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. Hence, in Kohel's and Fouquet-Morain algorithms, we take many steps before choosing the right direction. In particular, ascending or horizontal isogenies are usually found using a trial-and-error approach. In this paper, we propose an alternative method that efficiently finds all points P of order ℓ such that the subgroup generated by P is the kernel of an horizontal or an ascending isogeny. In many cases, our method is faster than previous methods.

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. Assume that E is an ordinary curve and let $\mathcal{O}_E$ denotes its ring of endomorphisms. We know [21, Th. V.3.1] that $\mathcal{O}_E$ is an order in an imaginary quadratic field K. 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. There are only a finite number of possibilities for $\mathcal{O}_E$, since $\mathbb{Z}[\pi] \subset \mathcal{O}_E \subset \mathcal{O}_{d_K}$. Indeed, this requires that f the conductor of $\mathcal{O}_E$ divides g the conductor of $\mathbb{Z}[\pi]$.

The cardinality of E over $\mathbb{F}_q$ is $\#E(\mathbb{F}_q) = q + 1 - t$. Two isogenous elliptic curves over $\mathbb{F}_q$ have the same cardinality, and thus the same trace t. In his thesis [14], Kohel studies how 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 $\mathrm{Ell}_t(\mathbb{F}_q)$. He relates this graph to orders in $\mathcal{O}_K$ and uses modular polynomials to find the conductor of $\mathrm{End}(E)$.

Fouquet and Morain [8] call the connected components of this graph *isogeny volcanoes* and extend Kohel's work. In particular, they give an algorithm that computes the ℓ-adic valuation of the trace t, for $\ell | g$. This can be used in Schoof's algorithm [20]. Recently, more applications of isogeny volcanoes were found: the computation of Hilbert class polynomials [1,23], of modular polynomials [4] and of endomorphism rings of elliptic curves [2].

G. Hanrot, F. Morain, and E. Thomé (Eds.): ANTS-IX 2010, LNCS 6197, pp. 201–218, 2010.

All the above methods make use of algorithms for traveling efficiently on volcanoes. These algorithms either need to walk on the crater, to descend from the crater to the floor or to ascend from the floor to the crater. In many cases, the structure of the ℓ-Sylow subgroup of the elliptic curve, allows, after taking a step on the volcano, to decide whether this step is ascending, descending or horizontal (see [16,17]). Note that, since a large fraction of isogenies are descending, finding one of them is much easier. However, no known method can find horizontal or ascending isogenies without using a trial-and-error approach. In this paper, we describe a first solution to this open problem, which applies when the cardinality of the curve is known, and propose a method that efficiently finds a point P of order ℓ that spans the kernel of an ascending (or horizontal isogeny). Our approach relies on the computation of a few pairings on E. We then show that our algorithms for traveling on the volcano are, in many cases, faster than the ones from [14] and [8]. Moreover, we obtain a simple method that detects most curves on the crater of their volcano. Until now, the only curves that were easily identified were those on the floor of volcanoes.

This paper is organized as follows: sections 2 and 3 present definitions and properties of isogeny volcanoes and pairings. Section 4 explains our method to find ascending or horizontal isogenies using pairing computations. Finally, in Section 5, we use this method to improve the algorithms for ascending a volcano and for walking on its crater.

2 Background on Isogeny Volcanoes

In this paper, we rely on some results from complex multiplication theory and on Deuring's lifting theorems. We denote by $\mathcal{Ell}_d(\mathbb{C})$ the set of $\mathbb{C}$-isomorphism classes of elliptic curves whose endomorphism ring is the order $\mathcal{O}_d$, with discriminant $d < 0$. In this setting there is an action of the class group of $\mathcal{O}_d$ on $\mathcal{Ell}_d(\mathbb{C})$. Let $E \in \mathcal{Ell}_d(\mathbb{C})$, Λ its corresponding lattice and $\mathfrak{a}$ an $\mathcal{O}_d$-ideal. We have a canonical homomorphism from $\mathbb{C}/\Lambda$ to $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ which induces an isogeny usually denoted by $E \to \hat{\mathfrak{a}} * E$. This action on $\mathcal{Ell}_d(\mathbb{C})$ is transitive and free [22, Prop. II.1.2]. Moreover [22, Cor. II.1.5], the degree of the application $E \to \hat{\mathfrak{a}} * E$ is $N(\mathfrak{a})$, the norm of the ideal $\mathfrak{a}$. Now from Deuring's theorems [6], if p is a prime number that splits completely, we get a bijection $\mathcal{Ell}_d(\mathbb{C}) \to \mathcal{Ell}_d(\mathbb{F}_q)$, where $q = p^r$. Furthermore, the class group action in characteristic zero respects this bijection, and we get an action of the class group also on $\mathcal{Ell}_d(\mathbb{F}_q)$.

Isogeny volcanoes. 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 an ℓ-isogeny, i.e. an isogeny of degree ℓ. As shown in [14], 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 ℓ-isogenies, where d is the discriminant of $\mathcal{O}_E$. If $\left(\frac{d}{\ell}\right)=1$, then ℓ is split in $\mathcal{O}_E$ and the two horizontal isogenies correspond to the two actions $E \to \hat{\mathfrak{l}} * E$ and $E \to \hat{\bar{\mathfrak{l}}} * E$, where the two ideals $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ satisfy $(\ell)=\mathfrak{l}\bar{\mathfrak{l}}$. In a similar way, if $\left(\frac{d}{\ell}\right)=0$, then ℓ is ramified, i.e. $(\ell)=\mathfrak{l}^2$ and there is exactly one horizontal isogeny starting from 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 recall the following definition [23].

Definition 1. *An ℓ-volcano is a connected undirected graph with vertices partitioned 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. The following proposition [23] follows essentially from [14, Prop. 23].

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 that do not contain curves with j-invariant 0 or 1728 are ℓ-volcanoes of height h and for each component V, we have :*

(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 $d_i = \ell^{2i} d_0$.

Elliptic curves are determined by their j-invariant, up to a twist[1]. Throughout the paper, we refer to a vertex in a volcano by giving the curve or its j-invariant.

Exploring the volcano. Given a curve E on an ℓ-volcano, two methods are known to find its neighbours. The first method relies on the use of modular polynomials. The ℓ-th *modular polynomial*, denoted by $\Phi_\ell(X, Y)$ is a polynomial with integer coefficients. It satisfies the following property: given two elliptic curves E and E' with j-invariants $j(E)$ and $j(E')$ in $\mathbb{F}_q$, there is an ℓ-isogeny defined over $\mathbb{F}_q$, if and only if, $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ and $\Phi_\ell(j(E), j(E')) = 0$. As a consequence, the curves related to E via an ℓ-isogeny can be found by solving $\Phi_\ell(X, j(E)) = 0$. As stated in [20], this polynomial[2] may have 0, 1, 2 or $\ell + 1$ roots in $\mathbb{F}_q$. In order to find an edge on the volcano, it suffices to find a root j' of this polynomial. Finally, if we need the equation of the curve E' with j-invariant j', we may use the formula in [20].

The second method to build ℓ-isogenous curves constructs, given a point P of order ℓ on E, the ℓ-isogeny $I : E \to E'$ whose kernel G is generated by P using

[1] For a definition of twists of elliptic curves, refer to [21].
[2] The case where the modular polynomial does not have any root corresponds to a degenerate case of isogeny volcanoes containing a single curve and no ℓ-isogenies.

Vélu's classical formulae [24] in an extension field $\mathbb{F}_{q^r}$. To use this approach, we need the explicit 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 [17], Miret and 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 $\mathrm{ord}_\ell(q)$.

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 $r_i | \ell - 1$ for $i = 1, 2$.

We also need the following corollary [17].

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

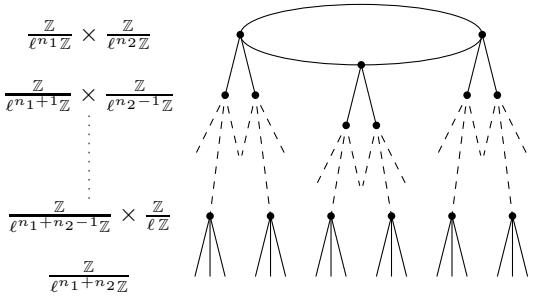

Fig. 1. A regular volcano

The group structure of the elliptic curve on the volcano. Lenstra [13] relates the group structure of an elliptic curve to its endomorphism ring by proving that $E(\mathbb{F}_q) \simeq \mathcal{O}_E/(\pi - 1)$ as $\mathcal{O}_E$-modules. It is thus natural to see how this structure relates to the isogeny volcano. From Lenstra's equation, we can deduce that $E(\mathbb{F}_q) \simeq \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. We write $\pi = a + g\omega$, with:

$$a = \begin{cases} (t-g)/2 \\ t/2 \end{cases} \text{ and } \omega = \begin{cases} \frac{1+\sqrt{d_K}}{2} & \text{if } d_K \equiv 1 \pmod 4 \\ \sqrt{d_K} & \text{if } d_K \equiv 2, 3 \pmod 4 \end{cases}$$

where d_K is the discriminant of the quadratic imaginary field containing $\mathcal{O}_E$. Note that N is maximal such that $E[N] \subset E(\mathbb{F}_q)$ and by [19, Lemma 1] we get that $N = \gcd(a-1, g/f)$. Note moreover that $N|M$, $N|(q-1)$ and $MN = \#E(\mathbb{F}_q)$. This implies 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 [16] (in the case $\ell = 2$, but the result is general), a is such that $v_\ell(a-1) \geq \min\{v_\ell(g), v_\ell(\#E(\mathbb{F}_q))/2\}$.

Since $N = \gcd(a-1, g/f)$ and $v_\ell(N) \leq v_\ell(\#E(\mathbb{F}_q))/2$, it follows that $v_\ell(N) = v_\ell(g/f)$. 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 h 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 $h - v_\ell(\#E(\mathbb{F}_q))/2$. From this level down, the structure of the ℓ-torsion groups starts changing as explained above. In the sequel, we call this level the *first stability level.*[3] A volcano with first stability level equal to 0, i.e. on the crater, is called *regular.*

Notations. Let $n \geq 0$. We denote by $E[\ell^n]$ the ℓ^n-torsion subgroup, i.e. the subgroup of points of order ℓ^n on the curve $E(\overline{\mathbb{F}}_q)$, by $E[\ell^n](\mathbb{F}_{q^k})$ the subgroup of points of order ℓ^n defined over an extension field of $\mathbb{F}_q$ and by $E[\ell^\infty](\mathbb{F}_q)$ the ℓ-Sylow subgroup of $E(\mathbb{F}_q)$.

Given a point $P \in E[\ell^n](\mathbb{F}_q)$, we also need to know the degree of the smallest extension field containing an ℓ^{n+1}-torsion point such that $\ell\tilde{P} = P$. The following result is taken from [7].

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 $\mathbb{F}_{q^\ell}$. We sketch here the proof in the case $n_1 = n_2 = n$, which is the only case in which we consider volcanoes over extension fields in this paper[4]. First of all, note that E lies on a ℓ-volcano $V/\mathbb{F}_q$ of height at least n. We consider a curve E' lying on the floor of $V/\mathbb{F}_q$ such that there is a descending path of isogenies between E and E'. Obviously, we have $E'[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{2n}\mathbb{Z}$. By proposition 3, $V/\mathbb{F}_{q^\ell}$ has one extra down level, which means that the curve E' is no longer on the floor, but on the level just above the floor. Consequently, we have that $E'[\ell] \subset E'(\mathbb{F}_{q^\ell})$ and, moreover, $E'[\ell^\infty](\mathbb{F}_{q^\ell}) \simeq \mathbb{Z}/\ell^{2n+\Delta}\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. By ascending on the volcano from E' to E, we deduce that the structure of the ℓ-torsion of E over $\mathbb{F}_{q^\ell}$ is necessarily

$$E[\ell^\infty](\mathbb{F}_{q^\ell}) \simeq \mathbb{Z}/\ell^{n+\Delta}\mathbb{Z} \times \mathbb{Z}/\ell^{n+1}\mathbb{Z}.$$

Moreover, $\Delta \geq 1$, because if it were 0, the height of $V/\mathbb{F}_{q^\ell}$ would be n.

[3] Miret et al. call it simply *the stability level.*

[4] For the proof in the general case, see [11].

3 Background on Pairings

Let E be an elliptic curve defined over some finite field $\mathbb{F}_q$, m a number such that $m | \gcd(\#E(\mathbb{F}_q), q-1)$. 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[5] is $m(P) - m(O)$, where O is the point at infinity of the curve E. 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 $T_m(P,Q) \neq 1$. The output of the pairing is only defined up to a coset of $(\mathbb{F}_q^*)^m$. However, for implementation purposes, it is useful to have a uniquely defined value and to use the *reduced* Tate pairing, i.e. $T_m(P,Q) = t_m(P,Q)^{(q-1)/m} \in \mu_m$, where μ_m denotes the group of m-th roots of unity. Pairing computation can be done in time $O(\log m)$ using Miller's algorithm [15]. For more details and properties of pairings, the reader can refer to [9]. Note that in the recent years, in view of cryptographic applications, many implementation techniques have been developed and pairings on elliptic curves can be computed very efficiently[6].

Suppose now that $m = \ell^n$, with $n \geq 1$ and ℓ prime. Now let P and Q be two ℓ^n-torsion points on E. We define the following symmetric pairing [12]

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

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. We focus on the case where the pairing S is non-constant. Suppose now that P and Q are two linearly independent ℓ^n-torsion points. Then all ℓ^n-torsion points R can be expressed as $R = aP + bQ$. Using bilinearity and symmetry of the S-pairing, we get

$$\log(S(R,R)) = a^2 \log(S(P,P)) + 2ab \log(S(P,Q)) + b^2 \log(S(Q,Q)) \pmod{\ell^n},$$

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

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

is identically zero modulo ℓ^k and nonzero modulo ℓ^{k+1}. Obviously, since S is non-constant we have $0 \leq k < n$. Dividing by ℓ^k, we may thus view $\mathcal{P}$ as a polynomial in $\mathbb{F}_\ell[a,b]$. When we want to emphasize the choice of E and ℓ^n, we write $\mathcal{P}_{E,\ell^n}$ instead of $\mathcal{P}$.

[5] For background on divisors, see [21].

[6] See [10] for a fast recent implementation.

Since $\mathcal{P}$ is a non-zero quadratic polynomial, it has at most two homogeneous roots, which means that that from all the $\ell+1$ subgroups of $E[\ell^n]/E[\ell^{n-1}] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$, at most 2 have self-pairings in μ_{ℓ^k} (see also [12]). In the remainder of this paper, we denote by N_{E,ℓ^n} the number of zeros of $\mathcal{P}_{E,\ell^n}$. Note that this number does not depend on the choice of the two generators P and Q of the ℓ^n-torsion subgroup $E[\ell^n]$. Moreover, we say that a ℓ^n-torsion point R has *degenerate self-pairing* if $T_{\ell^n}(R,R)$ is a ℓ^k-th root of unity and that R has *non-degenerate self-pairing* if $T_{\ell^n}(R,R)$ is a primitive ℓ^{k+1}-th root of unity. Also, if $T_{\ell^n}(R,R)$ is a primitive ℓ^n-th root of unity, we say that R has *primitive self-pairing.*

4 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 give some lemmas explaining the relations between pairings on two isogenous 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, $n \geq 1$. Denote by $\tilde{P},\tilde{Q} \in E[\bar{\mathbb{F}}_q]$ the points such that $\ell\tilde{P} = P$ and $\ell\tilde{Q} = Q$. We have the following relations 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. a. 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 functions at some points $Q+R$ and R (where R is carefully chosen) and raise the equality to the power $(q-1)/\ell^n$.
b. Due to the equality on divisors $\mathrm{div}(f_{\ell^{n+1},P}) = \mathrm{div}(f^{\ell}_{\ell^n,P})$, we have

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

where $T_{\ell^n}^{(\mathbb{F}_{q^\ell})}$ 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

$$\begin{aligned} T_{\ell^n}^{(\mathbb{F}_{q^\ell})}(P,\tilde{Q}) &= f_{\ell^n,P}([\tilde{Q}+R]-[R])^{\frac{(1+q+\cdots+q^{\ell-1})(q-1)}{\ell^n}} \\ &= f_{\ell^n,P}((\tilde{Q}+R)+(\pi(\tilde{Q})+R)+(\pi^2(\tilde{Q})+R)+\ldots \\ &\quad +(\pi^{\ell-1}(\tilde{Q})+R)-\ell(R))^{\frac{(q-1)}{\ell^n}} \end{aligned} \tag{3}$$

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 [21, Ex. II.2.11], it follows that the equation (3) 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 $Ker\,\phi = \langle \ell' P \rangle$ and Q a point on the curve E. Then we have $T_\ell(\phi(P), \phi(Q)) = T_{\ell\ell'}(P,Q)^\ell$.

Proof. Proof omitted for lack of space. See [3, Th. IX.9.4] for (a), [11] for (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 first stability level of the corresponding ℓ-volcano.*

Proof. Let $I_1 : E \to E_1$ be 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 $E[\ell^{n_2}] = \langle P, Q \rangle$ 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. Hence 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 first stability level. Suppose $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, $n_1 \geq n_2$. Then there is at least one ℓ^{n_2}-torsion point $R \in E(\mathbb{F}_q)$ with primitive self-pairing.*

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 Lemma 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 Lemma 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.

Two stability levels. Remember that in any irregular volcano, $v_\ell(\#E(\mathbb{F}_q))$ is even and the height h of the volcano is greater than $v_\ell(\#E(\mathbb{F}_q))$. Moreover, all curves at the top of the volcano have $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_2}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$ with $n_2 = v_\ell(\#E(\mathbb{F}_q))$. The existence of a primitive self-pairing of a ℓ^{n_2}-torsion point on any curve lying on the first stability level implies that the polynomial $\mathcal{P}$ is non-zero at every level from the first stability level up to the level $\max(h+1-2n_2, 0)$ (by Lemma 2). We call this level *the second level of stability*. On the second stability level there is at least one point of order ℓ^{n_2} with pairing equal to a primitive ℓ-th root of unity. At every level above the second stability level all polynomials $\mathcal{P}_{E,\ell^{n_2}}$ may be zero[7]. Consider now E a curve on the second stability level and $I : E \to E_1$ an ascending isogeny. Let P be a ℓ^{n_2}-torsion point on E and assume that $T_{\ell^{n_2}}(P, P) \in \mu_\ell^*$. We denote by $\tilde{P} \in E(\mathbb{F}_{q^\ell}) \backslash E(\mathbb{F}_q)$ the point such that $\ell\tilde{P} = P$. By Lemma 1 we get $T_{\ell^{n_2+1}}(\tilde{P}, \tilde{P})$ is a primitive ℓ^2-th root of unity. It follows by Lemma 2 that $T_{\ell^{n_2}}(I(P), I(P))$ is a primitive ℓ-th root of unity. We deduce that $\mathcal{P}_{E_1,\ell^{n_2+1}}$ corresponding to $E_1/\mathbb{F}_{q^\ell}$ is non-zero. Applying this reasoning repeatedly, we conclude that for every curve E above the second stability level there is an extension field $\mathbb{F}_{q^{s\ell}}$ such that the polynomial $\mathcal{P}_{E,\ell^{n_2+s}}$ associated to the curve defined over $\mathbb{F}_{q^{s\ell}}$ is non-zero. When the second stability level of a volcano is 0, we say that the volcano is *almost regular*.

We now make use of a result on the representation of ideal classes of orders in imaginary quadratic fields. This is Corollary 7.17 from [5].

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.*

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 2, 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 $\mathcal{O}_{d_i}$.

[7] In all the examples we considered for this case, $\mathcal{P}$ is always 0.

Now by taking into account the fact that the action of $\mathrm{Cl}(\mathcal{O}_{d_i})$ on $\mathcal{Ell}_{d_i}(\mathbb{F}_q)$ 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 independent ℓ^{n_2}-torsion points on E_1 and denote by $\mathcal{P}_{E_1,\ell^{n_2}}$ the quadratic polynomial corresponding to the ℓ^{n_2}-torsion on E_1 as in (2). We use Lemma 2 to compute $S(\phi(P), \phi(P))$, $S(\phi(P), \phi(Q))$ and $S(\phi(Q), \phi(Q))$ and deduce that a polynomial $\mathcal{P}_{E_2,\ell^{n_2}}(a, b)$ on the curve E_2 computed from $\phi(P)$ and $\phi(Q)$ is such that

$$\mathcal{P}_{E_1,\ell^{n_2}}(a, b) = \mathcal{P}_{E_2,\ell^{n_2}}(a, b).$$

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 degenerate 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-degenerate, 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 $\ell - 1$ 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-degenerate 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 $E/\mathbb{F}_{q^\ell}$, and we may apply Case 1.

A special case. If E is a curve lying under the first stability level and that $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, with $n_1 > n_2$, then it suffices to find a point P_1 of order ℓ^{n_1} and the point $\ell^{n_1-1}P_1$ generates the kernel of an horizontal or ascending isogeny (P_1 has degenerate self-pairing).

Crater detection. Assume that $\mathcal{P} \neq 0$. When ℓ is split in $\mathcal{O}_E$, there are two horizontal isogenies from E and this is equivalent, by propositions 6 and 7, to $N_{E,\ell^{n_2}} = 2$. Similarly, when ℓ is inert in $\mathcal{O}_E$, there are neither ascending nor

horizontal isogenies and $N_{E,\ell^{n_2}} = 0$. In these two cases, we easily detect that the curve E is on the crater.

Note. 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.

We conclude this section by presenting an algorithm which determines the group structure of the ℓ^∞-torsion group of a curve E and also an algorithm which outputs the kernel of an horizontal (ascending) isogeny from E, when $E[\ell^\infty](\mathbb{F}_q)$ is given.

Algorithm 1. Computing the structure of the ℓ^∞-torsion of E over $\mathbb{F}_q$ (assuming volcano height ≥ 1)

Require: A curve E defined over $\mathbb{F}_q$, a prime ℓ
Compute: Structure $\mathbb{Z}/\ell^{n_1}\mathbb{Z} \times \mathbb{Z}/\ell^{n_2}\mathbb{Z}$, generators P_1 and P_2
1: Check that $q \equiv 1 \pmod{\ell}$ (if not need to move to extension field: **abort**)
2: Let t be the trace of $E(\mathbb{F}_q)$
3: Check $q + 1 - t \equiv 0 \pmod{\ell}$ (if not consider twist or **abort**)
4: Let $d_\pi = t^2 - 4q$, let z be the largest integer such that $\ell^z | d_\pi$ and $h = \lfloor \frac{z}{2} \rfloor$
5: Let n be the largest integer such that $\ell^n | q + 1 - t$ and $N = \frac{q+1-t}{\ell^n}$
6: Take a random point R_1 on $E(\mathbb{F}_q)$, let $P_1 = N \cdot R_1$
7: Let n_1 be the smallest integer such that $\ell^{n_1} P_1 = 0$
8: **if** $n_1 = n$ **then**
9: **Output:** Structure is $\frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$, generator P_1. **Exit**
(E is on the floor, ascending isogeny with kernel $\langle \ell^{n-1} P_1 \rangle$)
10: **end if**
11: Take a random point R_2 on $E(\mathbb{F}_q)$, let $P_2 = N \cdot R_2$ and $n_2 = n - n_1$
12: Let $\alpha = \log_{\ell^{n_2} P_1}(\ell^{n_2} P_2) \pmod{\ell^{n_1 - n_2}}$
13: **if** α is undefined **then**
14: **Goto** 6 ($\ell^{n_2} P_2$ does not belong to $\langle \ell^{n_2} P_1 \rangle$)
15: **end if**
16: Let $P_2 = P_2 - \alpha P_1$
17: **If** $\text{WeilPairing}_\ell(\ell^{n_1 - 1} P_1, \ell^{n_2 - 1} P_2) = 1$ **goto** 6 (This checks linear independence)
18: **Output:** Structure is $\frac{\mathbb{Z}}{\ell^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{n_2}\mathbb{Z}}$, generators (P_1, P_2)

We assume that the height of the volcano is $h \leq 2n_2 + 1$, or, equivalently, that the curve E lies on or below the second stability level, which implies that the polynomial $\mathcal{P}$ is non-zero at every level in the volcano. This allows us to distinguish between different directions of ℓ-isogenies parting from E. Of course, similar algorithms can be given for curves lying above the second stability level, but in this case we are compelled to consider the volcano over an extension field $\mathbb{F}_{q^{s\ell}}$. Since computing points defined over extension fields of degree greater than ℓ is expensive, our complexity analysis in section 5 will show that it is more efficient to use Kohel's and Fouquet-Morain algorithms to explore the volcano until the second level of stability is reached and to use algorithms 1 and 2

Algorithm 2. Finding the kernel of ascending or horizontal isogenies (Assuming curve not on floor and below the second stability level)

Require: A curve E, its structure $\frac{\mathbb{Z}}{\ell^{n_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^{n_2}\mathbb{Z}}$ and generators (P_1, P_2)
if $n_1 > n_2$ **then**
  The isogeny with kernel $\langle \ell^{n_1-1} P_1 \rangle$ is ascending or horizontal
  To check whether there is another, continue the algorithm
end if
Let g be a primitive ℓ-th root of unity in $\mathbb{F}_q$
Let $Q_1 = \ell^{n_1-n_2} P_1$
Let $a = T_{\ell^{n_2}}(Q_1, Q_1)$, $b = T_{\ell^{n_2}}(Q_1, P_2) \cdot T_{\ell^{n_2}}(P_2, Q_1)$ and $c = T_{\ell^{n_2}}(P_2, P_2)$
If $(a, b, c) = (1, 1, 1)$ **abort** (Above the second stability level)
repeat
  Let $a' = a$, $b' = b$ and $c' = c$
  Let $a = a^\ell$, $b = b^\ell$ and $c = c^\ell$
until $a = 1$ and $b = 1$ and $c = 1$
Let $L_a = \log_g(a')$, $L_b = \log_g(b')$ and $L_c = \log_g(c') \pmod{\ell}$
Let $\mathcal{P}(x, y) = L_a x^2 + L_b xy + L_c y^2 \pmod{\ell}$
If $\mathcal{P}$ has no roots modulo ℓ, **Output:** No isogeny (a single point on the crater)
If single root (x_1, x_2) **Output:** One isogeny with kernel $\langle \ell^{n_2-1}(x_1 Q_1 + x_2 P_2) \rangle$
if $\mathcal{P}$ has two roots (x_1, x_2) and (y_1, y_2) **then**
  Two isogenies with kernel $\langle \ell^{n_2-1}(x_1 Q_1 + x_2 P_2) \rangle$ and $\langle \ell^{n_2-1}(y_1 Q_1 + y_2 P_2) \rangle$
end if

afterwards. We assume $\ell \geq 3$, even though in many cases these methods work also for $\ell = 2$.

5 Walking the Volcano: Modified Algorithms

As mentioned in the introduction, several applications of isogeny volcanoes have recently been proposed. These applications require the ability to walk descending and ascending paths on the volcano and also to walk on the crater of the volcano. We recall that a *path* is a sequence of isogenies that never backtracks. We start this section with a brief description of existing algorithms for these tasks, based on methods given by Kohel [14] and by Fouquet and Morain in [8]. We present modified algorithms, which rely on the method presented in Algorithm 2 to find ascending or horizontal isogenies. Then, we give complexity analysis for these algorithms and show that in many cases our method is competitive. Finally, we give two concrete examples in which the new algorithms can walk the crater of an isogeny volcano very efficiently compared to existing algorithms.

A brief description of existing algorithms. Existing algorithms rely on three essential properties in isogeny volcanoes. Firstly, it is easy to detect that a curve lies on the floor of a volcano, since in that case, there is a single isogeny from this curve. Moreover, this isogeny can only be ascending (or horizontal if the height is 0). Secondly, if in an arbitrary path in a volcano there is a descending isogeny,

then all the subsequent isogenies in the path are also descending. Thirdly, from a given curve, there is either exactly one ascending isogeny or at most two horizontal ones. As a consequence, finding a descending isogeny from any curve is easy: it suffices to walk three paths in parallel until one path reaches the floor. This shortest path is necessarily descending and its length gives the level of the starting curve in the volcano. To find an ascending or horizontal isogeny, the classical algorithms try all possible isogenies until they find one which leads to a curve either at the same level or above the starting curve. This property is tested by contructing descending paths from the all the neighbours of the initial curve and picking the curve which gave the longest path.

Note that alternatively, one could walk in parallel all of the $\ell+1$ paths starting from the initial curve and keep the (two) longest as horizontal or ascending. As far as we know, this has not been proposed in the literature, but this variant of existing algorithms offers a slightly better asymptotic time complexity. For completeness, we give a pseudo-code description of this parallel variant of Kohel and Fouquet-Morain algorithms as Algorithm 3.

Algorithm 3. Parallel variant of ascending/horizontal step (using modular polynomials)

Require: A j-invariant j_0 in $\mathbb{F}_q$, a prime ℓ, the modular polynomial $\Phi_\ell(X, Y)$.
Let $f(x) = \Phi_\ell(X, j_0)$
Compute J_0 the list of roots of $f(x)$ in $\mathbb{F}_q$
If $\#J_0 = 0$ **Output:** "Trivial volcano" **Exit**
If $\#J_0 = 1$ **Output:** "On the floor, step leads to:", $J_0[1]$ **Exit**
If $\#J_0 = 2$ **Output:** "On the floor, two horizontal steps to:", $J_0[1]$ and $J_0[2]$ **Exit**

Let $J = J_0$. Let J' and K be empty lists. Let Done = **false**.
repeat
  Perform multipoint evaluation of $\Phi_\ell(X, j)$, for each $j \in J$. Store in list F
  for i from 1 to $\ell + 1$ **do**
    Perform partial factorization of $F[i]$, computing at most two roots r_1 and r_2
    if $F[i]$ has less than two roots **then**
      Let Done = **true**. Append $\perp$ to K (Reaching floor)
    else
      If $r_1 \in J'$ **then** append r_1 to K **else** append r_2 to K. (Don't backtrack)
    end if
  end for
  Let $J' = J$, $J = K$ and K be the empty list
until Done
for each i from 1 to $\ell + 1$ such that $J[i] \neq \perp$ append $J_0[i]$ to K
Output: "Possible step(s) lead to:" K (One or two outputs)

Basic idea of the modified algorithms. In our algorithms, we first need to choose a large enough extension field to guarantee that the kernels of all required isogenies are spanned by ℓ-torsion points defined on this extension field. As explained in

Corollary 1, the degree r of this extension field is the order of q modulo ℓ and it can be computed very quickly after factoring $q-1$. As usual, we choose an arbitrary irreducible polynomial of degree r to represent $\mathbb{F}_{q^r}$. The necessary points of ℓ^∞-torsion are computed in Algorithm 1, multiplying random points over $\mathbb{F}_{q^r}$ by the cardinality of the curve divided by the highest possible power of ℓ. Once this is done, assuming that we are starting from a curve below the second level of stability, we use Algorithms 1 and 2 to find all ascending or horizontal isogenies from the initial curve. In order to walk a descending path, it suffices to choose any other isogeny. Note that, in the subsequent steps of a descending path, in the cases where the group structure satisfies $n_1 > n_2$, it is not necessary to run Algorithm 2 as a whole. Indeed, since we know that we are not on the crater, there is a single ascending isogeny and it is spanned by $\ell^{n_1-1}P_1$.

Finally, above the second stability level, we have two options. In theory, we can consider curves over larger extension fields (in order to get polynomials $\mathcal{P} \neq 0$. Note that this is too costly in practice. Therefore, we use preexisting algorithms, but it is not necessary to follow descending paths all the way to the floor. Instead, we can stop these paths at the second stabilty level, where our methods can be used.

5.1 Complexity Analysis

Computing a single isogeny. Before analyzing the complete algorithms, we first compare the costs of taking a single step on a volcano by using the two methods existing in the literature: modular polynomials and classical Vélu's formulae. Suppose that we wish to take a step from a curve E. With the modular polynomial approach, we have to evaluate the polynomial $f(X) = \Phi_\ell(X, j(E))$ and find its roots in $\mathbb{F}_q$. Assuming that the modular polynomial (modulo the characteristic of $\mathbb{F}_q$) is given as input and using asymptotically fast algorithms to factor $f(X)$, the cost of a step in terms of arithmetic operations in $\mathbb{F}_q$ is $O(\ell^2 + M(\ell)\log q)$, where $M(\ell)$ denotes the operation count of multiplying polynomials of degree ℓ. In this formula, the first term corresponds to evaluation of $\Phi_\ell(X, j(E_{i-1}))$ and the second term to root finding[8].

With Vélu's formulae, we need to take into account the fact that the required ℓ-torsion points are not necessarily defined over $\mathbb{F}_q$. Let r denotes the smallest integer such that the required points are all defined over $\mathbb{F}_{q^r}$. We know that $1 \leq r \leq \ell - 1$. Using asymptotically efficient algorithms to perform arithmetic operations in $\mathbb{F}_{q^r}$, multiplications in $\mathbb{F}_{q^r}$ cost $M(r)$ $\mathbb{F}_q$-operations. Given an ℓ-torsion point P in $E(\mathbb{F}_{q^r})$, the cost of using Vélu's formulae is $O(\ell)$ operations in $\mathbb{F}_{q^r}$. As a consequence, in terms of $\mathbb{F}_q$ operations, each isogeny costs $O(\ell M(r))$ operations. As a consequence, when q is not too large and r is close to ℓ, using Vélu formulae is more expensive by a logarithmic factor.

[8] Completely splitting $f(X)$ to find all its roots would cost $O(M(\ell)\log \ell \log q)$, but this is reduced to $O(M(\ell)\log q)$ because we only need a constant number of roots for each polynomial $f(X)$.

Computing an ascending or horizontal path. With the classical algorithms, each step in an ascending or horizontal path requires to try $O(\ell)$ steps and test each by walking descending paths of height bounded by h. The cost of each descending path is $O(h(\ell^2 + M(\ell)\log q))$ and the total cost is $O(h(\ell^3 + \ell M(\ell)\log q))$ (see [14,23]). When $\ell >> \log q$, this cost is dominated by the evaluations of the polynomial Φ_ℓ at each j-invariant. Thus, by walking in parallel $\ell + 1$ paths from the original curve, we can amortize the evaluation of $\Phi_\ell(X, j)$ over many j-invariants using fast multipoint evaluation, see [18, Section 3.7] or [25], thus replacing ℓ^3 by $\ell\, M(\ell)\log\ell$ and reducing the complexity of a step to $O(h\ell\, M(\ell)(\log\ell + \log q))$. However, this increases the memory requirements.

With our modified algorithms, we need to find the structure of each curve, compute some discrete logarithms in ℓ-groups, perform a small number of pairing computations and compute the roots of $\mathcal{P}_{E,\ell^{n_2}}$. Except for the computation of discrete logarithms, it is clear that all these additional operations are polynomial in n_2 and $\log\ell$ and they take negligible time in practice (see Section 5.2). Using generic algorithms, the discrete logarithms cost $O(\sqrt{\ell})$ operations, and this can be reduced to $\log\ell$ by storing a sorted table of precomputed logarithms. After this is done, we have to compute at most two isogenies, ignoring the one that backtracks. Thus, the computation of one ascending or horizontal step is dominated by the computation of isogenies and costs $O(\ell M(r))$.

For completeness, we also mention the complexity analysis of Algorithm 1. The dominating step here is the multiplication by N of randomly chosen points. When we consider the curve over an extension field $\mathbb{F}_{q^r}$, this costs $O(r\log q)$ operations in $\mathbb{F}_{q^r}$, i.e. $O(rM(r)\log q)$ operations in $\mathbb{F}_q$.

Finally, comparing the two approaches on a regular volcano, we see that even in the less favorable case, we gain a factor h compared to the classical algorithms. More precisely, the two are comparable, when the height h is small and r is close to ℓ. In all the other cases, our modified algorithms are more efficient. This analysis is summarized in Table 1. For compactness $O(\cdot)$s are omitted from the table.

Table 1. Walking the volcano: Order of the cost per step

	Descending path		Ascending/Horizontal
	One step	Many steps	
[14,8]	$h(\ell^2 + M(\ell)\log q)$	$(\ell^2 + M(\ell)\log q)$	$h(\ell^3 + \ell\, M(\ell)\log q)$
Parallel evaluation	–	–	$h\ell\, M(\ell)(\log\ell + \log q)$
Regular volcanoes	Structure determination		
Best case	$\log q$		$\log q$
Worst case $r \approx \ell/2$	$r\, M(r)\log q$		$r\, M(r)\log q$
Regular volcanoes	Isogeny construction		
Best case	ℓ		ℓ
Worst case $r \approx \ell/2$	$r\, M(r)$		$r\, M(r)$
Irregular volcanoes (worst case)	No improvement		

Irregular volcanoes. Consider a fixed value of q and let $s = v_\ell(q-1)$. First of all, note that all curves lying on irregular volcanoes satisfy $\ell^{2s}|q+1-t$ and $\ell^{2s+2}|t^2-4q$. For traces that satisfy only the first condition, we obtain a regular volcano. We estimate the total number of different traces of elliptic curves lying on ℓ-volcanoes by $\#\{t \text{ s.t. } \ell^{2s}|q+1-t \text{ and } t \in [-2\sqrt{q}, 2\sqrt{q}]\} \sim \frac{4\sqrt{q}}{\ell^{2s}}$.
Next, we estimate traces of curves lying on irregular volcanoes by

$$\#\{t \text{ s.t. } \ell^{2s}|q+1-t\ , \ell^{2s+2}|t^2-4q \text{ and } t \in [-2\sqrt{q}, 2\sqrt{q}]\} \sim \frac{4\sqrt{q}}{\ell^{2s+2}}.$$

Indeed, by writing $q = 1+\gamma\ell^s$ and $t = 2+\gamma\ell^s+\mu\ell^{2s}$, and imposing the condition $\ell^{2s+2}|t^2-4q$, we find that $t \cong t_0(\gamma,\mu) (\mathrm{mod}\ \ell^{2s+2})$.

Thus, we estimate the probability of picking a curve whose volcano is not regular, among curves lying on volcanoes of height greater than 0, by $\frac{1}{\ell^2}$. (This is a crude estimate because the number of curves for each trace is proportional to the Hurwitz class number[9] $H(t^2-4q)$). This probability is not negligible for small values of ℓ. However, since our method also works everywhere on almost regular volcano, the probability of finding a volcano where we need to combine our modified algorithm with the classical algorithms is even lower. Furthermore, in some applications, it is possible to restrict ourselves to regular volcanoes.

5.2 Two Practical Examples

A favorable case. In order to demonstrate the potential of the modified algorithm, we consider the favorable case of a volcano of height 2, where all the necessary ℓ-torsion points are defined over the base field $\mathbb{F}_p$, where $p = 619074283342666852501391$ is prime. We choose $\ell = 100003$.

Let E be the elliptic curve whose Weierstrass equation is
$y^2 = x^3 + 198950713578094615678321\,x + 32044133215969807107747$.
The group $E[\ell^\infty]$ over $\mathbb{F}_p$ has structure $\frac{\mathbb{Z}}{\ell^4\mathbb{Z}}$. It is spanned by the point
$P = (110646719734315214798587, 521505339992224627932173)$.

Taking the ℓ-isogeny I_1 with kernel $\langle \ell^3 P\rangle$, we obtain the curve
$E_1 : y^2 = x^3 + 476298723694969288644436\,x + 260540808216901292162091$,
with structure of the ℓ^∞-torsion $\frac{\mathbb{Z}}{\ell^3} \times \frac{\mathbb{Z}}{\ell}$ and generators
$P_1 = (226300457529970756040 69, 207694187789705800930332)$ and
$Q_1 = (304782745358080727058129, 193904829837168032791973)$.

The ℓ-isogeny I_2 with kernel $\langle \ell^2 P_1\rangle$ leads to the curve
$E_2 : y^2 = x^3 + 212075995767300038652790\,x + 471086215466928725193841$,
on the volcano's crater and with structure $\frac{\mathbb{Z}}{\ell^2\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^2\mathbb{Z}}$ and generators
$P_2 = (545333002760803067576755, 367548280448276783133614)$ and
$Q_2 = (401515368371004856400951, 225420044066280025495795)$.

Using pairings on these points, we construct the polynomial:

$$\mathcal{P}(x,y) = 97540\,x^2 + 68114\,x\,y + 38120\,y^2,$$

having homogeneous roots $(x,y) = (26568, 1)$ and $(72407, 1)$. As a consequence, we have two horizontal isogenies with kernels $\langle \ell(26568\,P_2 + Q_2)\rangle$ and $\langle \ell(72407\,P_2 + Q_2)\rangle$. We can continue and make a complete walk around the

[9] See [5, Th. 14.18] for q prime.

crater which contains 22 different curves. Using a simple implementation under Magma 2.15-15, a typical execution takes about 134 seconds[10] on a single core of an Intel Core 2 Duo at 2.66 GHz. Most of the time is taken by the computation of Vélu's formulas (132 seconds) and the computation of discrete logarithms (1.5 seconds) which are not tabulated in the implementation. The computation of pairings only takes 20 milliseconds.

A less favorable example. We have also implemented the computation for $\ell = 1009$ using an elliptic curve with j-invariant $j = 34098711889917$ in the prime field defined by $p = 953202937996763$. The ℓ-torsion appears in a extension field of degree 84. The ℓ-volcano has height two and the crater contains 19 curves. Our implementation walks the crater in 20 minutes. More precisely, 750 seconds are needed to generate the curves' structures, 450 to compute Vélu's formulas, 28 seconds for the pairings and 2 seconds for the discrete logarithms.

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 class polynomial [23] or of modular polynomials [4].

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

References

1. Belding, J., Broker, R., Enge, A., Lauter, K.: Computing Hilbert Class Polynomials. In: van der Poorten, A.J., Stein, A. (eds.) ANTS-VIII 2008. LNCS, vol. 5011, pp. 282–295. Springer, Heidelberg (2008)
2. Bisson, G., Sutherland, A.: Computing the endomorphism ring of an ordinary elliptic curve over a finite field. Journal of Number Theory (to appear 2010)
3. Blake, I.F., Seroussi, G., Smart, N.P.: Advances in Elliptic Curve Cryptography. London Mathematical Society Lecture Note Series, vol. 317. Cambridge University Press, Cambridge (2005)
4. Broker, R., Lauter, K., Sutherland, A.: Computing modular polynomials with the chinese remainder theorem (2009), `http://arxiv.org/abs/1001.0402`

[10] This timing varies between executions. The reason that we first try one root of $\mathcal{P}$, if it backtracks on the crater, we need to try the other one. On average, 1.5 root is tried for each step, but this varies depending on the random choices.

5. Cox, D.A.: Primes of the Form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication. John Wiley & Sons, Inc., Chichester (1989)
6. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkorper. Abh. Math. Sem. Hansischen Univ., vol. 14 (1941)
7. Fouquet, M.: Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques. PhD thesis, Ecole Polytechnique (2001)
8. Fouquet, M., Morain, F.: Isogeny Volcanoes and the SEA Algorithm. In: Fieker, C., Kohel, D.R. (eds.) ANTS 2002. LNCS, vol. 2369, pp. 276–291. Springer, Heidelberg (2002)
9. Frey, G.: Applications of arithmetical geometry to cryptographic constructions. In: Proceedings of the Fifth International Conference on Finite Fields and Applications, pp. 128–161. Springer, Heidelberg (2001)
10. Grabher, P., Großschädl, J., Page, D.: On software parallel implementation of cryptographic pairings. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 35–50. Springer, Heidelberg (2009)
11. Ionica, S.: Algorithmique des couplages et cryptographie. PhD thesis, Université de Versailles St-Quentin-en-Yvelines (2010)
12. Joux, A., Nguyen, K.: Separating decision Diffie–Hellman from computational Diffie–Hellman in cryptographic groups. Journal of Cryptology 16(4), 239–247 (2003)
13. Lenstra Jr., H.W.: Complex multiplication structure of elliptic curves. Journal of Number Theory 56(2), 227–241 (1996)
14. Kohel, D.: Endomorphism rings of elliptic curves over finite fields. PhD thesis, University of California, Berkeley (1996)
15. Miller, V.S.: The Weil pairing, and its efficient calculation. Journal of Cryptology 17(4), 235–261 (2004)
16. Miret, J., Moreno, R., Sadornil, D., Tena, J., Valls, M.: An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields. Applied Mathematics and Computation 176(2), 739–750 (2006)
17. Miret, J., Moreno, R., Sadornil, D., Tena, J., Valls, M.: Computing the height of volcanoes of l-isogenies of elliptic curves over finite fields. Applied Mathematics and Computation 196(1), 67–76 (2008)
18. Montgomery, P.L.: A FFT extension of the elliptic curve method of factorization. PhD thesis, University of California (1992)
19. Ruck, H.-G.: A note on elliptic curves over finite fields. Mathematics of Computation 179, 301–304 (1987)
20. Schoof, R.: Counting points on elliptic curves over finite fields. Journal de Theorie des Nombres de Bordeaux 7, 219–254 (1995)
21. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 106. Springer, Heidelberg (1986)
22. Silverman, J.H.: Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 151. Springer, Heidelberg (1994)
23. Sutherland, A.: Computing Hilbert Class Polynomials with the Chinese Remainder Theorem. Mathematics of Computation (2010)
24. Vélu, J.: Isogenies entre courbes elliptiques. Comptes Rendus De L'Academie Des Sciences Paris, Serie I-Mathematique, Serie A. 273, 238–241 (1971)
25. von zur Gathen, J., Shoup, V.: Computing Frobenius maps and factoring polynomials. Computational Complexity 2, 187–224 (1992)