Supersingular Isogeny Diffie-Hellman

Valeriia Kulynych
Université de Toulon

May 13, 2018

1 Supersingular Elliptic Curves

1.1 Various definitions

Let K be a field with algebraic closure $\bar{K}$.

Definition 1 (Projective space)**.** The *projective space of dimension* n, denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(\bar{K})$ is the set of all $(n+1)$-tuples

$$(x_0, \ldots, x_n) \in \bar{K}^{n+1}$$

such that $(x_0, dots, x_n) \neq (0, \ldots, 0)$ taken modulo the equivalence relation

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$$

if and only in there exists $\lambda \in \bar{K}, \lambda \neq 0$ such that $x_i = \lambda y_i$ for all i (Cf. [2, I]).

The equivalence class of a projective point $(x_0, \ldots, x_n)$ is denoted by $[x_0, \ldots, x_n]$. The set of K-rational points, denoted by $\mathbb{P}^n(K)$, is defined as

$$\mathbb{P}^n(K) = \{[x_0, \ldots, x_n] \in \mathbb{P}^n | x_i \in K \text{ for all } i\}$$

Definition 2 (Elliptic curve)**.** An *elliptic curve* is a pair (E, O), where E is a curve of genus 1 and $O \in E$. (We often just write E for the elliptic curve, the point O is being understood.) $E(K)$ is the subgroup of rational points over field k on the curve E. The elliptic curve E is defined over K, written E/K, if E is defined over K as a curve and $O \in E(K)$. (Cf. [14, III, §3]).

Let E be an elliptic curve given by a Weierstrass equation (see page 3). Remember that $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the Weierstrass equation together with the point $O = [0, 1, 0]$ at infinity. Let $L \subset \mathbb{P}^2$ be a line. Then since the equation has degree three, L intersects E at exactly 3 points, say P, Q, R. (Note if L is tangent to E, then P, Q, R may not be distinct. The fact that $L \cap E$ taken with multiplicities, consists of three points, is a special case of Bezout's theorem (Cf. [6, I.7, Corollary 7.8]).

Define a composition law $\oplus$ on E by the following rule.

Definition 3 (Composition law)**.** Let $P, Q \in E$, L be the line connecting P and Q (tangent line to E if $P = Q$), and R be the third point of intersection of L with E. Let L' be the line connecting R and O. Then $P \oplus Q$ is the point such that L' intersects E at R, O and $P \oplus Q$ (Cf. [14, III, §2]).

Let E be an elliptic curve defined over K. As E with composition law $\oplus$ has an abelian group structure, then we can define subgroup of its rational points over the field K and denote it $E(K)$.

Now we assume that the characteristic of K is $p > 0$.

Definition 4 (Supersingular elliptic curve)**.** For every n, we have a multiplication map

$$[n] : E \to E$$
$$P \mapsto \underbrace{P \oplus \cdots \oplus P}_{n \text{ times}}.$$

Its kernel is denoted by $E[n]$ and is called the n-torsion subgroup of E. Then one can show that for any $r \geq 1$:

$$E[p^r](\bar{K}) \simeq \begin{cases} 0 \\ \mathbb{Z}/p^r\mathbb{Z} \end{cases}$$

In the first case, E is called *supersingular*. Otherwise, it is called *ordinary* (Cf. [14, V, §3, Theorem 3.1]).

For each integer $r \geq 1$ we consider the p^r-power Frobenius morphism (Cf. [14, II, §2]) given by

$$\phi_r : E \to E^{(p^r)}$$
$$[x_0, \ldots, x_n] \mapsto [x_0^{p^r}, \ldots, x_n^{p^r}]$$

Let $m = \deg\phi_r$. Then we consider the morphism

$$\hat{\phi_r} : E^{(p^r)} \to E,$$

such that

$$\hat{\phi_r} \circ \phi_r = [m],$$

where $[m]$ is m-multiplication map. Such $\hat{\phi_r}$ is called *dual* of p^r-power Frobenius morphism (Cf. [14, III, §6, Theorem 6.1]).

We remind that morphism $f : X \to Y$ is separable if $K(X)$ is a separable extension of $K(Y)$ (Cf. [6, IV, 2]).

We remind the notion of separable extension. Let F be a finite extension of K. We say that F is separable over K if $[F : K]_S = [F : K]$, where $[F : K]_S$ is a separable degree of F over K. An element α algebraic over K is said to be separable over K if its minimal polynomial has no multiple roots.(Cf. [9, V, §4]) Then one can show that F is separable over K if and only if each element of F is sepable over K (Cf. [9, V, §4, Theorem 4.3]). Extensions which are not separable are called *inseparable*.

A finite extension K of field k is *purely inseparable* if for every $\alpha \in K$, $\alpha^{p^m} \in k$ for some $m \geq 0$ (Cf. [1]).

That brings us to another approach to define supersingular elliptic curve:

Definition 5 (Supersingular elliptic curve)**.** An elliptic curve E is supersingular if the map $\hat{\phi}_r$ is (purely) inseparable for one (all) $r \geq 1$ (Cf. [14, V, §3, Theorem 3.1]).

Definition 6 (Weierstrass equation)**.** An ellipric curve defined over K is the locus in $\mathbb{P}^2$ of an equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

with $a_1, \ldots, a_6 \in \bar{K}$. This equation is called a *Weierstrass equation* (Cf. [14, III, §1]).

To ease notation, we will usually write the Weierstrass equation for our elliptic curve using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

always remembering that there is the extra point $O = [0, 1, 0]$ out at infinity.

If $\mathrm{char}(\bar{K}) \neq 2$, then we can simplify the equation by completing the square. Replacing y by $\frac{1}{2}(y - a_1x - a_3)$ gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$b_2 = a_1^2 + 4a_2,$$
$$b_4 = 2a_4 + a_1a_3,$$
$$b_6 = a_3^2 + 4a_6.$$

We also define quantities

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4,$$
$$c_6 = b_2^3 + 36b_2b_4 - 216b_6,$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$
$$j = c_4^2/\Delta.$$

The quantity Δ given above is called the *discriminant* of the Weierstrass equation, j is called the *j-invariant* of the elliptic curve E. Now we can given another one definition of a supersingular elliptic curve:

Definition 7 (Supersingular elliptic curve)**.** If the map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$ then the curve E is called supersingular (Cf. [14, V, §3, Theorem 3.1]).

For the next definition of supersingular elliptic curve, we need to introduce the following notions.

Definition 8 (Order)**.** Let $\mathcal{K}$ be a (not necessarily commutative) algebra (i.e. vector space equipped with a bilinear product), finitely generated over $\mathbb{Q}$. An *order* $\mathcal{R}$ of $\mathcal{K}$ is a subring of $\mathcal{K}$ which is finitely generated as $\mathbb{Z}$-module (i.e. as an abelian group) and which satisfies $\mathcal{R}\otimes\mathbb{Q} = \mathcal{K}$, where $\otimes$ is the tensor product (Cf. [14, III, §9]).

Definition 9 (Quaternion algebra)**.** A *quaternion algebra* is an algebra of the form

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

with the multiplication rules

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

(Cf. [14, III, §9]).

Definition 10 (Supersingular elliptic curve)**.** An elliptic curve E is supersingular if the endomorphism ring $\mathrm{End}_{\bar{K}}(E)$ is an order in a quaternion algebra (Cf. [14, V, §3, Theorem 3.1]).

Remark 1. The endomorphism ring of an elliptic curve is either $\mathbb{Z}$ (if $p = 0$), an order in an imaginary quadratic number field (a number field of the form $\mathbb{Q}[\sqrt{-D}]$ for some $D > 0$), or an order in a quaternion algebra (Cf. [14, III, §, Corollary 9.4]).

Another way to define supersingular elliptic curve is based on a notion of a formal group.

Let R be a ring of characteristic $p > 0$.

Definition 11 (Formal group)**.** A *(one-parameter commutative) formal group* $\mathcal{F}$ *defined over* R is a power series $F(X, Y) \in R[\![X, Y]\!]$ satisfying:

1. $F(X, Y) = X + Y +$ (terms of degree ≥ 2).
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$ (associativity).
3. $F(X, Y) = F(Y, X)$ (commutativity).
4. There is unique power series $i(T) \in R[\![T]\!]$ such that $F(T, i(T)) = 0$ (inverse).
5. $F(X, 0) = 0$ and $F(0, Y) = Y$.

[14, IV, §2].

We call $F(X, Y)$ the *formal group law of* $\mathcal{F}$.

Returning now to formal power series, we look for the power series formally giving the addition law on E. Thus let z_1, z_2 be independent indeterminates, and let

$$w_i = w(z_i) = z_i^3(1 + A_1 z_i + A_2 z_i^2 + \cdots) \in \mathbb{Z}[a_1, \ldots, a_6][\![z_i]\!],$$

where $A_i \in \mathbb{Z}[a_1, \ldots, a_6]$, for $i = 1, 2$. In the (z, w)-plane, the line connecting (z_1, w_1) to (z_2, w_2) has slope

$$\lambda = \lambda(z_1, z_2) = \frac{w_2 - w_1}{z_2 - z_1} = \sum_{n=3}^{\infty} A_n \frac{z_2^n - z_1^n}{z_2 - z_1} \in \mathbb{Z}[a_1, \ldots, a_6][\![z_1, z_2]\!].$$

Letting

$$v = v(z_1, z_2) = w_1 - \lambda z_1 \in \mathbb{Z}[a_1, \ldots, a_6][\![z_1, z_2]\!],$$

the connecting line has equation $w = \lambda z + v$. Substituting this into the Weierstrass equation gives a cubic in z, two of whose roots are z_1 and z_2. Looking at the quadratic term, we see that the third z_3 can be expressed as a power series in z_1 and z_2:

$$\begin{aligned} z_3 &= z_3(z_1, z_2) = \\ &= -z_1 - z_2 + \frac{a_1\lambda + a_3\lambda^2 - a_2 v - 2a_4\lambda v - 3a_6\lambda^2 v}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3} \\ &\in \mathbb{Z}[a_1, \ldots, a_6][\![z_1, z_2]\!]. \end{aligned}$$

For the group law on E, the points $(z_1, w_1), (z_2, w_2), (z_3, w_3)$ add up to zero. Thus to add the first two, we need the formula for the inverse. In the (x, y)-plane, the inverse of (x, y) is $(x, -y - a_1 x - a_3)$. Hence the inverse of (z, w) will have z-coordinate $(z = -x/y)$

$$i(z) = \frac{x(z)}{y(z) + a_1 x(z) + a_3} = \frac{z^{-2} - a_1 z^{-1} - \ldots}{-z^{-3} + 2a_1 z^{-2} + \ldots}$$

This gives the formal additional law

$$\begin{aligned} F(z_1, z_2) &= i(z_3(z_1, z_2)) = \\ &= z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) - (2a_3 z_1^3 z_2 - (a_1 a_2 - 3a_3) z_1^2 z_2^2 + 2a_3 z_1 z_2^3) + \ldots \\ &\in \mathbb{Z}[a_1, \ldots, a_6][\![z_1, z_2]\!]. \end{aligned}$$

Let E be an elliptic curve given by a Weierstrass equation with coefficients in R. The *formal group associated to* E, denoted $\hat{E}$, is given by the power series $F(z_1, z_2)$ described above.

Definition 12 (Height of homomorphism; height of formal group)**.** Let $\mathcal{F}, \mathcal{G}$ defined over R be formal groups and $f : \mathcal{F} \to \mathcal{G}$ a homomorphism defined over R. The *height of* f, denoted $ht(f)$, is the largest integer h such that

$$f(T) = g(T^{p^h})$$

for some power series $g(T) \in R[\![T]\!]$. (If $f = 0$, then $ht(f) = \infty$.) The *height of* $\mathcal{F}$, denoted $ht(\mathcal{F})$, is the height of the multiplication by p map $[p] : \mathcal{F} \to \mathcal{F}$ [14, IV, §7].

Definition 13 (Supersingular elliptic curve)**.** If the formal group $\hat{E}/K$ associated to E has height 2, then E is supersingular [14, V, §3, Theorem 3.1].

For the next approach to define supersingular curve we introduce an important invariant of elliptic curve E defined over a perfect field K of characteristic $p > 0$.

Let $F : E \to E$ be the Frobenius morphism. Then F induces a map:

$$F^* : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$$

on cohomology. This map is not linear, but it is *p-linear*, namely $F^*(\lambda a) = \lambda^p F^*(a)$ for all $\lambda \in K, a \in H^1(E, O_E)$. Since E is elliptic, $H^1(E, O_E)$ is a one-dimensional vector space. Thus, since K is perfect, the map F^* is either 0 or bijective. For more information on cohomology see [6, III].

Definition 14 (Hasse invariant, Supersingular elliptic curve)**.** If $F^* = 0$, we say that E has *Hasse invariant* 0 or that E is *supersingular*; otherwise we say that E has *Hasse invariant 1* [6, IV, 4].

The next theorem also could be used as a definition.

Theorem 1. *An elliptic curve $E/\mathbb{F}_q$ is supersingular if and only if* $\mathrm{tr}\phi_E \cong 0 \mathrm{mod} p$*, where ϕ_E is the Frobenius morphism (Cf. [15, Lecture 14]).*

Proof. We first suppose that E is supersingular and assume $q = p^n$ so that $\phi_E = \phi^n$. Then $\ker[p] = \ker\phi\hat{\phi}$ is trivial, and therefore $\ker\hat{\phi}$ is trivial. Thus $\hat{\phi}$ is inseparable, since it has degree $p > 1$. The isogeny (see 8) $\hat{\phi}^n = \hat{\phi^n} = \hat{\phi}_E$ is also inseparable,as is ϕ_E, so $\mathrm{tr}\phi_E = \phi_E + \hat{\phi}_E$ is a sum of inseparable endomorphisms, hence inseparable (here we are viewing the integer $\mathrm{tr}\phi$ as an endomorphism). Therefore $\deg(\mathrm{tr}\phi_E) = (\mathrm{tr}\phi_E)^2$ is divisible by p, so $\mathrm{tr}\phi_E \cong 0 \mathrm{mod} p$.

Conversely, if $\mathrm{tr}\phi_E \cong 0 \mathrm{mod} p$, then p divides $\deg(\mathrm{tr}\phi_E) = (\mathrm{tr}\phi_E)^2$ and $\mathrm{tr}\phi_E$ is inseparable, as is $\hat{\phi}_E = \mathrm{tr}\phi_E - \phi_E$. This means that $\hat{\phi}^n$ and therefore $\hat{\phi}$ is inseparable. So $\ker\hat{\phi}$ is trivial, since it has prime degree p, and the same is true for ϕ. Thus the kernel of $[p] = \hat{\phi}\phi$ is trivial and E is supersingular. □

When $q = p$ is a prime greater than 3 this is equivalent to having the trace of Frobenius morphism equal to zero; this does not hold for $p = 2$ or 3.

1.2 Examples

In this section we are going to give some examples of supersingular curves.

Using definitions given in previous section may not always be a convenient way to identify a supersingular curves. But from those equivalent definitions we see thath up to isomorphism, there are only finitely many elliptic curves with Hasse invariant 0, since each has j-invariant in $\mathbb{F}_{p^2}$. For $p = 2$, once can easily check that the only one supersingular elliptic curve is

$$E : y^2 + y = x^3.$$

For $p > 2$, the following theorem gives a simple criterion for determining whether an elliptic curve is supersingular.

Theorem 2. *Let K be finite field of characteristic $p > 2$.*

(a) Let E/K be an elliptic curve with Weierstrass equation

$$E : y^2 = f(x)$$

where $f(x) \in K[x]$ is a cubic polynomial with distinct roots (in $\bar{K}$). Then E is supersingular if and only if the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is zero.

(b) Let $m = (p-1)/2$, and define a polynomial

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i.$$

Let $\lambda \in \bar{K}$, $\lambda \neq 0, 1$. Then the elliptic curve

$$E : y^2 = x(x-1)(x-\lambda)$$

is supersingular if and only if $H_p(\lambda) = 0$.

(c) The polynomial $H_p(t)$ has distinct roots in $\bar{K}$. Up to isomorphism, there are exactly

$$[\frac{p}{12}] + \varepsilon_p$$

supersingular elliptic curves in characteristic p, where $\varepsilon_3 = 1$, and for $p \geq 5$,

$$\varepsilon_p = 0, 1, 1, 2 \quad \textit{if} \quad p \cong 1, 5, 7, 11 (\text{mod} 12).$$

(Cf. [14, V, §4, Theorem 4.1])

Example 1. For which primes $p \geq 5$ is the elliptic curve

$$E : y^2 = x^3 + 1$$

supersingular?

Notice this curve has $j(E) = 0$. From the criterion of theorem 2(a), we must compute the coefficient of x^{p-1} in $(x^3+1)^{(p-1)/2}$. If $p \cong 2\text{mod}3$, then there is no x^{p-1} term, so E is supersingular; while if $p \cong 1\text{mod}3$, then the coefficients is $\binom{(p-1)/2}{(p-1)/3}$, which is non-zero modulo p, so in this case E is ordinary.

Example 2. Similary we compute for which primes $p \geq 3$ the $j = 1728$ elliptic curve

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

is supersingular.

This is determined by the coefficient of $x^{(p-1)/2}$ in $(x^2+1)^{(p-1)/2}$, which equals 0 if $p \cong 3\text{mod}4$ and $\binom{(p-1)/2}{(p-1)/4}$ if $p \cong 1\text{mod}4$. Hence E is supersingular if $p \cong 3\text{mod}4$ and ordinary if $p \cong 1\text{mod}4$.

Example 3. Let E be given by the equation

$$E : y^2 + y = x^3 - x^2 - 10x - 20,$$

so $j(E) = -\frac{2^{12}31^3}{11^5}$. Then by using the criterion of theorem 2 (a) directly one finds that the only primes $p < 100$ for which E is supersingular in characteristic p are $p = 19$ and $p = 29$. (D. H. Lehmer has calculated that there are exactly 27 primes $p < 31500$ for which this E is supersingular.)

2 Isogeny Graphs

We start this section with a notion of isogeny.

Definition 15. Let E_1 and E_2 be elliptic curves defined over a finite field $\mathbb{F}_q$ of characteristic p. An *isogeny* $\phi : E_1 \to E_2$ defined over $\mathbb{F}_q$ is a non-constant morphism that maps the identity into the identity (and this a is group homomorphism) (Cf. [13, 2.1]).

Two elliptic curves E_1 and E_2 defined over $\mathbb{F}_q$ are said to be *isogenous* over $\mathbb{F}_q$ if there exists an isgony $\phi : E_1 \to E_2$ defined over $\mathbb{F}_q$.

Theorem 3 (Sato-Tate)**.** *Two elliptic curves E_1 and E_2 are isogenous over $\mathbb{F}_q$ if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$ (Cf. [2, Theorem 13]).*

The degree of an isogeny ϕ is the degree of ϕ as a morphism. An isogeny of degree ℓ is called ℓ-isogeny.

Curves in the same isogeny class are either all supersingular or all ordinary.

For each isogeny $\phi : E_1 \to E_2$, there is a unique isogeny $\hat{\phi} : E_2 \to E_1$ which is called the *dual isogeny* of ϕ, satisfying $\phi\hat{\phi} = \hat{\phi}\phi = [\deg\phi]$.

If we have two isogenies $\phi : E_1 \to E_2$ and $\phi' : E_2 \to E_1$ such that $\phi\phi'$ and $\phi'\phi$ are the identity in their respective curves, we say that ϕ, ϕ' are *isomorphisms*, and that E, E' are *isomorphic*. Isomorphism classes of elliptic curves over $\mathbb{F}_q$ can be labeled with their j-invariants (see page 3). In this paper we write $j(E)$ for the j-invariant of E. By convention given a j-invariant $j \neq 0, 1728$, we write $E(j)$ for the curve defined by the equation

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}.$$

We also write $E(0)$ and $E(1728)$ for the curves with equations

$$y^2 = x^3 + 1 \quad \text{and} \quad y^2 = x^3 + x$$

respectively.

Definition 16 (Isogeny graph)**.** Let E be an elliptic curve over a field K of characteristic p. Let $S \subseteq \mathbb{N}$ be a finite set of primes. Define

$$X_{E,K,S}$$

to be the graph with vertex set being the K-isogeny class of E. Vertices are typically labelled by $j(E)$, though we also speak of "the vertex E". There is an edge $(j(E_1), j(E_2))$ labelled by ℓ for ezch equivalence class of ℓ-isogenies from E_1 to E_2 defined over K for some $\ell \in S$. We usually treat this as an undirected graph, since for every ℓ-isogeny $\phi : E_1 \to E_2$ there is a dual isogeny $\hat{\phi} : E_2 \to E_1$ of degree ℓ (Cf. [5, 25.2]).

2.1 Supersingular isogeny graph

For the supersingular isogey graph we work over $\bar{\mathbb{F}}_p$. The graph is finite. Indeed, theorem 2 (c) implies $\frac{p}{12} - 1 < \#X_{E,\bar{\mathbb{F}}_p,S} < \frac{p}{12} + 2$. Note that it suffices to consider elliptic curves defined over $\mathbb{F}_{p^2}$ (although the isogenies between them are over $\bar{\mathbb{F}}_p$ in genereal).

In contrast to the ordinary case , the supersingular graph is always connected using isogenies of any fixed degree (Cf. [10, 2.4]).

Theorem 4. *Let p be a prime and let E and $\tilde{E}$ be supersingular elliptic curves over $\bar{\mathbb{F}}_p$. Let ℓ be a prime different from p. Then there is an isogeny from E to $\tilde{E}$ over $\bar{\mathbb{F}}_p$ whose degree is a power of ℓ (Cf. [10, 2.4]).*

Hence, one can choose any prime ℓ and consider the ℓ-isogeny graphh $X_{e,\bar{\mathbb{F}}_p,\ell}$ on supersingular curves over $\bar{\mathbb{F}}_p$. It follows that the graph is $(\ell+1)$-regular and connected.

Now we will give some examples of supersingular isogeny graphs (cf. fig. 1, fig. 2, fig. 3)

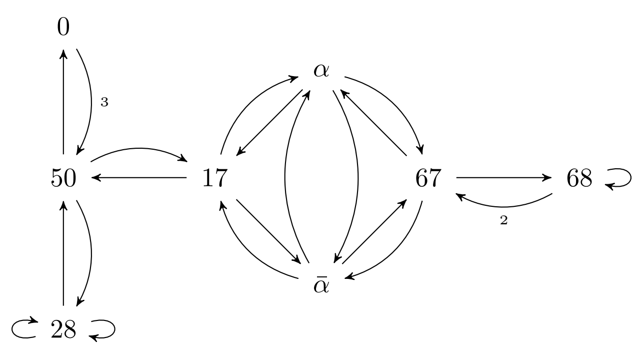

Figure 1: Supersingular Isogeny Graph $X_{\bar{\mathbb{F}}_{83},2}$

3 Application: Diffie-Hellman key exchange

Elliptic curves are widely used in modern cryptography. One of the most famous applications of the elliptic curves in cryptography is *Diffie-Hellman key*

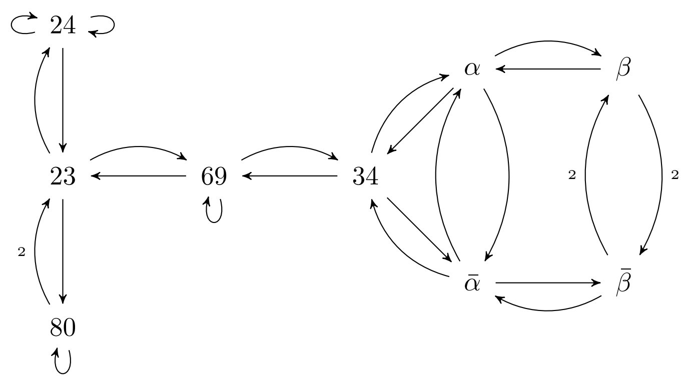

Figure 2: Supersingular Isogeny Graph $X_{\bar{\mathbb{F}}_103,2}$

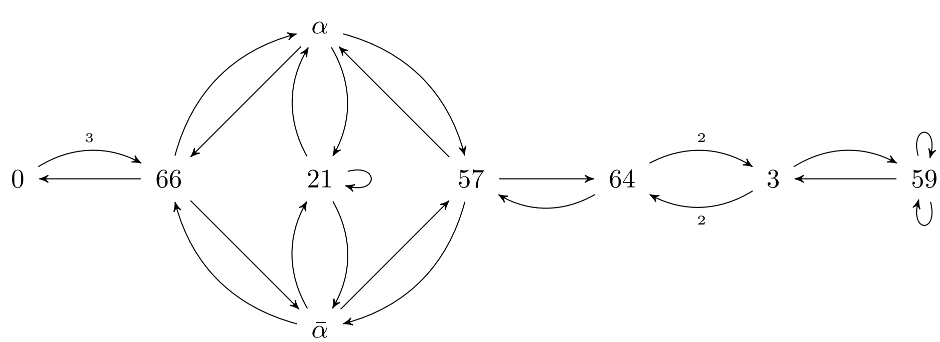

Figure 3: Supersingular Isogeny Graph $X_{\bar{\mathbb{F}}_{101},2}$

exchange, a cryptographic protocol by which two parties communicating over a public channel can agree on a common secret string unknown to any other party listening on the same channel.

We will first consider the original protocol, which was invented in the 1970s by Whitfield Diffie and Martin Hellman (cf. [4]), and constitutes the first practical example of public key cryptography. The two communicating parties are customarily called *Alice* and *Bob*, and the listening third party is a character called *Eve*.

Firstly, Alice and bob agree on a set of public parameters:

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

Then, Alice and Bob perform the following steps:

1. Each chooses a *secret* integer in the interval $]0, p-1[$: called a *Alice's secret* and b *Bob's secret*.

2. They respectively compute $A = g^a$ and $B = g^b$.

3. They exchange A and B over the public channel.

4. They respectively compute the *shared secret* $B^a = A^b = g^{ab}$.

The protocol can be generalized by replacing the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ with anny other cyclic group $G = \langle g \rangle$. So Eve is given the knowledge of the group G, its generator g and public data $A, B \in G$. Her goal is to recover the shared secret g^{ab}, which is mathematically possible, but not always easy to compute.

Definition 17 (Discrete logarithm)**.** Let G be a cycluc group generated by an element g. For any element $A \in G$, we define the *dicrete logarithm of A in base g*, denoted $\log_g(A)$, as the unique integer in the interval $[0, \#G[$ such that

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

It is obvious that if Eve can compute discrete logarithms in G efficiently, the she can also compute the shared secret. Thus, the strenth of the Diffie-Hellman key exchange protocol is entirely dependent on the hardness of the dicrete logarithm promblem in the group G.

There exists some algorithms to compute discrete logarithms in a generic group G that require $O(\sqrt{q})$ computational steps (see [7]), where q is the largest prime divisor of $\#G$. We also know that these algorithms are optimal for abstract cyclic groups. Therefore, the group G is usually chosen that way that the largest prime divisor Q has size at least $\log_2 q \simeq 256$. But there also exist algorithms of complexity better than $O(\sqrt{\#G})$ for the case $G = (\mathbb{Z}/p\mathbb{Z})^*$ (see [7]), thus requiring parameters of larger size to guarantee cryptographic strength.

However, no algorithms that solve discrete algorithm problem then generic ones are known for the case when G is a subgroup of $E(K)$, where E is an elliptic curve defined over a finite field K. For this reason, in the 1980s Miller ([11]) and Koblitz ([8]) suggested to replace $(\mathbb{Z}/p\mathbb{Z})^*$ in the Diffie-Hellman protocol by the group of rational point of an elliptic curve over a finite field. In this case public parameters of Elliptic Curves Diffie-Hellman (ECDH) protocol are:

- Finite field $\mathbb{F}_p$, with $\log_2 p \simeq 256$;

- Elliptic curve E over the finite field $\mathbb{F}_p$, such that $\#E(\mathbb{F}_p)$ is prime;

- A generator P of $E(\mathbb{F}_p)$.

And then Alice and Bob take the following steps:

1. Each chooses a secret from $]0, \#E(\mathbb{F}_p)[$, where we denote Alice's secret as a, and Bob's as b.

2. They compute public data $A = [a]P$ and $B = [b]P$.

3. Alice and Bob exchange public data.

4. Finally, they compute shared secret $S = [a]B = [b]A$.

It is already known that it is possible to reduce discrete logarithm problem on supersingular elliptic curves to the discrete logarithm problem in finite field (Cf. [12]). Hence it is possible to reduce the problem to one which is known to have sub-exponential complexity. That is why one should avoid using supersingular curves in ECDH.

In 2010 Stolbunov proposed a Diffie-Hellman type system based on the difficulty of computing isogenies between ordinary elliptic curves in order to get quantum-resistant cryptographic protocols. This paper concerns on using isogenies between *supersingular* elliptic curves instead of ordinary elliptic curves. The main technical difficulty is that, in the supersingular case, the endomorphism ring is noncommutative, whereas Diffie-Hellman type require commutativity.

Before moving to the Supersingular Isogeny Diffie-Hellman protocol description, we recall some concepts of graph theory.

We will restrict to undirected graphs. A *path* in undirected graph (E, V) between two vertices v, v' is a sequence of vertices $v \to v_1 \to \cdots \to v'$such that each vertex is connected to the next by an edge. The *adjacency matrix* of a graph G with vertex set $V = v_1, \ldots, v_n$ and edge set E, is $n \times n$ matrix where the (i, j)-th entry is 1 if there is an edge between v_i and v_j, and 0 otherwise. Since we have restricted to undirected graphs, the adjacency matrix is symmetric, thus it has n real eigenvalues

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

It is convenient to identify functions on V with vectors in $\mathbb{R}^n$, and therefore consider the adjacency matrix as a self-adjoint operator in $L^2(V)$. Then we can bound the eigenvalues of G.

Proposition 1. *if G is a k-regular graph, then its largest and smallest eigenvalues λ_1 and λ_n satisfy*

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

Definition 18 (Expander graph)**.** Let $\varepsilon > 0$ and $k \geq 1$. A k-regular graph is called a *(one-sided) ε-expander* if

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

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

$$\lambda_n \geq -(1 - \varepsilon)k.$$

References

[1] Lindsay N. Childs. *Purely Inseparable Field Extension.* `http://www.math.cornell.edu/~dkmiller/galmod/Childs_purely-inseparable.pdf`

[2] Luca De Feo. *Mathematics of isogeny based cryptography*, 2017.

[3] Luca De Feo, David Jao, Jerome Plut. *Towards Quantum-Resistant Cryptosystems From Supersingular Elliptic Curve Isogenies*, Journal of Mathematical Cryptology, 2014, 8 (3), pp. 209-247. `https://eprint.iacr.org/2011/506.pdf`

[4] Whitfield Diffie, Martin E. Hellman. *New Directions in Cryptography.* IEE Transactions of Information Theory, IT-22(6):644-654, 1976.

[5] Steven D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, 2012.

[6] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springler, New-York, 1977.

[7] Antoine Joux. *Algorithmic cryptanalysis.* CRC Press, 2009.

[8] Neal Koblitz. *Elliptic Curve Cryptosystems.* Mathematics of Computation, 48:203-209, 1987.

[9] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002.

[10] J-F Mestre. *La methode des graphes. Exemples et applications*, 2004.

[11] Victor Miller. *Use of elliptic curves in cryptography.* In Advances in Cryptology, CRYPTO 85, pages 417-426. Springer Verlag, LN CS 218, 1986.

[12] A. Menezes, T. Okamoto, S. Vanstone. *Reducing elliptic curve logarithms to a finite field.* IEEE Transactions on Information Theory, 39:1639-1646, 1993.

[13] Christophe Petit, Kristin Lauter. *Hard and Easy Problems for Supersingular Isogeny Graphs.* 2018

[14] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

[15] Andrew V. Sutherland. *Elliptic Curves (18.783)*, Lecture Notes, Spring 2015, full course is available on `http://dspace.mit.edu/handle/1721.1/111949#files-area`