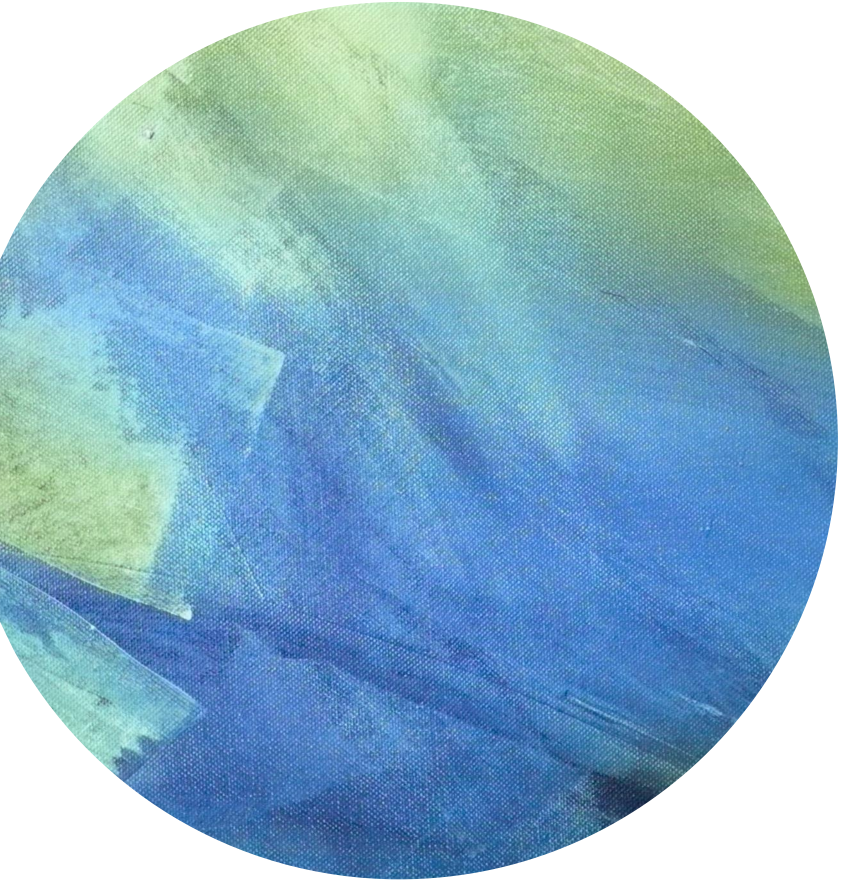
Lecture 17

Scribe: Alec



Outline

Schnorr Signatures

Commitments

Schnorr Signatures

Schnorr Signatures

- Signatures from groups
  - Gen outputs (vk = g^x, sign key = x)
  - Sign (m, sign key) :
  - Verify (σ, vk, m) :

vk : g^x sk : x

A B

$\xrightarrow{g^x}$

$\xleftarrow{g^y}$

$\xrightarrow{g^{xy}}$

For random x and y, given g^x, g^y

hard to compute g^{xy}

Schnorr Signatures

Prove I know x! without revealing x.

vk = g^x

sign key = x

$r \leftarrow \mathbb{Z}_p^*$

$s = (r + p \cdot x)$

$X = g^x, R = g^r \longrightarrow$

$\longleftarrow$ challenge $= p$

$s \longrightarrow$

$g^x = X$, $g^r = R$

$g^s = S$.

$g^s = g^r \cdot (g^x)^p$

$g^x, g^r, p, s = (r + p \cdot x)$

REWINDING. – Alice

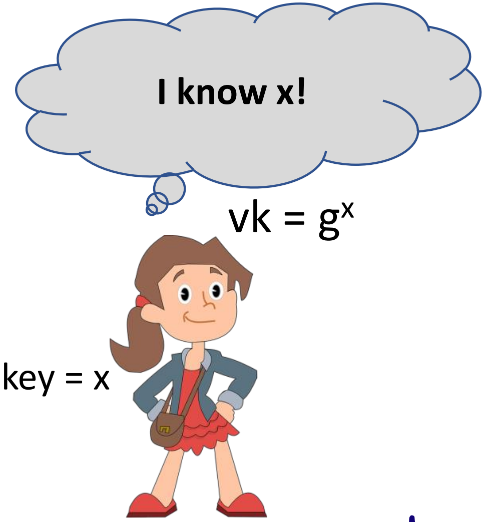
g^x, g^r

$\longleftarrow$ challenge ✓ $\longleftarrow$ challenge$_2$

response $\longrightarrow$ ✓ response$_2$ $\longrightarrow$

Schnorr Signatures

Wrapper



vk = g^x

sign key = x

$g^x, g^r \rightarrow$

$\leftarrow p_1$

$s_1 = r + p_1 x \rightarrow$

$\leftarrow p_2$

$s_2 = r + p_2 x \rightarrow$

If Alice responds w.p. $\frac{1}{2}$

then w.p. $1-2^{-(n-1)}$,

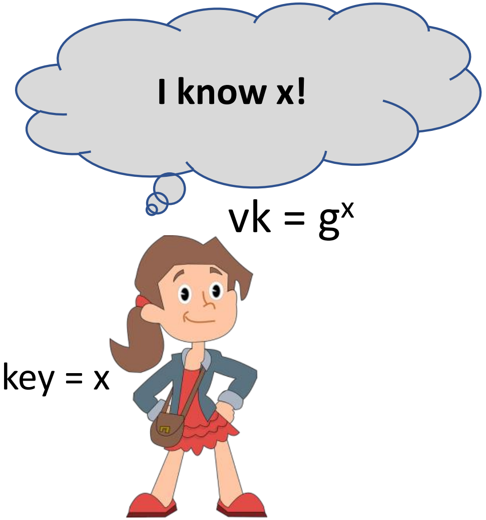
in n trials, she

responds in at least 2 trials

$$s_1 - s_2 = (p_1 - p_2)\,x$$

$$x = \left(\frac{s_1 - s_2}{p_1 - p_2}\right)$$

Schnorr Signatures



vk = g^x

sign key = x

g^x, g^r $\longrightarrow$

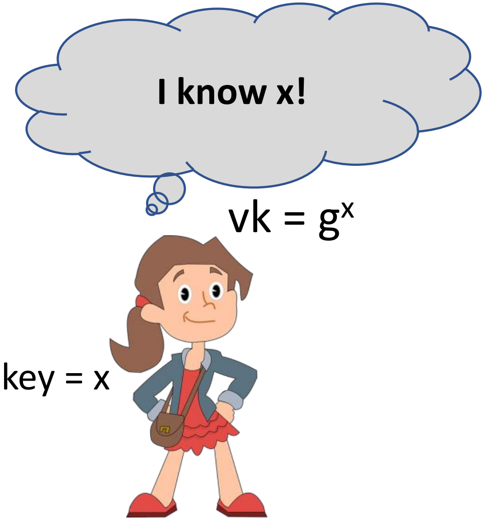
p $\longleftarrow$

p picked randomly

s $\longrightarrow$

$s = r + px$

Schnorr Signatures



vk = g^x

sign key = x

vk

randomness

$$g^x, \; g^r,$$

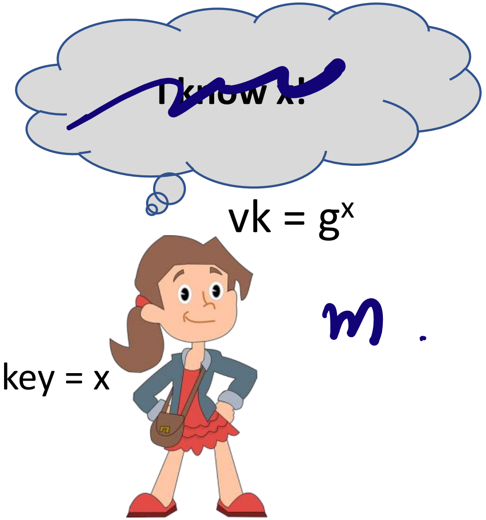
$$p = H(g^x \| g^r),$$

$$s = r + px$$

$$\xrightarrow{s = r + px}$$

Sign:

Schnorr Signatures



vk = g^x

sign key = x

m.

vk ↓ randomness ↓

$g^x, g^r, M.$

$$p = H(g^x \| g^r \| M)$$

$s = r + px$

$$s = r + px \longrightarrow$$

Schnorr Signatures

- Signatures from groups
  - Gen outputs (vk = g^x, sign key = x)
  - Sign (m, sign key) = $R=g^r$, $h=H(m,R)$, $s = r + hx$. Output (h,s)
  - Verify (σ, vk, m) : Check if $h = H(m,g^s X^{-h})$
- Is this secure?

Schnorr Signatures

$\mathcal{A}$

$\xrightarrow{vk}$

- Signatures from groups
  - Gen outputs (vk = g^x, sign key = x)
  - Sign (m, sign key) = $R=g^r$, h=H(m,R), s = r + hx. Output (R,s)
  - Verify (σ, vk, m) : Check if $g^s = RX^h$ for h = H(m,R)
- Is this secure?

A forger can be used to get distinct signatures (h1,s1), (h2,s2) with same (m,R) (different h, by programming the RO), and that lets us solve for x

Schnorr Signatures

$vk = g^x$

$\cancel{vk = g^x}$

(m, σ)

$(m, R = g^r)$

p

(p')

$s = r + p \cdot x$

$s' = r + p' \cdot x$

$$x = \frac{s - s'}{p - p'}$$

Schnorr Signatures

$vk = g^x$

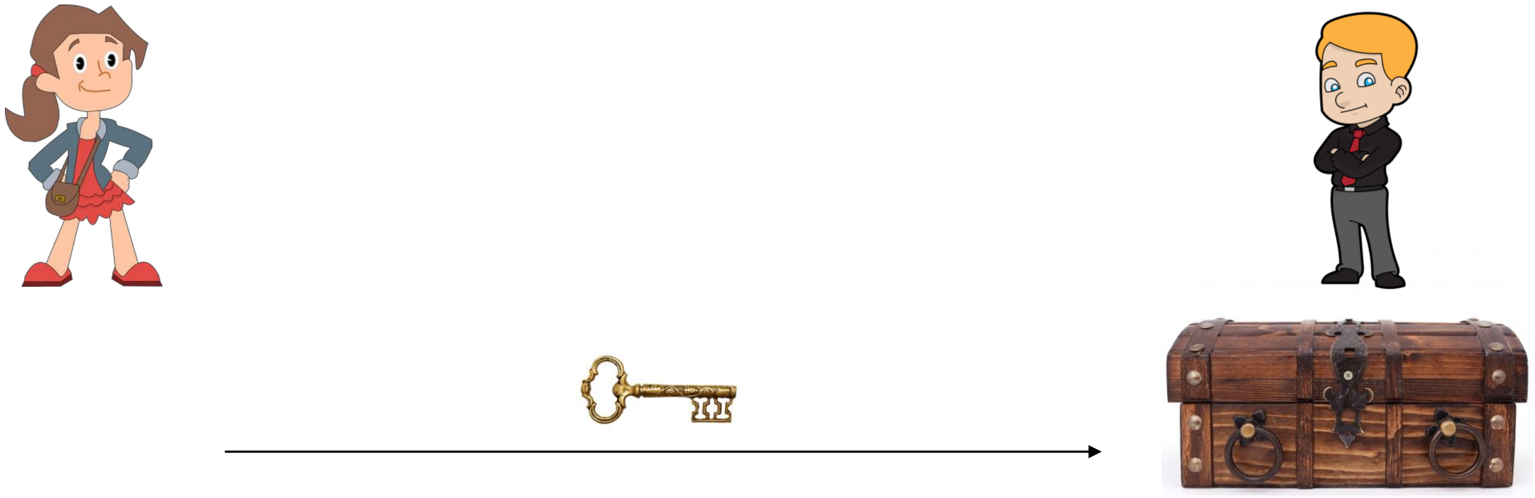
m

Commitments

Commitments

Commitments

Commitments



Commitments

- Hiding

- Binding

Examples

- If (g, g^x) a commitment to x?

- Ct = E (k, m) for a symmetric key encryption E

Examples

In practice, we use:

- To commit to message M, choose random, fixed-length r, send H(r || M)
- To open commitment, send r, M
- Receiver cannot fully recover M.

- Sender cannot find another M’ to open.