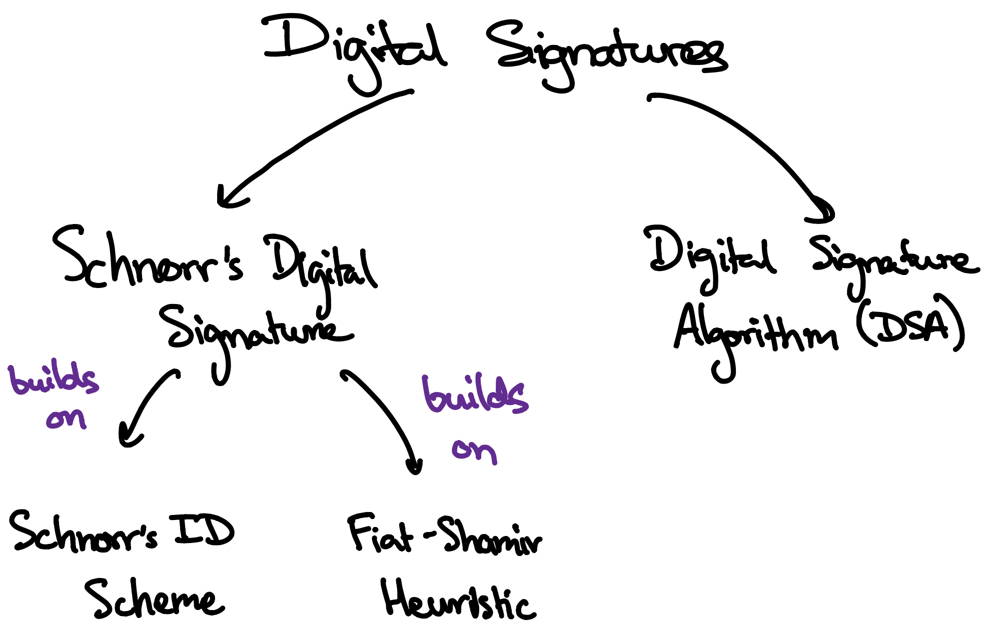
6.857 Recitation 6 4/2/21

I. Roadmap



II. Schnorr's ID Scheme

<u>Goal</u>: Holder of secret key (sk) should be able to convince others they hold the sk without revealing info about it

$\rightarrow (pk, sk) = (g^x, x)$

<u>Setup</u>:

- Pick prime number q
- We work in mod p, where $p = q \cdot r + 1$

- $G = \{h^r \bmod p,\ h \in \mathbb{Z}_p^*\}$

  r^{th} power residues

  $|G| = q$

- Generator g for G

  Choose $h \in \mathbb{Z}_p^*$ s.t. $h^r \neq 1 \pmod p$

  Let $g = h^r \pmod p$

Proof of Knowledge

- Holder picks secret key $x \in \mathbb{Z}_q$
  publishes PK g^x

Prover (P)		Verifier (V)
(knows x)		(knows g^x)

commit $\rightarrow$

$k \leftarrow \mathbb{Z}_q$ $\xrightarrow{r = g^k \pmod p}$

challenge $\leftarrow$

V picks $e \leftarrow \mathbb{Z}_q$

$\xleftarrow{e}$

response $\rightarrow$

P responds with quantity to convince V $\xrightarrow{s = k - xe}$ V accepts iff

$$g^s = \frac{r}{PK^e}$$

Why the check works?

$$g^s = g^{k-xe} = \frac{g^k}{(g^x)^e} = \frac{r}{PK^e} \quad \checkmark$$

Why does this work?

2 properties:

1) Prover must know x if he can answer most challenges

in the form $\xleftarrow{e_i}$ $\xrightarrow{s_i}$

Proof: Suppose P responds to challenges e_1 and e_2 with s_1 and s_2.

$$g^{s_1} = \frac{r}{pk^{e_1}} \qquad g^{s_2} = \frac{r}{pk^{e_2}}$$

$$\underbrace{g^{s_1} \cdot pk^{e_1} = g^{s_2} \cdot pk^{e_2}} = r$$

$$g^{s_1 - s_2} = pk^{(e_2 - e_1)}$$

$pk = g^x$

$$g^{s_1 - s_2} = g^{x(e_2 - e_1)}$$

$$s_1 - s_2 = x(e_2 - e_1)$$

$$x = \frac{s_1 - s_2}{e_2 - e_1}$$

P must know x!

2) V gains no information about x.

Key assumption: V is honest
(i.e. V picks e from $\mathbb{Z}_q$ at random)

Proof: Verifier can generate a valid interactive transcript on their own WITHOUT knowledge of x.

How?

V chooses e, s at random from $\mathbb{Z}_q$

V uses e, s to compute r:

$$r = g^s \cdot pk^e$$

V's transcript $= (pk, r, e, s)$

* The type of interaction seen in Schnorr's ID scheme is called Honest Verifier Zero Knowledge.

III. Fiat-Shamir Heuristic

- Converts an interactive proof of knowledge into a digital signature

How to convert Schorr's ID scheme?

- In challenge step, V sends to P
  $e = H(m, r)$
  * H is CR hash function
  * Assuming ROM

- Scheme:

  $\text{Sign}(sk, m) = (r, e, s)$

  $\text{Verify}(pk, m, (r, e, s))$:
  accept if ID scheme verifier accepts

IV. Schnorr's ID Scheme Example

- We'll use $q=5$ and $p=11$
  - → In practice, q is 160 bits to avoid discrete log attacks.
    p is selected to be 1024 bits to avoid birthday paradox attacks

Setup: $q=5$, $p = 5 \cdot \underset{\overset{\uparrow}{r}}{2} + 1 = 11$

$$G = \{h^2 \bmod 11, h \in \mathbb{Z}_{11}^*\}$$
$$= \{1, 4, 9, 5, 3\}$$

For generator g, we pick h from $\mathbb{Z}_{11}^*$.
Say we pick $h=9 \Rightarrow g = 9^2 \pmod{11}$
$g = 4$

PoK: User runs Gen to produce (SK, PK) pair (x, g^x).

Say we picked $x=3$ randomly from $\mathbb{Z}_q$
$\longrightarrow g^x = 4^3 \pmod{11} = 9$

Run 3-phase protocol:

P		V
$k \leftarrow \mathbb{Z}_q$, say P drew $k=2$		
commit $\rightarrow$	$r = 4^2 \pmod{11} = 5$ $\longrightarrow$	
		$e \leftarrow \mathbb{Z}_q$, Say V drew $e=1$
challenge $\leftarrow$	$\longleftarrow$ $e=1$	
response $\rightarrow$	$s = 2 - 3 \cdot 1 \pmod{q} = 4$ $\longrightarrow$	

Verifier's check:

$$g^s \pmod{p} = 4^4 \pmod{11}$$
$$= 3$$

$$r / pk^e \pmod{p} = r \cdot (pk^e)^{-1} \pmod{p}$$
$$= 5 \cdot (9^1)^{-1} \pmod{11}$$
$$= 5 \cdot 5 \pmod{11}$$
$$= 3 \checkmark$$

$\Longrightarrow$ P must know the discrete log of the public key $g^x = 9$ in modulo 11.

V. Digital Signature Algorithm (DSA)

- Nearly identical to Schnorr's Signature Scheme.

  Changes:

  - In the commit phase,

    $$r = g^k \pmod{p} \pmod{q}$$

    → produces shorter signatures

  - V's challenge to P is $e = H(m)$ instead of $H(m, r)$

Full scheme details are in Lecture 12 notes.