EECS 575: Advanced Cryptography
Fall 2021
Lecture 22

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- NP and NP-hardness
- Commitment schemes
- ZKPs for all NP
- ZKP for 3COL + analysis

Agenda for this lecture

- Announcements
- Recap from last time
- NP and NP-hardness
- Commitment schemes
- ZKPs for all NP
- ZKP for 3COL + analysis

Announcements

- HW6 due tonight

Recap from last time

ZKP with soundness error s for language $L \subseteq \{0,1\}^*$ is a pair (P, V) of algorithms

* Completeness: for all $x \in L$, $\text{Out}_V[P(x) \leftrightarrow V(x)] = 1$ w.p. 1

* Soundness: for $x \notin L$, any P^* $\Pr[\text{Out}_V[P^*(x) \leftrightarrow V(x)] = 1] \leq s$

* Zero-knowledge: $\forall$ nuppt V^*, $\exists$ nuppt S in $\mathcal{S}$ s.t. for all $x \in L$,

"Computational" ZK. could be "statistical" → $\text{View}_{V^*}[P(x) \leftrightarrow V^*(x)] \approx_{c(s)} \mathcal{S}(x)$

Agenda for this lecture

- Announcements
- Recap from last time
- NP and NP-hardness
- Commitment schemes
- ZKPs for all NP
- ZKP for 3COL + analysis

The complexity class NP

A language $L \in \{0,1\}^*$ is in NP if $\exists$ det. poly-time alg. $V(x, w)$ s.t.

$$x \in L \iff \exists w \in \{0,1\}^* \text{ s.t. } V(x, w) = 1$$

NP-hardness: A lang. L' is NP-hard if $\forall L \in NP$, $\exists R_L$ s.t. $x \in L \iff R_L(x) \in L'$

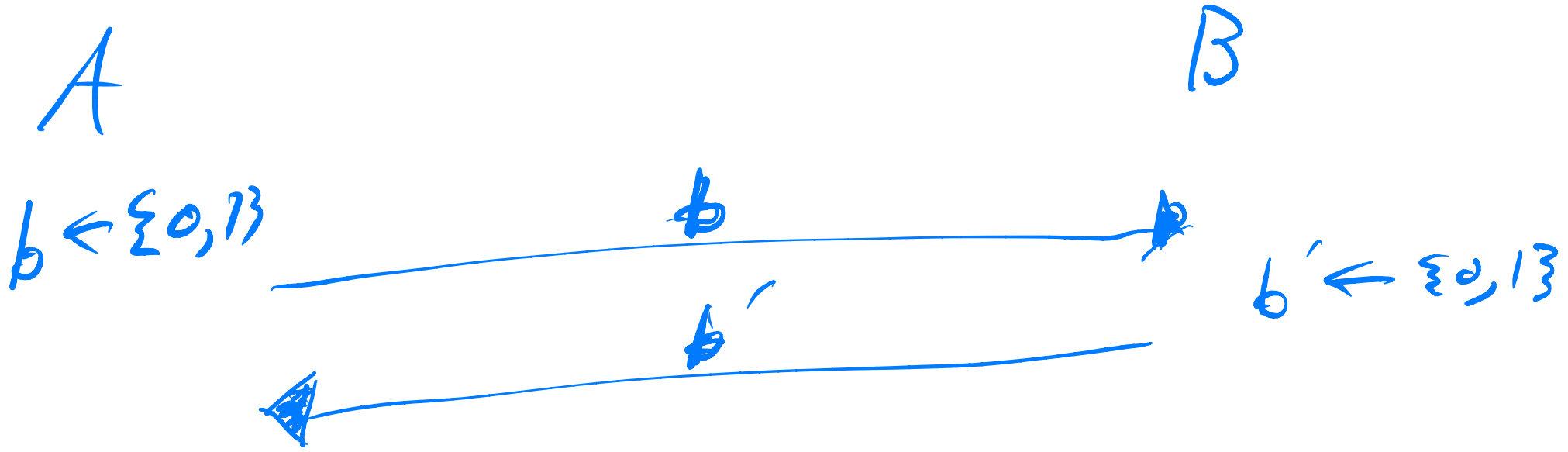
NP-complete: NP-hard and in NP

Thm: Graph 3-coloring is NP-complete

Agenda for this lecture

- Announcements
- Recap from last time
- NP and NP-hardness
- Commitment schemes
- ZKPs for all NP
- ZKP for 3COL + analysis

Commitment schemes



Problem: Can lie about coin flip!

Introduce commitment scheme - hides value
binds to value

Commitment schemes

Definition: A commitment for msg space $\{0,1\}^\ell$ is ppt alg $Com : \{0,1\}^\ell \to \mathcal{C}$

- "Computational" $*$ (statistical) binding: $\forall m_0, m_1 \in \{0,1\}^\ell$, $\forall r_0, r_1 \in \{0,1\}^*$, $Com(m_0; r_0) \neq Com(m_1; r_1)$
  - "Computational" = hard for nuppt algs to collide
  - run Com w/ randomness r_0 / r_1
- ("Statistical" $*$ (computational) hiding: $\forall m_0, m_1$, $Com(m_0) \approx_{c(s)} Com(m_1)$
  - (Prob. over randomness of Com)

Exercise: Show $\exists$ stat. hiding + binding commitment.

Commitment schemes

OWP $f: \{0,1\}^n \to \{0,1\}^n$ w/ hardcore predicate h

Define $\mathrm{Com}[f] : \{0,1\} \to \{0,1\}^n \times \{0,1\}$

$\mathrm{Com}[f](b) :=$

$r \leftarrow \{0,1\}^n$

Ret $(f(r), h(r) \oplus b)$

(Cf. Blum-Micali PRG)

Exercise: Verify $\mathrm{Com}[f]$ hiding + binding.

Thm: one-bit Com $\Rightarrow$ poly-bit Com

Agenda for this lecture

- Announcements
- Recap from last time
- NP and NP-hardness
- Commitment schemes
- ZKPs for all NP
- ZKP for 3COL + analysis

Zero-Knowledge Proofs for NP

(1) Present NP-complete language 3COL

(2) Give ZKP for 3COL, analyze

(1) lang L, $x \in L$. $R_L(x) = x'$ (x' is 3COL instance)

Prove $x' \in$ 3COL

Need to have efficient mapping of L-witnesses to 3COL witnesses.

Efficient mappings always exist.

Agenda for this lecture

- Announcements
- Recap from last time
- NP and NP-hardness
- Commitment schemes
- ZKPs for all NP
- ZKP for 3COL + analysis

ZKP for graph 3-coloring

Definition: Graph $G=(V,E)$ is 3-colorable if $\exists \pi: V \to \{1,2,3\}$ s.t. $\pi(i) \neq \pi(j)$ if $(i,j) \in E$ (*)

Language 3COL is $L = \{G \mid \begin{matrix} G \text{ is graph} \\ G \text{ is 3-colorable} \end{matrix}\}$

$W(G,\pi)$ verifies (*) for all edges

ZKP for graph 3-coloring

$G = [n] \times E$

P(G, π)

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

$k_i = \rho(\pi(i))\ \forall i$

$c_i \leftarrow com(k_i)$

(Let r_i be i^{th} vertex rand.)

V(G)

$c_i\ \forall i \in [n]$ →

$(u,v) \leftarrow E$

← (u, v)

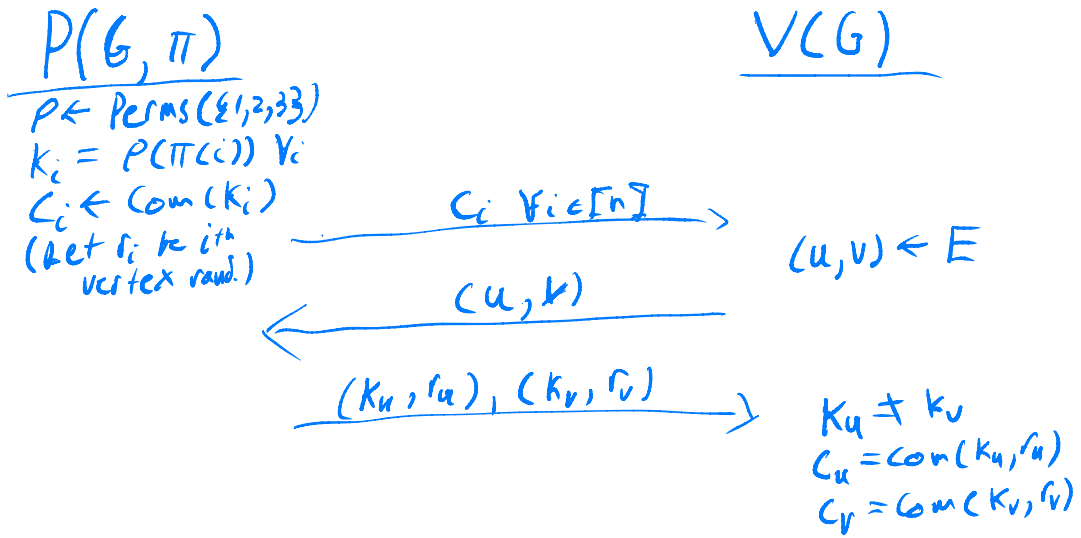
$(k_u, r_u), (k_v, r_v)$ →

$k_u \neq k_v$

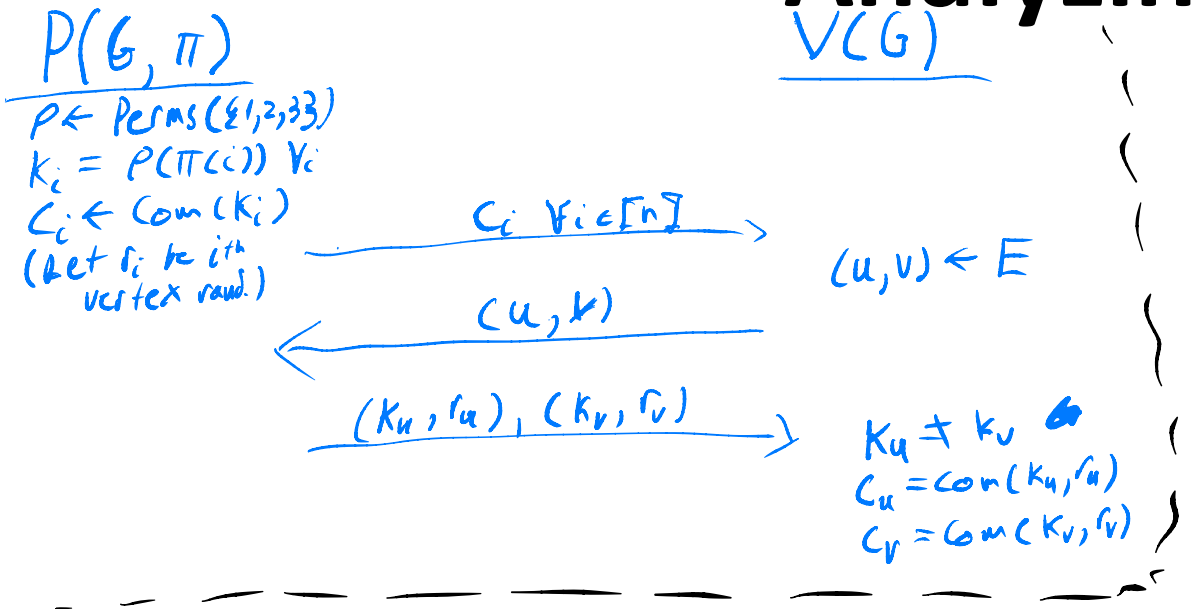
$c_u = com(k_u, r_u)$

$c_v = com(k_v, r_v)$

ZKP for graph 3-coloring



Analyzing 3COL ZKP



✳ Completeness

G is 3-colorable $\Leftrightarrow$ $\pi(u) \neq \pi(v)$

So $P(\pi(u)) \neq P(\pi(v))$

✳ Soundness

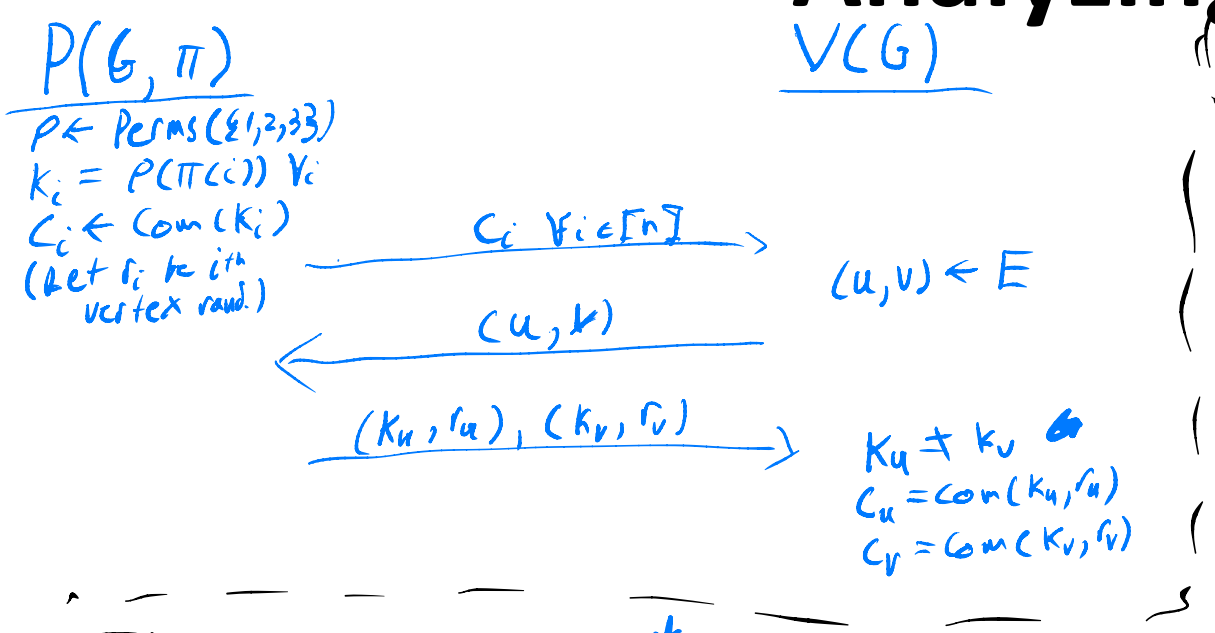
Soundness error $s \leq 1 - \frac{1}{|E|}$

Proof: Statistical binding $\Rightarrow$ Prover sends at least one "bad" edge in its commitments

$Pr[\text{"bad" edge}] \geq \frac{1}{E}$, so

$Pr[P^* \text{ convinces } V] \leq 1 - \frac{1}{|E|}$

Analyzing 3COL ZKP



* Zero-knowledge

$\mathcal{S}^{V^*}(G)$:

$(u,v) \leftarrow E$ (*)

$k_u \neq k_v \leftarrow \{1,2,3\}$

$k_i = 1$ $\forall i \neq u$ or v

$C_i \leftarrow Com(k_i)$

$(u^*, v^*) \leftarrow V^*(C_i\ \forall i)$

IF $(u,v) \neq (u^*, v^*)$: (††)
Goto (*) (at most n^3)

Else
Ret $(C_i, (u^*, v^*), (k_u, r_u), (k_v, r_v))$

Theorem: $\forall V^*$, $View_{V^*}[P(G) \leftrightarrow V^*] \approx_c \mathcal{S}^{V^*}(G)$

Proof sketch:
Conditioned on (††), simulated output is same as P's. Use hiding of Com.