Class 3: Elliptic Curves

Schedule

Project 1 is due **Friday, 30 January**.

Before the next class (Monday, Jan 26):

- **Read:** Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. The is the original bitcoin paper, which is quite readable.
- **Read:** *Chapter 5: Transactions* from Andreas Antonopoulos' book.

Asymmetric Cryptosystems Recap

For asymmetric cryptography, we need a one-way function with a trapdoor: a function that can be easily inverted given a secret key, but is hard to invert without knowledge of that key.

Signatures: Signer encrypts a message with her own private key. Verifier checks the message using the signer's public key.

Elliptic Curve Cryptography

Elliptic curve: points satisfying an equation like $y^2 = x^3 + 7$ (this is the curve used in bitcoin).

For real numbers, this is easy to solve: $y = \sqrt{(x^3 + 7)}$.

In a finite field, it is complex enough to form the basis of cryptographic operations.

Crash Course in Group Theory

Group: A group is a set, G, on which the operation $\oplus$ is defined with the following properties:

1. *Closure*: for all $a, b \in G$, $a \oplus b \in G$.
2. *Associative*: for all $a, b, c \in G$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. *Identity*: there is some element, $0 \in G$, such that for all $a \in G$, $a \oplus 0 = 0 \oplus a = a$.
4. *Inverse*: for all $a \in G$, there exists an inverse, $-a \in G$, such that $a \oplus (-a) = 0$.

Abelian Group: An abelian (or commutative) group has this additional property:

- *Commutative*: for all $a, b \in G$, $a \oplus b = b \oplus a$.

Are the integers and addition an abelian group?

Are the whole numbers and addition an abelian group?

Finite Field: A finite field is a set F of $N \geq 2$ elements on which the operators $\oplus$ and $\times$ are defined with these properties:

1. F is an *abelian group* with identity 0 under the $\oplus$ operation.
2. The set F - { 0 } is an *abelian group* with identity 1 under the $\times$ operation.
3. Distributive: For all $a, b, c \in F$, $(a \oplus b) \times c = (a \times c) \oplus (b \times c)$.

(Note that this requires for all a, $a \times 0 = 0$.)

Prime Field Theorem: For every prime number p, the set $0, 1, ..., p-1$ forms a finite field with the operations addition and multiplication modulo p.

Demonstrate that F_3 is a finite field.

See *Introduction to Finite Fields* (notes from David Forney's MIT 6.451 course) for a proof that all prime fields, Fp are finite fields, and more thorough introduction to finite fields.

Operations on Elliptic Curves

"Addition" on an elliptic curve is done by finding the a point on the line between the two inputs points, and reflecting that point over the x-axis.

Doing addition on elliptic curves over finite fields is more complex, and there has been a lot of research into how to do these operations efficiently. See the btcec.Add code for how it is done in the library.

Doubling (e.g., $P + P = R$) is the same idea, except instead of finding the intersection of the line formed by the two addends (which doesn't exist for the single point), finds the intersection between the tangent of the curve.

"Multiplication" is just repeated addition: $kP = P + P + ... + P$.

Is there a more efficient way to compute $9P$ than using 8 additions?

Signing with Elliptic Curves

Elliptic curve discrete logarithm problem: given points P and Q on an elliptic curve, it is hard to find an integer k such that $Q = kP$.

Parameters: curve, G (a point on curve), (large) n such that $nG = 0$.

**Key pair: **
Private key: d = pick a random integer in [1, n-1] Public key: point on the curve, $Q = dG$

Signing: pick random integer k in [1, n-1] compute curve point: $(x, y) = kG$ signature = (x mod n, k-1$(z + rd)$ mod n)

Bitcoin uses the elliptic curve $y^2 = x^3 + 7$ over the prime field, F_p where $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

How should random numbers be generated?

Dual-EC PRNG

NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators

Michael Wertheimer (NSA), *Encryption and the NSA Role in International Standards*, Notices of the American Mathematical Society, February 2015.