Pairing the Volcano

Sorina Ionica, Antoine Joux

Pairing the volcano

Sorina Ionica[1] and Antoine Joux[1,2]

[1] Université de Versailles Saint-Quentin-en-Yvelines, 45 avenue des États-Unis, 78035 Versailles CEDEX, France
[2] DGA
sorina.ionica,antoine.joux@m4x.org

Abstract. Isogeny volcanoes are graphs whose vertices are elliptic curves and whose edges are l-isogenies. Algorithms allowing to travel on these graphs were developed by Kohel in his thesis (1996) and later on, by Fouquet and Morain (2001). However, up to now, no method was known, to predict, before taking a step on the volcano, the direction of this step. Consequently, in Kohel's and Fouquet-Morain's algorithms, we always take more steps than necessary, before choosing the right direction. Suppose we know the cardinality of the curve. Given a point P of order l on the elliptic curve, we develop a method to decide whether the subgroup generated by P is the kernel of a horizontal isogeny, a descending or an ascending one. In most cases, our method is very efficient and gives simple algorithms, which are more efficient than previous ones. In the other cases, we show that the two methods should be combined in order to obtain efficient algorithms.

1 Introduction

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, where $q = p^r$ is a prime power. Let π be the Frobenius endomorphism, i.e. $\pi(x, y) \mapsto (x^q, y^q)$ and denote by t its trace. Moreover, we assume that E is an ordinary curve, so its endomorphism ring, which we denote by $\mathcal{O}_E$, is an order in a quadratic imaginary field K ([16, Theorem V.3.1]). Let $d_\pi = t^2 - 4q$ be the discriminant of π. We can write $d_\pi = g^2 d_K$, where d_K is the discriminant of the quadratic field K. So there are only a finite number of possibilities for $\mathcal{O}_E$, since

$$\mathbb{Z}[\pi] \subset \mathcal{O}_E \subset \mathcal{O}_{d_K}.$$

This also means that the conductor of $\mathcal{O}_E$, which we denote by f, divides g, the conductor of $\mathbb{Z}[\pi]$.
The number of points of E over $\mathbb{F}_q$ is given by $\#E(\mathbb{F}_q) = q+1-t$. Two isogenous elliptic curves over $\mathbb{F}_q$ have the same cardinality, and therefore the same trace t. In his thesis [11], Kohel studies how the curves in $\mathrm{Ell}_t(\mathbb{F}_q)$, the set of curves defined over $\mathbb{F}_q$ with trace t, are related via isogenies of degree ℓ. More precisely, he describes the structure of the graph of ℓ-isogenies defined on $\mathrm{Ell}_t(\mathbb{F}_q)$ and also explains how this graph is related to orders in $\mathcal{O}_K$. He uses modular polynomials to find the conductor of $\mathrm{End}(E)$, assuming that g is known.

In [7], Fouquet and Morain call the connected components of this graph *isogeny volcanoes*. They extend Kohel's work, by showing that it is actually

possible to find both g and f (also by using modular polynomials to move from one vertice of the volcano to another one). They also give an algorithm that computes the l-adic valuation of t, for $l|g$. This information can be used in Schoof's algorithm [15]. Recently, new applications to isogeny volcanoes were found: the computation of the Hilbert class polynomial ([1], [18]), that of modular polynomials ([19]) and that of the endomorphism ring of the curve ([20]).

More precisely, the methods enumerated above make use of algorithms that aim at travelling efficiently on the volcano. These algorithms can either walk on the crater, descend from the crater to the floor or, conversely, ascend from the floor to the crater. As explained in [13] and [14], the structure of the ℓ-Sylow subgroup of the elliptic curve may, in many cases, help deciding whether we have taken a step on the crater, or we have descended or ascended. However, no known method can distinguish in advance horizontal isogenies from descending isogenies, or descending isogenies from ascending ones. In this paper, we describe a new method to predict, given a point P of order ℓ, the type of the isogeny whose kernel is generated by P. Our approach, which implies only the computation of a pairing on E, presents several advantages. It allows, in most cases, to compute the conductor of the curve E without taking any steps on the volcano. This is important because computing isogenies of degree ℓ, even for moderately large values of ℓ, is a difficult task, since algorithms for isogeny computation are exponential (except for some particular cases, see [3]). We also show that our algorithms for traveling on the volcano are, in most cases, faster than the ones from [11] and [7].

The remainder of this paper is organised as follows: sections 2 and 3 present definitions and properties of isogeny volcanoes and pairings. Section 4 explains our method to find the type of the isogeny by means of pairing computation. Finally, in section 5, we present new algorithms for finding the level of a curve in a ℓ-volcano, for ascending and for walking on the crater of the volcano.

2 Background on isogeny volcanoes

In this paper we will rely on some results from complex multiplication theory and on the Deuring lifting theorem. We denote by $\mathrm{Ell}_d(\mathbb{C})$ the set of $\mathbb{C}$-isomorphism classes of elliptic curves whose endomorphism ring equals $\mathcal{O}_d$, for some $d < 0$. In this setting there is an action of the class group of the order $\mathcal{O}_d$ on $\mathrm{Ell}_d(\mathbb{C})$. Let $E \in \mathrm{Ell}_d(\mathbb{C})$, Λ its corresponding lattice and $\mathfrak{a}$ an $\mathcal{O}_d$-ideal. We have a natural homomorphism

$$\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda, \quad z \to z,$$

which induces an isogeny that we denote by $E \to \hat{\mathfrak{a}} * E$. The action described in this way is transitive and free (see [17], prop.II.1.2). Moreover, the degree of the application $E \to \hat{\mathfrak{a}} * E$ is $N(\mathfrak{a})$, the norm of the ideal $\mathfrak{a}$ (also [17], cor.II.1.5).

Now from Deuring's theorems (see [5]), if p is a prime number that splits completely, we get a bijection $\mathrm{Ell}_d(\mathbb{C}) \to \mathrm{Ell}_d(\mathbb{F}_q)$, where $q = p^r$. Furthermore, the class group action in characteristic zero respects this bijection, so we get an action of the class group also on $\mathrm{Ell}_d(\mathbb{F}_q)$.

2.1 Isogeny volcanoes and modular polynomials

Consider E an elliptic curve defined over a finite field $\mathbb{F}_q$. Let ℓ be a prime different from $\mathrm{char}(\mathbb{F}_q)$ and $I : E \to E'$ be a ℓ-isogeny, i.e. a isogeny of degree ℓ. As shown in [11], this means that $\mathcal{O}_E$ contains $\mathcal{O}_{E'}$ or $\mathcal{O}_{E'}$ contains $\mathcal{O}_E$ or the two endomorphism rings coincide. If $\mathcal{O}_E$ contains $\mathcal{O}_{E'}$, we say that I is a *descending* isogeny. Otherwise, if $\mathcal{O}_E$ is contained in $\mathcal{O}_{E'}$, we say that I is a *ascending* isogeny. If $\mathcal{O}_E$ and $\mathcal{O}_{E'}$ are equal, then we call the isogeny *horizontal*. In his thesis, Kohel shows that horizontal isogenies exist only if the conductor of $\mathcal{O}_E$ is not divisible by l. Moreover, in this case there are exactly $\left(\frac{d}{\ell}\right) + 1$ horizontal isogenies of degree ℓ. If $\left(\frac{d}{\ell}\right) = 1$, then ℓ is split in $\mathcal{O}_E$ and the two horizontal isogenies correspond to the action of the two ideals $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ via the action described at the beginning of this section. In a similar way, if $\left(\frac{d}{\ell}\right) = 0$, then ℓ is ramified in $\mathcal{O}_E$ there is one horizontal isogeny starting from E and this isogeny corresponds to the only prime ideal of norm ℓ in $\mathcal{O}_E$. In order to describe the structure of the graph whose vertices are curves with a fixed number of points and whose edges are ℓ-isogenies, we introduce the following definition (taken from [18]):

Definition 1. *An ℓ-volcano is a connected undirected graph with vertices partioned into levels $V_0, \ldots, V_h$, in which a subgraph on V_0 (the crater) is a regular connected graph of degree at most 2 and:*
(a) For $i > 0$, each vertex in V_i has exactly one edge leading to a vertex in V_{i-1}, and every edge not on the crater is of this form.
(b) For $i < h$, each vertex in V_i has degree $\ell + 1$.

We call the level V_h *the floor* of the volcano. Vertices lying on the floor have degree 1. Let $\mathrm{Ell}_t(\mathbb{F}_q)$ be the set of elliptic curves defined over $\mathbb{F}_q$ with trace t. The following proposition, formulated in [18] follows essentially from Proposition 23 in [11].

Proposition 1. *Let p be a prime number, $q = p^r$, and $d_\pi = t^2 - 4q$. Take $\ell \neq p$ another prime number. Let G be the undirected graph with vertex set $Ell_t(\mathbb{F}_q)$ and edges ℓ-isogenies defined over $\mathbb{F}_q$. We denote by ℓ^h the largest power of ℓ dividing the conductor of d_π. Then the connected components of G are ℓ-volcanoes of height h and for each component V:*
(a) The elliptic curve whose j-invariants lie in V_0 have endomorphism rings isomorphic to some $\mathcal{O}_{d_0} \supseteq \mathcal{O}_{d_\pi}$ whose conductor is not divisible by l.
(b) The elliptic curve whose j-invariants lie in V_i have endomorphism rings isomorphic to $\mathcal{O}_{d_i}$, where $d_i = l^{2i} d_0$.

Elliptic curves are determined by their j-invariant, up to a twist (the reader should refer to [16] for a definition of the twist of an elliptic curve). In the remainder of this paper, we refer to a vertex in a volcano either by naming the curve or its j-invariant.

Given a curve E, two methods are known to construct curves which are ℓ-isogenous to E and therefore to travel on the volcano. One relies on modular polynomials and the other on Vélu's formulae. We give below a brief survey of the two methods.

Modular polynomials The ℓth *modular polynomial*, usually denoted by $\Phi_\ell(X,Y)$ is a polynomial with integer coefficients, which satisfies the following property: given two elliptic curves E and E', there is a ℓ-isogeny defined over $\mathbb{F}_q$, if and only if, $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ and $\Phi_\ell(j(E), j(E')) = 0$, where $j(E)$ and $j(E')$ are the j-invariants of curves E and E'. So in order to find the curves related to E via a ℓ-isogeny, we need to solve the equation $\Phi_\ell(X, j(E)) = 0$. As stated in [15], this polynomial may have 1, 2 or $\ell+1$ roots in $\mathbb{F}_q$. So in order to find an edge on the volcano, it suffices to find a root j' of this polynomial. Note that the j-invariant determines the curve up to a twist. The formula for finding the equation of the curve $E' \in \mathrm{Ell}_t(\mathbb{F}_q)$ from $j(E')$ is also given in [15].

The group structure of the elliptic curve on the volcano Lenstra [10] relates the structure of the curve to the endomorphism ring by proving that:

$$E(\mathbb{F}_q) \simeq \mathcal{O}_E/(\pi - 1) \tag{1}$$

as $\mathcal{O}_E$-modules. It is thus natural to see how this structure relates to the isogeny volcano. From (1), we can deduce that $E(\mathbb{F}_q) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, where $n = \gcd(a-1, g/f)$, with

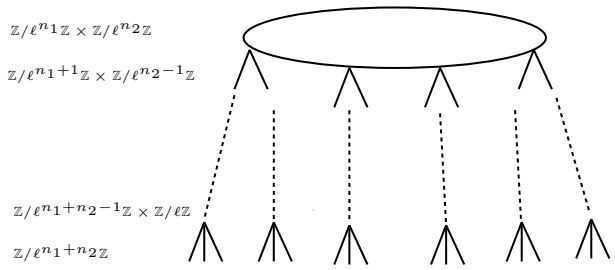
$$a = \begin{cases} (t-g)/2 \text{ if } d_K \equiv 1 \pmod 4, \\ t/2 \qquad \text{if } d_K \equiv 2,3 \pmod 4, \end{cases}$$

where d_K is the discriminant of the quadratic imaginary field containing $\mathcal{O}_E$. Moreover, $n|m$, $n|(q-1)$ and $mn = \#E(\mathbb{F}_q)$. This means that on a ℓ-volcano the structure of all the curves in a given level is the same.
Let E be a curve on the isogeny volcano such that $v_\ell(n) < v_\ell(m)$. As explained in [13] (in the case $\ell = 2$, but the result holds in the general case), we have the following inequality:

$$v_\ell(a-1) \geq \min\{v_\ell(g), v_\ell(\#E(\mathbb{F}_q))/2\}$$

As $n = \gcd(a-1, g/f)$ and $n \leq v_\ell(\#E(\mathbb{F}_q))/2$, it follows that $n = v_\ell(g/f)$. As we descend, the valuation at ℓ of the conductor f increases by 1 at each level (by proposition 1b). This implies that the ℓ-valuation of n for curves at each level decreases by 1 and is equal to 0 for curves lying on the floor. Note that if $v_\ell(\#E(\mathbb{F}_q))$ is even and the height of the volcano is greater than $v_\ell(\#E(\mathbb{F}_q))$, the structure of the ℓ-torsion group is unaltered from the crater down to the level $v_\ell(\#E(\mathbb{F}_q))/2$. From this level down, the structure of the ℓ-torsion groups starts changing as explained above. In the sequel we call this level the *stability level*. The volcanoes whose ℓ-torsion is different at each level are called *regular* volcanoes (see Figure 1). Their stability level is on the crater. This terminology is taken from [13]. Apart from modular polynomials, the problem of finding a ℓ-isogeny defined on E has another solution. Given P a point of order ℓ on E, the ℓ-isogeny $I : E \to E'$ whose kernel G is generated by P can be found by using Vélu's formulae (see [21])). If we want to use this approach, we are interested in explicitly computing the coordinates of points of order ℓ on E. We denote by G_i, $1 \leq i \leq \ell+1$, the $\ell+1$ subgroups of order ℓ of E. In [13] Miret and

Fig. 1. A regular volcano



al. give the degree r_i of the smallest extension field of $\mathbb{F}_q$ such that $G_i \subset \mathbb{F}_{q^{r_i}}$, $1 \leq i \leq \ell+1$. This degree is related to the order of q in the group $\mathbb{F}_\ell^*$, that we denote by $\mathrm{ord}_\ell(q)$. Notice that in the special case of $\ell = 2$, this degree is always 1.

Proposition 2. *Let E defined over $\mathbb{F}_q$ be an elliptic curve with k rational ℓ-isogenies, $\ell > 2$, and let G_i, $1 \leq i \leq k$, be their kernels, and let r_i be the minimum value for which $G_i \subset E(\mathbb{F}_{q^{r_i}})$.*

(a) If $k = 1$ then $r_1 = ord_\ell(q)$ or $r_1 = 2ord_\ell(q)$.
(b) If $k = \ell + 1$ then either $r_i = ord_\ell(q)$ for all i, or $r_i = 2ord_\ell(q)$ for all i.
(c) If $k = 2$ then $r_i | \ell - 1$, $i = 1, 2$.

The following corollary [13] will also be useful in the remainder of this paper.

Corollary 1. *Let $E/\mathbb{F}_q$ be an elliptic curve over $\mathbb{F}_q$. If $E/\mathbb{F}_q$ has 1 or $\ell+1$ rational ℓ-isogenies, then $\#E(\mathbb{F}_q^{ord_l q})$ or $\#\tilde{E}(\mathbb{F}_q^{ord_\ell q})$ is a multiple of ℓ. Moreover, if $E/\mathbb{F}_q^{ord_\ell q}$ has $\ell+1$ rational isogenies, then it is also a multiple of ℓ^2.*

Notations. Let $n \geq 0$. In the sequel, we denote by $E[\ell^n]$ the subgroup of points of order ℓ^n on the curve E, by $E[\ell^n](K)$ the subgroup of points of order n defined over K and by $E[\ell^\infty](K)$ the subgroup of points defined over K whose orders are powers of ℓ.

Given a point $P \in E[\ell^n](\mathbb{F}_q)$, we also need to know the degree of the extension field in which there is a ℓ^{n+1}-torsion point such that $\ell\tilde{P} = P$. The following result is taken from [6].

Proposition 3. *Let $E/\mathbb{F}_q$ be an elliptic curve which lies on a ℓ-volcano whose height $h(V)$ is different from 0. Then the height of V', the ℓ-volcano of the curve $E/\mathbb{F}_{q^s}$ is*

$$h(V') = h(V) + v_\ell(s)$$

From this proposition, it follows easily that if the structure of ℓ-torsion on the curve $E/\mathbb{F}_q$ is $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, then the smallest extension in which the structure of the ℓ-torsion changes is $\mathbb{F}_{q^\ell}$. Indeed, it suffices to see that the structure of the ℓ-volcano containing E modifies only over $\mathbb{F}_{q^\ell}$. Moreover, if we consider a curve E' lying on the floor of $V/\mathbb{F}_q$, this means this curve has one point of order ℓ defined over $\mathbb{F}_q$ and $\ell+1$ isogenies defined over $\mathbb{F}_{q^\ell}$. We conclude that E' has all the $\ell+1$ subgroups of order ℓ defined over $\mathbb{F}_q$, which means that (by ascending on the volcano) the structure of the ℓ-torsion of E over $\mathbb{F}_{q^\ell}$ is necessarily

$$E[\ell^\infty](\mathbb{F}_{q^\ell}) \sim \mathbb{Z}/\ell^{n_1+1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2+1}\mathbb{Z}.$$

This observation will be very useful in the sequel.

3 Background on pairings

Let E be an elliptic curve defined over some finite field $\mathbb{F}_q$, m a number coprime to q, such that $m|\#E(\mathbb{F}_q)$ and assume $m|(q-1)$. Let $P \in E[m](\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_q)/mE(\mathbb{F}_q)$. Let $f_{m,P}$ be the function whose divisor is $m(P)-m(O)$, where O is the point at infinity of the curve E (for background on divisors see [16]). Take R a random point in $E(\mathbb{F}_q)$ such as the support of the divisor $D = (Q+R)-(R)$ is disjoint from the support of $f_{m,P}$. Then we can define the Tate pairing as follows:

$$\begin{aligned} t_m : E[m] \times E(\mathbb{F}_q)/mE(\mathbb{F}_q) &\to \mathbb{F}_q^*/(\mathbb{F}_q^*)^m \\ (P,Q) &\to f_{m,P}(Q+R)/f_{m,P}(R) \end{aligned}$$

The Tate pairing is a bilinear non-degenerate application, i.e. for all $P \in E[m](\mathbb{F}_q)$ different from O there is a $Q \in E(\mathbb{F}_q)/mE(\mathbb{F}_q)$ such that $T_m(P,Q) \neq 1$. So the output of the pairing is only defined up to a coset of $(\mathbb{F}_{q^k}^*)^n$. However, for cryptographic use, we generally need a unique value and we define the *reduced* Tate pairing:

$$T_m(P,Q) = t_m(P,Q)^{(q-1)/m} \in \mu_m,$$

where by μ_m we denote the group of mth roots of unity. Pairing computation can be done in time $O(\log m)$ using Miller's algorithm [12]. For more details on pairings, the reader should refer to [8].
Suppose now that $m = \ell^n$, with $n \geq 1$ and ℓ prime. Now let P and Q be two linearly independant ℓ^n-torsion points on E. Then all ℓ^n-torsion points R can be expressed as $R = aP + bQ$. We define the following symmetric pairing [9]:

$$S(P,Q) = (T_{\ell^n}(P,Q)T_{\ell^n}(Q,P))^{\frac{1}{2}}. \tag{2}$$

Note that for any point P, $T_{\ell^n}(P,P) = S(P,P)$. In the remainder of this paper, we call $S(P,P)$ *the self pairing* of P. Any ℓ^n-torsion points R can be expressed as $R = aP + bQ$. By bilinearity and symmetry of the S-pairing we get:

$$\log(S(R,R)) = a^2\log(S(P,P)) + 2ab\,\log(S(P,Q)) + b^2\log(S(Q,Q)).$$

where log is a discrete logarithm function in μ_{l^n}. We denote by k the largest integer such that the polynomial

$$P(a,b) = a^2\log(S(P,P)) + 2ab\,\log(S(P,Q)) + b^2\log(S(Q,Q)) \tag{3}$$

is nonzero modulo ℓ^{k+1} and zero modulo ℓ^k. Obviously, $0 \leq k \leq n$. Dividing by ℓ^k, we may thus regard P as a polynomial in $\mathbb{F}_\ell[a,b]$. Therefore it has at most two roots, which means that that from all the $\ell+1$ subgroups of order ℓ^n, at most 2 have self pairings in μ_{ℓ^k} (see also [9]). In the remainder of this paper, we denote by N_{E,ℓ^n} the number of zeros of any polynomial like the one at (3). Note that this number does not depend on the choice of the two generators P and Q of the ℓ^n-torsion subgroup $E[\ell^n]$. We also denote by P_{E,ℓ^n} any quadratic polynomial as the one in equation (3). Moreover, we say that a ℓ^n-torsion point R has *degenerated self-pairing* if $T_{\ell^n}(R,R)$ is a primitive ℓ^k-th root of unity and that R has *non-degenerated self-pairing* otherwise. Also, if $T_{\ell^n}(R,R)$ is a primitive ℓ^n-th root of unity, we say that R has *primitive non-degenerated self pairing*.

4 Preliminary results. Determining directions on the volcano

In this section we explain how we can distinguish between different directions on the volcano by making use of pairings. We start by some lemmas, meant to explain the relations between pairings on two curves, whenever there exists an isogeny between the two curves.

Lemma 1. *Suppose $E/\mathbb{F}_q$ is an elliptic curve and P,Q are points in $E(\mathbb{F}_q)$ of order ℓ^n, $n \geq 1$. Suppose there are $\tilde{P},\tilde{Q} \in E[\bar{\mathbb{F}}_q]$ such that $\ell\tilde{P} = P$ and $\ell\tilde{Q} = Q$. Then we have the following relation for the Tate pairing:*
(a) If $\tilde{P},\tilde{Q} \in E[\mathbb{F}_q]$, then

$$T_{\ell^{n+1}}(\tilde{P},\tilde{Q})^{\ell^2} = T_{\ell^n}(P,Q).$$

(b) Suppose $\ell \geq 3$. If $\tilde{Q} \in E[\mathbb{F}_{q^\ell}]\backslash E[\mathbb{F}_q]$, then

$$T_{\ell^{n+1}}(\tilde{P},\tilde{Q})^{\ell} = T_{\ell^n}(P,Q).$$

Proof 1. By writing down the divisors of the functions $f_{\ell^{n+1},\tilde{P}}$, $f_{\ell^n,\tilde{P}}$, $f_{\ell^n,P}$, one can easily check that

$$f_{\ell^{n+1},\tilde{P}} = (f_{\ell,\tilde{P}})^{\ell^n} \cdot f_{\ell^n,P}.$$

We evaluate these fonctions at some points $Q+R$ and R (where R is carefully chosen) and raise the equality to the power $(q-1)/\ell^n$.
2. Due to the equality on divisors $\mathrm{div}(f_{\ell^{n+1},P}) = \mathrm{div}(f^\ell_{\ell^n,P})$, we have

$$T_{\ell^{n+1}}(\tilde{P},\tilde{Q})^l = T^{(\mathbb{F}_{q^\ell})}_{\ell^n}(P,\tilde{Q}),$$

where $T^{(\mathbb{F}_{q^\ell})}_{\ell^n}$ is the ℓ^n-Tate pairing for E defined over $\mathbb{F}_{q^\ell}$. It suffices then to show that

$$T_{\ell^n}^{(\mathbb{F}_{q^\ell})}(P,\tilde{Q}) = T_{\ell^n}(P,Q).$$

We have

$$\begin{aligned} T_{\ell^n}^{(\mathbb{F}_{q^\ell})}(P,\tilde{Q}) &= f_{\ell^n,P}([\tilde{Q}+R]-[R])^{\frac{(1+q+\cdots+q^{\ell-1})(q-1)}{\ell^n}} \\ &= f_{\ell^n,P}((\tilde{Q}+R)+(\pi(\tilde{Q})+R)+(\pi^2(\tilde{Q})+R)+\ldots \\ &+ (\pi^{\ell-1}(\tilde{Q})+R)-\ell(R))^{\frac{(q-1)}{\ell^n}} \end{aligned} \quad (4)$$

where R is a random point defined over $\mathbb{F}_q$. It is now easy to see that for $\ell \geq 3$,

$$\tilde{Q}+\pi(\tilde{Q})+\pi^2(\tilde{Q})+\ldots+\pi^{\ell-1}(\tilde{Q}) = \ell\tilde{Q} = Q,$$

because $\pi(\tilde{Q}) = \tilde{Q}+T$, where T is a point of order l. By applying Weil's reciprocity law ([16, Ex. II.2.11]), it follows that the equation (4) becomes:

$$T_{\ell^n}^{(\mathbb{F}_{q^\ell})}(P,\tilde{Q}) = \left(\frac{f_{\ell^n,P}(Q+R)}{f_{\ell^n,P}(R)}\right)^{\frac{q-1}{\ell^n}} f((P)-(O))^{q-1},$$

where f is such that $\mathrm{div}(f) = (\tilde{Q}+R)+(\pi(\tilde{Q})+R)+(\pi^2(\tilde{Q})+R)+...+(\pi^{\ell-1}(\tilde{Q})+R)-(Q+R)-(\ell-1)(R)$. Note that this divisor is $\mathbb{F}_q$-rational, so $f((P)-(O))^{q-1}=1$. This concludes the proof. □

.

Lemma 2. *(a) Let $\phi : E \to E'$ be a separable isogeny of degree d defined over $\mathbb{F}_q$, P a ℓ-torsion on the curve E such that $\phi(P)$ is a ℓ-torsion point on E', and Q a point on E. Then we have*

$$T_\ell(\phi(P),\phi(Q)) = T_\ell(P,Q)^d.$$

(b) Let $\phi : E \to E'$ be a separable isogeny of degree ℓ defined over $\mathbb{F}_q$, P a $\ell\ell'$-torsion point such that $Ker\ \phi =< \ell' P >$ and Q a point on the curve E. Then we have

$$T_\ell(\phi(P),\phi(Q)) = T_{\ell\ell'}(P,Q)^\ell.$$

Proof.

(a) We have

$$\begin{aligned} (\phi)^*(f_{\ell,\phi(P)}) &= \ell \sum_{K\in \mathrm{Ker}\phi}(P+K) - \ell \sum_{K\in\mathrm{Ker}\phi}(K) \\ &= \ell \sum_{K\in\mathrm{Ker}\phi}((P+K)-(K)) = \ell \sum_{K\in\mathrm{Ker}\phi}((P)-(O)) + \mathrm{div}\left(\left(\prod_{K\in\mathrm{Ker}\phi}\frac{l_{K,P}}{v_{K+P}}\right)^\ell\right), \end{aligned}$$

where $l_{K,P}$ is the straight line passing through K and P and v_{K+P} is the vertical line passing through $K+P$.
It follows that

$$f_{\ell,\phi(P)} \circ \phi(Q) = f_{\ell,P}^d(Q) \left(\prod_{K \in \mathrm{Ker}\phi} \frac{l_{K,P}(Q)}{v_{K+P}(Q)} \right)^\ell$$

So we obtain the desired formula by evaluating the equality above at two points carefully chosen $Q+R$ and R, and then by raising to the power $\frac{q-1}{\ell}$.

(b) The proof is similar to the one at point (a). □

Remark 1. Actually the statement at (a) stands for all isogenies, as shown in Theorem IX.9.4 of [2]. We kept our proof because a similar technique can be applied to prove (b).

Proposition 4. *Let E be an elliptic curve defined a finite field $\mathbb{F}_q$ and assume that $E[\ell^\infty](\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$ (with $n_1 \geq n_2$). Suppose that there is a ℓ^{n_2}-torsion point P such that $T_{\ell^{n_2}}(P,P)$ is a primitive ℓ^{n_2}th root of unity. Then the ℓ-isogeny whose kernel is generated by $\ell^{n_2-1}P$ is descending. Moreover, the curve E does not lie above the stability level of the corresponding ℓ-volcano.*

Proof. Consider $I_1 : E \to E_1$ the isogeny whose kernel is generated by $\ell^{n_2-1}P$ and suppose this isogeny is ascending or horizontal. This means that $E_1[\ell^{n_2}]$ is defined over $\mathbb{F}_q$. Take Q another ℓ^{n_2}-torsion point on E, such that $E[\ell^{n_2}] =< P, Q >$ and denote by $Q_1 = I_1(Q)$. One can easily check that the dual of I_1 has kernel generated by $\ell^{n_2-1}Q_1$. It follows that there is a point $P_1 \in E_1[\ell^{n_2}]$ such that $P = \hat{I}_1(P_1)$. By Lemma 2 this means that $T_\ell(P,P) \in \mu_{\ell^{n_2-1}}$, which is false. This proves not only that the isogeny is descending, but also that the structure of the ℓ-torsion is different at the level of E_1, so E cannot be above the stability level. □

Proposition 5. *Let $\ell \geq 3$ a prime number and suppose that $E/\mathbb{F}_q$ is a curve which lies in a ℓ-volcano and on the stability level. Suppose $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/l^{n_2}\mathbb{Z}$, $n_1 \geq n_2$. Then there is at least one l^{n_2}-torsion point on $R \in E(\mathbb{F}_q)$ whose pairing $T_{l^{n_2}}(R,R)$ is a primitive l^{n_2}-th root of unity.*

Proof. Let P be a ℓ^{n_1}-torsion point and Q be a ℓ^{n_2}-torsion point such that $\{P, Q\}$ generates $E[\ell^\infty](\mathbb{F}_q)$.

Case 1. Suppose $n_1 \geq n_2 \geq 2$. Let $E \xrightarrow{I_1} E_1$ be a descending ℓ-isogeny and denote by P_1 and Q_1 the ℓ^{n_1+1} and ℓ^{n_2-1}-torsion points generating $E_1[\ell^\infty](\mathbb{F}_p)$. Moreover, without loss of generality, we may assume that $I_1(P) = \ell P_1$ and $I_1(Q) = Q_1$. If $T_{\ell^{n_2-1}}(Q_1, Q_1)$ is a primitive ℓ^{n_2-1}-th root of unity, $T_{\ell^{n_2}}(Q,Q)$ is a primitive ℓ^{n_2}-th root of unity by Lemme 2. If not, from the non-degeneration of the pairing, we deduce that $T_{\ell^{n_2-1}}(Q_1, P_1)$ is a primitive ℓ^{n_2-1}-th root of unity, which means that $T_{\ell^{n_2-1}}(Q_1, \ell P_1)$ is a ℓ^{n_2-2}-th primitive root of unity. By applying Lemme 2, we get $T_{\ell^{n_2}}(Q,P) \in \mu_{\ell^{n_2-1}}$ at best. It follows that $T_{\ell^{n_2}}(Q,Q) \in \mu_{\ell^{n_2}}$ by the non-degeneracy of the pairing.

Case 2. If $n_2 = 1$, then consider the volcano defined over the extension field $\mathbb{F}_{q^\ell}$. There is a ℓ^2-torsion point $\tilde{Q} \in E(\mathbb{F}_{q^\ell})$ with $Q = \ell\tilde{Q}$. We obviously have $\ell^2 | q^\ell - 1$

and from Lemma 1, we get $T_{\ell^2}(\tilde{P},\tilde{P})^\ell = T_\ell(P,P)$. By applying Case 1, we get that $T_{\ell^2}(\tilde{P},\tilde{P})$ is a primitive ℓ^2-th root of unity, so $T_\ell(P,P)$ is a primitive ℓ-th root of unity.

We will now make use of a result concerning the representation of ideal classes of orders in imaginary quadratic fields:

Lemma 3. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Given a nonzero integer M, then every ideal class in $Cl(\mathcal{O})$ contains a proper $\mathcal{O}$-ideal whose norm is relatively prime to M.*

Proof. See [4], Corollary 7.17.

Proposition 6. *We use the notations and assumptions from Proposition 1. Furthermore, we assume that for all curves E_i lying at a fixed level i in V the curve structure is $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, with $n_1 \geq n_2$. The value of $N_{E_i,\ell^{n_2}}$, the number of zeros of the polynomial defined at 3, is constant for all curves lying at level i in the volcano.*

Proof. Let E_1 and E_2 be two curves lying at level i in the volcano V. Then by Proposition 1 they both have endomorphism ring isomorphic to some order $\mathcal{O}_{d_i}$. Now by taking into account the fact that the action of $\mathrm{Cl}(\mathcal{O}_{d_i})$ on $\mathrm{Ell}_{d_i}(\mathbb{F}_q)$ is transitive, we consider an isogeny $\phi : E_1 \to E_2$ of degree ℓ_1. By applying Lemma 3, we may assume that $(\ell_1, \ell) = 1$. Take now P and Q two independant ℓ^{n_2}-torsion points on E_1 and denote by $P_{E_1,\ell^{n_2}}$ the quadratic polynomial corresponding to the ℓ^{n_2}-torsion on E_1:

$$P_{E_1,\ell^{n_2}}(a,b) = a^2 \log(S(P,P)) + 2ab \log(S(P,Q)) + b^2 log(S(Q,Q)).$$

We use Lemma 2 to compute $S(\phi(P),\phi(P))$, $S(\phi(P),\phi(Q))$ and $S(\phi(Q),\phi(Q))$ and deduce easily that there is a polynomial $P_{E_2,\ell^{n_2}}(a,b)$ on the curve E_2 such that

$$P_{E_1,\ell^{n_2}}(a,b) = P_{E_2,\ell^{n_2}}(a,b)$$

This means that $N_{E_1,\ell^{n_2}}$ and $N_{E_2,\ell^{n_2}}$ coincide, which concludes the proof.□

Moreover, we have showed that the value of k for two curves lying on the same level of a volcano is the same.

Proposition 7. *Let E be an elliptic curve defined a finite field $\mathbb{F}_q$ and let $E[\ell^\infty](\mathbb{F}_q)$ be isomorphic to $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$ with $\ell \geq 3$ and $n_1 \geq n_2 \geq 1$. Suppose $N_{E,\ell^{n_2}} \in \{1,2\}$ and let P be a ℓ^{n_2}-torsion point with degenerated self pairing. Then the ℓ-isogeny whose kernel is generated by $\ell^{n_2-1}P$ is either ascending or horizontal. Moreover, for any ℓ^{n_2}-torsion point Q whose self-pairing is non-degenerated, the isogeny with kernel spanned by $< \ell^{n_2-1}Q >$ is descending.*

Proof. Case 1. Suppose $T_{\ell^{n_2}}(P,P) \in \mu_{\ell^k}$, $k \geq 1$ and that $T_{\ell^{n_2}}(Q,Q) \in \mu_{\ell^{k+1}} \backslash \mu_{\ell^k}$. Denote by $I_1 : E \to E_1$ the isogeny whose kernel is generated by $\ell^{n_2-1}P$ and $I_2 : E \to E_2$ the isogeny whose kernel is generated by $\ell^{n_2-1}Q$. By

repeatedly applying Lemmas 1 and 2, we get the following relations for points generating the ℓ^{n_2-1}-torsion on E_1 and E_2:

$$T_{\ell^{n_2-1}}(I_1(P), I_1(P)) \in \mu_{\ell^{k-1}},\ T_{\ell^{n_2-1}}(\ell I_1(Q), \ell I_1(Q)) \in \mu_{\ell^{k-2}} \backslash \mu_{\ell^{k-3}}$$
$$T_{\ell^{n_2-1}}(\ell I_2(P), \ell I_2(P)) \in \mu_{\ell^{k-3}},\ T_{\ell^{n_2-1}}(I_2(Q), I_2(Q)) \in \mu_{\ell^{k}} \backslash \mu_{\ell^{k-1}}$$

with the convention that $\mu_{\ell^h} = \emptyset$ whenever $h \leq 0$. From the relations above, we deduce that on the ℓ-volcano having E, E_1 and E_2 as vertices, E_1 and E_2 do not lie at the same level. Given the fact that there are at least $l-1$ descending rational ℓ-isogenies parting from E and that Q is any of the $\ell - 1$ (or more) ℓ^{n_2}-torsion points with non-degenerated self-pairing, we conclude that I_1 is horizontal or ascending and that I_2 is descending.
Case 2. Suppose now that $k = 0$. Note that the case $n_2 = 1$ was already treated in proposition 4. Otherwise, consider the curve E defined over $\mathbb{F}_{q^\ell}$. By lemma 1 we have $k = 1$ for points on $E/\mathbb{F}_{q^\ell}$, so we may apply Case 1. □

Note 1. All statements in the proof of *Case* 1 are true for $\ell = 2$ also. The statement in Proposition 4 is also true for $\ell = 2$. The only case that is not clear is what happens when $k = 0$ and $n_2 \geq 1$. We did not find a proof for the statement in proposition 5 for $\ell = 2$, but in our computations with MAGMA we did not find any counterexamples either.

Example 1. Let E be the elliptic curve whose Weierstrass equation is given by $y^2 = x^3 + 521631762x + 248125891$ defined over $\mathbb{F}_{1992187501}$. The 5^5-torsion is entirely defined over $\mathbb{F}_{1992187501}$. We take $P = (749718987, 838497160)$ a 5^5-torsion point with degenerated self-pairing, because $T_{5^5}(P, P) \in \mu_{5^4}$. The corresponding isogeny $I_1 : E \to E_1$ is a horizontal one. Consider now a point of order 5^5 with non-degenerated self-pairing, for example $Q = (139364112, 1455554413)$. One may easily check that $T_{5^5}(Q, Q) \in \mu_{5^5} \backslash \mu_{5^4}$ and that $I_2 : E \to E_2$ (whose kernel is generated by $5^4 Q$ is descending.

Consider now a curve E defined over $\mathbb{F}_q$ such that

$$E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$$

We conclude this section by presenting two algorithms which find a ℓ-torsion point on E generating the kernel of a descending isogeny and of an ascending (horizontal) one, respectively. We assume $\ell \geq 3$, even though in many cases these methods work also for $\ell = 2$.

Algorithm 1 Finding the kernel of a descending isogeny Input: A curve E, the structure of $E[\ell^\infty](\mathbb{F}_q)$.
Output: A ℓ-torsion point generating the kernel of a descending isogeny.

1. If $n_2 = 0$ exit.
2. Take a random P_1 of order ℓ^{n_2}. If $T_{\ell^{n_2}}(P_1, P_1)$ is a primitive ℓ^{n_2}th root of unity, return $\ell^{n_2-1} P_1$.

3. Take a random P_2 of order ℓ^{n_2}. If $W_{\ell_{n_2}}(P_1, P_2) \in \mu_{\ell^{n_2-1}}$[3] , take another random point P_2. If $T_{\ell^{n_2}}(P_2, P_2)$ is a primitive ℓ^{n_2}th root of unity, return $\ell^{n_2-1}P_2$.
4. Compute $P_{E,\ell^{n_2}}$. If $P_{E,\ell^{n_2}} \neq 0$ and both P_1 and P_2 have degenerated pairings, take $P_1 + P_2$. Else consider E over $\mathbb{F}_{q^\ell}$ and return to step 2.

Algorithm 2 Finding the kernel of a ascending (horizontal) isogeny
Input: A curve E, the structure of $E[\ell^\infty](\mathbb{F}_q)$.
Output: A ℓ-torsion point generating the kernel of a ascending isogeny.

1. If $n_2 = 0$ then take a random point P_1 of ℓ^{n_1} torsion and return $\ell^{n_1-1}P_1$.
2. Else compute $P_{E,\ell^{n_2}}$. If $P_{E,\ell^{n_2}} \neq 0$, compute its roots and find a point P with self-degenerated pairing. Return $\ell^{n_2-1}P$. Else consider E over $\mathbb{F}_{q^\ell}$ and return to step 2.

Note that proposition 5 guarantees that these algorithms terminate, because the existence of nondegenerated primitive self pairings on the stability level implies (by applying lemma 1 if necessary) that for any curve E lying on upper levels, there is an extension of $\mathbb{F}_{q^e}$ and points in $E[\ell^\infty](\mathbb{F}_{q^e})$ with nondegenerated self pairings.

5 Walking the volcano: some new algorithms

In his thesis [11], Kohel gave a deterministic algorithm to compute the conductor of the endomorphism ring of an ordinary curve E, assuming the trace t of the curve is known. His idea is to determine the ℓ-adic valuation of the conductor by determining the level of the vertex E in the ℓ-volcano.

Recently, new applications using efficient algorithms to travel along the volcano were given: the computation of the Hilbert class polynomial [1], [18], that of modular polynomials [19] and that of the endomorphism ring of the curve [20]. All these algorithms use modular polynomials or Vélu's formulae [21] to move from one elliptic curve to another curve on the volcano. In this section, we briefly describe existing algorithms used to compute the level of a curve on a volcano, to ascend one level on the volcano and to walk a path along the crater. These algorithms actually rely on methods given by Kohel [11] and by Fouquet and Morain in [7]).

We then present our new algorithms, which use the methods in Algorithms 1 and 2 to predict the direction of isogenies. We estimate the number of visited vertices during the execution of each algorithm and prove that in most cases our method is more efficient.

Before going into the details of the algorithms, we compare the costs of taking one step on a volcano by using the two methods existing in the literature: modular polynomials and Vélu's formulae. Suppose we have walked a path

[3] The Weil pairing W_m(see [16] for the definition) has the property that $W_m(P, P) = 1$ for all points of order m, so we can test wheather two points are independant by testing wheather their pairing is a primitive mth root of unity.

$E_1, ..., E_{i-1}$ on the volcano and we would like to take a new step (E_{i-1}, E_i). In the modular polynomial approach, we have to factor the polynomial $f(X) = \Phi_\ell(X, j(E_{i-1}))/(X - j(E_{i-2}))$. The cost of the step is then of

$$O(\ell^2 + M(\ell)\log q)$$

operations in $\mathbb{F}_q$, where $M(\ell) = \ell\log\ell\log\log\ell$. In this formula, the first term is the time to evaluate $\Phi_\ell(X, j(E_{i-1})$ and the second term is the time to compute $X^q \bmod f$. Now computing the isogeny with Vélu's formulae can be done in $O(\ell)$ operations, if we consider the time to compute ℓ-torsion points negligeable. However, in many cases, even though the ℓ-isogeny is defined over $\mathbb{F}_q$, the points of order ℓ are defined in an extension field of degree smaller than ℓ (see corollary 1). As a consequence, we need

$$O(\ell^2 \log \ell)$$

operations in $\mathbb{F}_q$ in order to compute the isogeny with Vélu's formulae. So using Vélu formulae is slightly more expensive. However, it becomes more efficient with our technique since we can determine the direction of the isogeny in advance.

Moreover, in our algorithms, we need to perform a small number of pairing computations, which cost $O(\log \ell)$, if we use Miller's algorithm **??**. Once these computations performed, the calculation of the polynomial $P_{E,\ell^{n_2}}$ costs $O(\log \ell)$ in time. The most expensive part of this computation is the computation of logs in the finite field $\mathbb{F}_\ell$. This can be done by precomputing all the logs, storing them in a ordered table (which costs $O(\ell)$ in memory), and then performing a dichotomic search every time we need to compute a log. This search costs $O(\log \ell)$ in time.

Suppose that we wish to compute the level of a curve in a volcano of height d. If $\deg(E) \neq \ell + 1$, then we are already on the floor and the level is d. Otherwise we start walking two paths, that we extend as far as possible, but never beyond length d. If E is on the surface, then both paths have length d. Otherwise at least one of them is a descending path of length k_2 and E is on the level $d - k_2$. The time complexity for this algorithm is $O(2d(\ell^2 + M(\ell)\log q))$. The pseudocode for this algorithm, given by Kohel [11], is given in [18].
There is a second approach to this problem given by Fouquet and Morain in [7]. The idea is to start walking three paths in parallel and extend them as far as possible. As at least one of them is descending, we stop when one path reaches the floor for the first time and return the length of this path. The complexity is $O(3d(\ell^2 + M(\ell)\log q))$. This algorithm is 50 percent slower, but it has the advantage of working for volcanoes whose height is not necessarily known.

Our new algorithm, based on the method presented in Algorithm 1 for finding the kernel of a descending isogeny, is very simple. We only need to apply Vélu's formulae in order to compute the descending isogeny. If the points of order ℓ are not defined over $\mathbb{F}_q$, but over an extension field $\mathbb{F}_{q^d}$, the cost of our algorithm is $O(\ell(\log \ell)^2 + \ell^2 \log \ell)$, where the first term comes from the computation of a small number of pairings and the second one is the complexity of the isogeny computation using Vélu's formulae. Of course, we have assumed that we our volcano is regular, so the polynomial $P_{E,\ell^{n_2}}$ is not zero over $\mathbb{F}_{q^d}$.

Suppose now we want to ascend one level in the volcano. If we are on the floor (i.e $\deg(E) \neq \ell+1$ or $n_2 = 0$), we take the curve given by the only rational ℓ-isogeny. Otherwise, we start walking descending paths for each of the $\ell + 1$ curves isogenous to E. We then compare the lengths of all paths and the longest one is the one given by the neighbor of E lying one level above. The running time of the algorithm is $O(\ell d(\ell^2 + M(\ell)\log q))$. The pseudocode for this algorithm can be found in [18].

Our new algorithm for finding a curve on the upper level in a volcano uses Algorithm 2 in order to find the kernel of the ascending isogeny and then computes the isogeny with Vélu's formulae. On regular volcanoes, the complexity of this algorithm is $O(\ell(\log \ell)^3 + \ell^2 \log \ell + 1)$, where the first term is the cost of 4 pairing computation and their logs, the second one is the cost of the isogeny computation and the last one comes from the factorization of a polynomial of degree 2.

In [18], Sutherland also makes use of an algorithm which, given a curve E on the crater of a volcano of height d, computes a path of length n on the crater starting at E. When $d = 0$, the algorithm necessarily returns a path contained in V_0. Otherwise, we construct a path of length $d+1$ and retain in the list of vertices on the crater the vertex E' obtained at the first step in our path. We continue the process, this time replacing E with E', until we get n curves on the crater. See [18] for a detailed description of the algorithm. According to [18, Proposition 4], the number of examined vertices is $O(\ell dn)$, so the running time of the algorithm is $O(\ell dn(\ell^2 + M(\ell)\log q))$. Our new algorithm for walking n steps on the crater calls Algorithm 2 in order to find the kernel of the horizontal isogeny starting from E and uses Vélu's formulae to take a step on the crater. This process is repeated until n steps on the crater have been taken. The complexity of our algorithm on a regular volcano is $O(n\ell(\log \ell)^3 + n\ell^2 \log \ell + n)$.

Assume that, for a fixed q, the traces of elliptic curves are uniformly distributed in Hasse's interval. Then the probability of picking a curve whose volcano is not regular, among curves lying on volcanoes of height greater than 0, is of approximatively $\frac{1}{\ell^2}$. This is not negligeable for small values of ℓ, and in these cases we believe both methods should be combined to achieve best performances. This means that on such a volcano, one should use the strategies given by Kohel and Fouquet and Morain for curves lying above the stability level and use our methods when the curves are on the stability level or underneath it.

Finally, in some applications, it might be possible, to restrict ourselves to regular volcanoes. The use of Vélu's formulae also has the advantage of avoiding the expensive precomputations of the modular polynomials or of the Hilbert polynomial. In the case of algorithms computing modular polynomials, for example, we do not need the precomputation of the Hilbert polynomial as in [19]. Moreover, our method of enumerating curves on the crater of the volcano is faster than the one using the action of the class group in [19].

6 Conclusion and perspectives

In this paper, we have proposed a method which allows, in the regular part of an isogeny volcano, to determine, given a curve E and a ℓ-torsion point P, the

type of the ℓ-isogeny whose kernel is spanned by P. In addition, this method also permits, given a basis for the ℓ-torsion, to find the ascending isogeny (or horizontal isogenies) from E. We expect that this method can be used to improve the performance of several volcano-based algorithms, such as the computation of the Hilbert's [18] or modular [19] polynomials.

7 Acknowledgments

The authors thank Jean Marc Couveignes for the idea in the proof of Lemma 1. The first author is grateful to Ariane Mézard for many discussions on number theory and isogeny volcanoes, prior to this work.

References

1. J. Belding, R. Broker, A. Enge, and K. Lauter. Computing hilbert Class Polynomials. In A.J. van der Poorten and A. Stein, editors, *Algorithmic Number Theory Symposium-ANTS VIII*, volume 5011 of *Lecture Notes in Computer Science*, pages 282–295. Springer Verlag, 2008.
2. I.F. Blake, G. Seroussi, and N.P. Smart. *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 2005.
3. R. Broker, D. Charles, and K. Lauter. Evaluating large degree isogenies and applications to pairing based cryptography. In *Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 282–295. Springer, 2008.
4. D. A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. John Wiley & Sons, Inc, 1989.
5. M. Deuring. *Die Typen der Multiplikatorenringe elliptischer Funktionenkorper*. Abh. Math. Sem. Hansischen Univ. 14, 1941.
6. M. Fouquet. *Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques*. Ph.D. thesis. 2001.
7. M. Fouquet and F. Morain. Isogeny Volcanoes and the SEA Algorithm. In *ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 276–291. Springer, 2002.
8. G. Frey. Applications of arithmetical geometry to cryptographic constructions. In *Proceedings of the Fifth International Conference on Finite Fields and Applications*, pages 128–161. Springer, 2001.
9. A. Joux and K. Nguyen. Separating Decision DiffieâĂŞHellman from Computational DiffieâĂŞHellman in Cryptographic Groups. *Journal of Cryptology*, 16(4):239–247, 2003.
10. H.W. Lenstra Jr. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, 56(2):227–241, 1996.
11. D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. Ph.D. thesis, University of California Berkeley. 1996.
12. V. Miller. The weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, 2004.
13. J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. *Applied Mathematics and Computation*, 196(1):67–76, 2008.

14. J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. Computing the height of volcanoes of l-isogenies of elliptic curves over finite fields. *Applied Mathematics and Computation*, 196(1):67–76, 2008.
15. R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Theorie des Nombres de Bordeaux*, 7:219–254, 1995.
16. J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.
17. J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994.
18. A. Sutherland. Computing Hilbert Class Polynomials with the Chinese Remainder Theorem. http://arxiv.org/abs/0903.2785, 2009.
19. A. Sutherland. Computing Modular Polynomials with the Chinese Remainder Theorem. http://www-math.mit.edu/ drew/, 2009.
20. A. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. http://eprint.iacr.org/2009/100, 2009.
21. J. Vélu. Isogenies entre courbes elliptiques. *Comptes Rendus De L Academie Des Sciences Paris, Serie I-Mathematique, Serie A.*, 273:238–241, 1971.