Elliptic Curve Cryptography

ANISHA JOSEPH

Elliptic Curves over finite fields

Definition. Let $p \geq 3$ be a prime. An *elliptic curve over* $\mathbb{F}_p$ is an equation of the form

$$E : Y^2 = X^3 + AX + B \qquad \text{with } A, B \in \mathbb{F}_p \text{ satisfying } 4A^3 + 27B^2 \neq 0.$$

The *set of points on E with coordinates in* $\mathbb{F}_p$ is the set

$$E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p \text{ satisfy } y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

Elliptic Curves over finite fields- Example

Consider the elliptic curve,

$$E : Y^2 = X^3 + 3X + 8 \quad \text{over the field } \mathbb{F}_{13}.$$

By substituting in all possible values X = 0, 1,2, . . . , 12 and checking for which X values,

For example, putting X = 0 gives 8, and 8 is not a square modulo 13. Next we try X = 1, which gives 1+3+8 = 12.

It turns out that 12 is a square modulo 13; in fact, it has two square roots,

$$5^2 \equiv 12 \pmod{13} \qquad \text{and} \qquad 8^2 \equiv 12 \pmod{13}$$

Elliptic Curves over finite fields

This gives two points (1, 5) and (1, 8) in $E(F_{13})$.

Continue this for all values of X, we get,

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}.$$

Elliptic Curves over finite fields

	$\mathcal{O}$	$(1,5)$	$(1,8)$	$(2,3)$	$(2,10)$	$(9,6)$	$(9,7)$	$(12,2)$	$(12,11)$
$\mathcal{O}$	$\mathcal{O}$	$(1,5)$	$(1,8)$	$(2,3)$	$(2,10)$	$(9,6)$	$(9,7)$	$(12,2)$	$(12,11)$
$(1,5)$	$(1,5)$	$(2,10)$	$\mathcal{O}$	$(1,8)$	$(9,7)$	$(2,3)$	$(12,2)$	$(12,11)$	$(9,6)$
$(1,8)$	$(1,8)$	$\mathcal{O}$	$(2,3)$	$(9,6)$	$(1,5)$	$(12,11)$	$(2,10)$	$(9,7)$	$(12,2)$
$(2,3)$	$(2,3)$	$(1,8)$	$(9,6)$	$(12,11)$	$\mathcal{O}$	$(12,2)$	$(1,5)$	$(2,10)$	$(9,7)$
$(2,10)$	$(2,10)$	$(9,7)$	$(1,5)$	$\mathcal{O}$	$(12,2)$	$(1,8)$	$(12,11)$	$(9,6)$	$(2,3)$
$(9,6)$	$(9,6)$	$(2,3)$	$(12,11)$	$(12,2)$	$(1,8)$	$(9,7)$	$\mathcal{O}$	$(1,5)$	$(2,10)$
$(9,7)$	$(9,7)$	$(12,2)$	$(2,10)$	$(1,5)$	$(12,11)$	$\mathcal{O}$	$(9,6)$	$(2,3)$	$(1,8)$
$(12,2)$	$(12,2)$	$(12,11)$	$(9,7)$	$(2,10)$	$(9,6)$	$(1,5)$	$(2,3)$	$(1,8)$	$\mathcal{O}$
$(12,11)$	$(12,11)$	$(9,6)$	$(12,2)$	$(9,7)$	$(2,3)$	$(2,10)$	$(1,8)$	$\mathcal{O}$	$(1,5)$

Table 6.1: Addition table for $E : Y^2 = X^3 + 3X + 8$ over $\mathbb{F}_{13}$

Elliptic Curve on a finite set of Integers

- Consider $y^2 = x^3 + 2x + 3 \pmod 5$

$x = 0 \Rightarrow y^2 = 3 \Rightarrow$ no solution (mod 5)

$x = 1 \Rightarrow y^2 = 6 = 1 \Rightarrow y = 1,4 \pmod 5$

$x = 2 \Rightarrow y^2 = 15 = 0 \Rightarrow y = 0 \pmod 5$

$x = 3 \Rightarrow y^2 = 36 = 1 \Rightarrow y = 1,4 \pmod 5$

$x = 4 \Rightarrow y^2 = 75 = 0 \Rightarrow y = 0 \pmod 5$

- Then points on the elliptic curve are

(1,1) (1,4) (2,0) (3,1) (3,4) (4,0)
and the point at infinity: ∞

Using the finite fields we can form an Elliptic Curve Group where we also have a DLP problem which is harder to solve...

The Elliptic Curve Discrete Logarithm Problem (ECDLP)

The Generalized Discrete Logarithmic Problem

- Given is a finite cyclic group G with the group operation $\circ$ and cardinality n.
- We consider a primitive element $\alpha \in G$ and another element $\beta \in G$.
- The discrete logarithm problem is finding the integer x, where $1 \leq x \leq n$, such that:

$$\beta = \underbrace{\alpha \circ \alpha \circ \alpha \circ \ldots \circ \alpha}_{\text{x times}} = \alpha^x$$

The Elliptic Curve Discrete Logarithm Problem (ECDLP)

Elliptic Curve Discrete Logarithmic Problem(ECDLP)

Cryptosystems rely on the hardness of the Elliptic Curve Discrete Logarithmic Problem.

Definition: Elliptic Curve Discerte Logarithmic Problem(ECDLP)
Given a primitive element P and another element T on an elliptic curve .
The ECDLP problem is to found the integer d, where 1<d<#E such that:

$$\underbrace{P + P + P \ldots\ldots\ldots P}_{d \text{ times}} = dP = T$$

Q=nP
n=P/Q
log n =Log$_Q$ P

Elliptic Curve Cryptography

Apply elliptic curves to cryptography.

We start with the easiest application, Diffie–Hellman key exchange, which involves little more than replacing the discrete logarithm problem for the finite field Fp with the discrete logarithm problem for an elliptic curve E(Fp).

Then elliptic analogues of the Elgamal public key cryptosystem.

Elliptic Diffie–Hellman Key Exchange

Alice and Bob agree to use a particular elliptic curve E(Fp) and a particular point P ∈ E(Fp).

Alice chooses a secret integer n_A and Bob chooses a secret integer n_B.

$$\overbrace{Q_A = n_A P}^{\text{Alice computes this}} \quad \text{and} \quad \overbrace{Q_B = n_B P}^{\text{Bob computes this}}$$

They exchange the values of QA and QB.

Alice then uses her secret multiplier to compute $n_A Q_B$, and Bob similarly computes $n_B Q_A$

$$n_A Q_B = (n_A n_B) P = n_B Q_A$$

Diffie–Hellman key exchange using elliptic curves

Public parameter creation	
A trusted party chooses and publishes a (large) prime p, an elliptic curve E over $\mathbb{F}_p$, and a point P in $E(\mathbb{F}_p)$.	
Private computations	
Alice	**Bob**
Chooses a secret integer n_A. Computes the point $Q_A = n_A P$.	Chooses a secret integer n_B. Computes the point $Q_B = n_B P$.
Public exchange of values	
Alice sends Q_A to Bob $\longrightarrow$	Q_A
Q_B $\longleftarrow$	Bob sends Q_B to Alice
Further private computations	
Alice	**Bob**
Computes the point $n_A Q_B$.	Computes the point $n_B Q_A$.
The shared secret value is $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A$.	

Diffie–Hellman key exchange using elliptic curves

Alice and Bob decide to use elliptic Diffie–Hellman with the following prime, curve, and point

$$p = 3851, \qquad E : Y^2 = X^3 + 324X + 1287, \qquad P = (920, 303) \in E(\mathbb{F}_{3851}).$$

Alice and Bob choose respective secret values nA = 1194 and nB = 1759, and then

$$\begin{array}{ll} \text{Alice computes} & Q_A = 1194P = (2067, 2178) \in E(\mathbb{F}_{3851}), \\ \text{Bob computes} & Q_B = 1759P = (3684, 3125) \in E(\mathbb{F}_{3851}). \end{array}$$

Diffie–Hellman key exchange using elliptic curves

Alice and Bob decide to use elliptic Diffie–Hellman with the following prime, curve, and point

$$p = 3851, \qquad E : Y^2 = X^3 + 324X + 1287, \qquad P = (920, 303) \in E(\mathbb{F}_{3851}).$$

Alice and Bob choose respective secret values nA = 1194 and nB = 1759, and then

$$\begin{array}{ll} \text{Alice computes} & Q_A = 1194P = (2067, 2178) \in E(\mathbb{F}_{3851}), \\ \text{Bob computes} & Q_B = 1759P = (3684, 3125) \in E(\mathbb{F}_{3851}). \end{array}$$

Diffie–Hellman key exchange using elliptic curves

Alice sends QA to Bob and Bob sends QB to Alice. Finally,

$$\begin{aligned} &\text{Alice computes} \quad n_A Q_B = 1194(3684, 3125) = (3347, 1242) \in E(\mathbb{F}_{3851}), \\ &\text{Bob computes} \quad n_B Q_A = 1759(2067, 2178) = (3347, 1242) \in E(\mathbb{F}_{3851}). \end{aligned}$$

Bob and Alice have exchanged the secret point (3347, 1242).

One way for Eve to discover Alice and Bob's secret is to solve the ECDLP.

$$nP = Q_A,$$

Keeping in mind that all calculations are in Finite Field.

Factorization using Elliptic Curve - Lenstra's algorithm

Let E be an elliptic curve mod N, where N is not necessarily prime, and let P be any point on the curve.

- There must be some k for which $kP = 0$, the point at infinity,
- Then the line between $(k-1)P$ and P must have undefined slope,
- Which will occur when the difference of the x-values shares a common factor with N.

This suggests we can use an elliptic curve to factor N as follows:

- Pick an arbitrary elliptic curve E and an arbitrary point P on the curve.
- Evaluate $k!P$ for $k = 2, 3, 4, \ldots$. Note that in general, this will require finding $p^{-1} \mod N$.
- If we are unable to find p^{-1}, then p, N must have a common divisor, which will be a factor of N.

Factorization using Elliptic Curve - Lenstra's algorithm

Input. Integer N to be factored.

1. Choose random values A, a, and b modulo N.

2. Set $P = (a, b)$ and $B \equiv b^2 - a^3 - A \cdot a \pmod{N}$.
Let E be the elliptic curve $E : Y^2 = X^3 + AX + B$.

3. Loop $j = 2, 3, 4, \ldots$ up to a specified bound.

- **4.** Compute $Q \equiv jP \pmod{N}$ and set $P = Q$.
- **5.** If computation in Step **4** fails,
  then we have found a $d > 1$ with $d \mid N$.
- **6.** If $d < N$, then **success**, return d.
- **7.** If $d = N$, go to Step **1** and choose a new curve and point.

8. Increment j and loop again at Step **2**.

ElGamal Public Key Cryptosystem for elliptic curves

$$C_1 = kP \qquad \text{and} \qquad C_2 = M + kQ_A.$$

He sends the two points (C_1, C_2) to Alice, who computes

$$C_2 - n_A C_1 = (M + kQ_A) - n_A(kP) = M + k(n_A P) - n_A(kP) = M$$

Public parameter creation	
A trusted party chooses and publishes a (large) prime p, an elliptic curve E over $\mathbb{F}_p$, and a point P in $E(\mathbb{F}_p)$.	
Alice	**Bob**
Key creation	
Choose a private key n_A. Compute $Q_A = n_A P$ in $E(\mathbb{F}_p)$. Publish the public key Q_A.	
Encryption	
	Choose plaintext $M \in E(\mathbb{F}_p)$. Choose a random element k. Use Alice's public key Q_A to compute $C_1 = kP \in E(\mathbb{F}_p)$. and $C_2 = M + kQ_A \in E(\mathbb{F}_p)$. Send ciphertext (C_1, C_2) to Alice.
Decryption	
Compute $C_2 - n_A C_1 \in E(\mathbb{F}_p)$. This quantity is equal to M.	