

Sept 29

- ✓ HW 1 & 2 → Markov process
- ✓ Groups (selfish mining)
- ✓ Diffie Helman & Attacks against finalization & parking
- ✓ Schnorr Signatures

Group Theory

Properties

- collection of elements
- operator $\oplus$
- $A \oplus I = A$ identity element
- $A \oplus A^{-1} = I$ there exists an inverse element
- Closure - $A \oplus B$ is element of the set
- associativity - $(A \oplus B) \oplus C = A \oplus (B \oplus C)$
- commutativity $A \oplus B = B \oplus A$ (Abelian groups)
- repeated group $\oplus$? multiplication by a scalar $n \oplus A = \underbrace{A \oplus A \oplus \dots \oplus A}_{n \text{ times}}$
- Cryptographically interesting groups do not have efficient inverse multiplication.

$$a \otimes (b \otimes c) \stackrel{?}{=} b \otimes (a \otimes c)$$

$$(C \oplus C \oplus \dots \oplus C)$$

$$\underbrace{(C \oplus \dots \oplus C)}_{b \text{ times}} \oplus \underbrace{(C \oplus \dots \oplus C)}_{b \text{ times}}$$

a times

$$C \oplus C \oplus \dots \oplus C$$

a * b times

group Generator (G)

element s.t. every element of group

is $x \otimes G$

Elliptic curve groups

$\Rightarrow \mathbb{Z}_p^*$ = Group of integers ($\mathbb{Z}$) operator multiplication over mod p

$$\mathbb{Z}_{120}^+ \quad G \text{ is } 10$$

10, 20, 30, 40, 50, ... 90

Diffie Helman key exchange

Construct a shared ^{private} key over a public channel

Alice

Bob

Pick random scalar

a

$$A = a \otimes G$$

b

$$B = b \otimes G$$

Share A

Share B

alice computes

$$a \otimes B$$

bob computes

$$b \otimes A$$

$$a \otimes (b \otimes G) \stackrel{?}{=} b \otimes (a \otimes G), \text{ Same \#}$$

Yay! But beware of MITM attack!

Schnorr Signatures

m = message

x = private key

G = group generator

k = random ^{secret} nonce

$$P = x \oplus G$$

$$R = k \oplus G$$

to sign calculate: $\Rightarrow$ Cryptographic hash use this value as a scalar in the field of G

$$\Rightarrow s = k + H(R.P.m) \cdot x$$



$$s - k = \frac{H(\dots) \cdot x}{H(R.P.m)}$$

Signature = (R, s)

Verify a signature:

$$s \oplus G = (k + H(R.P.m) \cdot x) \oplus G$$

$$= (k \oplus G) \oplus (H(R.P.m) \cdot x) \oplus G$$

$$= R \oplus H(R.P.m) \oplus P$$

$$\rightarrow \frac{s - k}{H(R.P.m)} = x$$

Verifies
has s & G

Verifier has all of these

$$\Rightarrow s = H(P.m) \cdot x$$

check

$$x = \frac{s}{H(P.m)}$$

$$s \oplus G = H(P.m) \cdot x \oplus G$$

$$H(P.m) \oplus P$$

Public

Verifier can compute!

• 2 sigs same nonce k

$$(R_0, S_0) \quad M, P \quad \left| \quad R_0 = R_1 \quad (R_1, S_1) \quad M, P \right.$$

$$S_0 - S_1 = k + H_0 x - (k + H_1 x)$$

$$= H_0 x - H_1 x$$

$$= (H_0 - H_1) x$$

$$\frac{S_0 - S_1}{H_0 - H_1} = x$$