Elliptic Curves and Cryptographic Applications

The Discrete Log Problem and Diffie-Hellman

Brian Zhang

Rutgers University

DRP Presentation, Spring 2023

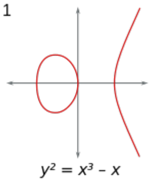
What is an Elliptic Curve?

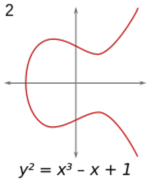
Definition

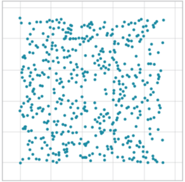
An elliptic curve $E(\mathbb{F}_q)$ is the group of points $(x, y) \in \mathbb{F}_q$ satisfying the **Short Weierstrass Equation**:

$$E : y^2 = x^3 + Ax + B$$

What do they look like?







The Group Law for Point Addition/Doubling

Problems:

- Given points P and Q, what is $P + Q$ and $[n]P = \sum_{i=1}^{n} P$?
- How do we preserve group laws?
    1. closure under addition/multiplication
    2. identity and inverse? (infinity point $\mathcal{O}$)
    3. associativity?

Solution: the **chord-and-tangent rule**

The EC Discrete Log Problem

Given points $P, [a]P \in E(\mathbb{F}_q)$, find a.

Solving the Discrete Log Problem

Pairings

Let $\mathbb{F}_{q^k}$ be some finite extension of $\mathbb{F}_q$ with $k \geq 1$. Then we can define a bilinear map

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

Where $\mathbb{G}_1, \mathbb{G}_2$ are defined in $\mathbb{F}_{q^k}$ and $\mathbb{G}_T$ is defined in the multiplicative group $\mathbb{F}_{q^k}^*$

Since e is bilinear, we have:

- $e(P + P', Q) = e(P, Q) \cdot e(P', Q)$
- $e(P, Q + Q') = e(P, Q) \cdot e(P, Q')$

Consequence: $e([a]P, Q) = e(P, Q)^a$

Defining Pairings: Divisors

Divisor on E

A divisor D is a multi-set of points on $E(\mathbb{F}_q)$, written as the formal sum

$$D = \sum_{P \in E(\mathbb{F}_q)} n_p(P)$$

- The set of all divisors on E, $\mathrm{Div}(E)$, forms an additive group, with identity divisor $\mathrm{O} = \sum 0(P)$.
- We denote the degree of a divisor $\deg(D) = \sum n_P$, and the support of a divisor $\mathrm{supp}(D) = \{P \in E(\mathbb{F}_q) : n_P \neq 0\}$

Defining Pairings: Divisors

Divisor of a Function

We can define the divisor of a function f, denoted (f), as follows:

$$(f) = \sum_{P \in E(\mathbb{F}_q)} \mathrm{ord}_P(f)(P)$$

Where ord_P counts the multiplicty of f at P.

Weil Reciprocity Law

Let f and g be non-zero functions on a curve such that (f) and (g) have disjoint supports. Then $f((g)) = g((f))$

$$f(D) = \prod f(P)^{n_P}$$

Weil Reciprocity allows for efficient computation of pairings.

Defining Pairings: Torsion Groups

To calculate the pairing $e(P, Q)$, points P and Q must come from **disjoint cyclic subgroups** of the same prime order r.

r-torsion

The points order r on $E(\mathbb{F}_q)$ is the r-torsion group, denoted

$$E[r] = \{P \in E : [r]P = \mathcal{O}\}$$

Interestingly, $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r \implies \#E[r] = r^2$.

We want to find two points $P, Q \in E[r]$ that are disjoint.

Defining Pairings: Torsion Groups

- Problem: for $E(\mathbb{F}_q)$, there are only about q points. How do we find all r^2 points in $E[r]$ if $r^2 > q$?
- Field extensions: we can extend $\mathbb{F}_q$ to $\mathbb{F}_{q^k}$, where we uncover more r-torsion points if k is large enough.
- The smallest integer $k \geq 1$ such that $\mathbb{F}_{q^k}$ captures all r^2 points in $E[r]$ is called the **embedding degree** of $E[r]$.

Properties of Embedding

1. k is the smallest integer such that $r | (q^k - 1)$
2. If $r || \# E(\mathbb{F}_q)$, then the r-torsion subgroup in $E(\mathbb{F}_q)$ is unique. In this case, $k > 1$, and $\mathbb{F}_{q^k}$ **fully covers** $E[r]$.

Defining Pairings: Torsion Groups

We can create beautiful "petal" diagrams that display the how torsion subgroups are connected:

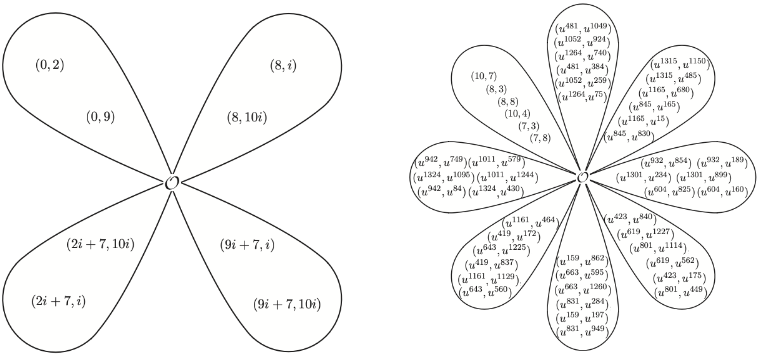


Figure: $E[3]$ for $E(\mathbb{F}_{11}) : y^2 = x^3 + 4$, $E[7]$ for $E(\mathbb{F}_{11}) : y^2 = x^3 + 7x + 2$

Defining Pairings: Trace/Antitrace Maps

Frobenius Endomorphism

The Frobenius Endomorphism, π, identifies which elements of $E[r]$ lie in the base field $\mathbb{F}_q$:

$$\pi : E(\mathbb{F}_q) \to E(\mathbb{F}_q) \text{ defined by } (x, y) \mapsto (x^q, y^q)$$

Using the Frobenius, we can define the Trace of a point as

$$\mathrm{Tr}(P) = \sum_{i=0}^{k-1} \pi_q^i(P) = \sum_{i=0}^{k-1} (x^{q^i}, y^{q^i})$$

And the Anti-Trace, the inverse of the Trace, as

$$\mathrm{aTr}(P) = [k]P - \mathrm{Tr}(P) = [k]P - \sum_{i=0}^{k-1} \pi_q^i(P)$$

Defining Pairings: Trace/Antitrace Maps

1. Using the petal diagram, there is one unique subgroup order r in $E[r]$ called the base-field subgroup, $\mathbb{G}_1 = E[r] \cap \ker(\pi_q - [1])$, where $\mathrm{Tr}(P) \in \mathbb{G}_1 \ \ \forall P$.
2. Similarly, we can define $\mathbb{G}_2 = \mathrm{im}(\mathrm{aTr}(P))$ as the trace-zero subgroup, where $\mathrm{Tr}(P) = 0 \ \ \forall P \in \mathbb{G}_2$.

This $\mathbb{G}_1$ and $\mathbb{G}_2$ are exactly the disjoint cyclic subgroups order r we need to calculate pairing $e(P, Q)$.

Defining Pairings: Trace/Antitrace Maps

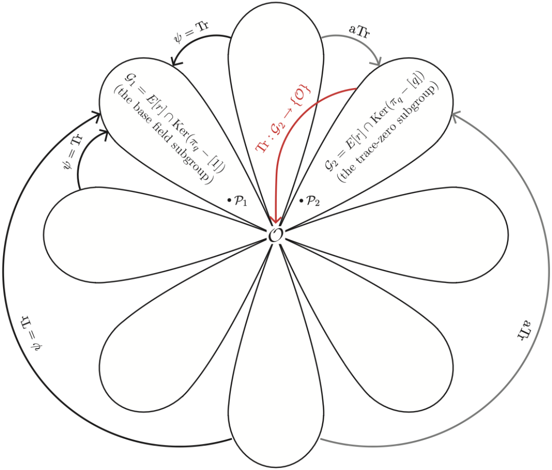


Figure: The behavior of the trace and anti-trace maps on $E[r]$

The Weil and Tate Pairings

The Weil Pairing

$$w_r(P,Q) = \frac{f_{r,P}(D_Q)}{g_{r,Q}(D_P)}$$

where functions $f_{r,P}$ and $g_{r,Q}$ are defined such that $(f) = rD_p$, $(g) = rD_Q$, and D_P, D_Q are degree zero divisors such that $D_P \sim (P) - (\mathcal{O})$, $D_Q \sim (Q) - (\mathcal{O})$.

The Tate Pairing

$$T_r(P,Q) = f_{r,P}(D_Q)^{\frac{q^k-1}{r}}$$

where $f_{r,P}$ is defined such that $(f) = r(P) - r(\mathcal{O})$, and D_Q is a degree zero divisor over $\mathbb{F}_{q^k}$ equivalent to $(Q) - (\mathcal{O})$, disjoint to (f).

In Practice: Bilinearity, Diffie-Hellman, and the MOV attack

- Diffie-Hellman: Alice and Bob have secret keys a, b. Using a public $P \in E(\mathbb{F}_q)$, they compute public keys aP, bP separately, and send them to each other. The shared secret is abP.
- As mentioned before, the bilinearity of pairings allows for computation of the discrete log problem:

  $$e([a]P, Q) = e(P, Q)^a$$

  Allows us to recover a from $P, aP \in E(\mathbb{F}_q)$.
- What happens if the curve is unsafe in terms of ECDLP? Then we can solve the ECDLP using an MOV attack.