

Supersingular Isogeny Diffie-Hellman

Valeriia Kulynych
Université de Toulon

April 30, 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

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

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

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

if and only if 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, \dots, x_n) is denoted by $[x_0, \dots, x_n]$. The set of K -rational points, denoted by $\mathbb{P}^n(K)$, is defined as

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

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. [7, 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. [4, 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. [7, 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

$$\begin{aligned} [n] : E &\rightarrow E \\ P &\mapsto \underbrace{P \oplus \cdots \oplus P}_{n \text{ times}}. \end{aligned}$$

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. [7, V, §3, Theorem 3.1]).

For each integer $r \geq 1$ we consider the p^r -power Frobenius morphism (Cf. [7, II, §2]) given by

$$\begin{aligned} \phi_r : E &\rightarrow E^{(p^r)} \\ [x_0, \dots, x_n] &\mapsto [x_0^{p^r}, \dots, x_n^{p^r}] \end{aligned}$$

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

$$\hat{\phi}_r : E^{(p^r)} \rightarrow E,$$

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. [7, III, §6, Theorem 6.1]).

We remind that morphism $f : X \rightarrow Y$ is separable if $K(X)$ is a separable extension of $K(Y)$ (Cf. [4, 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. [5, V, §4]) Then one can show that F is separable over K if and only if each element of F is separable over K (Cf. [5, 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. [7, V, §3, Theorem 3.1]).

Definition 6 (Weierstrass equation). An elliptic 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 $a_1, \dots, a_6 \in \bar{K}$. This equation is called a *Weierstrass equation* (Cf. [7, 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 $\text{char}(\bar{K}) \neq 2$, 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 give another one definition of a supersingular elliptic curve:

Definition 7 (Supersingular elliptic curve). If the map $[p] : E \rightarrow E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$ then the curve E is called supersingular (Cf. [7, 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. [7, 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. [7, III, §9]).

Definition 10 (Supersingular elliptic curve). An elliptic curve E is supersingular if the endomorphism ring $\text{End}_{\bar{K}}(E)$ is an order in a quaternion algebra (Cf. [7, 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. [7, 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 $F(0, Y) = Y$.

[7, 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

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

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

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

Letting

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

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 :

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

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 $(z = -x/y)$

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

This gives the formal additional law

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

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 $f : \mathcal{F} \rightarrow \mathcal{G}$ 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 $[p] : \mathcal{F} \rightarrow \mathcal{F}$ [7, IV, §7].

Definition 13 (Supersingular elliptic curve). If the formal group \hat{E}/K associated to E has height 2, then E is supersingular [7, 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 $F : E \rightarrow E$ be the Frobenius morphism. Then F induces a map:

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

on cohomology. This map is not linear, but it is p -linear, namely $F^*(\lambda a) = \lambda^p F^*(a)$ for all $\lambda \in K, a \in H^1(E, \mathcal{O}_E)$. Since E is elliptic, $H^1(E, \mathcal{O}_E)$ 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 [4, 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* [4, 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 $\text{tr}\phi_E \cong 0 \pmod{p}$, where ϕ_E is the Frobenius morphism (Cf. [8, 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 6) $\hat{\phi}^n = \hat{\phi}^n = \hat{\phi}_E$ is also inseparable, as is ϕ_E , so $\text{tr}\phi_E = \phi_E + \hat{\phi}_E$ is a sum of inseparable endomorphisms, hence inseparable (here we are viewing the integer $\text{tr}\phi$ as an endomorphism). Therefore $\deg(\text{tr}\phi_E) = (\text{tr}\phi_E)^2$ is divisible by p , so $\text{tr}\phi_E \cong 0 \pmod{p}$.

Conversely, if $\text{tr}\phi_E \cong 0 \pmod{p}$, then p divides $\deg(\text{tr}\phi_E) = (\text{tr}\phi_E)^2$ and $\text{tr}\phi_E$ is inseparable, as is $\hat{\phi}_E = \text{tr}\phi_E - \phi_E$. 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. \square

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.

2 Supersingular 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* $\phi : E_1 \rightarrow E_2$ defined over \mathbb{F}_q is a non-constant morphism that maps the identity into the identity (and this is a group homomorphism) [6, 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 isogeny $\phi : E_1 \rightarrow E_2$ defined over \mathbb{F}_q .

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

Supersingular curves are all defined over \mathbb{F}_{p^2} , and for every prime $\ell \nmid p$, there exist $\ell + 1$ isogenies (counting multiplicities) of degree ℓ originating from any given such supersingular curve. An isogeny can be identified with its kernel. Given a subgroup G of E , we can use Velu's formulas [2, Proposition 39] to compute an isogeny $\phi : E_1 \rightarrow E_2$ with kernel G and such that $E_2 \simeq E_1/G$.

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

If we have two isogenies $\phi : E_1 \rightarrow E_2$ and $\phi' : E_2 \rightarrow E_1$ 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 (ℓ -isogeny graph). For any prime $\ell \neq p$, one can construct a so-called *ℓ -isogeny graph*, where each vertex is associated to a supersingular j -invariant, and an edge between two vertices is associated to a degree ℓ isogeny between the corresponding curves [6, 2.1].

Isogeny graphs are regular with regularity degree $\ell + 1$; they are undirected since to any isogeny from j_1 to j_2 corresponds a dual isogeny from j_2 to j_1 .

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] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, New-York, 1977.
- [5] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
- [6] Christophe Petit, Kristin Lauter. *Hard and Easy Problems for Supersingular Isogeny Graphs*. 2018
- [7] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.
- [8] 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>