Elliptic curve based cryptography

Based on notes of Luca De Feo

Kecheng Shi

SUSTech

July 29, 2022

Diffie-Hellman protocol

Setup the public parameters:

- A large enough prime number p, such that $p-1$ has a large enough prime factor.
- A multiplicative generator $g \in \mathbb{Z}/p\mathbb{Z}$.

Then they run the protocol as follows:

- Each chooses a secret integer from $\{0, ..., p-1\}$, call a Alice's secret and b Bob's secret.
- They repectively compute $A = g^a$ and $B = g^b$.
- They exchange A and B over the public channel.
- They respectively compute the shared secret $B^a = A^b = g^{ab}$.

Discrete logarithm

Definition

Let G be a cyclic group generated by an element g. For any element $A \in G$, we define the discrete logarithm of A in base g, denoted $log_g(A)$, as the unique integer in the $\{0, ..., \#G\}$ such that

$$g^{log_g(A)} = A$$

.

ECC

- Algorithms to compute discrete logarithms in a generic group G that requires $O(\sqrt{q})$ computational steps, where q is the largest prime divisor of $\#G$.
- We also know that these algorithms are optimal for abstract cyclic groups.
- No algorithms better than the generic ones are known when G is a subgroup of $E(k)$, where E is an elliptic curve defined over a finite field k.
- Miller and Koblitz suggest to replace $(\mathbb{Z}/p\mathbb{Z})^{\times}$ by the group of rational points of an elliptic curve of (almost) prime order over a finite field.

Weil pairing and Tate pairing I

Assume E is an elliptic curve defined over $\mathbb{F}_q$, with $q = p^n$. Assume that l divides $p^{rn} - 1$ for some reasonably small value of r. Given a function f in $K(E)$ and a point P of E, f can be evaluated at a divisor $D = \sum_i a_i(P_i)$,

$$f(D) = \prod_i f(P_i)^{a_i}$$

where D_Q denotes a divisor from the class $(Q) - (O)$. We need to carefully choose D_Q for computing $f_P(D_Q)$, the most popular one is to choose $D_Q = (Q + R) - (R)$.

Weil pairing and Tate pairing II

Definition

Given two l-torsion points P and Q we can define their Weil pairing as

$$w(P, Q) = f_P(D_Q)/f_Q(D_p)$$

and their Tate pairing as

$$t(P, Q) = f_P(D_Q)^{\frac{p^{rn}-1}{l}}$$

Definition (Complex lattice)

A complex lattice Λ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}$-basis.

Definition (Complex torus)

Let Λ be a complex lattice, the quotient $\mathbb{C}/\Lambda$ is called a complex torus

Definition (Homothetic lattices)

Two complex lattices Λ and Λ' are said to be homothetic if there is a complex number $\alpha \in \mathbb{C}$ such that $\Lambda = \alpha\Lambda'$.

Theorem (Modular j-invariant)

The modular j-invariant is the function on complex lattices defined by

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2}$$

Two lattices are homothetic if and only if they have the same modular j-invariant.

Definition

Let Λ be a complex lattice, the Weierstrass $\mathcal{P}$ function associated of Λ is the series

$$\mathcal{P}(z;\Lambda) = 1/z^2 + \sum (1/(z-w)^2 - 1/w^2)$$

The Weierstrass function has the following properties:

- It is an elliptic function for Λ.
- Its Laurent series around $z = 0$ is

$$\mathcal{P}(z) = 1/z^2 + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}$$

- It satisfies the differential equation

$$\mathcal{P}'(z)^2 = 4\mathcal{P}(z)^3 - g_2\mathcal{P}(z) - g_3$$

  for all $z \notin \Lambda$
- The curve

$$E : y^2 = 4x^3 - g_2x - g_3$$

  is an elliptic curve over $\mathbb{C}$.The map

$$\mathbb{C}/\Lambda \to E(\mathbb{C})$$

$$z \mapsto (\mathcal{P}(z) : \mathcal{P}'(z) : 1)$$

  is an isomorphism of Riemann surfaces and a group morphism.

The endomorphism ring

Theorem

Let E be an elliptic curve defined over a field k of characteristic p. The ring $End(E)$ is isomorphic to one of the following:

- $\mathbb{Z}$, *only if* $p = 0$.
- *An order* $\mathcal{O}$ *in a quadratic imaginary field. In this case we say that* E *has complex multiplication by* $\mathcal{O}$.
- *Only if* $p > 0$, *a maximal order in the quaternion algebra ramified at* p *and* ∞; *in this case we say that* E *is supersingular.*

Isogeny graphs

We now look at the graph structure that isogenies creates on the set of j-invariants defined over a finite field.

Theorem (Sato-Tate)

Two elliptic curves E, E' defined over a finite field are isogenous if and only if their endomorphism algebras $End(E) \otimes \mathbb{Q}$ and $End(E') \otimes \mathbb{Q}$ are isomorphic.

Definition (Isogeny graph)

An isogeny graph is a (multi)-graph whose nodes are the j-invariants of isogeneous curves, and whose edges are isogenies between them.

Expander graphs

Definition (Graph theory)

- The degree of a vertex is the number of edges pointing to (or from) it.
- A graph where every edge has degree k is called k-regular.
- The adjacency matrix of a graph G with vertex set $V = \{v_1, ..., v_n\}$ and edge set E, is the $n \times n$ matrix where the $(i, j) - th$ entry is 1 if there is an edge between v_i and v_j. and 0 otherwise.
- Our graphs are undirected, the adjacency matrix is symmetric, thus it has n real eigenvalues

$$\lambda_1 \geq ... \geq \lambda_n$$

Proposition

If G is a k-regular graph, then its largest and smallest eigenvalues λ_1, λ_n satisfy

$$k = \lambda_1 \geq \lambda_n \geq -k$$

Definition (Expander graph)

Let $\epsilon > 0$ and $k \geq 1$. A k-regular graph is called a (one-sided) ϵ-expander if

$$\lambda_2 \leq (1-\epsilon)k$$

and a two-sided ϵ-expander if it also satisfies

$$\lambda_n \geq -(1-\epsilon)k$$

A sequence $G_i = (V_i, E_i)$ of k-regular graphs with $\# V_i \to \infty$ is said to be a one-sided(resp. two-sided) expander family if there is an $\epsilon > 0$ such that G_i is a one-sided(resp. two-sided ϵ-expander for all sufficiently large i).

Ramanujan graph

Theorem (Ramanujan graph)

Let $k \geq 1$, and let G_i be a sequence of k-regular graphs, then

$$max(|\lambda_2|, |\lambda_n|) \geq 2\sqrt{k-1} - o(1)$$

as $n \to \infty$. A graph such that $|\lambda_i| \leq 2\sqrt{k-1}$ for any λ_i except λ_1 is called a Ramanujan graph.

Theorem (Supersingular graphs are Ramanujan)

Let p, l be distinct primes, then

- *All supersingular j-invariants of curves in $\overline{\mathbb{F}_p}$ are defined in $\mathbb{F}_{p^2}$.*
- *The graph of supersingular curves in $\overline{\mathbb{F}_p}$ with l-isogenies is connected, $l+1$ regular, and has the Ramanujan property.*

First application: Examples of discrete logarithm problem in elliptic curves

Problem (Isogeny computation)

Given an elliptic curve E with Frobenius endomorphism π, and a subgroup $G \subset E$ such that $\pi(G) = G$, compute the rational functions and the image curve of the separable isogeny ϕ with kernel G.

Problem (Explicit isogeny)

Given two elliptic curves E, E' over a finite field, isogenous of known degree d, find an isogeny $\phi : E \to E'$ of degree d.

Problem (Isogeny path)

Given two elliptic curves E, E' over a finite field k, such that $\#E = \#E'$, find an isogeny $\phi : E \to E'$ of smooth degree.

Provably secure hash functions

Proposition (mixing theorem)

In an expander graph, random walks of length close to its diameter terminate on any vertex with probability close to uniform.

Problem

Given a vertex j in the graph, find a path from the start vertex j_0 to j.

Problem

Find a non-trivial loop from j_0 to itself.

Post-quantum key exchange

There are two protocols all based on random walks in an isogeny graph.

- The two participants, Alice and Bob, start from the same common curve E_0, and take a (secret) random walk to some curves E_A, E_B.
- After publishing their respective curves, Alice start a new walk from E_B, while Bob starts from E_A.
- By repeating the "same" secret steps, they both eventually arrive on a shared secret curve E_S, only known to them.
- The most important is that we must use the algebraic properties of the isogeny graphs to ensure their walks "commute".

Ordinary Case

Theorem (Key theorem)

- *Let* $\mathbb{F}_q$ *be a finite field, and let* $\mathcal{O}\subset\mathbb{Q}[\sqrt{-D}]$ *be an order in a quadratic imaginary field. Denote by* $Ell_q(\mathcal{O})$ *the elliptic curves defined over* $\mathbb{F}_q$ *with complex multiplication by* $\mathcal{O}$*.*
- *Assume that* $Ell_q(\mathcal{O})$ *is non-empty, then the class group* $Cl(\mathcal{O})$ *acts freely and transitively on it.*

Supersingular case

There are two attractive features compared to the ordinary case

- One isogeny degree is sufficient to obtain an expander graph.
- There is no action of an abelian group, such as $Cl(\mathcal{O})$, on them.