Schnorr Signatures
Schnorr Signatures

• Signatures from groups
  • Gen outputs (vk = g^x, sign key = x)

• Sign (m, sign key) :

• Verify (σ, vk, m) :
Schnorr Signatures

\[ g^x = X, \quad g^r = R \]
\[ g^s = S \]

**Prove I know x!**

\[ \text{vk} = g^x \]

\[ \text{sign key} = x \]

\[ r \leftarrow Z_p^* \]

\[ B = (r + p \cdot x) \]

**Challenge**

\[ X = g^x, R = g^r \]

\[ \text{challenge} = p \]

**Rewinding**

\[ g^s = g^r \cdot (g^x)^p \]

\[ g^x, g^r, p, s = (r + p \cdot x) \]
Schnorr Signatures

I know x!

sign key = x

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

\[ S_1 = r + px \]

\[ S_2 = r + p_2x \]

\[ S_1 - S_2 = (p_1 - p_2)x \]

\[ x = \frac{S_1 - S_2}{p_1 - p_2} \]
Schnorr Signatures

\[ \text{sign key} = x \]

\[ \text{I know } x! \]

\[ \text{vk} = g^x \]

\[ S = r + px \]
Schnorr Signatures

\[ vk = g^x \]

I know \( x \)!

sign key = \( x \)

\[ S = r + px \]

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

\[ S = r + px \]
Schnorr Signatures

\[ \text{Sign} \]

- Public key: \( \text{vk} = g^x \)
- Sign key: \( x \)
- Message: \( m \)
- Randomness: \( r \)

Signature calculation:

\[ S = r + px \]

Verification:

\[ v_k = g^x \]

\[ p = H(g^x || g^r || M) \]
Schnorr Signatures

- Signatures from groups
  - Gen outputs (vk = g^x, sign key = x)

  \[
  \text{Sign} (m, \text{sign key}) = R = g^r, h = H(m, R), s = r + px. \quad \text{Output} (h, s)
  \]

- Verify (\sigma, vk, m) : Check if \( h = H(m, g^sX^{-h}) \)

- Is this secure?
Schnorr Signatures

• Signatures from groups
  • Gen outputs \((vk = g^x, \text{sign key} = x)\)
  
  • Sign \((m, \text{sign key}) = R = g^r, h = H(m, R), s = r + hx. \text{Output} (R,s)\)

  • Verify \((σ, vk, m) : \text{Check if } g^s = RX^h \text{ for } h = H(m, R)\)

• Is this secure?

  A forger can be used to get distinct signatures \((h_1, s_1), (h_2, s_2)\) with same \((m, R)\) (different \(h\), by programming the RO), and that lets us solve for \(x\)
Schnorr Signatures

$$vk = g^x$$

$$(m, \sigma)$$

$$s = r + px$$

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

$$x = \frac{S - S'}{p - p'}$$
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.