

# Evaluating large degree isogenies and applications to pairing based cryptography

Reinier Bröker, Denis Charles, and Kristin Lauter

Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA  
reinierb@microsoft.com, cdx@microsoft.com, klauter@microsoft.com

**Abstract.** We present a new method to evaluate large degree isogenies between elliptic curves over finite fields. Previous approaches all have *exponential* running time in the logarithm of the degree. If the endomorphism ring of the elliptic curve is ‘small’ we can do much better, and we present an algorithm with a running time that is *polynomial* in the logarithm of the degree. We give several applications of our techniques to pairing based cryptography.

## 1 Introduction

Various algorithms using elliptic curves rely on the efficient computation of *isogenies* between them. A noteworthy example is the ‘Schoof-Elkies-Atkin’ algorithm [10] to compute the group order of an elliptic curve over a finite field. Here, it is crucial that we are able to efficiently compute small degree isogenies. The known algorithms to evaluate an isogeny are all exponential time algorithms (in the logarithm of the degree), and the practicality of these algorithms is therefore limited to relatively small degrees. A lot of effort has gone into speeding up the algorithms [2]. In this paper we propose an algorithm to evaluate an isogeny between ordinary elliptic curves over finite fields that, in special cases, has a run time that is *polynomial* in the logarithm of its degree.

In Section 2 we explain how to represent certain prime degree  $l$  isogenies that are defined over  $\mathbf{F}_q$  with at most  $3 \log l$  bits. This is a big contrast with the representation by rational functions or by its ‘kernel polynomial’ as these representations take roughly  $l$  bits. We show that our representation applies to almost all isogenies: the only condition is that not all subgroups of order  $l$  are defined over the base field  $\mathbf{F}_q$ . As the  $l$ -torsion has  $l^2$  elements for  $l \neq \text{char}(\mathbf{F}_q)$ , this condition is harmless for large  $l$ .

We present our approach to evaluate an isogeny  $\varphi : E \rightarrow E'$  in Sections 3 and 4. The run time is polynomial in the class number of the endomorphism ring of  $E$ , and is therefore only fast when this class group is *small*. This certainly limits the practicality of the method since randomly chosen elliptic curves over  $\mathbf{F}_q$  will have an associated class group of size roughly  $\sqrt{q}$ . However, if the elliptic curve in question is constructed by *complex multiplication techniques* then the class group will always be small. In particular, our method applies to the curves with prescribed prime order constructed in [3], the curves with prime order of

prescribed size constructed in e.g. [7] and the pairing friendly curves constructed in e.g. [9].

Section 5 gives several examples of the new evaluation algorithm. Our approach is so fast that isogenies of degree  $l \approx 10^{100}$  are easily computed. We focus on applications to pairing-based cryptography in Section 6. We first describe a variant of the ‘BLS signature scheme’ [1] where two different isogenous elliptic curves are used instead of a single elliptic curve as in the basic BLS scheme. As another application, we show how our technique can be used in the isogeny variant of BLS which was proposed by Jao and Venkatesan [5]. Their scheme replaces a secret integer by a secret isogeny. For the security of the scheme, the secret isogeny must have degree of cryptographic size. Until the present paper, efficient evaluation of such large degree isogenies was only possible in special cases such as integer multiplication, or integer multiplication composed with a small degree isogeny.

## 2 Representation of isogenies

Let  $E, E'$  be two elliptic curves defined over some field  $F$ . An *isogeny*  $\varphi$  between  $E$  and  $E'$  is a non-constant morphism  $\varphi : E \rightarrow E'$ . It is well known that isogenies are geometrically surjective, i.e., for every point  $P \in E'(F)$  there exists a point  $Q \in E(\overline{F})$  with  $\varphi(Q) = P$ . We say that  $\varphi$  is defined over  $F$  if the kernel of  $\varphi$  is as a group defined over  $F$ , meaning that the absolute Galois group of  $F$  maps the kernel of  $\varphi$  into itself. This does not mean that all the points of the kernel of  $\varphi$  are  $F$ -rational. Indeed, the multiplication by  $n$ -map is  $F$ -rational, yet most  $n$ -torsion points will not be defined over  $F$ .

An isogeny  $\varphi$  induces an inclusion  $F(E') \subset F(E)$  of function fields, and the degree  $[F(E) : F(E')]$  is called the *degree*  $\deg(\varphi)$  of  $\varphi$ . If  $\deg(\varphi)$  is coprime to the characteristic of  $F$ , the extension  $F(E)/F(E')$  is separable and the degree of  $\varphi$  equals the number of points in its kernel. Most of the isogenies we consider in this article are separable.

The ‘standard’ way to represent an isogeny  $\varphi$  is to give 3 homogeneous polynomials  $f_1, f_2, f_3 \in \overline{F}[X, Y, Z]$  satisfying  $\varphi((x : y : z)) = (f_1(x, y, z) : f_2(x, y, z) : f_3(x, y, z)) \in \mathbf{P}^2(\overline{F})$ . If  $l$  denotes the degree of  $\varphi$ , then usually one of these polynomials will have degree roughly  $l$ , and this representation takes *exponential* time in  $\log l$  to write down. In this section we explain a representation of isogenies between elliptic curves over finite fields whose length is *polynomial* in  $\log l$ .

Assume that  $E/F$  has complex multiplication, meaning that the endomorphism ring  $\text{End}_F(E)$  is isomorphic to the imaginary quadratic order  $\mathcal{O}_\Delta$  for some  $\Delta < 0$ . By writing  $\mathcal{O}_\Delta = \mathbf{Z}[\alpha]$  and fixing a root in  $F$  of the minimal polynomial of  $\alpha$ , we view  $F$  as an  $\mathcal{O}_\Delta$ -algebra. There are  $|\mathcal{O}_\Delta^*| > 1$  isomorphisms  $\text{End}_F(E) \xrightarrow{\sim} \mathcal{O}_\Delta$  and throughout this article we assume that we have *fixed* the normalized isomorphism, i.e., the unique isomorphism  $\iota$  with the property that  $\iota^*(x)\omega = x\omega$  for all invariant differentials  $\omega$  and all  $x \in \mathcal{O}_\Delta$ . In particular, we will identify the rings  $\text{End}_F(E)$  and  $\mathcal{O}_\Delta$ .

We let  $\text{Ell}_\Delta(F)$  be the set of  $\overline{F}$ -isomorphism classes of elliptic curves over  $F$  whose endomorphism ring equals  $\mathcal{O}_\Delta$ . It is well known that for  $F = \mathbf{C}$ , the set  $\text{Ell}_\Delta(\mathbf{C})$  is a finite set of cardinality  $h_\Delta$ , the class number of the order  $\mathcal{O}_\Delta$ . The key to this result is that the class group acts in a natural way on  $\text{Ell}_\Delta(\mathbf{C})$ . Indeed, if we let

$$E[\mathfrak{L}] = \{P \in E(\mathbf{C}) \mid \forall \alpha \in \mathfrak{L} : \alpha(P) = 0\}$$

denote the group of ‘ $\mathfrak{L}$ -torsion points’ for an  $\mathcal{O}_\Delta$ -ideal  $\mathfrak{L}$ , then the map

$$j(E) \mapsto j(E/E[\mathfrak{L}]) = j(E)^\mathfrak{L}$$

factors through the class group. One then proves that this action is transitive and free [11, Prop. II.1.2].

As there are only finitely many isomorphism classes of complex elliptic curves with endomorphism ring equal to  $\mathcal{O}_\Delta$ , the  $j$ -invariant  $j(E)$  is algebraic for  $j(E) \in \text{Ell}_\Delta(\mathbf{C})$ . In fact, we have  $\text{Ell}_\Delta(\mathbf{C}) = \text{Ell}_\Delta(H_\mathcal{O})$  where  $H_\mathcal{O}$  is the ring class field associated to  $\mathcal{O}_\Delta$ , i.e., the unique abelian extension inside  $\mathbf{C}$  of  $\mathbf{Q}(\sqrt{\Delta})$  whose Galois group is isomorphic to the class group  $\text{Pic}(\mathcal{O}_\Delta)$  under the Artin map. If  $p$  is a prime that does not ramify in  $H_\mathcal{O}/\mathbf{Q}$ , then we get a natural injection

$$g : \text{Ell}_\Delta(H_\mathcal{O}) \rightarrow \text{Ell}_\Delta(\mathbf{F}_q).$$

Here,  $\mathbf{F}_q$  is the finite field with  $q = p^f$  elements and  $f$  equals the residue class degree of a prime lying over  $p$ . In particular, if  $p$  splits completely we get an injection  $\text{Ell}_\Delta(H_\mathcal{O}) \rightarrow \text{Ell}_\Delta(\mathbf{F}_p)$ . By the Deuring lifting theorem [8, Th. 13.12], the map  $g$  is surjective as well. Furthermore, the class group action in characteristic zero respects the reduction map, and we get a natural action of  $\text{Pic}(\mathcal{O}_\Delta)$  on  $\text{Ell}_\Delta(\mathbf{F}_q)$ . Just like in characteristic zero, an  $\mathcal{O}_\Delta$ -ideal  $\mathfrak{L}$  acts on  $j(E) \in \text{Ell}_\Delta(\mathbf{F}_q)$  by  $j(E) \mapsto j(E/E[\mathfrak{L}]) = j(E)^\mathfrak{L}$ . Since the Frobenius endomorphism of  $E$  commutes with all endomorphisms in  $\mathfrak{L}$ , the group  $E[\mathfrak{L}]$  is  $\mathbf{F}_q$ -rational.

**Lemma 1.** *Let  $E/\mathbf{F}_q$  be an ordinary elliptic curve and let  $\varphi : E \rightarrow E'$  be an  $\mathbf{F}_q$ -isogeny of prime degree  $l \neq \text{char}(\mathbf{F}_q)$ . Let  $\pi_q$  be the Frobenius morphism of  $E$  and let  $\mathfrak{L} \subset \text{End}(E)$  be an ideal of norm  $l$ . If  $l$  does not divide the index  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$  then the kernel of  $\varphi$  equals either  $E[\mathfrak{L}]$  or  $E[\overline{\mathfrak{L}}]$ .*

*Proof.* The kernel of  $\varphi$  is a subgroup of order  $l$  of the  $l$ -torsion of  $E$ . We have  $E[l] \cong \mathbf{Z}/l\mathbf{Z} \times \mathbf{Z}/l\mathbf{Z}$  and there are  $l+1$  subgroups of order  $l$ . A slight generalization of [6, Prop. 23] gives that only  $(\frac{\Delta}{l}) + 1 \in \{0, 1, 2\}$  of those are  $\mathbf{F}_q$ -rational if  $l$  does not divide  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$ . As  $\varphi$  is defined over  $\mathbf{F}_q$ , the group  $E[\mathfrak{L}]$  is  $\mathbf{F}_q$ -rational and the lemma follows.  $\square$

This lemma shows that ‘most’ of the  $\mathbf{F}_q$ -rational prime degree isogenies between ordinary elliptic curves over finite fields have a kernel of the form  $E[\mathfrak{L}]$ . Every  $\mathcal{O}_\Delta$ -ideal of prime norm  $l$  not dividing  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$  can be written in the form

$$\mathfrak{L} = (l, c + d\pi_q),$$

and we can therefore represent the *kernel* of  $E \rightarrow E/E[\mathfrak{L}]$  by specifying the  $\text{End}(E)$ -ideal  $\mathfrak{L} = (l, c + d\pi_q)$ . This representation requires only  $3 \log l$  bits.

The kernel  $C$  of a separable isogeny  $\varphi : E \rightarrow E'$  does not uniquely determine  $\varphi$ . Indeed, if we compose  $\varphi$  with an isomorphism  $E' \xrightarrow{\sim} E''$  then the kernel is unchanged. To keep track of isomorphisms, we choose Weierstraß equations for  $E$  and  $E'$  and note that the pull back  $\varphi^*(\omega_{E'})$  of the invariant differential of  $E'$  equals a constant multiple of the invariant differential  $\omega_E$  of  $E$ . If we have

$$\varphi^*(\omega_{E'}) = \omega_E$$

then the isogeny  $\varphi$  is said to be *normalized*. It is easy to see that a subgroup  $C \subset E[l]$  of order  $l$  defines a unique elliptic curve  $E'$  such that there exists a normalized isogeny  $E \rightarrow E'$  with kernel  $C$ . The isogeny  $E \rightarrow E'$  is uniquely determined up to automorphisms of the curve  $E'$ . We conclude that a subgroup  $C \subset E[l]$  determines a well-defined map  $E \rightarrow E'/\text{Aut}(E')$ . The quotient  $E'/\text{Aut}(E')$  is isomorphic to the projective line  $\mathbf{P}^1$  and in practice we will often map a point  $P \in E'(\mathbf{F}_q)$  to its  $x$ -coordinate in  $\mathbf{P}^1(\mathbf{F}_q)$ . If  $E'$  has endomorphism ring  $\mathbf{Z}[i]$  or  $\mathbf{Z}[\zeta_3]$  we need to consider the square resp. cube of the  $x$ -coordinate. With this convention, the main result of the paper is the following.

**Theorem 1.** *Let  $E/\mathbf{F}_q$  be an ordinary elliptic curve with Frobenius  $\pi_q$ , given by a Weierstraß equation, and let  $P \in E(\mathbf{F}_{q^n})$  be a point on  $E$ . Let  $\Delta = \text{disc}(\text{End}(E))$  be given. Assume that  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$  and  $\#E(\mathbf{F}_{q^n})$  are coprime, and let  $\mathfrak{L} = (l, c + d\pi_q)$  be an  $\text{End}(E)$ -ideal of prime norm  $l \neq \text{char}(\mathbf{F}_q)$  not dividing the index  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$ . Then Algorithm 4.1 computes the unique elliptic curve  $E'$  such that there exists a normalized isogeny  $\varphi : E \rightarrow E'$  with kernel  $E[\mathfrak{L}]$ . Furthermore, it computes the  $x$ -coordinate of  $\varphi(P)$  if  $\text{End}(E)$  does not equal  $\mathbf{Z}[i]$  or  $\mathbf{Z}[\zeta_3]$  and the square resp. cube of the  $x$ -coordinate of  $\varphi(P)$  otherwise. The running time of the algorithm is polynomial in  $\log l$ ,  $\log q$ ,  $n$  and  $|\Delta|$ .*

Although the run time algorithm is polynomial in the discriminant  $\Delta$  of the endomorphism ring  $\text{End}(E)$ , the description of the algorithm in Section 4 shows that this ‘bottleneck’ disappears once  $\mathfrak{L}$  is *principal*. Hence, it gives a polynomial time algorithm to evaluate all endomorphisms of the curve, regardless of the size of endomorphism ring of  $E$ .

### 3 Evaluating small degree isogenies

Throughout this section,  $E/\mathbf{F}_q$  is a fixed ordinary elliptic curve and  $\mathfrak{L} = (l, c + d\pi_q)$  is an  $\text{End}(E)$ -ideal of prime norm  $l \neq \text{char}(\mathbf{F}_q)$  not dividing the index  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$ . In this section we explain two methods to compute the image  $\varphi(P) \in E'/\text{Aut}(E') \cong \mathbf{P}^1$  of a point  $P \in E(\mathbf{F}_{q^n})$  under ‘the’ normalized isogeny  $\varphi : E \rightarrow E'$  defined by  $\mathfrak{L}$ . As the run time of these approaches is polynomial in  $l$ , the prime  $l$  should be small for these methods to be practical.

The first method is strongly based on the techniques that Atkin and Elkies used to improve Schoof’s original point counting algorithm [10, Sec. 6–8]. It does not work in some special cases and we will make assumptions while describing the method. The second method works in general, but is typically slower.

### 3.1 Atkin-Elkies techniques

We assume  $p = \text{char}(\mathbf{F}_q) > l \geq 3$  in this subsection, and we let  $E$  be given by a Weierstraß equation  $Y^2 = X^3 + aX + b$ . We assume that  $\text{End}(E)$  does not equal  $\mathbf{Z}[i]$  or  $\mathbf{Z}[\zeta_3]$ . We will compute a polynomial  $f_{\mathcal{L}} \in \mathbf{F}_q[X]$  with the property that its roots are the  $x$ -coordinates of the points in  $E[\mathcal{L}]$ . Once we know  $f_{\mathcal{L}}$  it is an easy matter to compute the image  $\varphi(P)$ . Indeed, Vélu’s formulas [13] give us the normalized isogeny  $\varphi$  as rational function and we can simply evaluate at the point  $P$ .

To compute  $f_{\mathcal{L}} \in \mathbf{F}_q[X]$ , we start by computing the  $j$ -invariant of  $E'$ . As  $E'$  is  $l$ -isogenous to  $E$ , we know that  $j(E')$  is a root of the  $l$ -th modular polynomial  $\Phi_l(j(E), X) \in \mathbf{F}_p[X]$  specialized in  $j(E)$ . The modular polynomial has degree  $l + 1$ , but the assumption  $l \nmid [\text{End}(E) : \mathbf{Z}[\pi_q]]$  ensures that it has either 1 (if  $\mathcal{L}$  is ramified) or 2 (if  $\mathcal{L}$  splits) roots in  $\mathbf{F}_q$ . We fix a root  $h \neq 0, 1728$ . If  $\mathcal{L}$  splits, then  $h$  is either  $j(E') = j(E)^{\mathcal{L}}$  or  $j(E)^{\overline{\mathcal{L}}}$ . We do not know which one yet.

The ‘Atkin-Elkies techniques’ only work if the partial derivative  $\Phi_Y$  of  $\Phi_l \in \mathbf{F}_q[X, Y]$  with respect to  $Y$  does not vanish when evaluated in  $(X, Y) = (j(E), h)$ . Using some algebraic geometry, one can prove [10, Sec. 7] that this only happens when  $l$  is larger than  $4|\Delta|$ , with  $\Delta$  the discriminant of  $\text{End}(E)$ . Hence, it only fails for ‘large’  $l$ . In the examples we computed, this hardly caused any problems. If it does happen, we switch to the second method described below. For the remainder of this subsection we assume that  $\Phi_Y(j(E), h)$  is not zero.

Next we compute an elliptic curve  $E_1$  with  $j$ -invariant  $h$  such that the isogeny  $E \rightarrow E_1$  with kernel  $E[\mathcal{L}]$  or  $E[\overline{\mathcal{L}}]$  is normalized. As in [10, Sec. 7], we put

$$s = -\frac{18b}{l} \frac{\Phi_X(j(E), h)}{a \Phi_Y(j(E), h)} j(E) \in \mathbf{F}_q$$

and with

$$a' = -\frac{1}{48} \frac{s^2}{h(h - 1728)} \in \mathbf{F}_q$$

$$b' = -\frac{1}{864} \frac{s^3}{h^2(h - 1728)} \in \mathbf{F}_q,$$

the equation for  $E_1$  is given by  $Y^2 = X^3 + a'X + b'$ .

Let  $C$  be the kernel of the normalized isogeny  $E \rightarrow E_1$ , i.e.,  $C$  is either  $E[\mathcal{L}]$  or  $E[\overline{\mathcal{L}}]$ . Theoretically, the hard part is computing the constant term  $p_1$  of the kernel polynomial  $f_C$  describing  $C$ . The formulas are rather involved and can be found in [10, Sec. 8]. The other coefficients of  $f_C$  can now be found using a recursive relation involving the coefficients of the Laurent series of the Weierstraß- $\varphi$  function. The key point is that computing  $f_C$  involves nothing

more than simple arithmetic in  $\mathbf{F}_q$ . Once we have the equation for  $E_1$ , there are other methods as well to find  $f_C$ ; we refer to [2] for an overview.

Knowing the polynomial  $f_C$ , it remains to check if our initial guess  $h$  was correct. We either have  $f_C = f_{\mathfrak{L}}$  or  $f_C = f_{\overline{\mathfrak{L}}}$  and to check in which case we are, we note that with  $\mathfrak{L} = (l, c + d\pi_q)$ , the Frobenius  $\pi_q$  acts as multiplication by  $-c/d \in \mathbf{F}_l$  on the points in  $E[\mathfrak{L}]$ . We test if  $(X^q, Y^q) = (-c/d) \cdot (X, Y)$  holds for the points in  $C$ , i.e., we compute both  $(X^q, Y^q)$  and  $(-c/d) \cdot (X, Y)$  in the ring

$$\mathbf{F}_q[X, Y]/(f_C(X), Y^2 - X^3 - aX - b).$$

Note that the  $\cdot$  means repeated adding *on the curve* and  $(-c/d) \cdot (X, Y)$  can be computed by employing division polynomials.

If we find that  $f_C$  does not equal  $f_{\mathfrak{L}}$  we know that the unique other zero  $h_2 \in \mathbf{F}_q$  of

$$\gcd(X^q - X, \Phi_l(j(E), X)) \in \mathbf{F}_q[X]$$

must be the  $j$ -invariant of  $E'$  and we repeat the computation with  $h$  replaced by  $h_2$  to find the polynomial  $f_C = f_{\mathfrak{L}} \in \mathbf{F}_q[X]$ .

### 3.2 General technique

The approach described in this subsection works for any prime power  $q$  and any prime  $l \neq \text{char}(\mathbf{F}_q)$ . Let  $\Psi_l$  be the division polynomial for  $E/\mathbf{F}_q$ . For  $l > 2$ , the polynomial  $\Psi_l$  has degree  $(l^2 - 1)/2$ . By computing roots of  $\Psi_l$ , we compute two generators  $G_1, G_2$  of the group  $E[l] \cong \mathbf{Z}/l\mathbf{Z} \times \mathbf{Z}/l\mathbf{Z}$ . The points will typically be defined over an extension of  $\mathbf{F}_q$  of degree close to  $l$ . Indeed, if  $L$  denotes the field of definition of the  $l$ -torsion, then the degree  $[L : \mathbf{F}_q]$  equals the order of  $\pi_q$  in the group  $(\mathcal{O}_{\Delta}/l)^*$ , and this order is usually close to  $l$ .

The goal is to find a point  $Q$  in the kernel  $E[\mathfrak{L}]$ . With  $\mathfrak{L} = (l, c + d\pi_q)$  we need to find an  $l$ -torsion point  $Q$  with  $\pi_q(Q) = (-c/d)Q$ . We can simply list the generators  $\alpha G_1 + \beta G_2$  of the  $l + 1$  subgroups of order  $l$  of  $E[l]$  and check for each generator if Frobenius acts as multiplication by  $-c/d$ .

Once we find  $Q$ , we compute the subgroup generated by  $Q$  and use Vélú's formulas [13] to evaluate the isogeny.

## 4 Evaluating large degree isogenies

The method described in Section 3 is intended for relatively small primes  $l$ . In this section we explain how to use the class group of the endomorphism ring  $\text{End}(E) = \mathcal{O}_{\Delta}$  to reduce the computation of a large degree isogeny to the computation of small degree isogenies. As before,  $E/\mathbf{F}_q$  is an ordinary curve and  $\mathfrak{L} = (l, c + d\pi_q)$  is an  $\text{End}(E)$ -ideal of prime norm  $l \nmid [\text{End}(E) : \mathbf{Z}[\pi_q]]$ . Let  $P \in E(\mathbf{F}_{q^n})$  be a point. For reasons to become clear, we demand in this section that  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$  and  $\#E(\mathbf{F}_{q^n})$  are coprime. The goal is to compute  $\varphi(P) \in E'/\text{Aut}(E')$  with  $\varphi : E \rightarrow E'$  an isogeny with kernel  $E[\mathfrak{L}]$ .

We have an equality

$$[\mathfrak{L}] = [\mathfrak{p}_1]^{e_1} \dots [\mathfrak{p}_k]^{e_k} \quad (4.1)$$

inside the class group  $\text{Pic}(\mathcal{O}_\Delta)$  for some suitable choice of generators  $\mathfrak{p}_i$ . The key observation is that the norms of  $\mathfrak{p}_i$  can be *much* smaller than the norm of  $\mathfrak{L}$ . Indeed, the size of  $\mathfrak{p}_i$  depends only on the discriminant of  $\text{End}(E)$  and not of the norm of  $\mathfrak{L}$ . We can write  $\mathfrak{L} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}(\alpha)$  for some fractional principal  $\mathcal{O}_\Delta$ -ideal  $(\alpha)$ . To find  $\alpha$ , we compute the integral ideal  $\mathfrak{L}\bar{\mathfrak{p}}_1^{e_1} \dots \bar{\mathfrak{p}}_k^{e_k}$  and use Cornacchia's algorithm [4, Sec. 1.5.2] to find a generator  $\beta \in \mathcal{O}_\Delta$ . The choice  $\alpha = \beta/m$ , with  $m$  the product of the norms of the ideals occurring in (4.1), works.

To evaluate 'the' isogeny  $\varphi$  associated to  $\mathfrak{L}$ , it suffices to evaluate the isogenies associated to the  $\mathfrak{p}_i$ 's and to  $(\alpha)$ . If the  $\mathfrak{p}_i$ 's don't divide  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$ , we can use the method from Section 3 in the following way. We compute the isogeny

$$E \longrightarrow E_1 = E/E[\mathfrak{p}_1]$$

and note that we have a canonical isomorphism  $\text{End}(E) \xrightarrow{\sim} \mathcal{O}_\Delta \xrightarrow{\sim} \text{End}(E_1)$  that allows us to interpret the 'next' ideal occurring in (4.1) as an  $\text{End}(E_1)$ -ideal. Multiplication of  $\mathcal{O}_\Delta$ -ideals and composition of isogenies is compatible in the sense that we have

$$E/[\mathfrak{p}_1\mathfrak{p}_2] \cong E_1/[\mathfrak{p}_1].$$

By applying the method from Section 3 iteratively, we compute the normalized isogeny  $\phi_c : E \rightarrow E_c = E/[\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}]$ .

We now explain how to deal with the ideal  $(\alpha)$ . The element  $\beta$  will typically *not* lie in the subring  $\mathbf{Z}[\pi_q]$  of  $\mathcal{O}_\Delta$ . However, we can write  $\alpha = (u + v\pi_q)/(mz)$  with  $z \in \mathbf{Z}$  dividing the index  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$ . The curves  $E_c$  and  $E' = E/E[\mathfrak{L}]$  are  $\mathbf{F}_q$ -isomorphic because  $(\alpha)$  is a principal ideal. The space of invariant differentials for  $E'$  is a 1-dimensional  $\mathbf{F}_q$ -vector space, and because  $\pi_q$  is inseparable we have  $\pi_q^*(\omega_{E'}) = 0$ . Hence, the invariant differentials for the Weierstraß equations of  $E_c$  and  $E'$  satisfy

$$\omega_{E'} = (u/mz)\omega_{E_c}$$

if  $m$  is non-zero in  $\mathbf{F}_q$ . To find the equation for  $E'$ , we need to apply an isomorphism  $\eta : E_c \xrightarrow{\sim} E'$  with  $\eta^*(\omega_{E'}) = (u/mz)\omega_{E_c}$ . This is easy: if  $E_c$  is given by  $Y^2 = X^3 + a'X + b'$  then for  $\lambda \in \mathbf{F}_q^*$  the isomorphism  $(X, Y) \mapsto (\lambda^2 X, \lambda^3 Y)$  multiplies  $\omega_{E_c}$  by  $1/\lambda$ . Hence, the curve  $E'$  is given by  $Y^2 = X^3 + (u/mz)^4 a'X + (u/mz)^6 b'$ .

Having found the equation for  $E'$ , we need to compute the action of  $(\alpha)$  on the image  $\eta(\phi_c(P)) \in E'(\mathbf{F}_{q^n})$ . By assumption, the integer  $z$  in the denominator of  $\alpha$  is coprime to  $\#E(\mathbf{F}_{q^n})$ . If  $m$  is also coprime to the group order of  $E(\mathbf{F}_{q^n})$  then we can simply compute the inverse of  $zm$  modulo  $\#E(\mathbf{F}_{q^n})$  and compute  $R = ((zm)^{-1}(u + v\pi_q))(Q) \in E'(\mathbf{F}_{q^n})$ . A suitable power of the  $x$ -coordinate of  $R$  is the value we are looking for. Summarizing everything, we have the following algorithm.

#### Algorithm 4.1

Input: a discriminant  $\Delta$ , an elliptic curve  $E/\mathbf{F}_q$  with  $\text{End}(E) = \mathcal{O}_\Delta$  and a

point  $P \in E(\mathbf{F}_{q^n})$  such that  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$  and  $\#E(\mathbf{F}_{q^n})$  are coprime, an  $\text{End}(E)$ -ideal  $\mathfrak{L} = (l, c + d\pi_q)$  of prime norm  $l \neq \text{char}(\mathbf{F}_q)$  not dividing  $[\text{End}(E) : \mathbf{Z}[\pi_q]]$ .

Output: the elliptic curve  $E'$  such that an isogeny  $\varphi : E \rightarrow E'$  with kernel  $E[\mathfrak{L}]$  is normalized and the  $x$ -coordinate of  $\varphi(P)$  for  $\Delta \neq -3, 4$  and the cube resp. square of the  $x$ -coordinate otherwise.

1. Compute the direct sum decomposition  $\text{Pic}(\mathcal{O}_\Delta) = \bigotimes \langle \mathfrak{p}_i \rangle$  of  $\text{Pic}(\mathcal{O}_\Delta)$  into cyclic groups generated by the degree 1 prime ideals  $\mathfrak{p}_i$  of smallest norm that are coprime to the product  $p \cdot \#E(\mathbf{F}_{q^n}) \cdot [\text{End}(E) : \mathbf{Z}[\pi_q]]$ .
2. Write  $\mathfrak{L} = \mathfrak{p}_1^{e_1} \cdot \dots \cdot \mathfrak{p}_k^{e_k} \cdot (\alpha)$  with the  $\mathfrak{p}_i$ 's as in Step 1.
3. Compute a sequence of isogenies  $(\phi_1, \dots, \phi_s)$  such that the composition  $\phi_c : E \rightarrow E_c$  has kernel  $E[\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}]$  using the method from Section 3. Evaluate  $\phi_c(P) \in E_c(\mathbf{F}_{q^n})$ .
4. Write  $\alpha = (u + v\pi_q)/(zm)$ . Compute an isomorphism  $\eta : E_c \xrightarrow{\sim} E'$  with  $\eta^*(\omega_{E'}) = (u/zm)\omega_{E_c}$ . Compute  $Q = \eta(\phi_c(P))$ .
5. Compute the inverse  $(zm)^{-1}$  of  $zm$  modulo  $\#E(\mathbf{F}_{q^n})$  and compute  $R = ((zm)^{-1}(u + v\pi_q))(Q)$ .
6. Put  $r = x(R)^{|\mathcal{O}_\Delta|^*/2}$  and return  $(E', r)$ .

An analysis of the algorithm yields Theorem 1:

*Proof of Theorem 1.* To prove the correctness of the algorithm, it suffices to show that we can take the generators in Step 1 coprime to  $p \cdot \#E(\mathbf{F}_{q^n}) \cdot [\text{End}(E) : \mathbf{Z}[\pi_q]]$ . This follows from the fact that every element in the class group is represented by infinitely many ideals.

The exact run time of Step 1 depends on the method we choose and what we are willing to assume, i.e., whether we want a probabilistic/deterministic algorithm and whether we are willing to assume GRH. We refer to [4, Sec. 5.4–5.5] for an overview. It can be done in deterministic polynomial time in  $|\Delta|$ , and the primes  $\mathfrak{p}_i$  can be taken of polynomial size in  $|\Delta|$ . If we are willing to assume GRH, then we may even take  $\mathfrak{p}_i$  to be of size  $O((\log |\Delta|)^2)$ . However, as we possibly have very large exponents in relation (4.1) this does not affect the total run time.

The computation of the exponents  $e_i$  in Step 1 can be done in various ways. The most naïve way of looping over all elements  $I \in \text{Pic}(\mathcal{O}_\Delta)$  and checking whether  $I^{-1}\mathfrak{L}$  is principal using Cornacchia's algorithm already has a run time that is polynomial in  $\log l$  and  $|\Delta|$  and this suffices for the proof of Theorem 1. This computation yields  $\alpha$  as a by product.

Computing the cycle in Step 3 takes time polynomial in the norms of the  $\mathfrak{p}_i$ 's using the method in subsection 3.2. As the norms are of polynomial size in  $|\Delta|$ , this step takes polynomial time in  $|\Delta|$ . The computation of  $\phi_c(P)$  takes polynomial time in  $n \log q$  and  $|\Delta|$ . Steps 4–6 take time polynomial in  $n \log q$  and the theorem follows.  $\square$

## 5 Examples

In this section we give two examples of Algorithm 4.1. The first example is rather small, and we check the result of the computation by employing the method of Section 3 directly. In the second example we use an isogeny of degree roughly  $10^{21}$ , and checking the result using the method from Section 3 is impossible in this case.

### 5.1 Small example

We fix  $q = p = 101$  for this subsection. The elliptic curve  $E : Y^2 = X^3 + 79X + 44$  has  $j$ -invariant  $93 \in \mathbf{F}_p$  and we will show how to evaluate an isogeny of degree  $l = 31$  using the class group algorithm from Section 4. An easy computation shows that  $E$  has trace of Frobenius  $t = 15$ , and as  $\Delta = t^2 - 4p = -179$  is prime, we have  $\text{End}(E) \cong \mathcal{O}_\Delta$ . By fixing a root  $\pi_p$  in  $\mathcal{O}_\Delta$  of the polynomial  $X^2 - tX + p$ , we identify the rings  $\text{End}(E)$  and  $\mathcal{O}_\Delta$ .

We will compute the normalized isogeny  $\varphi$  corresponding to the  $\mathcal{O}_\Delta$ -ideal  $\mathfrak{L} = (31, \pi_p + 3)$  lying over 31. The class group  $\text{Pic}(\mathcal{O}_\Delta)$  is cyclic of order 5. To find a suitable generator, we compute  $\#E(\mathbf{F}_p) = 101 + 1 - 15 = 87 = 3 \cdot 29$ . We see that we cannot use a prime lying over 3 to generate  $\text{Pic}(\mathcal{O}_\Delta)$ , and we choose

$$\text{Pic}(\mathcal{O}_\Delta) = \langle [\mathfrak{p}_5] \rangle$$

with  $\mathfrak{p}_5 = (5, -2\pi_p + 1)$ . We have  $\mathfrak{L} = \mathfrak{p}_5(\alpha)$  with  $\alpha = \frac{-3-\pi_p}{5}$ .

Using the method from Section 3.1, we compute the kernel polynomial  $f_{\mathfrak{p}_5} = X^2 + 59X + 81 \in \mathbf{F}_p[X]$  associated to  $\mathfrak{p}_5$ . By applying Vélú's formulas, we find that the isogenous curve  $E_c = E/E[\mathfrak{p}_5]$  has Weierstraß equation  $Y^2 = X^3 + 30X + 63$ . To find the Weierstraß equation for  $E' = E/E[\mathfrak{L}]$ , we compute  $-3/5 = 60 \in \mathbf{F}_p$  and compute

$$Y^2 = X^3 + 30 \cdot 60^4 X + 63 \cdot 60^6$$

to find the equation  $Y^2 = X^3 + 96X + 75$  for  $E'$ . We let  $\eta : E_c \rightarrow E'$  be an isomorphism.

Take a random point  $P = (68, 53) \in E(\mathbf{F}_p)$ . We apply the isogeny  $\phi_c$  associated to  $\mathfrak{p}_5$  and find  $\phi_c(P) = (30, 17) \in E_c(\mathbf{F}_p)$ . The point  $Q = \eta(\phi_c(P)) = (31, 44) \in E'(\mathbf{F}_p)$  lies on the right curve. As it lies in the base field, the Frobenius acts as the identity on this point and we multiply  $Q$  by  $(-3-1)/5 = 34 \in \mathbf{Z}/87\mathbf{Z}$  to find the image  $R = (46, 25) \in E'(\mathbf{F}_p)$ . The output of the algorithm is  $(Y^2 = X^3 + 96X + 75, 46)$ .

The degree  $l = 31$  is small enough that we can check this output by using the method from Section 3 directly. The kernel polynomial associated to  $\mathfrak{L}$  is  $f_{\mathfrak{L}} = X^{15} + 39X^{14} + 88X^{13} + \dots + 17X^2 + 65X + 4 \in \mathbf{F}_p[X]$  and we compute the image  $\varphi(P) = (46, 25)$  for the isogeny  $\varphi : E \rightarrow E'$  directly from Vélú's formulas.

## 5.2 Medium-sized example

Our algorithm is capable of handling much larger inputs than the  $l = 31$  from section 5.1. Evaluating isogenies of degree roughly  $10^{100}$  is no problem. As displaying large numbers is not especially pleasing to the human eye, we give a ‘medium sized’ example in this section. Using the method from [3], we construct a curve with small endomorphism ring having exactly  $10^{20} + 39 = \text{nextprime}(10^{20})$  points.

With  $p = 9999999980010207001$ , the elliptic curve  $E/\mathbf{F}_p$  defined by

$$Y^2 = X^3 + 93111780581619358815X + 13776438796781696372$$

has  $10^{20} + 39$  points. The endomorphism ring  $\text{End}(E)$  is isomorphic to  $\mathcal{O}_\Delta$  for  $\Delta = -3635$ . The prime  $l = 10^{21} + 117 = \text{nextprime}(10^{21})$  splits in  $\mathcal{O}_\Delta$  and we take the  $\mathcal{O}_\Delta$ -ideal  $\mathfrak{L} = (l, \pi_p + 469155077064851443344)$ . Here,  $\pi_p$  is the image of the Frobenius morphism under the normalized isomorphism  $\text{End}(E) \xrightarrow{\sim} \mathcal{O}_\Delta$ .

The smallest prime not dividing  $[\text{End}(E) : \mathbf{Z}[\pi_p]] = 3^4 \cdot 19^2 \cdot 31^2 \cdot 1999^2$  that splits in  $\mathcal{O}_\Delta$  is 37 and we have  $\text{Pic}(\mathcal{O}_\Delta) \cong \mathbf{Z}/10\mathbf{Z} \cong \langle [\mathfrak{p}_{37}] \rangle$  with  $\mathfrak{p}_{37} = (37, \pi_p + 15)$ . An easy computation yields the equality  $\mathfrak{L} = \mathfrak{p}_{37}(\alpha)$  with

$$\alpha = \frac{-2947049\pi_p - 708893381093724965}{3 \cdot 19 \cdot 31 \cdot 1999 \cdot 37}.$$

The primes in the denominator of  $\alpha$  are 37 and the primes dividing the index  $[\text{End}(E) : \mathbf{Z}[\pi_p]]$ .

We compute the isogeny  $\phi_c$  corresponding to  $\mathfrak{p}_{37}$  using the method from Section 3. The kernel polynomial equals  $X^{18} + 67504589328326227502X^{17} + \dots + 35418368365443750601 \in \mathbf{F}_p[X]$  and the isogenous curve  $E_c$  has Weierstraß equation

$$Y^2 = X^3 + 8082765115516817778X + 51575975418311029503.$$

We multiply the coefficients of this equation by the 4th resp. 6th power of  $-708893381093724965/(3 \cdot 19 \cdot 31 \cdot 1999 \cdot 37) = 98412218672392141083 \in \mathbf{F}_p$  to find the Weierstraß equation

$$Y^2 = X^3 + 83032917062416905069X + 31170711888319926172$$

for  $E'$ . We let  $\eta : E_c \xrightarrow{\sim} E'$  be an isomorphism.

Take a random point  $P = (73931099962253475826, 29177286940991158970)$  on  $E$ . We compute  $Q = \eta(\phi_c(P)) \in E'(\mathbf{F}_p)$  and multiply this by  $(-2947049 - 708893381093724965)/(3 \cdot 19 \cdot 31 \cdot 1999 \cdot 37) = 89908927599601102372 \in \mathbf{Z}/(10^{20} + 39)\mathbf{Z}$  to find

$$R = (95529214469768926304, 49609901207400538475) \in E'(\mathbf{F}_p).$$

The output of the algorithm is the equation for  $E'$  and 95529214469768926304.

## 6 Applications to Pairing-based cryptography

In the last decade, bilinear pairings have been used to enable new cryptographic functionality and have been proposed as the basis for a wide variety of cryptographic protocols, from Identity Based Encryption (IBE) to tri-partite Diffie-Hellman to shorter digital signatures. The first digital signature scheme (BLS) based on bilinear pairings was introduced in 2001 by Boneh, Lynn, and Shacham [1].

### 6.1 BLS digital signatures

Here is an informal description of how the basic BLS signature scheme works on an elliptic curve  $E$  with the Weil pairing.

*Public parameters.* Let  $E$  be an elliptic curve over a field  $\mathbf{F}_q$  of characteristic  $p$ . Let  $m$  be a positive integer and let  $e_m(P, Q)$  denote the Weil pairing of two points  $P$  and  $Q$  in the group of  $m$ -torsion points  $E[m]$ . The Tate pairing or other modified pairings, such as the squared Tate pairing, can also be substituted in the scheme and in its security assumptions. The set-up for the scheme includes a public point  $Q \in E[m]$ . We assume that  $m$  is prime.

*Public/Private Key.* Each user has a secret key which is an integer,  $s$ , and a corresponding public key,  $sQ$ , which is published.

*Signing.* A message,  $M$ , to be transmitted and signed with signature  $\sigma$  is signed as follows. The message is first hashed to a point  $P \in E[m]$ , following for example the procedure outlined in [1, Section 3.2]. The signer has a secret integer  $s$ , and signs the message by computing  $\sigma = sP$ .

*Verifying.* To verify the signature  $\sigma = sP$  on a message  $M$ , the verifier uses the same hashing procedure as above to hash  $M$  to the point  $P$  on the elliptic curve. Then the verifier computes two Weil pairings  $e_m(P, sQ)$  and  $e_m(\sigma, Q)$  and checks that they are equal.

*Note:* For ordinary elliptic curves with  $m$  co-prime to  $p$ , the group  $E[m]$  has rank 2, and the points  $P$  and  $Q$  in the above scheme are chosen to be linearly independent when using the Weil pairing, since otherwise the pairing would be trivial. For efficiency reasons,  $E$  is usually chosen or constructed [9] to be such that all the  $m$ -torsion is defined over a small degree extension of  $\mathbf{F}_q$ , and messages are hashed into the smallest possible field, to minimize the bit-length of the signature.

*Security.* In order for the above scheme to be secure, it is assumed that the groups generated by  $P$  and  $Q$  are a *co-GDH pair* ([1, Definition 2.1]), meaning that the co-Gap Diffie Hellman problem is hard for the two pieces of the  $m$ -torsion. The security proof models the hash function which maps messages to points as a random oracle.

### 6.2 Isogeny variants of BLS

The techniques described in Algorithm 4.1 can be used to enable several different variants of the BLS signature scheme. These variants require expanded security

assumptions and depend on the ability to efficiently evaluate a large degree isogeny (the degree should be of cryptographic size, such as on the order of  $2^{160}$ ). Isogenies of such large degree were previously impossible to evaluate in a reasonable amount of time, other than multiplication by an integer, possibly composed with a small degree isogeny.

**A.** One extension of the basic BLS scheme described above is to use points  $P$  and  $Q$  on two different isogenous elliptic curves.

In other words, let  $E_1/\mathbf{F}_p$  be an ordinary elliptic curve with endomorphism ring  $\text{End}(E) \neq \mathbf{Z}[i], \mathbf{Z}[\zeta_3]$  and let  $\varphi : E_1 \rightarrow E_2$  be specified by an ideal  $\mathfrak{L}$  as in Section 2. The triple  $(E_1, \mathfrak{L}, E_2)$  is public. Assume that the conditions from Theorem 1 are satisfied for the elliptic curve  $E_1$ . This is a rather harmless condition, since for pairing friendly curves, the degree  $l$  of  $\varphi$  does not divide  $[\text{End}(E) : \mathbf{Z}[\pi_p]]$ . For a user with secret key  $s \in \mathbf{Z}$ , the public key is  $sQ \in E_2[m]$ . The message  $M$ , is hashed to a point  $P \in E_1[m]$  and signed as above, with  $\sigma = sP$ , but the verification is accomplished by computing two pairings in  $E_2[m]$  namely  $e_m(\varphi(P), sQ)$  and  $e_m(\varphi(\sigma), Q)$ . As only the  $x$ -coordinate of  $\varphi(P)$  is well-defined, we now accept the signature if  $e_m(\varphi(P), sQ) = \pm e_m(\varphi(\sigma), Q)$  holds.

This scheme requires two evaluations of the isogeny in the verification step. Here the isogeny is public, and need not have large degree. Whereas it was essential to choose  $P$  and  $Q$  to be linearly independent in the original BLS-scheme, we now require  $P$  and  $Q$  to be such that  $\varphi(P)$  and  $Q$  are linearly independent in  $E_2[m]$ . The security depends again on the co-Gap-Diffie-Hellman Assumption, this time for the two groups  $G_1 = \langle P \rangle \subset E_1[m]$  and  $G_2 = \langle Q \rangle \subset E_2[m]$ .

**B.** Our original motivation for developing a polynomial time algorithm for evaluating large degree isogenies was for application to a BLS-variant proposed in [5] where the isogeny is the secret key of the user.

The set-up is as follows. Two ordinary elliptic curves  $E_1$  and  $E_2$  over a field  $\mathbf{F}_p$  with isomorphic endomorphism rings of discriminant  $\Delta < -4$ , and a point  $Q$  in  $E_2[m]$  are public parameters. A user has a secret key, which is an isogeny  $\varphi : E_1 \rightarrow E_2$  specified by an ideal  $\mathfrak{L}$  as in Theorem 1. Let  $\hat{\varphi} : E_2 \rightarrow E_1$  denote the dual isogeny, i.e.,  $\hat{\varphi}$  corresponds to the complex conjugate  $\overline{\mathfrak{L}} \subset \text{End}(E_2) = \mathcal{O}_\Delta$  of  $\mathfrak{L}$ . The corresponding public key is the image  $\hat{\varphi}(Q)$ .

*Signing.* A user signs a message  $M$  by computing the hash of the message onto a point  $P \in E_1[m]$ , and then applying the secret isogeny  $\varphi$  to get the signature  $\sigma = \varphi(P)$ .

*Verification.* The verification step depends on the adjoint property of  $\varphi$  and  $\hat{\varphi}$  with respect to the Weil pairing [12, Ch. 3, Prop. 8.2]. The verifier checks that  $e_m(Q, \sigma) = \pm e_m(\hat{\varphi}(Q), P)$  holds.

This system also requires two applications of an isogeny, one for setting up the user's public key and one for signing. Verification does not require computation of an isogeny. Since the two elliptic curves are public, it is clear that the secret isogeny must have large degree to avoid exhaustive search attacks. We note that

there are *many* isogenies of large degree that fit our theorem, since half of the primes split in the ring  $\text{End}(E)$  and lead to an ideal  $\mathfrak{L}$  that we can use.

**Acknowledgement.** We thank René Schoof for helpful discussions.

## References

- [1] D. Boneh, B. Lynn, H. Shacham: *Short signatures from the Weil pairing*. Advances in Cryptology – Asiacrypt, Springer Lecture Notes in Computer Science **2248**, (2001), 514–532.
- [2] A. Bostan, F. Morain, B. Salvy, E. Schost: *Fast algorithms for computing isogenies between elliptic curves*, Math. Comp. **77**, (2008), 1755–1778.
- [3] R. Bröker, P. Stevenhagen: *Constructing elliptic curves of prime order*, Contemp. Math. **463**, (2008), 17–28.
- [4] H. Cohen: *A course in computational algebraic number theory*, Springer Graduate Texts in Mathematics **138**, (1993).
- [5] D. Jao, R. Venkatesan: *Use of isogenies for design of cryptosystems*, patent online at <http://www.freepatentsonline.com/EP1528705.html>.
- [6] D. Kohel: *Endomorphism Rings of Elliptic Curves over Finite Fields*, PhD thesis, University of California at Berkeley, 1996.
- [7] E. Konstantinou, Y. C. Stamatiou, C. D. Zaroliagis: *On the construction of prime order elliptic curves*, Progress in cryptology—INDOCRYPT 2003, Springer Lecture Notes in Computer Science **2904**, (2003), 309–322
- [8] S. Lang: *Elliptic functions*, 2nd edition Springer Graduate Texts in Mathematics **112**, (1987).
- [9] A. Miyaji, M. Nakabayashi, S. Takano: *New explicit conditions of elliptic curve traces for FR-reduction*, IEICE Trans. on Fund., E84-A **5**, (2001), 1234–1243.
- [10] R. Schoof: *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux **7**, (1995), 219–254.
- [11] J. Silverman: *Advanced topics in the arithmetic of elliptic curves*, Springer Graduate Texts in Mathematics **151** (1994).
- [12] J. Silverman: *The arithmetics of elliptic curves*, 2nd edition, Springer Graduate Texts in Mathematics **106** (1992)
- [13] J. Vélu: *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A–B **273**, (1971), A238–A241.