EECS 575: Advanced Cryptography
Fall 2022
Lecture 24

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Knowledge error of Schnorr's PoK
- Non-interactive proofs via Fiat-Shamir
- Polynomial commitments (PCs)
- PCs from pairings (KZG)

Monday

Agenda for this lecture

- Announcements
- Recap from last time
- Knowledge error of Schnorr's PoK
- Non-interactive proofs via Fiat-Shamir
- Polynomial commitments (PCs)
- PCs from pairings (KZG)

Announcements

- HW6 due TODAY
- Final exam released TODAY, due 12/7

Agenda for this lecture

- Announcements
- Recap from last time
- Knowledge error of Schnorr's PoK
- Non-interactive proofs via Fiat-Shamir
- Polynomial commitments (PCs)
- PCs from pairings (KZG)

Schnorr's proof of knowledge

$G = \langle g \rangle$ $\text{ord}(G) = q$

$P(x, X)$:

$r \leftarrow \mathbb{Z}_q$

$R = g^r$

R →

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

← b

$z = r + b \cdot x$

z →

$V(X)$

Ret $g^z \stackrel{?}{=} X^b \cdot R$

Agenda for this lecture

- Announcements
- Recap from last time
- Knowledge error of Schnorr's PoK
- Non-interactive proofs via Fiat-Shamir
- Polynomial commitments (PCs)
- PCs from pairings (KZG)

Defining proofs of knowledge

NP Relation $R \subseteq \{0,1\}^* \times \{0,1\}^*$

Det. alg. $W(x, w)$

- poly-time in $|x|$
- 0/1 output reject/accept

$R = \{(x, w) : W(x, w) \text{ accepts}\}$

language $L_R = \{x : \exists w \text{ s.t. } W(x, w) \text{ accepts}\}$

$W(\overline{x}, x) = \begin{cases} 1 & \text{if } g^x = \overline{x} \\ 0 & \text{o/w} \end{cases}$; $R_{dl} = \{(\overline{x}, x) : g^x = \overline{x}\}$

G Z_q

Defining proofs of knowledge

An IP (P,V) is a PoK for an NP relation R with knowledge error $\beta \in [0,1]$

if $\exists K$, n.u.ppt TM with oracle access to P^*

s.t. $\forall x \in L_R$, $\forall P^*$ s.t.

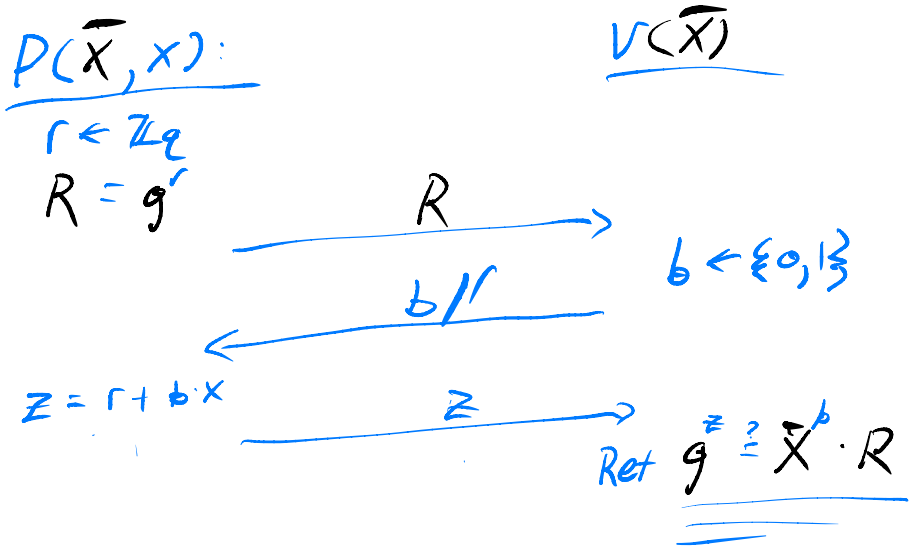
$R = 0$?

$R(x) = \{w : (x,w) \in R\}$

$\varepsilon_x^{P^*} = \Pr[\text{out}_V[P^*(x) \leftrightarrow V(x)] = 1] > \beta$

$\Pr[K^{P^*}(x) \in R(x)] \geq \text{poly}(\varepsilon_x^{P^*} - \beta)$ (non-trivial)

Knowledge error of Schnorr



$P^*(\bar{x})$:

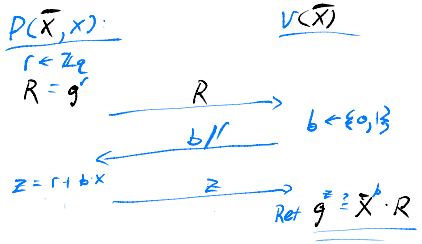
[$b \leftarrow \{0,1\}$]

$z \leftarrow \mathbb{Z}_q$

$R = g^z / \bar{x}^b$

↳ Cheating prover wins w.p. $1/2$

Knowledge error of Schnorr



Thm: Schnorr protocol is PoK with knowledge error $k = 1/2$

Proof:

$K^{P^*}(\bar{x})$:

1. Run $P^*(\bar{x})$, get R
2. Reply with $b=0$, gets a_0
3. Rewind P^* to before (2), reply $b=1$ to get a_1
4. Output $a_1 - a_0$

If P^* convinces V w.p. $\geq 1/2 + \epsilon$,

then

$\Pr[K^{P^*}(\bar{x}) \in R(\bar{x})] \geq \epsilon^2/2$

$\Pr[a_0$ and a_1 correct$] \geq \epsilon^2/2$

(R, b, a_b) is accepting

$g^{a_b} = \bar{x}^b \cdot R$

Knowledge error of Schnorr

$P_r = Pr[P^*(\bar{x}) \text{ convinces } V \mid R = r]$

Have that $Pr_{r \leftarrow P^*}[P_r \geq 1/2 + \alpha/2] \geq \alpha/2$

by averaging (see Pass-shelat)

Now take r s.t. $P_r \geq 1/2 + \alpha/2$

Define $P_{r,b} = Pr[P^* \text{ convinces } V \mid R = r, \text{challenge } b]$

Both $P_{r,0}$ and $P_{r,1} \geq \alpha$

$Pr[P^* \text{ convinces } V \text{ with } b=0 \wedge P^* \text{ convinces } V \text{ with } b=1 \mid R=r] \geq \alpha^2$

$Pr[q_0 \text{ and } a_1 \text{ correct}] \geq \alpha^2 \cdot \alpha/2 = \alpha^3/2$

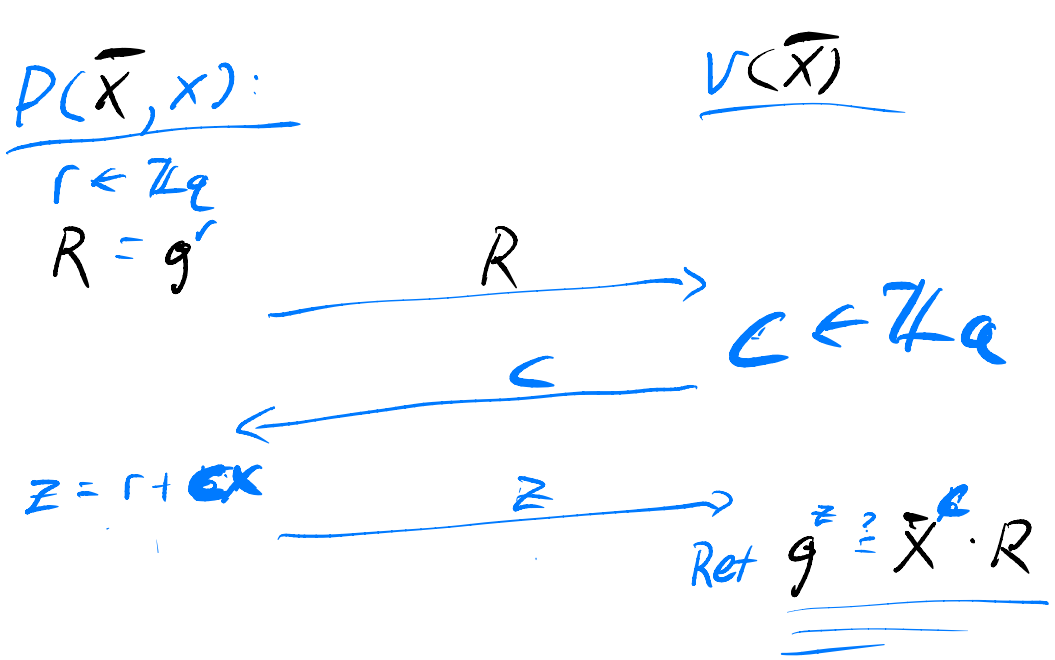
Boneh-Shoup Section on Schnorr/Sigma protocols "forking"

$\boxtimes$

Agenda for this lecture

- Announcements
- Recap from last time
- Knowledge error of Schnorr's PoK
- Non-interactive proofs via Fiat-Shamir
- Polynomial commitments (PCs)
- PCs from pairings (KZG)

The Fiat-Shamir transform



H(R) ≈ without public input x̄

breaks adaptive Knowledge Soundness

Fiat-Shamir:

Prover "simulates" verifier via random oracle.

Applx H(x̄, R) to derive b.

Output (R, H(x̄, R) =: b, z = r + bx)

Agenda for this lecture

- Announcements
- Recap from last time
- Knowledge error of Schnorr's PoK
- Non-interactive proofs via Fiat-Shamir
- Polynomial commitments (PCs)
- PCs from pairings (KZG)

Polynomial commitments

Agenda for this lecture

- Announcements
- Recap from last time
- Knowledge error of Schnorr's PoK
- Non-interactive proofs via Fiat-Shamir
- Polynomial commitments (PCs)
- PCs from pairings (KZG)

Background on pairings

KZG commitments