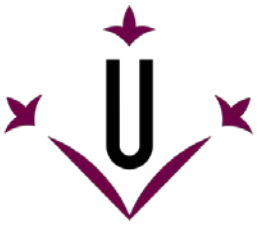

Isogeny Volcanoes of Elliptic Curves and Sylow Subgroups

Mireille Fouquet[1], Josep M. Miret[2], and Javier Valera[2]

[1] Institut de Mathématiques de Jussieu, Université Paris Diderot - Paris 7, France
fouquet@math.univ-paris-diderot.fr
[2] Dept. de Matemàtica, Universitat de Lleida, Spain
{miret,jvalera}@matematica.udl.cat

Abstract. Given an ordinary elliptic curve over a finite field located in the floor of its volcano of ℓ-isogenies, we present an efficient procedure to take an ascending path from the floor to the level of stability and back to the floor. As an application for regular volcanoes, we give an algorithm to compute all the vertices of their craters. In order to do this, we make use of the structure and generators of the ℓ-Sylow subgroups of the elliptic curves in the volcanoes.

Keywords: Elliptic curves · Isogeny volcanoes · Sylow subgroups · Finite fields

1 Introduction

In the last decades, the usage of elliptic curves over finite fields in the design of secure cryptography protocols has grown significantly. Nevertheless, not all elliptic curves are useful in cryptography based on the discrete logarithm problem, since they must satisfy certain requirements related to their group orders or their embedding degrees. Concerning their group orders, they must be of the form $f \cdot q$ with q prime and f a small integer, otherwise the curves are vulnerable to the Pohlig-Hellman attack [17]. Regarding their embedding degrees, they must be ≥ 6 for curves of 160 bits, otherwise the curves are vulnerable to the MOV attack [12].

Isogenies between elliptic curves over finite fields, in particular, prime degree isogeny chains, have long been a subject of study with different approaches, since they play a central role in the SEA algorithm (see [3,18]) to compute the group order of an elliptic curve. The basic idea of this algorithm is the computation of the trace of the Frobenius endomorphism of a curve modulo different suitably chosen small primes ℓ.

Given two ordinary elliptic curves E and E' over a finite field $\mathbb{F}_q$ with endomorphism rings $\mathcal{O}$ and $\mathcal{O}'$, respectively, and an isogeny $\mathcal{I} : E \to E'$ of degree a prime ℓ such that $\ell \nmid q$, Fouquet and Morain [6] introduced, from the Kohel's Ph.D. thesis [9], the notion of direction of an ℓ-isogeny. It is *ascending, horizontal* or *descending* whether the index $[\mathcal{O}' : \mathcal{O}]$ is ℓ, 1 or $1/\ell$ respectively. With this notion of direction for the ℓ-isogenies, the set of isomorphism classes

of ordinary elliptic curves over $\mathbb{F}_q$ with group order $N = q+1-t$, $|t| \leq 2\sqrt{q}$, can be represented as a directed graph, whose vertices are the isomorphism classes and its arcs represent the ℓ-isogenies between curves in two vertices. It is worth remarking that if two vertices are connected by an arc, the corresponding dual ℓ-isogeny is represented as an arc in the other direction.

Each connected component of this graph is called *volcano of ℓ-isogenies* due to its peculiar shape. Indeed, it consists of a cycle that can be reduced to one point, called *crater*, where from its vertices hang $\ell + 1 - m$ complete ℓ-ary trees being m the number of horizontal ℓ-isogenies. Then, the vertices can be stratified into levels in such a way that the curves in each level have the same endomorphism ring. The bottom level is called the *floor* of the volcano.

Knowing the cardinality of an elliptic curve, Kohel [9] and recently Bisson and Sutherland [1] describe algorithms to determine its endomorphism ring taking advantage of the relationship between the levels of its volcano and the endomorphism rings at those levels. When the cardinality is unknown, Fouquet and Morain [6] give an algorithm to determine the *height* (or depth) of a volcano using exhaustive search over several paths on the volcano to detect the crater and the floor levels. As a consequence, they obtain computational simplifications for the SEA algorithm, since they extend the moduli ℓ in the algorithm to prime powers ℓ^s.

In [15], Miret et al. showed the relationship between the levels of a volcano of ℓ-isogenies and the ℓ-Sylow subgroups of the curves. All curves in a fixed level have the same ℓ-Sylow subgroup. At the floor, the ℓ-Sylow subgroup is cyclic. When ascending by the *volcanoside*, that is, by the levels which are between the floor and the crater, the ℓ-Sylow subgroup structure is becoming balanced. The first level, if it exists, where the ℓ-Sylow subgroup is balanced, is called *stability level*. If this level does not exist, the stability level is the crater of the volcano. Recently, Ionica and Joux [7] have developed a method to decide whether the isogeny with kernel a subgroup generated by a point of order ℓ is an ascending, horizontal or descending ℓ-isogeny using a symmetric pairing over the ℓ-Sylow subgroup of a curve [8].

Volcanoes of ℓ-isogenies have also been used by Sutherland [20] to compute the Hilbert class polynomials. Another application has been provided by Bröker, Lauter and Sutherland [2] in order to compute modular polynomials. To reach these goals, in both works, it is necessary to determine the vertices of the craters of the volcanoes. On the other hand, some specific side channel attacks, the so-called Zero Value Point attacks, can be avoided using isogenies or more precisely volcanoes of ℓ-isogenies [16].

In this paper, given an ordinary elliptic curve $E/\mathbb{F}_q$, the structure $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$, $r > s$, of its ℓ-Sylow subgroup and a point P_r of order ℓ^r, we construct a chain of ℓ-isogenies starting from E and ending at a curve at the floor of the volcano. This chain first is ascending, then horizontal and finally descending. When $h \geq 1$ and $2h < r + s$, being h the height of the volcano, all the vertices of its crater can be obtained by using repeatedly this sort of chains. Therefore we present an algorithm to perform this task.

In the following, we consider ordinary elliptic curves defined over a finite field $\mathbb{F}_q$, with cardinality unknown. We assume that the characteristic p of $\mathbb{F}_q$ is different from 2 and 3. We denote by ℓ a prime that does not divide q. Furthermore, in Sections 3 and 4 we assume that the ℓ-Sylow subgroup of the considered curve is not trivial.

2 Preliminaries

In this section we introduce some notations that are used in the sequel concerning ℓ-isogenies, volcanoes of ℓ-isogenies and ℓ-Sylow subgroups of elliptic curves.

We denote by $E/\mathbb{F}_q$ an elliptic curve defined over the finite field $\mathbb{F}_q$, by $E(\mathbb{F}_q)$ its group of rational points with O_E its neutral element and by $j(E)$ its j-invariant.

Given an ordinary elliptic curve $E/\mathbb{F}_q$ with group order $N = q+1-t$, where t is the trace of the Frobenius endomorphism of $E/\mathbb{F}_q$, its endomorphism ring $\mathcal{O} = \mathrm{End}(E)$ can be identified with an order of the imaginary quadratic field $\mathcal{K} = \mathbb{Q}(\sqrt{t^2-4q})$ (see [19]). The order $\mathcal{O}$ satisfies [4]

$$\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathcal{K}},$$

where $\mathcal{O}_{\mathcal{K}}$ is the ring of integers of $\mathcal{K}$ and π is the Frobenius endomorphism of $E/\mathbb{F}_q$. Writing $t^2-4q = g^2 D_{\mathcal{K}}$, where $D_{\mathcal{K}}$ is the discriminant of $\mathcal{K}$, it turns out that g is the conductor of the order $\mathbb{Z}[\pi]$ in the maximal order $\mathcal{O}_{\mathcal{K}}$. Then the conductor f of $\mathcal{O}$ divides g.

A volcano of ℓ-isogenies [6] is a directed graph whose vertices are isomorphism classes of ordinary elliptic curves over a finite field $\mathbb{F}_q$ and where the arcs represent ℓ-isogenies among them. These graphs consist of a unique cycle (with one, two or more vertices) at the top level, called crater, and from each vertex of the cycle hang $\ell+1$, ℓ or $\ell-1$ (depending of the number of horizontal ℓ-isogenies) ℓ-ary isomorphic complete trees, except in the case where the volcano is reduced to the crater. The vertices at the bottom level, called floor of the volcano, have only one ascending outgoing arc. In the other cases each vertex has $\ell+1$ outgoing arcs: for the vertices in the volcanoside, one is ascending and ℓ are descending, while for the vertices on the crater it depends on its typology (and it can be easily explained for each case). The case where we encounter a vertex with j-invariant $j=0$ or $j=1728$ is slightly different and is not treated in this paper. We denote by $V_\ell(E/\mathbb{F}_q)$ the volcano of ℓ-isogenies where $E/\mathbb{F}_q$ belongs. We remark that if $E'/\mathbb{F}_q$ is another curve on the volcano, $V_\ell(E'/\mathbb{F}_q) = V_\ell(E/\mathbb{F}_q)$.

Lenstra [11] proved that $E(\mathbb{F}_q) \simeq \mathcal{O}/(\pi-1)$ as $\mathcal{O}$-modules, from where one can deduce that $E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$. By writing $\pi = a + g\omega$ with

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

we obtain that $n_2 = \gcd(a-1, g/f)$, $n_2 \mid n_1$, $n_2 \mid q-1$ and $\#E(\mathbb{F}_q) = n_1 n_2$. This implies that on a volcano of ℓ-isogenies the group structure of all the curves with same endomorphism ring, i.e. at the same level, is identical.

From this classification of the elliptic curves, the relationship between the structure of the ℓ-Sylow subgroup $E[\ell^\infty](\mathbb{F}_q)$ of an elliptic curve $E/\mathbb{F}_q$ and its location in the volcano of ℓ-isogenies $V_\ell(E/\mathbb{F}_q)$ is deduced.

Proposition 1 *[15] Let $E/\mathbb{F}_q$ be an elliptic curve whose ℓ-Sylow subgroup is isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$, $r \geq s \geq 0$, $r + s \geq 1$.*

- *If $s < r$ then E is at level s in the volcano with respect to the floor;*
- *If $s = r$ then E is at least at level s with respect to the floor.*

As said in the introduction, we call stability level the level where from this one down to the floor, the structure of the ℓ-Sylow subgroup is different at each level (we therefore allow the stability level to be the crater). Ionica and Joux [7] call it the first level of stability. The curves located above the stability level (including this one) until the crater, if they exist, have ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z} \times \mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z}$, being $n = v_\ell(N)$, n even and N the cardinality of the curves (see [15]). A volcano whose crater is equal to the stability level is called a *regular* volcano. Otherwise it is called an *irregular* volcano. Notice that if n is odd, then the volcano is regular. If n is even, it can be regular or irregular.

The height h of a volcano of ℓ-isogenies coincides with the ℓ-valuation of the conductor g of $\mathbb{Z}[\pi]$. This value, assuming n is kwown, can be completely determined in most cases (see [15]).

Concerning the ℓ-Sylow subgroup $E[\ell^\infty](\mathbb{F}_q)$ of an elliptic curve $E/\mathbb{F}_q$, Miret et al. [14] gave a general algorithm to determine its structure $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$, $r \geq s \geq 0$, together with generators P_r and Q_s, without knowing the cardinality of the curve. Their method starts computing either one point of order ℓ of $E(\mathbb{F}_q)$, if the ℓ-Sylow subgroup is cyclic, or two independent points of order ℓ, otherwise. Then, in an inductive way, the algorithm proceeds computing one point of order ℓ^{k+1} for one or two points of order ℓ^k until reaching those of maximum order. If the cardinality of the curve is known, Ionica and Joux [7] give a probabilistic algorithm to compute the ℓ-Sylow structure more efficiently than the preceeding one.

Finally, we say that a point $Q \in E(\mathbb{F}_q)$ is ℓ-divisible or ℓ-divides if there exists another point $P \in E(\mathbb{F}_q)$ such that $\ell P = Q$. We say, as well, that P is an ℓ-divisor of Q.

3 A Particular Chain of ℓ-Isogenies

Given an elliptic curve $E/\mathbb{F}_q$, which is on the floor of the volcano $V_\ell(E/\mathbb{F}_q)$, we determine a chain of ℓ-isogenies in the volcano from the floor to the stability level and back to the floor. More precisely, if $h \geq 1$ and the ℓ-Sylow subgroup of $E/\mathbb{F}_q$ is isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z}$, then we give a chain of length n starting at the floor to the stability level and descending back to the floor.

3.1 Behaviour of the ℓ-Sylow Subgroup through Particular ℓ-Isogenies

In this subsection, we study the changes in the ℓ-Sylow subgroup when we consider isogenies defined by the quotient of subgroups of order ℓ.

Lemma 2 *Let $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ with $r > s > 0$ be the group isomorphic to the ℓ-Sylow subgroup of an elliptic curve $E/\mathbb{F}_q$. Let $P_r \in E(\mathbb{F}_q)$ and $Q_s \in E(\mathbb{F}_q)$ be two linearly independent points whose orders are respectively ℓ^r and ℓ^s. Denote $P_1 = \ell^{r-1}P_r$ and $Q_1 = \ell^{s-1}Q_s$.*

i) Either the isogenous curve $E' \simeq E/\langle P_1\rangle$ has ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^{r-1}\mathbb{Z} \times \mathbb{Z}/\ell^{s+1}\mathbb{Z}$ and the ℓ-isogeny of kernel $\langle P_1\rangle$ is ascending or the isogenous curve $E' \simeq E/\langle P_1\rangle$ has ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ and the ℓ-isogeny of kernel $\langle P_1\rangle$ is horizontal.

ii) Either the isogenous curve $E'' \simeq E/\langle Q_1\rangle$ has ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^{r+1}\mathbb{Z} \times \mathbb{Z}/\ell^{s-1}\mathbb{Z}$ and the ℓ-isogeny of kernel $\langle Q_1\rangle$ is descending or the isogenous curve $E'' \simeq E/\langle Q_1\rangle$ has ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ and the ℓ-isogeny of kernel $\langle Q_1\rangle$ is horizontal.

iii) In the case that $E/\mathbb{F}_q$ is on the crater of the volcano, then the ℓ-Sylow subgroup of $E'/\mathbb{F}_q$ is isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$, that is, the ℓ-isogeny of kernel $\langle P_1\rangle$ is horizontal.

Proof. By [15] the action of an ℓ-isogeny over the ℓ-Sylow subgroup of an elliptic curve $E/\mathbb{F}_q$ is, if $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ with $r > s > 0$, of the form $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$, $\mathbb{Z}/\ell^{r+1}\mathbb{Z} \times \mathbb{Z}/\ell^{s-1}\mathbb{Z}$ or $\mathbb{Z}/\ell^{r-1}\mathbb{Z} \times \mathbb{Z}/\ell^{s+1}\mathbb{Z}$ depending on the direction of the ℓ-isogeny. By looking at the orders of the images of P_r and Q_s with the considered ℓ-isogeny, we can conclude.

Lemma 3 *Let $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ with $r > s > 0$ be the group isomorphic to the ℓ-Sylow subgroup of an elliptic curve $E/\mathbb{F}_q$. Let $P_r \in E(\mathbb{F}_q)$ and let $Q_s \in E(\mathbb{F}_q)$ be two linearly independent points whose orders are respectively ℓ^r and ℓ^s. Let $\mathcal{I}$ denote the isogeny from E to E' of degree ℓ such that $\ker\mathcal{I} = \langle \ell^{r-1}P_r\rangle$. Then there exists exactly one point R of the form*

$$Q_s \quad \text{or} \quad P_r + kQ_s, \quad 0 \le k < \ell,$$

which does not ℓ-divide in $E(\mathbb{F}_q)$ and $\mathcal{I}(R)$ ℓ-divides in $E'(\mathbb{F}_q)$, but does not ℓ^2-divide.

Proof. First of all, the set of points R in the ℓ-Sylow subgroup $\langle P_r, Q_s\rangle$ which do not ℓ-divide are, up to multiples, of one of the following forms

$$P_r + k_1\ell P_r + k_2 Q_s, \qquad 0 \le k_1 < \ell^{r-1},\ 0 \le k_2 < \ell^s \tag{1}$$

$$Q_s + k_1\ell^{r-s}P_r + k_2\ell Q_s, \qquad 0 \le k_1 < \ell^s,\ 0 \le k_2 < \ell^{s-1} \tag{2}$$

$$Q_s + k_1\ell^{r-s-i}P_r + k_2\ell Q_s, \qquad \begin{array}{c} 0 \le k_1 < \ell^{s+i},\ 0 \le k_2 < \ell^{s-1}, \\ 0 < i < r-s \end{array} \tag{3}$$

Since all the points of the form $k_1\ell P_r$ and $k_2\ell Q_s$ ℓ-divide in $E(\mathbb{F}_q)$, if some point of the form (1), (2) or (3) has an image point under $\mathcal{I}$ that ℓ-divides in $E'(\mathbb{F}_q)$, then at least one of the points Q_s or $P_r + kQ_s$, $0 \leq k < \ell$, has an image point under $\mathcal{I}$ that also ℓ-divides.

We denote $\hat{\mathcal{I}}$ the dual of $\mathcal{I}$. We denote by $Q'_s = \mathcal{I}(Q_s)$. We have seen in our first lemma that $|Q'_s| = \ell^s$. Suppose there exists $Q'_{s+x} \in E'(\mathbb{F}_q)$ such that $\ell^x Q'_{s+x} = Q'_s$ with $x > 1$. We have

$$\ell Q_s = \hat{\mathcal{I}}(\mathcal{I}(Q_s)) = \hat{\mathcal{I}}(Q'_s) \quad \text{and} \quad \ell^x \hat{\mathcal{I}}(Q'_{s+x}) = \hat{\mathcal{I}}(\ell^x Q'_{s+x}) = \hat{\mathcal{I}}(Q'_s) = \ell Q_s.$$

Therefore $|\hat{\mathcal{I}}(Q'_{s+x})| = \ell^{x+s-1}$. Since $x > 1$, we get $x + s - 1 > s$ and this is not possible since the elements of $\langle Q_s \rangle$ have at most order equal to ℓ^s. The same argument holds to prove that the image of $P_r + kQ_s$ at most ℓ-divides in $E'(\mathbb{F}_q)$.

There is at least one point that does not ℓ-divide in $E(\mathbb{F}_q)$ whose image by $\mathcal{I}$ ℓ-divides since the order of the ℓ-Sylow subgroup is invariant by isogeny. The same argument shows that there is only one point, up to multiples, that does not ℓ-divide in $E(\mathbb{F}_q)$ whose image by $\mathcal{I}$ ℓ-divides.

Let us remark that the points R of the form (1) are of order ℓ^r, the ones of the form (2) are of order ℓ^s and the ones of the form (3) are of order ℓ^{s+i}. This consideration shows us that if the ℓ-isogeny is ascending the unique R that does not ℓ-divide whose image ℓ-divides in $E'(\mathbb{F}_q)$ is of the form (2), while if the ℓ-isogeny is horizontal the unique R is of the form (3) with order ℓ^{r-1}.

Proposition 4 *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let $P_n \in E(\mathbb{F}_q)$ be a point of order ℓ^n which does not ℓ-divide. Denote by R a point of order ℓ of $E(\overline{\mathbb{F}_q})$ which generates a Galois invariant subgroup G of $E(\mathbb{F}_q)$. Let P_{n+1} be a point of E in some extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ such that $\ell P_{n+1} = P_n$. Let $\mathcal{I} : E \to E'$ the isogeny of kernel G. Then, the abscissa of the point $\mathcal{I}(P_{n+1})$ is rational, that is $x(\mathcal{I}(P_{n+1})) \in \mathbb{F}_q$, if and only if*

$$f_{\mathcal{I}}(x) = (x - x(P_{n+1}))(x - x(P_{n+1} + R)) \cdots (x - x(P_{n+1} + (\ell - 1)R)) \in \mathbb{F}_q[x].$$

Proof. The coefficients of the polynomial $f_{\mathcal{I}}(x)$ are the elementary symmetric polynomials $\mathbf{S}_r$, $1 \leq r \leq \ell$, in the abscissas of the points in $P_{n+1} + \langle R \rangle$. In [13], these elementary symmetric polynomials are given in terms of the so called generalized Vélu parameters w_i of the curve,

$$w_i = (2i+3)S^{(i+2)} + \frac{(i+1)b_2}{2}S^{(i+1)} + \frac{(2i+1)b_4}{2}S^{(i)} + \frac{ib_6}{2}S^{(i-1)}, \qquad (4)$$

where $S^{(j)}$ indicates the j-th power sum of the abscissas of the points in $\langle R \rangle \setminus \{O_E\}$. Therefore, the r-th elementary symmetric polynomial in the abscissas of the points in $P_{n+1} + \langle R \rangle$ is given by

$$\mathbf{S}_r = S_{r-1}X + S_r + \sum_{i=0}^{r-2}(-1)^i w_i S_{r-i-2},$$

where X is the abscissa of the isogenous point $\mathcal{I}(P_{n+1})$ and S_j is the j-th elementary symmetric polynomial in the abscissas of points in $\langle R\rangle \setminus \{O_E\}$. Therefore, $X = x(\mathcal{I}(P_{n+1})) \in \mathbb{F}_q$ if and only if $\mathbf{S}_r \in \mathbb{F}_q$, $\forall r \in \{1, \ldots, \ell\}$.

Lemma 5 *Let E' be an elliptic curve defined over $\mathbb{F}_q$. We suppose that the ℓ-torsion subgroup of $E'/\mathbb{F}_q$ is generated by two points P' and Q' linearly independent. Let $\mathcal{I} : E' \to E$ be the isogeny of kernel $\langle P'\rangle$. We denote by Q the image of Q' by $\mathcal{I}$. Then the dual isogeny $\hat{\mathcal{I}}$ is the isogeny from E with kernel equal to $\langle Q\rangle$.*

Proof. Let $\mathcal{I}'$ be the isogeny from E with kernel equal to $\langle Q\rangle$. The kernel of the isogeny $\mathcal{I}' \circ \mathcal{I}$ is the ℓ-torsion subgroup of E'. Therefore, the composition $\mathcal{I}' \circ \mathcal{I}$ is equal to the multiplication by $[\ell]$ over the curve E', and hence $\mathcal{I}' = \hat{\mathcal{I}}$. Therefore $(\hat{\mathcal{I}} \circ \mathcal{I})(P') = O_{E'}$ and $(\hat{\mathcal{I}} \circ \mathcal{I})(Q') = O_{E'}$. By definition of $\mathcal{I}$, we have $\mathcal{I}(P') = O_E$ and $\mathcal{I}(Q') = Q$. Hence $\hat{\mathcal{I}}(Q) = O_{E'}$ and the subgroup generated by Q is in the kernel of $\mathcal{I}'$. But $\hat{\mathcal{I}}$ is an isogeny of degree ℓ and since Q is a point of order ℓ over E, $\ker \hat{\mathcal{I}} = \langle Q\rangle$.

We now show how we can obtain a chain of points on isogenous curves that do not ℓ-divide. This chain of non ℓ-divisible points gives us the key of our chain of ℓ-isogenies.

Proposition 6 *Let E be an elliptic curve defined over $\mathbb{F}_q$ with ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ with $r \geq s \geq 0$ and $r \geq 2$. Let $P_k \in E(\mathbb{F}_q)$ of order ℓ^k, $k \geq 2$, such that P_k is not ℓ-divisible. Consider the isogeny $\mathcal{I}_1 : E \to E^{(1)}$ of kernel $\langle P_1\rangle$, where $P_1 = \ell^{k-1}P_k$, and the isogeny $\mathcal{I}_2 : E^{(1)} \to E^{(2)}$ of kernel $\langle \mathcal{I}_1(P_2)\rangle$, where $P_2 = \ell^{k-2}P_k$.*
Suppose that the point $\mathcal{I}_1(P_k)$ in $E^{(1)}(\mathbb{F}_q)$ does not ℓ-divide.

We, then, have two different cases depending on the value of k.

- *Case $k > 2$: the point $\mathcal{I}_2(\mathcal{I}_1(P_k))$ in $E^{(2)}(\mathbb{F}_q)$ does not ℓ-divide.*
- *Case $k = 2$: the point $\mathcal{I}_2(\mathcal{I}_1(P_k))$ is $O_{E^{(2)}}$ and the ℓ-torsion subgroup of $E^{(2)}/\mathbb{F}_q$ is cyclic.*

Proof. In the case $k > 2$, in order to prove that, under the isogeny $\mathcal{I}_2 : E^{(1)} \to E^{(2)}$, the point $\mathcal{I}_2(\mathcal{I}_1(P_k))$ does not ℓ-divide, let $P_{k+1} \in E(\overline{\mathbb{F}_q})$ such that $\ell P_{k+1} = P_k$. Assume $\mathcal{I}_2(\mathcal{I}_1(P_{k+1})) \in E^{(2)}(\mathbb{F}_q)$. From Proposition 4, if $x(\mathcal{I}_2(\mathcal{I}_1(P_{k+1}))) \in \mathbb{F}_q$, the polynomial

$$\prod_{m=0}^{\ell-1} (x - x(\mathcal{I}_1(P_{k+1}) + m\mathcal{I}_1(P_2)))$$

would have all its coefficients in $\mathbb{F}_q$. Nevertheless, if we consider the dual isogeny $\hat{\mathcal{I}}_1 : E^{(1)} \to E$ with kernel $\langle R\rangle$, where $R \in E^{(1)}(\overline{\mathbb{F}_q})$ and $\langle R\rangle \neq \langle \mathcal{I}_1(P_2)\rangle$ by Lemma 5, it turns out that $\hat{\mathcal{I}}_1(\mathcal{I}_1(P_{k+1})) = \ell P_{k+1} = P_k$. Hence the abscissa

$x(\hat{\mathcal{I}}_1(\mathcal{I}_1(P_{k+1}))) \in \mathbb{F}_q$ and again from Proposition 4, the coefficients of the polynomial

$$\prod_{m=0}^{\ell-1} (x - x(\mathcal{I}_1(P_{k+1}) + mR))$$

belong to $\mathbb{F}_q$. Therefore, since the greatest common divisor of these two polynomials is the linear factor $x - x(\mathcal{I}_1(P_{k+1}))$, we get $x(\mathcal{I}_1(P_{k+1})) \in \mathbb{F}_q$. Besides, if the ordinate of the point $\mathcal{I}_2(\mathcal{I}_1(P_{k+1}))$ belongs to $\mathbb{F}_q$ as well, then the ordinate of $\mathcal{I}_1(P_{k+1}) \in E^{(1)}(\mathbb{F}_q)$, which is a contradiction. The relationship between these ordinates can be derived from the formula which expresses the ordinate of the image of a point P under an isogeny of kernel G in terms of the coordinates of P and the elementary symmetric polynomials in the abscissas of points of G (see [10]). If $k = 2$, we can see that $E_1[\ell](\mathbb{F}_q)$ is a non cyclic subgroup generated by $\mathcal{I}_1(P_2)$ and another point Q. Assume $E_2[\ell](\mathbb{F}_q)$ is as well a non cyclic group. Then $E_2[\ell](\mathbb{F}_q)$ is generated by $\mathcal{I}_2(Q)$ and another point P. Therefore there exists a point $P_3 \in E(\overline{\mathbb{F}_q})$ such that $\ell P_3 = P_2$ and $\mathcal{I}_2(\mathcal{I}_1(P_3)) = P$. By using the same argument as for the case $k > 2$, we get $P_3 \in E(\mathbb{F}_q)$, which is a contradiction.

Corollary 7 *Let E be an elliptic curve defined over $\mathbb{F}_q$ with ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ with $r > s \geq 0$ and $r \geq 2$ such that E is under the crater of its volcano of ℓ-isogenies. Let $P_r \in E(\mathbb{F}_q)$ such that P_r is of order ℓ^r. We denote by $E^{(1)}$ (resp. $E^{(2)}$, $E^{(3)}$, ..., $E^{(r)}$) the quotient of the curve E (resp. $E^{(1)}$, $E^{(2)}$, ..., $E^{(r-1)}$) by the subgroup generated by P_1 (resp. the images of P_2, P_3, ..., P_r). Then the successive images of P_r in $E^{(1)}$, $E^{(2)}$, ..., $E^{(r-1)}$ never ℓ-divide unless in $E^{(r)}$ where the image of P_r is $O_{E^{(r)}}$ and the ℓ-torsion subgroup of $E^{(r)}/\mathbb{F}_q$ is cyclic.*

Proof. Since the curve is below the crater, by *i)* of Lemma 2, the first ℓ-isogeny is ascending and therefore the ℓ-Sylow subgroup of $E^{(1)}/\mathbb{F}_q$ is isomorphic to $\mathbb{Z}/\ell^{r-1}\mathbb{Z} \times \mathbb{Z}/\ell^{s+1}\mathbb{Z}$ and hence the image of P_r does not ℓ-divide. By induction of Proposition 6, the result follows.

3.2 From Floor to Stability Level and Back to Floor

The preceding results lead us to consider the chain of ℓ-isogenies defined by the succesive quotients of subgroups of order ℓ determined from a point of the initial curve whose order is the maximum power of ℓ.

Theorem 8 *Let E be an elliptic curve defined over $\mathbb{F}_q$ with ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z}$. Let P_n be a generator of this subgroup and, for all $k \in \mathbb{N}$, $k < n$, we denote by P_k the point $\ell^{n-k}P_n$. We suppose that the height h of the volcano $V_\ell(E/\mathbb{F}_q)$ is ≥ 1.*

i) If the curves of the crater of the volcano $V_\ell(E/\mathbb{F}_q)$ have ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z} \times \mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z}$, then the chain of ℓ-isogenous succesive curves E, $E^{(1)}$, $E^{(2)}$, ..., $E^{(n-1)}$ given by the subgroups generated by P_1, resp. the

images of P_2, P_3, ..., P_n consists of $n/2$ ascending ℓ-isogenies until reaching the stability level and $n/2$ descending ℓ-isogenies.

ii) If the curves of the crater of the volcano $V_\ell(E/\mathbb{F}_q)$ have ℓ-Sylow subgroups isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ with $r > s = h$, then the chain of ℓ-isogenous succesive curves E, $E^{(1)}$, $E^{(2)}$, ..., $E^{(n-1)}$ given by the subgroups generated by P_1, resp. the images of P_2, P_3, ..., P_n consists of h ascending ℓ-isogenies until reaching the crater, $n-2h$ horizontal ℓ-isogenies and finally h descending ℓ-isogenies.

Proof. Consider the successive isogenies $\mathcal{I}_i : E^{(i-1)} \to E^{(i)}$, $i = 1, \ldots, n$, where $E^{(0)} = E$, whose kernels are the subgroups generated by the successive images of the points $P_i = \ell^{n-i}P_n$ under the previous isogenies. Since the ℓ-Sylow subgroup of E is cyclic, E is at the floor of the volcano and it has a unique isogeny $\mathcal{I}_1 : E \to E^{(1)}$ which is ascending. The following isogenies of the sequence, from Lemma 2, must be ascending or horizontal until reaching either a curve, if it exists, with a balanced ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z} \times \mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z}$ or a curve on the crater. Thus, the isogenies of the sequence are ascending from the floor to the stability level.

In the case *i)*, n is even and the curve $E^{(\frac{n}{2})}$ has ℓ-Sylow subgroup isomorphic to $\mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z}\times\mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z}$. From Corollary 7, the image of the point P_n under the isogeny $\mathcal{I}_{\frac{n}{2}}$ does not ℓ-divide in the curve $E^{(\frac{n}{2})}$. This implies that the ℓ-Sylow subgroup of the curve $E^{(\frac{n}{2}+1)}$ cannot be of the form $\mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z} \times \mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z}$ since the point P_n does not ℓ-divide. Hence, the isogeny $\mathcal{I}_{\frac{n}{2}+1} : E^{(\frac{n}{2})} \to E^{(\frac{n}{2}+1)}$ is descending. By Lemma 2, the following isogenies of the sequence are descending.

In the case *ii)*, by Lemma 2, we might encounter a sequence of horizontal isogenies and then the rest of the isogenies will be descending.

We will first treat the case $r > s + 1$. We reach the crater with the curve $E^{(s)}$. Its ℓ-Sylow subgroup is generated by $P_n^{(s)}$ the successive image of P_n of order ℓ^r, $r = n-s$, and a point $Q_s^{(s)}$ of order ℓ^s. The isogeny $\mathcal{I}_{s+1}$ is the quotient of $E^{(s)}$ by $\langle \ell^{r-1}P_n^{(s)} \rangle$. Therefore $\mathcal{I}_{s+1}(P_n^{(s)})$ is of order ℓ^{r-1} and $\mathcal{I}_{s+1}(Q_s^{(s)})$ is of order ℓ^s. Since the isogeny cannot be ascending, it has to be horizontal and therefore a point of the form $\mathcal{I}_{s+1}(P_n^{(s)} + kQ_s^{(s)})$ ℓ-divides in $E^{(s+1)}$ by Lemma 3. By Corollary 7, we have that $1 \leq k < \ell$. This point $P_n^{(s)} + kQ_s^{(s)}$ is an ℓ^s-divisor of $P_r^{(s)}$ but not an ℓ^{s-1}-divisor of $P_{r+1}^{(s)}$. This argument can be repeated until we reach the isogeny $\mathcal{I}_{n-s}$ defined by the quotient by $\langle P_{n-s}^{(n-s-1)} \rangle$. In the curve $E^{(n-s)}$, the point $P_{n-s+1}^{(n-s)} = \ell^{s-1}P_n^{(n-s)}$ does not have ℓ^i-divisors with $i \geq s$. Therefore the point $P_n^{(n-s)}$ is now a generator of order ℓ^s of the ℓ-Sylow subgroup of $E^{(n-s)}$. A $\mathbb{Z}/\ell^r\mathbb{Z}$ component of the ℓ-Sylow subgroup is obtained with the ℓ^i-divisors of the point $P_n^{(n-s)} + kQ_s^{(n-s)}$. By Lemma 2, the isogeny $\mathcal{I}_{n-s+1}$ defined by the quotient by $\langle P_{n-s+1}^{(n-s)} \rangle$ is either horizontal or descending and by Corollary 7 the isogeny is descending. By Lemma 2, the following isogenies are descending and since we have $s-1$ left, the last curve is at the floor of the volcano.

At last, we treat the case $r = s + 1$. The isogeny $\mathcal{I}_{s+1}$ is the quotient of $E^{(s)}$ by $\langle \ell^{r-1} P_n^{(s)} \rangle$. Therefore $\mathcal{I}_{s+1}(P_n^{(s)})$ is of order ℓ^{r-1}, $r-1 = s$, and $\mathcal{I}_{s+1}(Q_s^{(s)})$ is of order ℓ^s. Here, we can have either, like the precedent case, a point $\mathcal{I}_{s+1}(P_n^{(s)} + kQ_s^{(s)})$ that ℓ-divides in $E^{(s+1)}$ or the point $\mathcal{I}_{s+1}(Q_s^{(s)})$ that ℓ-divides in $E^{(s+1)}$. By a similar argument as the previous one, the following isogenies are descending until the floor of the volcano.

The same method given in Theorem 8 works when considering an elliptic curve $E/\mathbb{F}_q$ located in a level higher than the floor and lower than the stability level, in the sense that the ℓ-isogeny chain obtained is ascending from $E/\mathbb{F}_q$ to the stability level and descending to the floor.

3.3 An Example

Now we show an example of ℓ-isogeny chain starting from a curve at the floor of the volcano determined by the kernels of the successive images of the points in the ℓ-Sylow subgroup of the initial curve.

Let us consider the curve over the field $\mathbb{F}_p$, $p = 10009$, given by the equation

$$E/\mathbb{F}_p : \; y^2 = x^3 + 8569x + 2880,$$

whose 3-Sylow subgroup is cyclic isomorphic to $\mathbb{Z}/3^5\mathbb{Z}$ generated by the point $P_5 = (9137, 1237)$. Then, the chain of 3-isogenies determined by this point is given by

$$\begin{array}{ccccccccccc} 996 & \to & 8798 & \to & 8077 & \to & 2631 & \to & 3527 & \to & 8123 \\ (5,0) & & (4,1) & & (3,2) & & (3,2) & & (4,1) & & (5,0) \end{array}$$

where we give the curves by their j-invariants ($j(E) = 996$) and we put in brackets the integers (r, s) which determine the structure $\mathbb{Z}/3^r\mathbb{Z} \times \mathbb{Z}/3^s\mathbb{Z}$ of the 3-Sylow subgroups of the curves.

The corresponding sequence of the generators $\langle P, Q \rangle$ of the 3-Sylow subgroups, together with the integers (r, s) of the structure $\mathbb{Z}/3^r\mathbb{Z} \times \mathbb{Z}/3^s\mathbb{Z}$ and the point determining the kernel of the isogeny is:

$$\begin{array}{ccccccc} \langle P_5 \rangle & \to & \langle P_5^{(1)},\, Q_1^{(1)} \rangle & \to & \langle P_5^{(2)},\, Q_2^{(2)} \rangle & \to & \\ (5,0)\ 3^4 P_5 & & (4,1) & & 3^3 P_5^{(1)} \quad (3,2) & & 3^2 P_5^{(2)} \end{array}$$

$$\begin{array}{ccccccc} \langle Q_3^{(3)},\, P_5^{(3)} \rangle & \to & \langle Q_4^{(4)},\, P_5^{(4)} \rangle & \to & \langle Q_5^{(5)} \rangle \\ (3,2) \quad 3P_5^{(3)} & & (4,1) \quad P_5^{(4)} & & (5,0) \end{array}$$

4 Going Around the Crater

In this section we give an application of the ℓ-isogeny chains introduced in the previous section. More precisely, given a regular volcano of ℓ-isogenies $V_\ell(E/\mathbb{F}_q)$ with height $h \geq 1$ satisfying $2h < v_\ell(\#E(\mathbb{F}_q))$ and whose crater has length $c > 2$, we present an algorithm to walk around the vertices of its crater. In

order to do this we make use of the horizontal ℓ-isogenies of our particular chains. Throughout this section we suppose that the craters of the volcanoes have lengths > 2.

Proposition 9 *Let $E/\mathbb{F}_q$ be an elliptic curve whose ℓ-Sylow subgroup is isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$ with $r > s > 0$ located in the crater of $V_\ell(E/\mathbb{F}_q)$. Let $E[\ell^\infty](\mathbb{F}_q) = \langle P, Q\rangle$ with $|P| = \ell^r$ and $|Q| = \ell^s$. Let $\mathcal{I}_1 \colon E \to E'$ be the ℓ-isogeny of kernel $\langle \ell^{r-1}P\rangle$ which is horizontal from Lemma 2.iii). Let $\mathcal{I}_2 \colon E \to E''$ be the other horizontal ℓ-isogeny of E. Then the dual ℓ-isogeny $\hat{\mathcal{I}}_2 \colon E'' \to E$ has kernel $\langle \ell^{r-1}\mathcal{I}_2(P)\rangle$ with $|\mathcal{I}_2(P)| = \ell^r$.*

Proof. The kernel of $\mathcal{I}_2$ is $\langle \ell^{s-1}Q + k\ell^{r-1}P\rangle$ for some $k \in \{0, \ldots, \ell - 1\}$. From Lemma 5 the kernel of $\hat{\mathcal{I}}_2$ is $\langle \ell^{r-1}\mathcal{I}_2(P)\rangle$. Note that $\mathcal{I}_2(P)$ has order ℓ^r. Indeed, if $|\mathcal{I}_2(P)| < \ell^r$, then $\mathcal{I}_2(\ell^{r-1}P) = O_{E''}$. Hence $\ell^{r-1}P \in \ker \mathcal{I}_2 = \langle \ell^{s-1}Q + k\ell^{r-1}P\rangle$, which is a contradiction.

Corollary 10 *Let $E_0 \xrightarrow{\mathcal{I}_0} E_1 \xrightarrow{\mathcal{I}_1} \cdots \xrightarrow{\mathcal{I}_{c-2}} E_{c-1} \xrightarrow{\mathcal{I}_{c-1}} E_0$ be the cycle of ℓ-isogenies of the crater of $V_\ell(E_0/\mathbb{F}_q)$. For all $i \in \{0, 1, \ldots, c-1\}$, let $E_i[\ell^\infty](\mathbb{F}_q) = \langle P_i, Q_i\rangle$ such that $|P_i| = \ell^r$ and $|Q_i| = \ell^s$ with $r > s > 0$. Then either, $\forall i \in \{0, 1, \ldots, c-1\}$, $\langle \ell^{r-1}P_i\rangle$ is the kernel of $\mathcal{I}_i$ or, $\forall i \in \{0, 1, \ldots, c-1\}$, $\langle \ell^{r-1}P_i\rangle$ is the kernel of $\hat{\mathcal{I}}_{(i-1) \bmod c}$.*

As a consequence of Corollary 10 we can obtain, by using succesive ℓ-isogeny chains, all vertices of the crater of $V_\ell(E/\mathbb{F}_q)$, since the horizontal ℓ-isogenies of the chains all go in the same direction (see Figure 1). This idea is implemented in Algorithm 1.

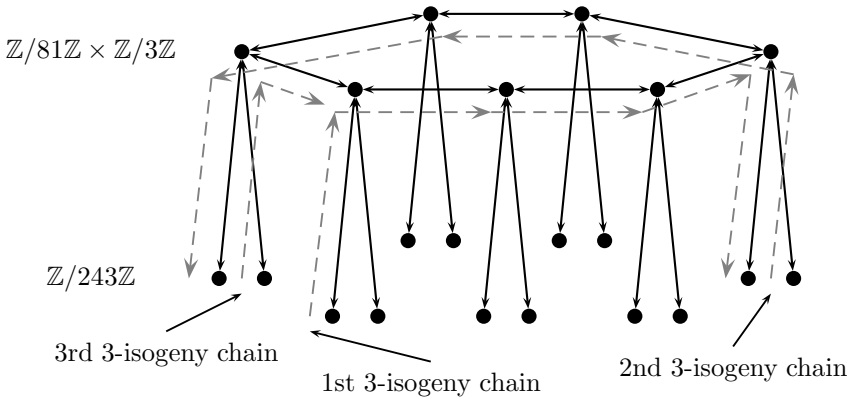

Fig. 1. Going around the crater by using 3-isogeny chains.

In order to study the cost of Algorithm 1 we need first to know the suitable number of chains to go around all the vertices in the crater. Knowing the

Algorithm 1 $\textsc{Crater}(E, \ell, n, h) \longrightarrow S$

Input: An ordinary elliptic curve E over $\mathbb{F}_q$ such that $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^n\mathbb{Z}$ and the height h of $V_\ell(E/\mathbb{F}_q)$ is greater than 0 and $2h < n$.
Output: A sequence S containing an elliptic curve of each vertex of the crater of $V_\ell(E/\mathbb{F}_q)$.

```
S ← [ ];
Compute a point P ∈ E(F_q) of order ℓ^n;
Compute the ℓ^h-isogeny I: E → E' of kernel ⟨ℓ^{n−h} P⟩;
E ← E';   P ← I(P);   E_final ← E;
repeat
   i ← n − h;
   repeat
      i ← i − 1;
      Compute the ℓ-isogeny I: E → E' of kernel ⟨ℓ^i P⟩;
      E ← E';   P ← I(P);   S[#S + 1] ← E;
      final ← E ≃ E_final;
   until final ∨ i = h;
   if ¬final then
      Compute the ℓ^h-isogeny I: E → E' of kernel ⟨P⟩;
      Compute a point P' ∈ E'(F_q) of order ℓ^n;
      Compute the ℓ^h-isogeny I': E' → E'' of kernel ⟨ℓ^{n−h} P'⟩;
      E ← E'';   P ← I'(P');
   end if
until final;
return S;
```

parameters of the Algorithm 1 and assuming the length of the crater is c, the number of ℓ-isogeny chains required is $k = \left\lceil \frac{c}{n-2h} \right\rceil$. Indeed, since by the second part of Theorem 8 each of our ℓ-isogeny chains has $n-2h$ horizontal ℓ-isogenies, we can go around all the curves on the crater by using k ℓ-isogeny chains. More precisely, starting in a curve on the floor of the volcano we ascend up to the crater and we walk through $n-2h$ curves of the crater to descend again to the floor and we repeat the same process. From Corollary 10 we always take the same direction.

Thus, the cost of Algorithm 1 is given by $k(C_1 + n(C_2 + C_3))$ where C_1 is the cost to find a point of order ℓ^n, C_2 is the cost to compute an ℓ-isogeny using Vélu's formulae [21], and C_3 is the cost to compute the image of a given point under an ℓ-isogeny.

The cost C_1 of finding a point of order ℓ^n, assuming $\ell \ll \log q$ and the Extended Riemann Hypothesis, is $O(nM(\ell)\,\log\,q)$ with $M(\ell) = \ell \log \ell \log\log \ell$. Indeed, according to [14] it corresponds to compute a root of a polynomial of degree ℓ in $\mathbb{F}_q[x]$, which has cost $O(M(\ell)\log q)$, a total of $2n$ times. If we suppose known the cardinality of the elliptic curve, using the Algorithm 1 of [7], we have $C_1 = O(\log q)$. The cost C_2 of computing an ℓ-isogeny using Vélu's formulae is $O(\ell)$. Finally, by [5], the cost C_3 of evaluating a given point under an ℓ-isogeny

is $O(\ell)$. Therefore, the total cost is either $O(knM(\ell)\log q)$ or $O(k\log q)$ whether the cardinality is unknown or not.

In Table 1 we give the costs to go around all the vertices in the crater of a volcano of ℓ-isogenies using the proposed procedure by Ionica and Joux [7] and using our Algorithm 1 assuming the cardinality is known. Notice that while Ionica-Joux's algorithm computes ℓ-Sylow subgroups for each curve on the crater, our proposal computes $k = \left\lceil \frac{c}{n-2h} \right\rceil$ ℓ-Sylow subgroups of curves on the floor.

Table 1. Different costs with known cardinality.

Case	Ionica-Joux	Our Proposal
Regular: $2h < n$	$O(c\log q)$	$O(\left\lceil \frac{c}{n-2h} \right\rceil \log q)$
Regular: $2h = n$	$O(c\log q)$	—

The Algorithm 1 has been implemented with MAGMA V2.10-8. It has been tested with several elliptic curves over $\mathbb{F}_q$ over an Intel Pentium M with 1.73 GHz. In Table 2 we give a sample of them including information about their volcanoes of ℓ-isogenies and timings. In the second and third columns of the table we have denoted by a and b the coefficients of the elliptic curve with equation $y^2 = x^3 + ax + b$. In the eighth and ninth columns we provide the timings t_1 and t_2 (in seconds) corresponding to our implementation of Algorithm 1 assuming the cardinality is known or not.

Table 2. Some timings about several volcanoes of ℓ-isogenies.

$q = p$	a	b	ℓ	n	h	c	t_1	t_2
15559	4188	7183	3	4	1	40	0.07	0.02
10000000141	7034565020	8371535734	3	6	1	5612	64.99	13.83
1000000001773	464414175298	982044907463	3	7	2	37906	1955.42	979.54
10000000061	5760822374	8478355374	5	4	1	4982	196.90	15.54
10000000061	4382731032	4661390138	5	5	1	5153	134.63	13.35
1000000011151	875978249672	248043522958	5	6	2	11310	506.98	104.69
1000000000063	676232083726	397006774798	7	5	1	3486	151.98	6.61
100000231	58130720	83739022	11	5	1	190	0.83	0.09

Acknowledgments. The authors thank the reviewers for their valuable comments and specially Sorina Ionica for her suggestions which have improved this article. Research of the second and third authors was supported in part by grants MTM2013-46949-P (Spanish MINECO) and 2014 SGR1666 (Generalitat de Catalunya).

References

1. G. Bisson and A.V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field, *J. Number Theory* 131, no. 5, 815-831, 2011.
2. R. Bröker, K. Lauter, and A.V. Sutherland. Modular polynomials via isogeny volcanoes, *Math. Comp.* 81, no. 278, 1201-1231, 2012.
3. J.M. Couveignes, L. Dewaghe, and F. Morain. *Schoof's algorithm and isogeny cycles*, ANTS-I, LNCS 877, 43-58, 1994.
4. D.A. Cox. *Primes of the form* $x^2 + ny^2$, Wiley-Interscience, 1989.
5. C. Doche, T. Icart, and D. Kohel. *Efficient scalar multiplication by isogeny decompositions*, PKC 2006, LNCS 3958, 191-206, 2006.
6. M. Fouquet and F. Morain. *Isogeny volcanoes and the SEA algorithm*, ANTS-V, LNCS 2369, 276-291, 2002.
7. S. Ionica and A. Joux. Pairing the volcano, *Math. Comp.* 82, no. 281, 581-603, 2013.
8. A. Joux and K. Nguyen. Separating decision Diffie-Hellman from computational Diffie-Hellman in cryptographic groups, *J. Cryptology* 16, no. 4, 239-247, 2003.
9. D. Kohel. *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California, Berkeley, 1996.
10. R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis*, Ph.D. thesis, École Polytechnique, Paris, 1997.
11. H.W. Lenstra Jr. Complex multiplication structure of elliptic curves, *J. Number Theory* 56, no. 2, 227-241, 1996.
12. A. Menezes, T. Okamoto, and S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39, 1639-1646, 1993.
13. J. Miret, R. Moreno, and A. Rio. Generalization of Vélu's formulae for isogenies between elliptic curves, *Publicacions Matemàtiques*, 147-163, 2007.
14. J. Miret, R. Moreno, A. Rio, and M. Valls. Computing the ℓ-power torsion of an elliptic curve over a finite field, *Math. Comp.* 78, no. 267, 1767-1786, 2009.
15. 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, *Appl. Math. Comput.* 196, no. 1, 67-76, 2008.
16. J. Miret, D. Sadornil, J. Tena, R. Tomàs, and M. Valls. *On avoiding ZVP-attacks using isogeny volcanoes*, WISA 2008, LNCS 5379, 266-277, 2009.
17. S. Pohlig and M. Hellman. An improved algorithm for computing algorithms over $GF(p)$ and its cryptographyc significance, *IEEE Transactions on Information Theory*, 24, 106-110, 1978.
18. R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux* 7, no. 1, 219-254, 1995.
19. J.H. Silverman. *The arithmetic of elliptic curves*, Graduate Texts in Mathemathics 106, Springer-Verlag, 1986.
20. A.V. Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem, *Math. Comp.* 80, no. 273, 501-538, 2011.
21. J. Vélu. Isogenies entre courbes elliptiques. *Comptes Rendus De L'Academie Des Sciences Paris, Serie I-Mathematique, Serie A*, 273, 238-241, 1971.