Number theory and Cryptography June 13, 2024

Lecture 12 : Elliptic Curves in Cryptography

Instructor: Chao Qin *Notes written by: Wenhao Tong and Yingshu Wang*

1 Applications of elliptic curves over finite fields

There are several factors that make elliptic curves over finite fields particularly well suited to practical applications:

- There are many groups available, even when the finite field is fixed.
- The underlying group operation can be made very efficient.
- here are techniques to construct a group of any desired size.
- The representation of group elements appears to be "opaque".

There are three particular applications that we will explore in some detail:

- factoring integers
- primality proving
- cryptography

In the next ten slides we will take a whirlwind tour of these applications.

1.1 Diffie-Hellman key exchange

Diffie and Hellman proposed a method for two parties to establish a secret key over a public network, based on the discrete log problem. Their method is generic, it works in a cyclic subgroup of any given group. Let $E/\mathbb{F}_p$ be an elliptic curve with a point $P \in E(\mathbb{F}_p)$. Alice and Bob, who both know E and P,establish a secret S as follows:

1. Alice chooses a random integer a and sends aP to Bob
2. Bob choses a random integer b and sends bP to Alice.

3. Alice computes $abP = S$ and Bob computes $baP = S$.

The coordinates of S depend on the random integer ab and can be hashed to yield a shared secret consisting of $\log_2 ab$ random bits.[2]
An eavesdropper may know E, P, aP and bP,but not a, b,or S. It is believed that computing S from these values is as hard as computing discrete logarithms in $E(\mathbb{F}_p)$ (but this is not proven)

1.2 Ephemeral Diffie-Hellman (ECDHE)

With ephemeral Diffie-Hellman (ECDHE) the elliptic cunve E is fixed, but a new base point P is chosen for each key exchange.
This provides what is known as perfect forward secrecy, which compartmentalizes the security of each communication session (breaking one session should not make it easier to break others).
ECDHE was adopted by Google in late 2011 and is now used by essentially all major internet sites to establish a secure session, including:
Amazon, Bing, Dropbox, Facebook, Flickr, GitHub, Instagram, LinkedIn, MSN, Netflix, Pinterest, PirateBay, Quora, Snapchat, SoundCloud, Spotify, StackOverflow, Tumblr, Twitter, Uber, Vimeo, Vine, Yahoo, Yelp, YouTube, Wikipedia, Wordpress, ...

1.3 Pairing-based cryptography

Elliptic curves also support bilinear pairings $\varepsilon : E(\overline{\mathbb{F}}_p) \times E(\overline{\mathbb{F}}_p) \to \overline{\mathbb{F}}_p^{\times}$, which satisfy $\varepsilon(aP, bQ) = \varepsilon(P, Q)^{ab}$. Pairings facilitate some more sophisticated cryptographic protocols

For suitably pairing friendly elliptic curves $E/\mathbb{F}_p$, one can define a pairing $\varepsilon : E(\mathbb{F}_p) \times E(\mathbb{F}_p) \to \mathbb{F}_{p^k}$,where $\#E(\mathbb{F}_p)$ divides $p^k - 1$ and k is small.
As an example, here is how Alice, Bob, and Carol can establish a shared secret using a single round of communication (as proposed by Joux).

1. Alice chooses a random a and sends aP to Bob and Carol,
   Bob chooses a random b and sends bP to Alice and Carol,
   Carol chooses a random c and sends cP to Alice and Bob.

2. Alice computes $\varepsilon(bP, cP)^a = \varepsilon(P, P)^{bca} = S$,
   Bob computes $\varepsilon(aP, cP)^b = \varepsilon(P, P)^{acb} = S$,
   Carol computes $\varepsilon(aP, bP)^c = \varepsilon(P, P)^{abc} = S$.

An eavesdropper may know E, P, aP, bP, cP, but not a, b, c or S.

Now the security of the system depends both on the difficulty of the discrete log problem in $E(\mathbb{F}_p)$,and the discrete log problem in $\mathbb{F}_{p^k}$.
The complexity of the discrete log problem in $E(\mathbb{F}_p)$ is believed to be $\Omega(\sqrt{p})$, whereas the fastest known algorithm for computing discrete logarithms in $\mathbb{F}_{p^k}$ has complexity

$$L[1/3, c] = \exp\big((c + o(1))(\log n)^{1/3}(\log\log n)^{2/3}\big),$$

where $n = p^k$ and c is a constant that may be as small as about 1.4 (for binary fields).
If $p \approx 2^{256}$ and $k = 12$, then $p^k \approx 2^{3072}$ and the two complexities are roughly comparable.

1.4 Quantum security

Both factoring and the discrete logarithm problem can be solved in polynomial-time on a quantum computer.
SIDH is a variant of the Diffie Hellman protocol that replaces scalar multiplication with a walk on a supersingular isogeny graph:
Alice and Bob, who both know a supersingular elliptic curve $E/\mathbb{F}_{p^2}$,establish a secret S as follows:

1. Alice chooses a random a encoded in base-2 and computes E_a by taking an a-walk in the 2-isogeny graph; she sends E_a to Bob.[3]

2. Bob choses a random b encoded in base-3 and computes E_b by taking a b-walk in the 3-isogeny graph; he sends E_b to Alice.[4]

3. Alice computes $(E_b)_a$ and Bob computes $(E_a)_b$. The j-invariant $j((E_b)_a) = j((E_a)_b) \in \mathbb{F}_{p^2}$ is their shared secret S.

No efficient algorithm is known for computing $j((E_b)_a) = j((E_a)_b)$ given E, E_a, E_b, not even on an quantum computer.

2 What Does $E(K)$ Look Like?

theorem 1. *(Mordell, 1922) Let E be an elliptic curve given by an equation*

$$E : y^2 = x^3 + Ax + B \quad \textit{with } A, B \in \mathbb{Q}.$$

Then the group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group. In other words, there is a finite set of points $P_1, \ldots, P_t \in E(\mathbb{Q})$ so that every point $P \in E(\mathbb{Q})$ can be written in the form

$$P = n_1P_1 + n_2P_2 + \cdots + n_tP_t$$

for some $n_1, n_2, \ldots, n_t \in \mathbb{Z}$.

A standard theorem about finitely generated abelian groups tells us that $E(\mathbb{Q})$ looks like

$$E(\mathbb{Q}) \cong (\text{Finite Group}) \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ copies}}.$$

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ copies}}.$$

The finite group $E(\mathbb{Q})_{\text{tors}}$ is called the Torsion Subgroup of $E(\mathbb{Q})$.
The integer r is called the Rank of $E(\mathbb{Q})$.
The description of all possible torsion subgroups for $E(\mathbb{Q})$ is very easy, although the proof is extremely difficult.

theorem 2. *(Mazur, 1977) The torsion subgroup of the group of rational points $E(\mathbb{Q})$ on an elliptic curve must be one of the following 15 groups:*

$$C_N \quad \textit{with } 1 \leq N \leq 10 \textit{ or } N = 12,$$

$$C_2 \times C_{2N} \quad \textit{with } 1 \leq N \leq 4.$$

In particular, $E(\mathbb{Q})_{tors}$ has order at most 16.

The rank is a far more mysterious quantity, although there is a folklore conjecture.
Conjecture. There exist elliptic curve groups $E(\mathbb{Q})$ of arbitrarily large rank.

The evidence for this conjecture is fragmentary at best. An example of rank at least 24 (Martin-McMillen 2000):

$$y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x + 504224992484910670010801799168082726759443756222911415116$$

And here is the only example known of higher rank. It has rank at least 28 (Elkies 2006):

$y^2+xy+y = x^3-2006776241557552658503320820933854275093023031217895650 2x$
$+344816117950305564670329856903907203748559443593191803612660082962919394487322434 2$

Slightly more convincing is the fact that there do exist elliptic curves with coefficients in the field $\mathbb{F}_p(T)$ such that the rank of $E(\mathbb{F}_p(T))$ is arbitrarily large.

The ring $\mathbb{Z}$ is not a field, so the set

$$E(\mathbb{Z}) = \{(x,y) \in E(\mathbb{Q}) : x,y \in \mathbb{Z}\} \cup \{O\}$$

is usually not a subgroup of $E(\mathbb{Q})$.
Indeed, even if P_1 and P_2 have integer coordinates, the formula for $P_1 + P_2$ is so complicated, it seems unlikely that the point $P_1 + P_2$ will have integer coordinates.
Complementing Mordell's Theorem describing $E(\mathbb{Q})$ is a famous finiteness result for $E(\mathbb{Z})$.

theorem 3. *(Siegel, 1928) Let E be an elliptic curve given by an equation*

$$E : y^2 = x^3 + Ax + B \quad \textit{with } A,B \in \mathbb{Z}.$$

Then E has only fnitely many points $P = (x,y)$ with integer coordinates $x,y \in \mathbb{Z}$, i.e., $E(\mathbb{Z})$ is a fnite set.

Siegel actually proves something much stronger.
For each point $P \in E(\mathbb{Q})$, write

$$x(P) = \frac{a(P)}{b(P)} \in \mathbb{Q} \quad \text{as a fraction in lowest terms.}$$

theorem 4. *(Siegel, 1928)*

$$\lim_{\substack{P \in E(\mathbb{Q}) \\ \max\{|a(P)|,|b(P)|\} \to \infty}} \frac{\log|a(P)|}{\log|b(P)|} = 1.$$

Roughly speaking, Siegel's result says that the numerator and the denominator of $x(P)$ tend to have approximately the same number of digits.

The group $E(\mathbb{F}_p)$ is obviously a finite group. Indeed, it clearly has no more than $2p+1$ points.

For each $x \in \mathbb{F}_p$, there is a“50
Thus we might expect $E(\mathbb{F}_p)$ to contain approximately

$$\#E(\mathbb{F}_p) \approx \frac{1}{2} \cdot 2 \cdot p + 1 = p + 1 \text{ points}$$

A famous theorem of Hasse makes this precise:

theorem 5. *(Hasse, 1922) Let E be an elliptic curve*

$$y^2 = x^3 + Ax + B \quad \textit{with } A, B \in \mathbb{F}_p.$$

Then

$$\left|\#E(\mathbb{F}_p) - (p+1)\right| \leq 2\sqrt{p}.$$

3 Elliptic Curves Over Finite Fields

3.1 The Order of the Group $E(\mathbb{F}_p))$

The Frobenius Map is the function

$$\tau_p : E(\bar{\mathbb{F}}_p) \longrightarrow E(\bar{\mathbb{F}}_p), \quad \tau_p(x,y) = (x^p, y^p).$$

One can check that τ_p is a group homomorphism
The quantity

$$a_p = p + 1 - \#E(\mathbb{F}_p)$$

is called the Trace of Frobinius, because one way to calculate it is to use the Frobenius map to get a linear transformation on a certain vector space $V_\ell(E)$. Then a_p is the trace of that linear transformation.
Hasse's Theorem says that

$$|a_p| \leq 2\sqrt{p}.$$

For cryptography, we need $E(\mathbb{F}_p)$ to contain a subgroup of large prime order.
How does $\#E(\mathbb{F}_p)$ vary for different E?

3.2 The Distribution of the Trace of Frobenius

There are approximately $2p$ different elliptic curves defined over $\mathbb{F}_p$.
If the $a_p(E)$ values for different E were uniformly distributed in the interval from $-2\sqrt{p}$ to $2\sqrt{p}$ then we would expect each value to appear approximately

$\frac{1}{2}\sqrt{p}$ times.
This is not quite true, but it is true that the values a_p between (say) $-\sqrt{p}$ and $\sqrt{p}$ appear quite frequently The precise statement says that the a_p values follow a Sato-Tate distribution:

theorem 6. *(Birch)*

$$\#\{E/\mathbb{F}_p : \alpha \le a_p(E) \le \beta\} \approx \frac{1}{\pi}\int_\alpha^\beta \sqrt{4p - t^2}dt.$$

3.3 The Group of Points on E with Coordinates in a Field K

The elementary observation on the previous slide leads to the important result that points with coordinates in a particular field form a subgroup of the full set of points.

theorem 7 (Poincareé, $\approx$1900)**.** *Let K be a field and suppose that an elliptic curve E is given by an equation of the form*

$$E : y^2 = x^3 + Ax + B \quad \text{with} \quad A, B \in K.$$

Let $E(K)$ denote the set of points of E with coordinates in K,

$$E(K) = \{(x, y) \in E : x, y \in K\} \cup \{O\}.$$

Then $E(K)$ is a subgroup of the group of all points of E.

4 The L-Series of an Elliptic Curve

Let E be an elliptic curve given as usual by an equation

$$y^2 = x^3 + Ax + B \quad \text{with } A, B \in \mathbb{Z}.$$

For each prime p, we can reduce E modulo p,count its points, and compute the trace of Frobenius:

$$a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

The L**- Series of** E encodes all of the a_p values into a singlefunction:

$$L(E, s) = \prod_{p \text{ prime}} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

The variable s is a complex variable $s \in \mathbb{C}$. Using Hasse's estimate $|a_p| \leq 2\sqrt{p}$, it is easy to prove that the product defining $L(E,s)$ converges for $\mathrm{Re}(s) > \frac{3}{2}$.

4.1 The Analytic Continuation of $L(E,s)$

theorem 8. *(Wiles' Theorem) The function $L(E,s)$ extends to an analytic function on all of $\mathbb{C}$. Further, there is an integer N (the Conductor of E) so that the function*

$$\xi(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$$

satisfies the functional equation

$$\xi(E,2-s) = \pm\xi(E,s).$$

A more precise form of Wiles Theorem says to write

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad \text{and set} \quad f(E,\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n\tau}.$$

Then $f(E,\tau)$ is a modular form (weight 2 cusp form) for $\Gamma_0(N)$. This statement combined with ideas of Frey and Serre and a theorem of Ribet are used to prove Fermat's I ast Theorem

4.2 The Behavior of $L(E,s)$ Near $s = 1$

It is a truth universally acknowledged that L-series satisfying a functional equation have interesting behavior at the center of their critical strip. For elliptic curves,this is at the point $s = 1$.A formal (and completely unjustified) calculation yields

$$L(E,1) = \prod_p \left(1 - \frac{a_p}{p} + \frac{1}{p}\right)^{-1} = \prod_p \frac{p}{\#E(\mathbb{F}_p)}.$$

Thich suggests that if $\#E(\mathbb{F}_p)$ is large, then $L(E,1) = 0$.Birch and Swinnerton-Dyce observed that if $E(\mathbb{Q})$ is infinite, then the reduction of the points in $E(\mathbb{Q})$ tend to make $\#E(\mathbb{F}_p)$ larger than usual. So they conjectured

$$L(E,1) = 0 \quad \text{if and only if } \#E(\mathbb{Q}) = \infty.$$

4.3 The Conjecture of Birch and Swinnerton-Dyer

More generally, as the group $E(\mathbb{Q})$ gets"larger", the size of$\#E(\mathbb{F}_p)$ seems to get larger, too.
Birch-Swinnerton-Dyer Conjecture.

$$\operatorname{ord}_{s=1} L(E,s) = \operatorname{rank} E(\mathbb{Q}).$$

This amazing conjecture says that the order of vanishing of the function $L(E,s)$, which recall is created entirely from information about the elliptic curve modulo various primes p, governs how many rational points are needed to generate the full group $E(\mathbb{Q})$.
The BSwD conjecture is one of the Clay Millenium Problems, so its solution is worth 1,000,000.
There is a refined conjecture $L(E,s) \sim c(s-1)^r$. The constant c depends, among other things, on the elliptic regulator $\mathcal{R}_E$.