EECS 575 FA 21

Lecture 21

Proofs of knowledge

Announcements

- HW6 due 11/22
- Explaining absence

Recap from last time

- HVZK

An interactive proof system P, V is HVZK for L if $\exists$ nuppt S s.t. $\forall x \in L$

$$\text{View}_V[P(x) \leftrightarrow V(x)] \approx_c S(x)$$

"View" includes prover's msgs, verifier's msgs, and random coins of verifier

"Full" zero-knowledge

An IP for lang L is fZK if $\forall$ nuppt V^*
$\exists$ nuppt simulator S s.t. $\forall x \in L$:

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

Exercise: what are the differences b/ws this fZK and the previous HVZK?

Proof of Knowledge

- "Soundness" meaning
  ∃ witness s.t. statement is true

Identification protocols
Smart cards
Prove your identity to a verifier

Public/identity g^x
priv key : x

Regular soundness doesn't guarantee "knowledge" of x

PoK of discrete logarithm

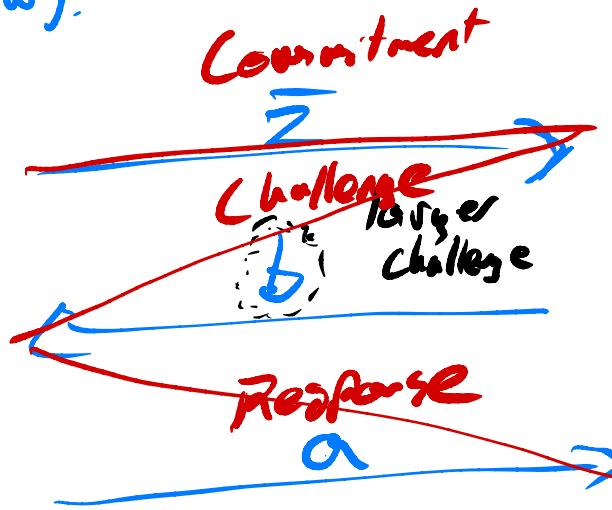
Let $G = \langle \bar{g} \rangle$, $ord(g) = q$.

Public group element $\bar{X}$, $\log_{\bar{g}}(\bar{X}) = w$

Prover$(\bar{X}, w)$:

$r \leftarrow \mathbb{Z}_q$

$\bar{z} = \bar{g}^r$



Verifier$(\bar{X})$

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

$a = r + bw$

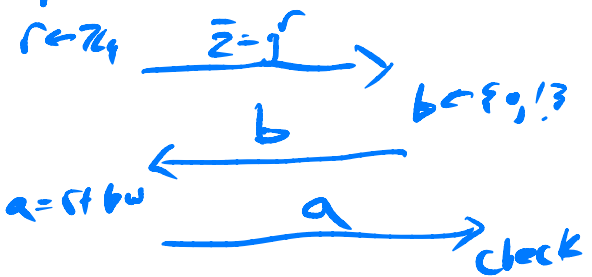
Output

$\bar{g}^a = \bar{z} \cdot \bar{X}^b$

Schnorr protocol

Fiat-Shamir

Sigma protocol



Discrete log PoK:

- Complete?
  If $x = g^w$ then
  (*) $g^a = g^{r+wb} = z \cdot x^b$ ✓
- Zero knowledge? ✓

Idea: come up with simulator $S^{V^*}(x)$ that simulates view of any supposed V^*

- Sample $r \leftarrow Z_q$; output g^r
- Sample random $b \leftarrow \{0,1\}$; return b
- Sample random $a \leftarrow Z_q$, output either a or r

1 Choose random bit $b \leftarrow \{0,1\}$, random $a \leftarrow Z_q$

2 Send $z = g^a / x^b$ to V^*, get back bit b^*

3 If $b^* = b$, output (z, b, a). Else "rewind" V^* and try again (goto 1)

Check: dist. of S^{V^*}'s output is comp. ind. from real exec.

PoK for discrete log

- Does a prover who convinces a verifier "know" the discrete log w of $\bar{x}$?
  → Formalize new "proof of knowledge"

Auxiliary notion: NP relation.

$R \subseteq \{0,1\}^* \times \{0,1\}^*$ given by det. alg. $W(\cdot,\cdot)$, runs in poly-time in first input length

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

Can get NP lang $L_R = \{x : \exists w \text{ s.t. } W(x,w) \text{ accepts}\}$

E.g. discrete log:

$$R = \{(\bar{x} \in \mathbb{G}, w \in \mathbb{Z}_q) : \bar{g}^w = \bar{x}\}$$

PoK for discrete log

An (P,V) is a PoK for R with "knowledge error" K if $\exists$ oracle machine K (the "extractor") s.t.

$\forall x \in L_R$, $\forall P^*$ s.t. $\Pr[\text{out}_V[P^* \leftrightarrow V(x)] = 1] = p_x^*$

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

- $\forall x$: every x
- P^*: possibly unbounded
- $K^{P^*} \in R(x)$: efficient to check
- p_x^*

PoK for discrete log

Theorem: The previous dlog protocol is a proof of knowledge for the discrete log relation, with $\kappa = 1/2$.

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

- Run P^*, obtain $\bar{z}$ $(= \bar{g}^r)$
- Send $b=0$ to P^*, get a_0
- Rewind P^*, send $b=1$, get a_1
- output $a_1 - a_0$

$a_1 = r + w$

$a_0 = r + 0 \cdot w$

$a_1 - a_0 = w$

To finish: Show that $P_1[K^{P^*} \in R(\bar{x})] \geq \text{poly}(\alpha)$

PoK for discrete logarithm

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

- Run P^*, obtain $\bar{z}$ $(= g^r)$
- Send $b=0$ to P^*, get a_0
- Rewind P^*, send $b=1$, get a_1
- output $a_1 - a_0$

Suppose

$$\Pr[\text{out}_V[P^* \leftrightarrow V] = 1] = \tfrac{1}{2} + \alpha$$

Claim:

$$\Pr[K^{P^*}(\bar{x}) = w] = \Pr[a_0 \text{ and } a_1 \text{ correct}] \geq \alpha^3/2 = \text{poly}(\alpha)$$

Proof:

Define $P_{\bar{z}} = \Pr[P \text{ convinces } V(x) \mid P^*\text{'s first message is } \bar{z}]$

Must have $\Pr_{\bar{z} \leftarrow P^*}\left[P_{\bar{z}} > \tfrac{1}{2} + \alpha/2\right] \geq \alpha/2$

Define $P_{\bar{z},b}[P^* \text{ convinces } V(x) \mid P^*\text{'s first msg is } \bar{z} \text{ and } V(x)\text{'s bit is } b]$

$P_{\bar{z}} = (P_{\bar{z},0} + P_{\bar{z},1})/2$, so $P_{\bar{z},0}$ and $P_{\bar{z},1} \geq \alpha$. $P_{\bar{z},0}$ and $P_{\bar{z},1}$ indep.

$$\Pr[a_0 \text{ and } a_1 \text{ correct}] \geq \alpha^3/2 \quad \boxtimes$$