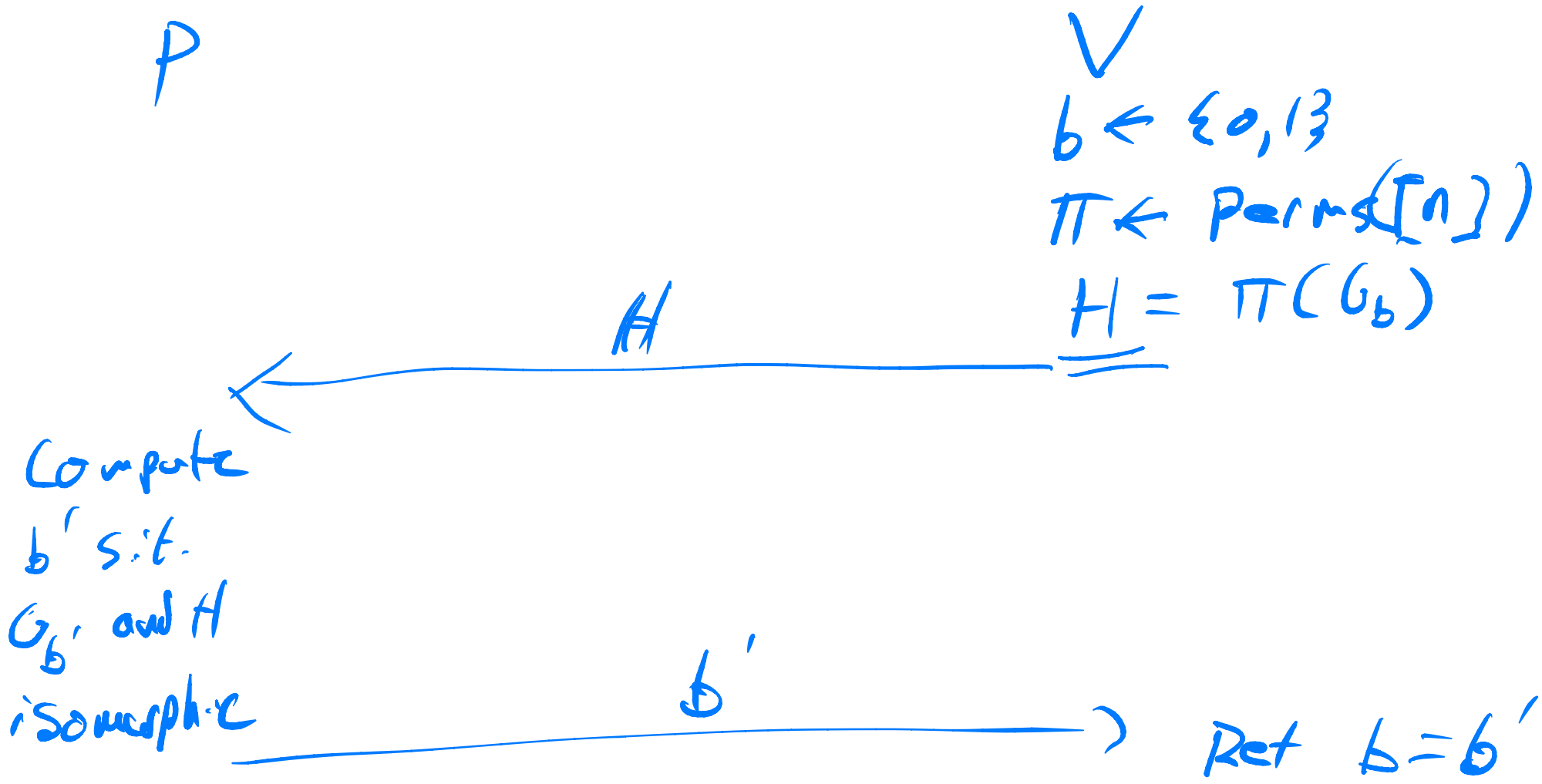
$\hookrightarrow (p(u_0), p(u_1))$

GNI language:

$L = \{(G_0, G_1) : G_0 \not\cong G_1 \text{ not isomorphic}\}$

IP for graph non-isomorphism

$X = (G_0, G_1)$



IP for graph non-isomorphism

Thm: prev. protocol is IP for GNI w/ $s = 1/2$

- Completeness
  - If (G_0, G_1) not iso.,
    $\text{out}_V[P(G_0,G_1) \leftrightarrow V(G_0,G_1)] = 1$ w.p. 1
  - $\rightarrow$ P can always guess b, even if it enumerates all bijections
- Soundness $(G_0, G_1) \notin$ GNI
  $P[\text{out}_V P^*(G_0,G_1) \leftrightarrow V(G_0,G_1)] = 1] \leq 1/2$
  True b/c H is indep. of b
  P^* guesses b w.p. $\leq 1/2$ ☒