EECS 575: Advanced Cryptography
Fall 2022
Lecture 22

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proofs
- The class NP
- Commitment schemes
- Zero-knowledge proof for graph 3-coloring

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proofs
- The class NP
- Commitment schemes
- Zero-knowledge proof for graph 3-coloring

Announcements

- HW5 due **tonight**
- HW6 released today (or tomorrow), due date TBD
- Exam timing TBD

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proofs
- The class NP
- Commitment schemes
- Zero-knowledge proof for graph 3-coloring

Interactive proofs

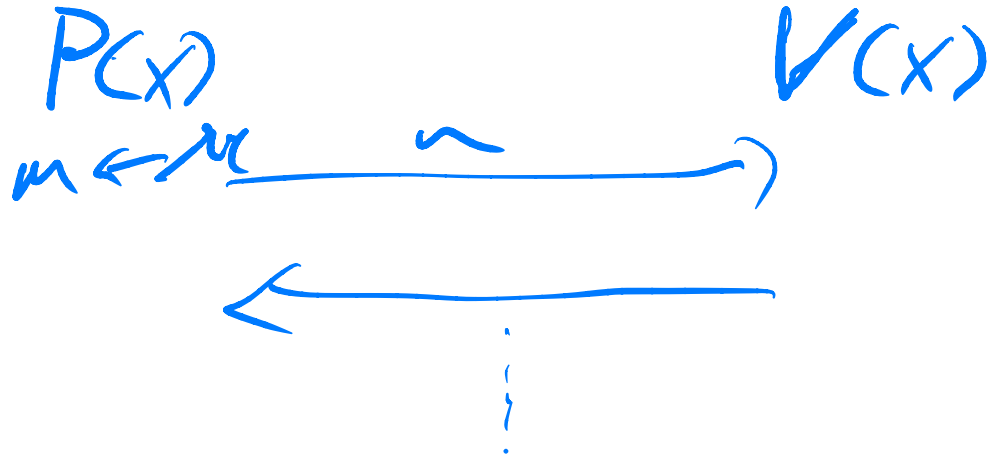
IP system w/ soundness error $\leq$ for $L \subseteq \{0,1\}^*$ is pair of algos (P, V) s.t.

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

Interactive proofs

- Coke vs. Pepsi
- Graph non-isomorphism
- Graph isomorphism



Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proofs
- The class NP
- Commitment schemes
- Zero-knowledge proof for graph 3-coloring

Honest-verifier zero-knowledge

- Zero-knowledge encryption
  - Simulator for ciphertexts, without message

An $IP = (P, V)$ is statistical HVZK if $\exists$ nuppt S s.t. $x \in L$,

$$view_V[P(x) \leftrightarrow V(x)] \overset{s}{\approx}_c S(x)$$

$view_V$ → input, random coins, and all prover messages

- Verifier is honest: follows the protocol

Honest-verifier zero-knowledge

→ non-interactive proofs

Apply "Fiat-Shamir" transform,

only need HVZK to get "full" NIZK

NIZK = non-interactive zero-knowledge

Full zero-knowledge

- Verifier can misbehave!

An IP = (P, V) is statistical ZK if $\forall$ nuppt V^*, $\exists$ $\$$ s.t. $\forall x \in L$,

$$view_{V^*}[P(x) \leftrightarrow V^*(x)] \overset{s}{\approx_c} \$(x)$$

↑ instance x, random coins, prover messages

3COL:

X instance: graph on n nodes

w witness: 3-coloring

$W(x, w)$: check all nodes have distinct colors

- What are we hiding?

→ Prover's "witness"

$x \in L$ if $\exists w$ s.t. $(x, w) \in R$

$W(x, w) = 1$

Agenda for this lecture

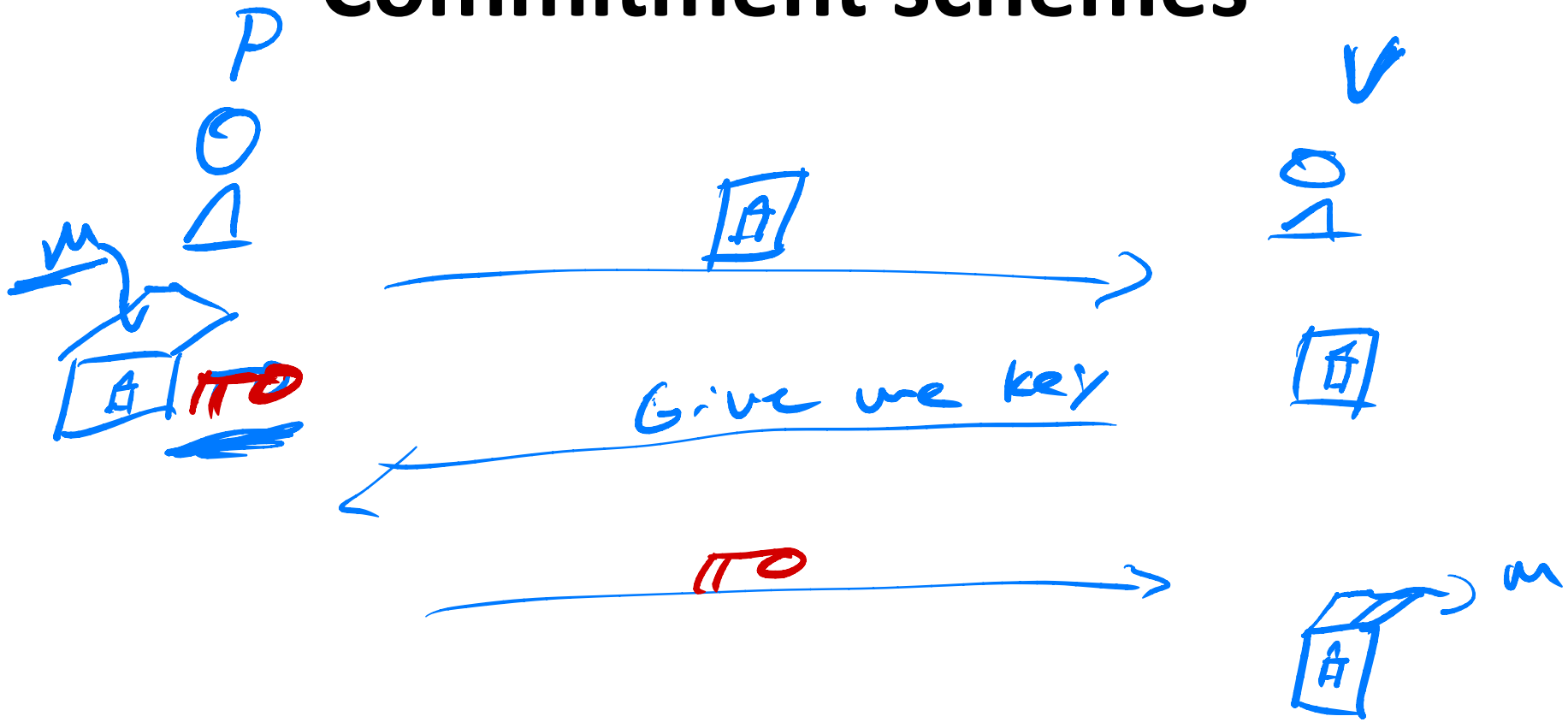
- Announcements
- Recap from last time
- Zero-knowledge proofs
- The class NP
- Commitment schemes
- Zero-knowledge proof for graph 3-coloring

The class NP of languages

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proofs
- The class NP
- Commitment schemes
- Zero-knowledge proof for graph 3-coloring

Commitment schemes



P can't change contents after locking

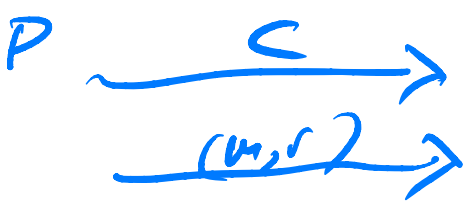
V can't see inside lockbox

Security of commitments

A commitment scheme $Com(m; r)$ has properties:

- binding: $\forall m_0, m_1, m_0 \neq m_1, \forall r_0, r_1,$ $Com(m_0, r_0) \neq Com(m_1, r_1)$
- Hiding: $\forall m_0, m_1$ $\{Com(m_0)\} \approx_c \{Com(m_1)\}$

"open" C:
reveal (m, r),
check
$com(m, r) = C$



Security of commitments

Exercise:

Prove impossibility of statistically hiding + binding commitments.

Pedersen commitments

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proofs
- The class NP
- Commitment schemes
- Zero-knowledge proof for graph 3-coloring

ZKP for 3-colorability

- Graph G is 3-colorable if $\exists\ \pi : V \to \{1,2,3\}$ s.t. $\forall (v_i, v_j) \in E,\ \pi(v_i) \neq \pi(v_j)$

$P(G, \pi)$:

$\rho \leftarrow Perms(\{1,2,3\})$

$v_i, k_i = \rho(\pi(v_i))$

$c_i = Com(k_i; r_i)$

$\{c_i\}$ →

$V(G)$

$(v_i, v_j) \leftarrow E$

← (v_i, v_j)

→ $(k_i, r_i), (k_j, r_j)$

$c_i = Com(k_i, r_i)$

$c_j = Com(k_j, r_j)$

$k_i, k_j \in \{1,2,3\}$

$k_i \neq k_j$

ZKP for 3-colorability

- Completeness: obvious
- Soundness:

  Soundness error $s \leq 1 - \frac{1}{|E|} \leq 1 - \frac{1}{n^2}$

  Proof: let $G \notin 3COL$, P^*
  - statistical binding prevents P^* from opening C_i / C_j to anything other than k_i / k_j
  - at least one edge has same color vertices
  - verifier chooses w.p. $\frac{1}{|E|}$

ZKP for 3-colorability

Thm: This protocol is zero-knowledge.

Proof: Define $\$^{V^*}(G)$:

1. Hiding Coms
2. Conditioned on (*), V^* has right dist.
3. failure w/ negl prob.

$(v_i, v_j) \in E$

$k_i \neq k_j \leftarrow \{1,2,3\}^2$

$c_i \leftarrow Com(k_i, r_i)$

$c_j \leftarrow Com(k_j, r_j)$

All others: $c_k \leftarrow Com(1, r_k) \leftarrow$

$(v_i^*, v_j^*) \leftarrow \underline{V^*}(G, \{c_i\}, r_v)$

If $(v_i, v_j) = (v_i^*, v_j^*)$: (*)

Finish protocol, output view

Else:

GOTO 1 (up to n^3 iterations)