EECS 575: Advanced Cryptography
Fall 2022
Lecture 23

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proof for graph 3-coloring
- Proofs of knowledge (PoK)
- Schnorr’s PoK of discrete log

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proof for graph 3-coloring
- Proofs of knowledge (PoK)
- Schnorr's PoK of discrete log

Announcements

- HW6 due **11/30** (Wednesday)
- Final exam released 11/30, due 12/7
- Go Blue!

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proof for graph 3-coloring
- Proofs of knowledge (PoK)
- Schnorr's PoK of discrete log

Zero-knowledge proofs

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

$P(G, \pi)$:

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

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

$c_i = \text{Com}(k_i; r_i)$

$V(G)$

Hiding

$\{c_i\}$ →

$(v_i, v_j) \leftarrow E$ //

(v_i, v_j) ←

$(k_i, r_i), (k_j, r_j)$ →

$k_i \neq k_j$

$c_i = \text{Com}(k_i, r_i)$

$c_j = \text{Com}(k_j, r_j)$

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

$k_i \neq k_j$.

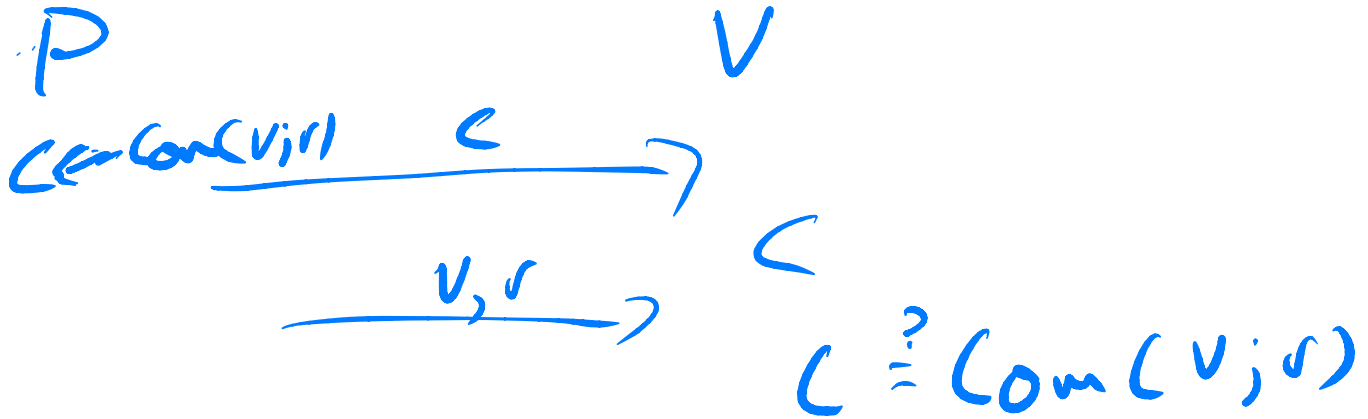
Hides the coloring π from V

ZKP for graph 3-coloring

- Commitment

  $C \leftarrow Com(v; r)$

  - opened:



  - Two security properties
    - Hiding: $\forall v_i, v_j$,
      $\{Com(v_i; r)\} \approx \{Com(v_j; r)\}$
    - Binding: $\exists v_i \neq v_j, r_i, r_j$ s.t.
      $Com(v_i; r_i) = Com(v_j; r_j)$

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proof for graph 3-coloring
- Proofs of knowledge (PoK)
- Schnorr's PoK of discrete log

Analyzing the ZKP for 3-coloring

Thm:
$View_{V^*}[P(G,\pi) \leftrightarrow V^*(G)]$
$\approx_c \$(G)$

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

$(v_i, v_j) \leftarrow E$ (1)
$k_i \neq k_j \leftarrow \{1,2,3\}^2$.
$c_i \leftarrow Com(k_i, r_i)$
$c_j \leftarrow Com(k_j; r_j)$
All others: $c_k \leftarrow Com(1, r_k)$.
$(v_i^*, v_j^*) \leftarrow V^*(G, \{c_i\}, r_V)$
If $(v_i, v_j) = (v_i^*, v_j^*)$:
Finish protocol, output view
Else:
GOTO 1 (up to n^3 iterations)

$View_V[P(x) \leftrightarrow V(x)]$
- all V inputs, randomness, msgs sent by prover

$View_{V^*}[P(G,\pi) \leftrightarrow V^*(G)]$
$= (G, r_V, \{c_i\}, (k_i, r_i), (k_j, r_j))$

- Com hiding
- PCRM P
- negl failure prob.

Analyzing the ZKP for 3-coloring

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

$(u_i, u_j) \leftarrow E$ (1)

$K_i \neq K_j \leftarrow \{1,2,3\}^2$

$C_i \leftarrow Com(K_i; r_i)$

$C_j \leftarrow Com(K_j; r_j)$

All others: $C_k \leftarrow Com(\perp; r_k)$

$(V_i^*, V_j^*) \leftarrow \underbrace{V^*(G, \{C_k\}; r_V)}$

If $(u_i, u_j) = (V_i^*, V_j^*)$:
  Finish protocol, output view

Else:
  GOTO 1 (up to n^3 iterations)

H_0: $View_{V^*}[P(G,\pi) \leftrightarrow V^*(G)]$

H_1: $View_{V^*}[P'(G,\pi) \leftrightarrow V^*(G)]$

P' is honest prover, except rewinds as $\$$

H_2 $View_{V^*}[P''(G,\pi) \leftrightarrow V^*(G)]$

P'' commits to 1 instead of real colors

H_3 $\$^{V^*}(G)$

Analyzing the ZKP for 3-coloring

$V^*(G)$:

$(v_i, v_j) \leftarrow E$ (1)

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

$c_i \leftarrow Com(k_i; r_i)$

$c_j \leftarrow Com(k_j; r_j)$

All others: $c_k \leftarrow Com(\cdot; r_k)$

$(v_i^*, v_j^*) \leftarrow V^*(G, \{c_k\}; r_{V^*})$

If $(v_i, v_j) = (v_i^*, v_j^*)$:
Finish protocol, output view

Else:
Goto 1 (up to n^3 iterations)

H_0: $view_{V^*}[P(G,\pi) \leftrightarrow V^*(G)]$

H_1: $view_{V^*}[P'(G,\pi) \leftrightarrow V^*(G)]$

P' is honest prover, except rewinds as $

$P'(G, \pi)$:

$(v_i, v_j) \leftarrow E$ (1)

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

$\forall k$, $c_k = Com(\rho(\pi(v_k)); r_k)$

$(v_i^*, v_j^*) \leftarrow V^*(G, \{c_k\})$

If $(v_i, v_j) = (v_i^*, v_j^*)$:
Finish with $V^*((\rho(\pi(v_i)), r_i), (\rho(\pi(v_j)), r_j))$

Else
Goto (1) up to n^3 times

$$\left(1 - \frac{1}{x}\right)^x \le e^{-1}$$

$$\left(\left(1 - \frac{1}{n^2}\right)^{n^2}\right)^n \le \left(e^{-1}\right)^n$$

$$\le e^{-n}$$

- Conditioned on $E = (v_i, v_j) = (v_i^*, v_j^*)$,
  $View_{V^*}[P(G,\pi) \leftrightarrow V^*(G)] \approx$
  $View_{V^*}[P'(G,\pi) \leftrightarrow V^*(G)]$
- $Pr[\neg E] = negl$, $\left[(v_i, v_j) \text{ is stat. indep. of } V^* \text{ msgs}!\right]$

$H_0 \approx H_1$

Analyzing the ZKP for 3-coloring

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

$(v_i, v_j) \in E$ (1)

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

$c_i \leftarrow Com(k_i; r_i)$

$c_j \leftarrow Com(k_j; r_j)$

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

$(v_i^*, v_j^*) \leftarrow V^*(G, \{c_i\}; r_V)$

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

Finish protocol, output view

Else:

GOTO 1 (up to n^3 iterations)

H_0: $view_{V^*}[P(G,\pi) \leftrightarrow V^*(G)]$

H_1: $view_{V^*}[P'(G,\pi) \leftrightarrow V^*(G)]$

P' is honest prover, except rewinds as $\$$

H_2 $view_{V^*}[P''(G,\pi) \leftrightarrow V^*(G)]$

P'' commits to 1 instead of real colors

$P''(G,\pi)$:

$(v_i, v_j) \in E$; $P \leftarrow Perms(\{1,2,3\})$ (1)

$c_i = Com(P(\pi(v_i)); r_i)$

$c_j = Com(P(\pi(v_j)); r_j)$

$\forall k \neq i,j$: $c_k = Com(1; r_k)$

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

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

Finish with openings of c_i's

Else

Goto (1) up to n^3 times

$H_1 \approx_c H_2$ by hiding of Com

Analyzing the ZKP for 3-coloring

To finish, argue $View_{V^*}[P''(G,\pi) \leftrightarrow V(G)] \approx \$(G)$

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

$(v_i, v_j) \leftarrow E$ (1)

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

$c_i \leftarrow Com(k_i; r_i)$

$c_j \leftarrow Com(k_j; r_j)$

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

$(v_i^*, v_j^*) \leftarrow V^*(G, \{c_i\}; r_{V^*})$

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

Finish protocol, output view

Else:

GOTO 1 (up to n^3 iterations)

$P''(G, \pi)$:

$(v_i, v_j) \leftarrow E$; $P \leftarrow Perm(\{1,2,3\})$ (1)

$c_i = Com(P(\pi(v_i)); r_i)$

$c_j = Com(P(\pi(v_j)); r_j)$

$\forall k \neq i,j$: $c_k = Com(1; r_k)$

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

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

Finish with openings of c_i's

Else

Goto (1) up to n^3 times

Because P is random perm,

$View_{V^*}$ is identical in H_2 and H_3

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proof for graph 3-coloring
- Proofs of knowledge (PoK)
- Schnorr's PoK of discrete log

NP relations

Proofs of knowledge (PoK)

$G = \langle g \rangle$ $\quad L = \{(x, X) : g^x = X\}$

$P(x)$ $\quad V(X)$

Return 1

Want to require prover to "know why"

$X \in L$ if it convinces verifier

Formalize via "extraction":

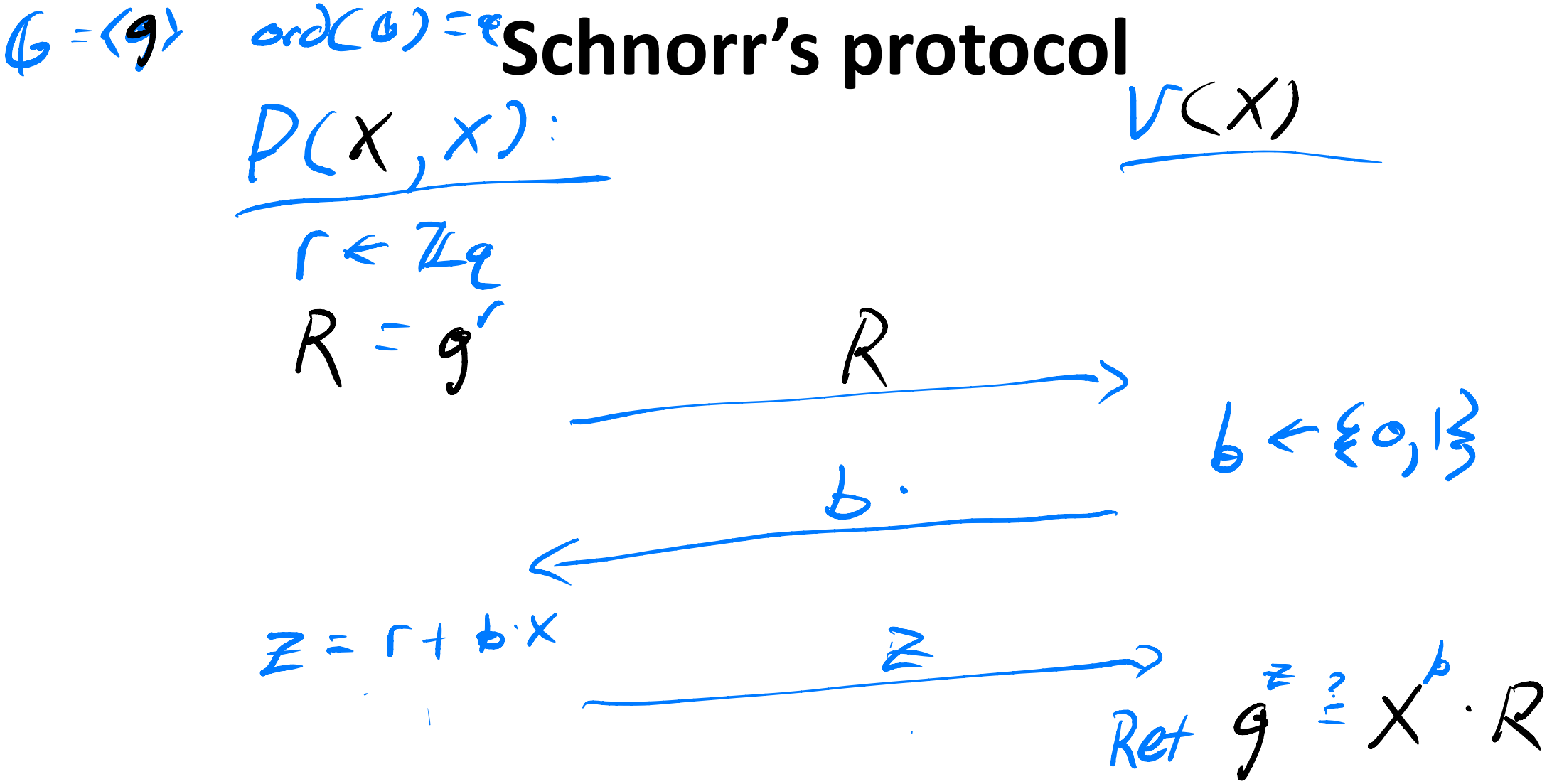
can obtain witness from prover

Proofs of knowledge (PoK)

Agenda for this lecture

- Announcements
- Recap from last time
- Zero-knowledge proof for graph 3-coloring
- Proofs of knowledge (PoK)
- Schnorr's PoK of discrete log

Schnorr's protocol



Schnorr's protocol

Why can we extract x from P?

If prover can answer z for $b=0$ and $b=1$, z_0 z_1

can compute $x = z_1 - z_0$

Continue Wednesday