Breaking the decisional Diffie-Hellman problem for class group actions using genus theory

Wouter Castryck[1], Jana Sotáková[2], and Frederik Vercauteren[1]

wouter.castryck@esat.kuleuven.be, j.s.sotakova@uva.nl,
frederik.vercauteren@kuleuven.be

[1] COSIC, research group at imec and KU Leuven, Belgium
[2] QuSoft/University of Amsterdam, The Netherlands

Abstract. In this paper, we use genus theory to analyze the hardness of the decisional Diffie–Hellman problem (DDH) for ideal class groups of imaginary quadratic orders, acting on sets of elliptic curves through isogenies; such actions are used in the Couveignes–Rostovtsev–Stolbunov protocol and in CSIDH. Concretely, genus theory equips every imaginary quadratic order $\mathcal{O}$ with a set of assigned characters $\chi : \mathrm{cl}(\mathcal{O}) \to \{\pm 1\}$, and for each such character and every secret ideal class $[\mathfrak{a}]$ connecting two public elliptic curves E and $E' = [\mathfrak{a}] \star E$, we show how to compute $\chi([\mathfrak{a}])$ given only E and E', i.e. without knowledge of $[\mathfrak{a}]$. In practice, this breaks DDH as soon as the class number is even, which is true for a density 1 subset of all imaginary quadratic orders. For instance, our attack works very efficiently for all supersingular elliptic curves over $\mathbb{F}_p$ with $p \equiv 1 \bmod 4$. Our method relies on computing Tate pairings and walking down isogeny volcanoes.

Keywords: Decisional Diffie-Hellman, isogeny-based cryptography, class group action, CSIDH.

1 Introduction

"The Decision Diffie–Hellman assumption (DDH) is a gold mine", Dan Boneh wrote in his 1998 overview paper [3]. This statement still holds true (maybe even more so), since DDH is fundamental to prove security of many widely used protocols such as Diffie–Hellman key agreement [17], El Gamal encryption [19], but can also be used to construct pseudo-random functions [25], and more advanced functionalities such as circular-secure encryption [4] and UC-secure oblivious transfer [26].

Let $(G, \cdot)$ be a finite cyclic group with generator g, then the DDH problem states that it is hard to distinguish the distributions (g^a, g^b, g^{ab}) and (g^a, g^b, g^r)

* This work was supported in part by the Research Council KU Leuven grants C14/18/067 and STG/17/019, and by CyberSecurity Research Flanders with reference number VR20192203. JS was supported by the Dutch Research Council (NWO) through Gravitation-grant Quantum Software Consortium - 024.003.037. Date of this document: 8th March 2020.

where a, b, r are chosen randomly in $[1, \#G]$. Due to its very definition as a distinguishing problem, DDH can be used quite naturally as a building block for provably secure constructions, i.e. IND-CPA or IND-CCA encryption [12]. In practice, the group G is typically chosen as a cyclic prime order subgroup of a finite field $\mathbb{F}_p^*$ or of an elliptic curve group $E(\mathbb{F}_q)$. Although Diffie and Hellman [17] originally worked in the full multiplicative group $\mathbb{F}_p^*$, it is easy to see that DDH is not secure in this case since the Legendre symbol easily distinguishes both distributions. An equivalent interpretation is that the Legendre symbol provides an efficiently computable character, mapping $\mathbb{F}_p^*$ onto the group $\{\pm 1\}$, which acts as a distinguisher.

The classical hardness of DDH is well understood and clear recommendations [13] to attain certain security levels have been agreed upon by the cryptographic community. In the quantum setting however, DDH is easy as shown by Shor [29], who devised an algorithm to solve the discrete logarithm problem (DLP) in any group in polynomial time and space. The DLP asks, given a tuple (g, g^a), to recover the exponent a. Solving DLP efficiently implies solving DDH efficiently.

Class group actions Shor's algorithm relies on the fact that the group operation in G can be efficiently computed, and thus a priori, that it is computable. To devise a post-quantum secure alternative for group-based DDH one could try to represent the group G by an object with much less inherent structure, e.g. a set X. Such a representation can be obtained from a group action, which is a map $\star : G \times X \to X : (g, E) \mapsto g \star E$ compatible with the group operation, i.e. $(g \cdot h) \star E = g \star (h \star E)$. If the group action is free and transitive, i.e. for every $E, E' \in X$ there exists exactly one $g \in G$ such that $E' = g \star E$, then X is called a principal homogeneous space for G. Note that for every fixed base point $E \in X$ we thus obtain a representation of the group G by mapping g to $g \star E$.

As first observed by Couveignes [10] and later independently by Rostovtsev and Stolbunov [27], generalizing the Diffie–Hellman key agreement to group actions is immediate: Alice and Bob agree on a base point $E \in X$, each choose a secret element a and b in G, and exchange $a \star E$ and $b \star E$. Since G is commutative and $\star$ a group action, both can compute the common element $(a \cdot b) \star E$. Recovering $a \in G$ from $a \star E$ is called the vectorization problem (generalizing DLP), and recovering $(a \cdot b) \star E$ from $a \star E$ and $b \star E$ is called parallelization (generalizing CDH). When both problems are hard, Couveignes called X a hard homogeneous space for G. Couveignes, Rostovtsev and Stolbunov (CRS) and more recently CSIDH [8] by Castryck, Lange, Martindale, Panny and Renes instantiated this framework as follows: G is the class group $\mathrm{cl}(\mathcal{O})$ of an order $\mathcal{O}$ in an imaginary quadratic field, and $X = \mathcal{E}\ell\ell_p(\mathcal{O}, t)$ is the set of elliptic curves over a finite prime field $\mathbb{F}_p$ with $\mathbb{F}_p$-rational endomorphism ring $\mathcal{O}$ and trace of Frobenius t. Whereas CRS restricted to ordinary elliptic curves, CSIDH uses supersingular elliptic curves and is several orders of magnitude faster than CRS.

Using the above group action can be seen as a trade-off: the lack of a natural operation on the set X itself makes the construction possibly post-quantum

secure, but also limits its flexibility, i.e. it is not possible to simply translate any DLP-based protocol into an equivalent one using group actions. Furthermore, since X is supposed to "hide" G, it is generally assumed that the group structure of G itself has little influence on the hardness of the underlying group action problems. In this paper, we disprove this assumption.

Contributions The decisional Diffie-Hellman problem (sometimes called decisional parallelization) for class group actions asks to distinguish between the distributions $([\mathfrak{a}]\star E, [\mathfrak{b}]\star E, ([\mathfrak{a}]\cdot[\mathfrak{b}])\star E)$ and $([\mathfrak{a}]\star E, [\mathfrak{b}]\star E, [\mathfrak{r}]\star E)$ with $[\mathfrak{a}], [\mathfrak{b}], [\mathfrak{r}]$ random elements in $\mathrm{cl}(\mathcal{O})$. A natural attack strategy would be to try to exploit the group structure of $\mathrm{cl}(\mathcal{O})$, as was done for DDH in $\mathbb{F}_p^*$ using the Legendre symbol. We immediately run into two problems:

1. In general, very little is known about the concrete structure of $\mathrm{cl}(\mathcal{O})$ as an abelian group. For instance, computing the order of $\mathrm{cl}(\mathcal{O})$ is already a highly non-trivial task [20, 1]. A notable exception is the structure of the 2-torsion subgroup of $\mathrm{cl}(\mathcal{O})$: genus theory [11, I.§3 & II.§7] provides a very explicit description of $\mathrm{cl}(\mathcal{O})[2] \simeq \mathrm{cl}(\mathcal{O})/\mathrm{cl}(\mathcal{O})^2$ by defining a set of characters $\chi_i : \mathrm{cl}(\mathcal{O}) \to \{\pm 1\}$ and recovering $\mathrm{cl}(\mathcal{O})^2$ as the intersection of the kernels of the χ_i. The characters χ_i correspond to the prime factors m_i of the discriminant $\Delta_\mathcal{O}$ (with the prime 2 requiring special treatment) and can be computed in time polynomial in the size of m_i. Note that each of these characters χ_i (if non-trivial) can be used to break DDH in $\mathrm{cl}(\mathcal{O})$ itself; however we are not trying to solve DDH in $\mathrm{cl}(\mathcal{O})$, but DDH for class group *actions*.
2. Given the structure of $\mathrm{cl}(\mathcal{O})[2]$ through genus theory, it is unclear how the characters χ_i can be computed directly on elements in X, i.e. given an element $[\mathfrak{a}] \star E$ for some unknown $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$, we need to compute $\chi_i([\mathfrak{a}])$ (without computing $[\mathfrak{a}]$ first, since vectorization is assumed hard).

The main contribution of this paper is an algorithm to compute the characters χ_i directly on the set $X = \mathcal{E}\ell\ell_p(\mathcal{O}, t)$ in time exponential in the size of m_i. Since we only need to compute one such χ_i efficiently to break DDH, we conclude that DDH for class group actions is insecure when $\mathrm{cl}(\mathcal{O})[2]$ is non-trivial and the discriminant $\Delta_\mathcal{O}$ is divisible by a small enough prime factor. Since $\mathrm{cl}(\mathcal{O})[2]$ is only trivial when $\Delta_\mathcal{O} = -q$ or $\Delta_\mathcal{O} = -4q$ with $q \equiv 3 \bmod 4$ prime, and since almost all integers contain polynomially small prime factors (this follows, at least heuristically, from Mertens' third theorem; see [33, III.§6] for more precise statements), we expect that our attack works in polynomial time (in $\log p$) for a subset of density 1 of all imaginary quadratic orders.

In the special case of supersingular elliptic curves over $\mathbb{F}_p$, our attack does not apply for primes $p \equiv 3 \pmod 4$. However, for $p \equiv 1 \pmod 4$, we have $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ and $\Delta_\mathcal{O} = -4p$. Genus theory defines a non-trivial character δ associated with the prime divisor 2 of $\Delta_\mathcal{O}$. We derive a very simple formula to compute $\delta([\mathfrak{a}])$ that uses only the Weierstrass equations of E and $E' = [\mathfrak{a}] \star E$. In this case, our attack is particularly efficient and we can break DDH using a few exponentiations in $\mathbb{F}_p$.

High level overview of the attack To explain the main underlying ideas, we detail the thought process we followed to derive the attack in a simple (yet very general) setting. Fixing a base curve E, the class group action $\star$ gives us a representation of $\mathrm{cl}(\mathcal{O})$ on the set $X = \mathcal{E}\ell\ell_p(\mathcal{O}, t)$ by mapping a class $[\mathfrak{a}]$ to $E' = [\mathfrak{a}]\star E$. For every odd prime divisor m of the discriminant $\Delta_{\mathcal{O}}$, genus theory provides a character

$$\chi : \mathrm{cl}(\mathcal{O}) \to \{\pm 1\} : [\mathfrak{a}] \mapsto \left(\frac{\mathrm{N}(\mathfrak{a})}{m}\right),$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol and the representative $\mathfrak{a}$ of the class $[\mathfrak{a}]$ is chosen such that its norm $\mathrm{N}(\mathfrak{a})$ is coprime to m. The goal is to compute $\chi([\mathfrak{a}])$ given only the pair (E, E').

Let $\varphi : E \to E'$ denote the isogeny corresponding to $\mathfrak{a}$, then $\mathrm{N}(\mathfrak{a}) = \deg(\varphi)$, so to compute χ, it suffices to determine $\deg(\varphi) \bmod m$, up to non-zero squares in $\mathbb{Z}/(m)$. The starting idea is the following: assume we know a tuple $(P, Q) \in E^2$ and the corresponding tuple $(\varphi(P), \varphi(Q)) \in E'^2$, computing $\deg(\varphi) \bmod m$ is easy thanks to the compatibility of the reduced m-Tate pairing T_m

$$T_m(\varphi(P), \varphi(Q)) = T_m(P, Q)^{\deg(\varphi)}.$$

If the pairing is non-trivial, both sides will be primitive m-th roots of unity, so computing discrete logs gives $\deg(\varphi) \bmod m$.

The difficulty is of course, that in practice we are not given such corresponding tuples (P, Q) and $(\varphi(P), \varphi(Q))$, so we need to find a workaround. The only information we really have about φ is that it is an $\mathbb{F}_p$-rational isogeny of degree coprime to m. Under the assumption that $E(\mathbb{F}_p)$ has a *unique* subgroup of order m, this implies that $E'(\mathbb{F}_p)$ similarly has such a unique subgroup, and furthermore, $\varphi(E(\mathbb{F}_p)[m]) = E'(\mathbb{F}_p)[m]$. If we let P be a generator of $E(\mathbb{F}_p)[m]$ and P' a generator of $E'(\mathbb{F}_p)[m]$, then we know there exists some $k \in [1, m-1]$ such that $\varphi(P) = kP'$. Note however, that if we assume we know a point Q and its image $\varphi(Q)$ (but not the image of P under φ), we do not learn anything since the values $T_m(kP', \varphi(Q)) = T_m(P', \varphi(Q))^k$ run through the whole of μ_m for $k = 1, \ldots, m-1$ and we do not know k.

The main insight now is that we do not need to recover $\deg(\varphi)$ exactly but only up to squares, so if we could recover $k^2 \deg(\varphi)$ then it is clear we can still compute $\chi([\mathfrak{a}])$. This hints at a possible solution as long as Q is somehow derived from P and that the *same* unknown scalar k can be used to compensate for the difference not only between $\varphi(P)$ and P', but also between $\varphi(Q)$ and Q'. Indeed, computing $T_m(P', Q')$ would then recover the correct value up to a square in the exponent, namely $T_m(P, Q)^{\deg(\varphi)k^2}$. The simplest choice clearly is to take $Q = P$ and $Q' = P'$, and if there is no $\mathbb{F}_p$-rational m^2-torsion, we can show that the self-pairings $T_m(P, P)$ and $T_m(P', P')$ are non-trivial. This feature is specific to the Tate pairing, and resorting to the Weil pairing would fail. Denote with $\mathrm{val}_m(N)$ the m-adic valuation of N, i.e. the maximum power v such that $m^v \mid N$, then $\mathrm{val}_m(\#E(\mathbb{F}_p)) = 1$ is equivalent to the existence of a unique rational subgroup of order m and the non-existence of rational m^2-torsion.

In the more general case of $v = \mathrm{val}_m(\#E(\mathbb{F}_p)) > 1$, we first walk down to the floor of the m-isogeny volcano reaching a curve E_0 with $E_0(\mathbb{F}_q)[m^\infty] = \mathbb{Z}/(m^v)$, and then choose points P and P' of order m and corresponding points Q and Q' of order m^v satisfying $m^{v-1}Q = P$ and $m^{v-1}Q' = P'$. Note that also in this case, the same unknown scalar k will compensate for both differences.

To sum up, we use the Tate pairing of certain points to obtain information on $\deg \varphi$ (up to squares $\bmod m$). By genus theory, we see that we are actually computing the assigned characters of $\mathrm{cl}(\mathcal{O})$ directly from curves in $\mathcal{E}\ell\ell_p(\mathcal{O}, t)$. Whenever the characters are non-trivial, their multiplicative property allows us to break DDH in $\mathcal{E}\ell\ell_p(\mathcal{O}, t)$.

Paper organization In Section 2 we recall the necessary background on isogenies and isogeny volcanoes, class group actions, genus theory and the Tate pairing. In Section 3 we derive an algorithm to compute the assigned characters in the case of ordinary elliptic curves, whereas in Section 4 we deal with supersingular curves. In Section 5 we analyze the impact on the DDH problem for class group actions, report on our implementation of the attack, and propose countermeasures. Finally, Section 6 concludes the paper and provides avenues for further research.

Acknowledgements The authors would like to thank Steven Galbraith for useful feedback on an earlier version of the paper.

2 Background

2.1 Isogenies

Let $E, E'/\mathbb{F}_q$ be elliptic curves. An *isogeny* $\varphi : E \to E'$ is a non-constant morphism such that $\varphi(\mathbf{0}_E) = \mathbf{0}_{E'}$, where $\mathbf{0}$ denotes the point at infinity. Equivalently, an isogeny is a surjective group homomorphism of elliptic curves, which is also an algebraic morphism. An *endomorphism* of E is either the zero map or an isogeny from E to itself, and the set of endomorphisms forms a ring $\mathrm{End}(E)$ under addition and composition. We write $\mathrm{End}_{\mathbb{F}_q}(E)$ to denote the subring of endomorphisms defined over $\mathbb{F}_q$. Two important examples of endomorphisms are: the multiplication-by-n map $[n] : E \to E, P \mapsto [n]P$ (often simply denoted by n) and the q-power Frobenius endomorphism $\pi_q : E \to E : (x, y) \mapsto (x^q, y^q)$. If q is clear from the context, we will simply write π. In $\mathrm{End}(E)$, the Frobenius endomorphism satisfies $\pi^2 - t\pi + q = 0$ where $t = \mathrm{tr}\,\pi$ is called the *trace of Frobenius* and satisfies $|t| \leq 2\sqrt{q}$. Alternatively, the trace of Frobenius is characterized by $\#E(\mathbb{F}_q) = q + 1 - t$. If $\gcd(t, q) = 1$, the curve is called ordinary, otherwise it is called supersingular. Unless $|t| = 2\sqrt{q}$, which can only happen for supersingular elliptic curves over even degree extension fields, we have that $\mathcal{O} = \mathrm{End}_{\mathbb{F}_q}(E)$ is an order in the imaginary quadratic field $K = \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{t^2 - 4q})$. Since $\mathcal{O}$ always contains $\mathbb{Z}[\pi]$ as a suborder, its discriminant $\Delta_\mathcal{O}$ satisfies $\Delta_{\mathbb{Z}[\pi]} = t^2 - 4q = c^2\Delta_\mathcal{O}$ for some non-zero $c \in \mathbb{Z}$.

The degree of an isogeny φ is just its degree as a morphism, which equals the size of the kernel $\ker(\varphi)$ (we say φ is a *separable* isogeny) unless $\mathrm{char}(\mathbb{F}_q) | \deg(\varphi)$ (we say φ is an *inseparable* isogeny). Separable isogenies can always be reconstructed from their kernel. When the kernel $\ker(\varphi)$ is invariant under Frobenius (as a set), the corresponding isogeny φ is $\mathbb{F}_q$-rational. Note that we do not necessarily have $\ker(\varphi) \subset E(\mathbb{F}_q)$, but only that φ can be given by $\mathbb{F}_q$-rational maps. The kernel of the multiplication by n map is denoted as $E[n]$, and we set $E[n^\infty] = \cup_{k \in \mathbb{N}_{>0}} E[n^k]$.

For a prime $m \nmid \mathrm{char}\, \mathbb{F}_q$, isogenies of degree m are called *m-isogenies* and their kernel $\ker \varphi \subset E[m]$ is always a cyclic subgroup of $E[m]$. It is therefore natural that the m-isogenies of an elliptic curve E depend on the structure of $E(\mathbb{F}_q)[m^\infty]$. Moreover, for any isogeny $\varphi : E \to E'$, there is a *dual isogeny* $\hat{\varphi} : E' \to E$ satisfying $\varphi \circ \hat{\varphi} = [\deg \varphi]$ and $\hat{\varphi} \circ \varphi = [\deg \varphi]$. Since $\deg[n] = n^2$ for any $n \in \mathbb{Z}_{>0}$, the dual isogeny $\hat{\varphi}$ has the same degree as φ.

2.2 Volcanoes

By Tate's theorem [32], two elliptic curves over $\mathbb{F}_q$ are isogenous (over $\mathbb{F}_q$) if and only if they have the same number of $\mathbb{F}_q$-rational points, which is equivalent to having the same trace of Frobenius. Let $\mathcal{E}\ell\ell_q(t)$ be the set of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ with trace of Frobenius t, and assume that $\mathcal{E}\ell\ell_q(t)$ is non-empty.

For a prime number $m \nmid q$, we define the *m-isogeny graph* $G_{q,m}(t)$ as follows: the set of vertices is $\mathcal{E}\ell\ell_q(t)$ and the edges are m-isogenies. Away from elliptic curves with extra automorphisms (i.e., away from the curves with j-invariant 0 or 1728), this graph can be made undirected by identifying dual isogenies.

An *m-volcano* is a connected undirected graph with vertices partitioned into levels $V_0, \ldots, V_h$ such that

- the subgraph V_h (the *crater*) is a regular connected graph of degree ≤ 2,
- for all $0 \leq i < h$, every vertex in level V_i is connected to exactly one vertex in V_{i+1},
- for all $i > 0$, every vertex in V_i has degree $m + 1$.

Note that this implies that all the vertices on level V_0 (*the floor*) have degree 1. We call h the *height* of the volcano (some authors swap V_h and V_0 and call h the depth). The crater V_h is also sometimes called the surface of the volcano. An example of a volcano can be seen in Figure 1.

Theorem 1. *Let $G_{q,m}(t)$ be as above, and assume that $\gcd(t, q) = 1$, so that we are in the ordinary case. Take any connected component V of $G_{q,m}(t)$ that does not contain curves with j-invariant 0 or 1728. Then V is a volcano, say of height h, and*

1. *the elliptic curves on level i all have the same endomorphism ring $\mathcal{O}_i$, with discriminant $\Delta_{\mathcal{O}_i} = m^{2i} \Delta_{\mathcal{O}_h}$,*

2. *the endomorphism ring* $\mathcal{O}_h$ *of the elliptic curves on the surface* V_h *is locally maximal at* m*; equivalently, if* m *is odd then* $m^2 \nmid \Delta_{\mathcal{O}_h}$*, while if* $m = 2$ *and* $4 \mid \Delta_{\mathcal{O}_h}$ *then* $\Delta_{\mathcal{O}_h}/4 \equiv 2, 3 \bmod 4$*,*
3. *the endomorphism ring* $\mathcal{O}_0$ *of the elliptic curves on the floor* V_0 *satisfies* $\mathrm{val}_m(\Delta_{\mathcal{O}_0}) = \mathrm{val}_m(t^2 - 4q)$*.*

In particular, if m *is odd then* $h = \lfloor \mathrm{val}_m(t^2 - 4q)/2 \rfloor$*, while if* $m = 2$ *then* h *may be* 1 *less than this value.*

Proof. This follows from Proposition 23 in [22] (note that the name volcano was introduced only later by [18]).

An analogous volcano structure for supersingular curves over $\mathbb{F}_p$ was given in [16], but will not be needed in our discussion of supersingular curves in Section 4.

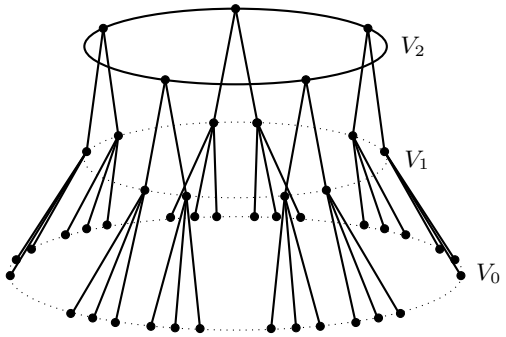

Figure 1. A 3-volcano of height $h = 2$, together with its levels. This corresponds to the case where the prime 3 splits in $\mathcal{O}_h$, into two degree 3 prime ideals whose ideal-classes (which are each other's inverses) have order 5.

Suppose $E \in V_i$ and $E' \in V_j$. We say that an m-isogeny $\varphi : E \to E'$ is *ascending* (*descending*, *horizontal*) if $j = i+1$ ($j = i-1$, $i = j$). On the volcano, this corresponds to the crater being on top, the floor on the bottom, while the only horizontal steps are permitted along the crater.

Remark 2. If $j = 0$ or $j = 1728$ do appear in V, then the theorem remains "sufficiently valid" for our purposes; the only difference is that $G_{q,m}(t)$ may become undirected: there may exist descending isogenies from the crater V_h to level V_{h-1} which need to be considered with multiplicity, while the dual ascending isogeny still accounts for multiplicity 1. We will ignore this issue in what follows. Note that the endomorphism rings of the curves with j-invariant 0 or 1728 have trivial class groups, so this remark only affects suborders of (certain) numbers fields having class number 1. Such suborders are usually not considered in isogeny-based cryptography, although they make an appearance in the recent OSIDH protocol due to Colò and Kohel [9].

2.3 Diffie–Hellman for class group actions

Let $\mathcal{O}$ be an order in an imaginary quadratic number field and let $t \in \mathbb{Z}$. To each prime power $q = p^n$ we associate the set

$$\mathcal{Ell}_q(\mathcal{O}, t) = \{ \text{ elliptic curves } E/\mathbb{F}_q \mid \mathrm{End}_{\mathbb{F}_q}(E) \cong \mathcal{O} \text{ and } \operatorname{tr} \pi_q = t \}/\cong_{\mathbb{F}_q} .$$

If this set is non-empty, then the ideal-class group $\mathrm{cl}(\mathcal{O})$ acts freely on $\mathcal{Ell}_q(\mathcal{O}, t)$: for any ideal $\mathfrak{a} \subset \mathrm{End}_{\mathbb{F}_q}(E)$ of norm coprime with p (every ideal class contains such ideals), we set $E[\mathfrak{a}] = \cap_{\alpha \in \mathfrak{a}} \ker \alpha$ and define

$$[\mathfrak{a}] \star E = E/E[\mathfrak{a}].$$

In other words, we let $[\mathfrak{a}]\star E$ be the (unique) codomain of a separable $\mathbb{F}_q$-rational isogeny φ with domain E and kernel $E[\mathfrak{a}]$.

The action is usually transitive but exceptionally there may be two orbits; this happens if and only if the discriminant $\Delta_{\mathcal{O}}$ is a quadratic non-residue modulo p (which is a very rare event, and not possible in the case of ordinary elliptic curves because $t^2 - 4q = c^2\Delta_{\mathcal{O}}$ for some c). For a proof of the above claims, see [34] and the erratum pointed out in [28, Thm. 4.5].

Remark 3. The set $\mathcal{Ell}_q(t)$ is not the same as $\mathcal{Ell}_q(\mathcal{O}, t)$. One should think of the sets $\mathcal{Ell}_q(\mathcal{O}, t)$ for the various orders $\mathcal{O}$ as horizontal slices of $\mathcal{Ell}_q(t)$. Indeed, in Theorem 1, we saw that the curves on the same level of an m-volcano have the same endomorphism ring $\mathcal{O}$.

When $\#\,\mathrm{cl}(\mathcal{O})$ is large, the set $\mathcal{Ell}_q(\mathcal{O}, t)$ is conjectured to be a hard homogeneous space in the sense of Couveignes [10], who was the first to propose its use for Diffie–Hellman style key exchange; we refer to [15, 8] for recent advances in making this construction efficient. Couveignes' proposal was rediscovered by Rostovtsev and Stolbunov [27], and elaborated in greater detail in Stolbunov's PhD thesis, which contains the first appearance of the decisional Diffie–Hellman problem for group actions [30, Prob. 2.2].

Definition 4 (DDH-CGA). *Let $\mathbb{F}_q, t, \mathcal{O}$ be as above and let $E \in \mathcal{Ell}_q(\mathcal{O}, t)$. The decisional Diffie–Hellman problem is to distinguish with non-negligible advantage between the distributions $([\mathfrak{a}]\star E, [\mathfrak{b}]\star E, [\mathfrak{ab}]\star E)$ and $([\mathfrak{a}]\star E, [\mathfrak{b}]\star E, [\mathfrak{c}]\star E)$ where $[\mathfrak{a}], [\mathfrak{b}], [\mathfrak{c}]$ are chosen at random from $\mathrm{cl}(\mathcal{O})$.*

Stolbunov writes: "As far as we are concerned, the most efficient approach is to solve the corresponding $\mathcal{CL}$ group action inverse problem ($\mathcal{CL}$-GAIP)." In our terminology, this reads that in order to break DDH-CGA, one needs to obtain $[\mathfrak{a}]$ from $[\mathfrak{a}] \star E$. This paper clearly disproves this statement.

2.4 Genus theory

Genus theory studies which natural numbers arise as norms of ideals in a given ideal class of an imaginary quadratic order $\mathcal{O}$. It shows that this question is

governed by the coset of $\mathrm{cl}(\mathcal{O})^2$, the subgroup of squares inside $\mathrm{cl}(\mathcal{O})$, to which the ideal class belongs. The details are as follows; this section summarizes parts of [11, I.§3 & II.§7].

Let $\Delta_\mathcal{O} \equiv 0, 1 \bmod 4$ be the discriminant of $\mathcal{O}$, say with distinct odd prime factors $m_1 < m_2 < \ldots < m_r$. If $\Delta_\mathcal{O} \equiv 1 \bmod 4$ then we call

$$\chi_i : (\mathbb{Z}/\Delta_\mathcal{O})^* \to \{\pm 1\} : a \mapsto \left(\frac{a}{m_i}\right) \qquad (\text{for } i = 1, \ldots, r)$$

the *assigned characters* of $\mathcal{O}$. If $\Delta_\mathcal{O} = -4n \equiv 0 \bmod 4$, then we extend this list with δ if $n \equiv 1, 4, 5 \bmod 8$, with ϵ if $n \equiv 6 \bmod 8$, with $\delta\epsilon$ if $n \equiv 2 \bmod 8$, and with both δ and ϵ if $n \equiv 0 \bmod 8$. Here

$$\delta : a \mapsto (-1)^{(a-1)/2} \qquad \text{and} \qquad \epsilon : a \mapsto (-1)^{(a^2-1)/8}.$$

If $n \equiv 3, 7 \bmod 8$ then the list is not extended.

Let $\mu \in \{r, r+1, r+2\}$ denote the total number of assigned characters and consider the map $\Psi : (\mathbb{Z}/\Delta_\mathcal{O})^* \to \{\pm 1\}^\mu$ having these assigned characters as its components. Then Ψ is surjective and its kernel H consists precisely of those integers that are coprime with (and that are considered modulo) $\Delta_\mathcal{O}$ and arise as norms of non-zero principal ideals of $\mathcal{O}$. This leads to a chain of maps

$$\Phi : \mathrm{cl}(\mathcal{O}) \longrightarrow \frac{(\mathbb{Z}/\Delta_\mathcal{O})^*}{H} \xrightarrow{\cong} \{\pm 1\}^\mu,$$

where the first map sends an ideal class $[\mathfrak{a}]$ to the norm of $\mathfrak{a}$ (it is always possible to choose a representant of norm coprime with $\Delta_\mathcal{O}$) and the second map is induced by Ψ. Basically, genus theory tells us that $\ker \Phi = \mathrm{cl}(\mathcal{O})^2$, the subgroup of squares in $\mathrm{cl}(\mathcal{O})$; the cosets of $\mathrm{cl}(\mathcal{O})^2$ inside $\mathrm{cl}(\mathcal{O})$ are called *genera*, with $\mathrm{cl}(\mathcal{O})^2$ itself being referred to as the *principal genus*.

Remark 5. By abuse of notation, we can and will also view $\chi_1, \chi_2, \ldots, \chi_r, \delta, \epsilon$ as morphisms $\mathrm{cl}(\mathcal{O}) \to \{\pm 1\}$, obtained by composing Φ with projection on the corresponding coordinate.

It can be shown that the image of Φ is a subgroup of $\{\pm 1\}^\mu$ having index 2, so that the cardinality of $\mathrm{cl}(\mathcal{O})/\mathrm{cl}(\mathcal{O})^2 \cong \mathrm{cl}(\mathcal{O})[2]$ equals $2^{\mu-1}$. More precisely, if we write $\Delta_\mathcal{O} = -2^a b$ with $b = m_1^{e_1} m_2^{e_2} \cdots m_r^{e_r}$, then this is accounted for by the character

$$\chi_1^{e_1} \cdot \chi_2^{e_2} \cdots \chi_r^{e_r} \cdot \delta^{\frac{b+1}{2} \bmod 2} \cdot \epsilon^{a \bmod 2}, \tag{1}$$

which is non-trivial when viewed on $(\mathbb{Z}/\Delta_\mathcal{O})^*$, but becomes trivial when viewed on $\mathrm{cl}(\mathcal{O})$. For example, if $\Delta_\mathcal{O}$ is squarefree and congruent to 1 mod 4, then the image of Φ consists of those tuples in $\{\pm 1\}^r$ whose coordinates multiply to 1.

Our main goal is to break DDH in $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$. To do this, we will compute the coordinate components of the map Φ, i.e. upon input of two elliptic curves $E, E' \in \mathcal{E}\ell\ell_q(\mathcal{O}, t)$ that are connected by a secret ideal class $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$, for each assigned character χ we will describe how to compute $\chi(E, E') := \chi([\mathfrak{a}])$. This is done in the next sections.

Example 6. In Section 4, we will study supersingular elliptic curves defined over $\mathbb{F}_p$ with $p \equiv 1 \bmod 4$. Here $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has discriminant $-4p$, thus there are two assigned characters: δ and the Legendre character χ_p associated with p. But (1) tells us that $\chi_p([\mathfrak{a}]) = \delta([\mathfrak{a}])$ and also that χ_p and δ are necessarily non-trivial characters of $\mathrm{cl}(\mathcal{O})$. So it suffices to compute $\delta([\mathfrak{a}])$, which as we will see can be done very efficiently.

2.5 The Tate pairing

We briefly recall the main properties of the (reduced) *Tate pairing* T_m, which is defined as

$$T_m : E(\mathbb{F}_{q^k})[m] \times E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k}) \to \mu_m : (P, Q) \mapsto f_{m,P}(D)^{(q^k-1)/m}.$$

Here k is the embedding degree, i.e. the smallest extension degree k such that $\mu_m \subset \mathbb{F}_{q^k}^*$; the function $f_{m,P}$ a so-called Miller function, i.e. a function with divisor $(f_{m,P}) = m(P) - m(\mathbf{0})$; D a divisor equivalent to $(Q) - (\mathbf{0})$ coprime to the support of $(f_{m,P})$. If the Miller function $f_{m,P}$ is normalized, and $Q \neq P$, then the pairing can be simply computed as $T_m(P, Q) = f_{m,P}(Q)^{(q^k-1)/m}$.

The reduced Tate pairing T_m has the following properties:

1. Bilinearity: $T_m(P, Q_1 + Q_2) = T_m(P, Q_1)T_m(P, Q_2)$ and $T_m(P_1 + P_2, Q) = T_m(P_1, Q)T_m(P_2, Q)$.
2. Non-degeneracy: for all $P \in E(\mathbb{F}_{q^k})[m]$ with $P \neq \mathbf{0}$, there exists a point $Q \in E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k})$ such that $T_m(P, Q) \neq 1$. Similarly, for all $Q \in E(\mathbb{F}_{q^k})$ with $Q \notin mE(\mathbb{F}_{q^k})$, there exists a $P \in E(\mathbb{F}_{q^k})[m]$ with $T_m(P, Q) \neq 1$.
3. Compatibility: let φ be an $\mathbb{F}_q$-rational isogeny, then
$$T_m(\varphi(P), \varphi(Q)) = T_m(P, Q)^{\deg(\varphi)}.$$
4. Galois invariance: let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ then $T_m(\sigma(P), \sigma(Q)) = \sigma(T_m(P, Q))$.

3 Computing the characters for ordinary curves

Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with endomorphism ring $\mathcal{O}$ and let m be a prime divisor of $\Delta_{\mathcal{O}}$. Note that $m \nmid q$, since otherwise $m \mid \Delta_{\mathcal{O}} \mid t^2 - 4q$ would imply that $\gcd(t, q) \neq 1$, contradicting that E is ordinary. By extending the base field if needed, we can assume without loss of generality that $\mathrm{val}_m(\#E(\mathbb{F}_q)) \geq 1$. The approach described in the introduction corresponds to $\mathrm{val}_m(\#E(\mathbb{F}_q)) = 1$, which implies that $E(\mathbb{F}_q)[m^\infty] \cong \mathbb{Z}/(m)$. The idea was to recover the character from the self-pairings $T_m(P, P)$ and $T_m(P', P')$, with P (resp. P') any non-zero $\mathbb{F}_q$-rational m-torsion point on E (resp. E').

In general we have $E(\mathbb{F}_q)[m^\infty] \cong \mathbb{Z}/(m^r) \times \mathbb{Z}/(m^s)$ for integers $1 \leq r \geq s \geq 0$. The next theorem shows that by walking all the way down to the floor of the m-isogeny volcano, we always end up on a curve $E_0/\mathbb{F}_q$ with $E_0(\mathbb{F}_q)[m^\infty] \cong \mathbb{Z}/(m^v)$, where $v = \mathrm{val}_m(\#E(\mathbb{F}_q))$.

Theorem 7. *Consider an m-isogeny volcano of ordinary elliptic curves over a finite field $\mathbb{F}_q$, and let N be their (common) number of $\mathbb{F}_q$-rational points. Assume $v = \mathrm{val}_m(N) \geq 1$ and let h denote the height of the volcano.*

- *If v is odd and E is a curve on level $0 \leq i \leq h$, or if v is even and E is a curve on level $0 \leq i \leq v/2$, then*

$$E(\mathbb{F}_q)[m^\infty] \cong \frac{\mathbb{Z}}{(m^{v-i})} \times \frac{\mathbb{Z}}{(m^i)}.$$

- *If v is even and E is a curve on level $v/2 \leq i \leq h$, then*

$$E(\mathbb{F}_q)[m^\infty] \cong \frac{\mathbb{Z}}{(m^{v/2})} \times \frac{\mathbb{Z}}{(m^{v/2})}.$$

(Note that the latter range may be empty, i.e. one may have $h < v/2$.)

Proof. See [23, Cor. 1] for $m = 2$ and [24, Thm. 3] for m odd.

Note that it is easy to verify whether a given curve $E/\mathbb{F}_q$ is located on the floor of its volcano. Indeed, for λ random points $P \in E(\mathbb{F}_q)$ one simply tests whether $(N/m)P = \mathbf{0}$. As soon as one point fails the test, we know that E is on the floor. If all points pass the test, we are on the floor with probability $1/m^\lambda$. Given such a verification method, a few random walks allow one to find a shortest path down to the floor, see e.g. the algorithm FindShortestPathToFloor in [31]. Note that this is considerably easier than navigating the volcano in a fully controlled way, see again [31] and the references therein.[3]

Once we are on E_0, the natural generalization of the case $v = 1$ is to compute the m-Tate pairing $T_m(P, Q)$ with $\mathrm{ord}(P) = m$ and $\mathrm{ord}(Q) = m^v$ satisfying $m^{v-1}Q = P$. The following theorem shows that the m-Tate pairing is non-trivial and, for a fixed P, independent of the choice of Q.

Theorem 8. *Let $E_0/\mathbb{F}_q$ be an ordinary elliptic curve with endomorphism ring $\mathcal{O}$ and let m be a prime divisor of $\Delta_\mathcal{O}$. Assume that*

$$E_0(\mathbb{F}_q)[m^\infty] \cong \frac{\mathbb{Z}}{(m^v)}$$

for some $v \geq 1$. Then for any P, Q with $\mathrm{ord}(P) = m$ and $\mathrm{ord}(Q) = m^v$, the reduced Tate pairing $T_m(P, Q)$ is a primitive m-th root of unity. Furthermore, for a fixed P, the pairing $T_m(P, \cdot)$ is constant for all Q with $\mathrm{ord}(Q) = m^v$ and $m^{v-1}Q = P$.

Proof. Set $N = \#E_0(\mathbb{F}_q)$. Since

$$m \mid \Delta_\mathcal{O} \mid t^2 - 4q = (q-1)^2 - 2(q+1)N + N^2,$$

[3] In the context of this paper, it is worth highlighting the work of Ionica and Joux [21] on this topic, who use the Tate pairing as an auxiliary tool for travelling through the volcano.

we see that $q \equiv 1 \bmod m$, hence $\mu_m \subset \mathbb{F}_q$, so the embedding degree of the Tate pairing is 1. By assumption, Q is a generator of $E_0(\mathbb{F}_q)[m^\infty] = E_0(\mathbb{F}_q)[m^v]$ and thus clearly not in $mE_0(\mathbb{F}_q)$ since $\mathrm{ord}(Q) = m^v$. Since m is prime, the non-degeneracy of the Tate pairing implies that $T_m(P,Q)$ is a primitive m-th of unity. Indeed, assume that $T_m(P,Q) = 1$, then $T_m(P,\cdot) = 1$ on the whole of $E_0(\mathbb{F}_q)/mE_0(\mathbb{F}_q)$, since the cosets can be represented by iQ for $i = 0, \ldots, m-1$, contradicting non-degeneracy.

Using again $E_0(\mathbb{F}_q)[m^\infty] \cong \mathbb{Z}/(m^v)$, it is easy to see that all points of order exactly m^v with $m^{v-1}Q = P$ are of the form $Q + R$ for $\mathrm{ord}(R) | m^{v-1}$. But any such $R \in mE_0(\mathbb{F}_q)$, which shows that $T_m(P,R) = 1$, and so $T_m(P,Q)$ is independent of the choice in Q. □

3.1 Computing the characters χ_i

Let χ be one of the characters χ_i associated with an odd prime divisor $m = m_i$ of $\Delta_\mathcal{O}$. As before, we let $\varphi : E \to E'$ denote the isogeny corresponding to $\mathfrak{a}$ of degree $\deg(\phi) = \mathrm{N}(\mathfrak{a})$. Recall that the goal is to compute $\chi([\mathfrak{a}]) = \left(\frac{\mathrm{N}(\mathfrak{a})}{m}\right)$.

Since $\mathrm{End}(E) = \mathrm{End}(E')$, by Theorem 1, the curves E and E' are on the same level of their respective volcanoes. By taking the same number of steps down from E and E' to the floor on their respective isogeny volcanoes, we end up with two respective elliptic curves E_0, E_0' in $\mathcal{Ell}_q(\mathcal{O}_0, t)$, where $\mathcal{O}_0 \subset \mathcal{O}$ is a suborder having discriminant $\Delta_{\mathcal{O}_0} = m^{2s}\Delta_\mathcal{O}$, with s the number of steps taken to reach the floor.

Since both curves E_0 and E_0' are now on the floor, we can choose non-trivial points $P \in E_0[m](\mathbb{F}_q)$ and $P' \in E_0'[m](\mathbb{F}_q)$, and corresponding points Q, Q' of order exactly m^v satisfying $m^{v-1}Q = P$ and $m^{v-1}Q' = P'$. We know that the class group $\mathrm{cl}(\mathcal{O}_0)$ acts transitively on $\mathcal{Ell}_q(\mathcal{O}_0, t)$, see Section 2.3, so there exists an invertible ideal $\mathfrak{b} \subset \mathcal{O}_0$ such that

$$E_0' = [\mathfrak{b}] \star E_0,$$

where by [11, Cor. 7.17] it can be assumed that $\mathrm{N}(\mathfrak{b})$ is coprime with $\Delta_{\mathcal{O}_0}$, hence coprime with m. Let $\varphi_0 : E_0 \to E_0'$ denote the corresponding degree $\mathrm{N}(\mathfrak{b})$ isogeny. Then there exists a $k \in \{1, \ldots, m-1\}$ with $k\varphi_0(P) = P'$. Clearly, the point $k\varphi_0(Q)$ also has order m^v and satisfies $m^{v-1}X = P'$. From Theorem 8 and the compatibility of the Tate pairing, it then follows:

$$T_m(P', Q') = T_m(k\varphi_0(P), k\varphi_0(Q)) = T_m(P,Q)^{k^2 \deg(\varphi_0)},$$

and thus

$$\left(\frac{\mathrm{N}(\mathfrak{b})}{m}\right) = \left(\frac{\deg(\varphi_0)}{m}\right) = \left(\frac{\log_{T_m(P,Q)} T_m(P', Q')}{m}\right).$$

We now show that this in fact equals $\chi([\mathfrak{a}])$. Indeed, since $\mathrm{N}(\mathfrak{b})$ is coprime with $\Delta_{\mathcal{O}_0}$, from [11, Prop. 7.20] we see that the ideal $\mathfrak{b}\mathcal{O} \subset \mathcal{O}$ is invertible and

again has norm $\mathrm{N}(\mathfrak{b})$. From the second paragraph of the proof of [31, Lem. 6] we see that $E' = [\mathfrak{b}\mathcal{O}] \star E$, and because the action of $\mathrm{cl}(\mathcal{O})$ on $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ is free we conclude that $[\mathfrak{b}\mathcal{O}] = [\mathfrak{a}]$. Summing up, we can compute

$$\chi([\mathfrak{a}]) = \chi([\mathfrak{b}\mathcal{O}]) = \left(\frac{\mathrm{N}(\mathfrak{b}\mathcal{O})}{m}\right) = \left(\frac{\mathrm{N}(\mathfrak{b})}{m}\right) = \left(\frac{\log_{T_m(P,Q)} T_m(P', Q')}{m}\right).$$

Note that, in particular, this outcome is independent of the choice of the walks to the floor of the isogeny volcano.

Remark 9. In the appendix we provide an alternative (but more complex) proof that shows it is not needed to walk all the way down to the floor. However, since the height of the volcano is about $\frac{1}{2}\operatorname{val}_m(t^2 - 4q)$ (see Theorem 1), the volcanoes cannot be very high (in the worst case a logarithmic number of steps), so walking to the floor of the volcano is efficient. Furthemore, for odd m, the probability of the volcano being height zero is roughly $1 - 1/m$.

3.2 Computing the characters δ, $\delta\epsilon$ and ϵ

For $\Delta_{\mathcal{O}} = -4n$, genus theory (Section 2.4) may give extra characters δ, ϵ or $\delta\epsilon$ depending on n mod 8. Recall that these characters are defined as

$$\delta : [\mathfrak{a}] \mapsto (-1)^{(\mathrm{N}(\mathfrak{a})-1)/2} \qquad \text{and} \qquad \epsilon : [\mathfrak{a}] \mapsto (-1)^{(\mathrm{N}(\mathfrak{a})^2-1)/8},$$

where the ideal $\mathfrak{a}$ is chosen to have odd norm. Determining δ is easily seen to be equivalent to computing $\mathrm{N}(\mathfrak{a})$ mod 4. In case both δ and ϵ exist (i.e. when $n \equiv 0 \bmod 8$), it is equivalent to computing $\mathrm{N}(\mathfrak{a})$ mod 8.

Note that the general approach using Theorem 8 remains valid, but does not result in sufficient information since it only determines $\mathrm{N}(\mathfrak{a})$ mod 2, which is known beforehand since the norm is odd. The solution is to use a 4-pairing to derive δ and an 8-pairing in the case both δ and ϵ exist. The following theorem is a generalization of Theorem 8; the main difference is that some care is required to prove that the values $T_m(P, Q)$ are primitive roots of unity (and not just different from 1 which follows from the non-degeneracy of the Tate pairing).

Theorem 10. *Let $E_0/\mathbb{F}_q$ be an ordinary elliptic curve with endomorphism ring $\mathcal{O}$ and let m be a prime divisor of $\Delta_{\mathcal{O}}$. Furthermore, assume that $m^n | (q-1)$ for $n > 1$ and that*

$$E_0(\mathbb{F}_q)[m^\infty] \cong \frac{\mathbb{Z}}{(m^v)}$$

for some $v \geq n$. Then for any P, Q with $\mathrm{ord}(P) = m^n$ and $\mathrm{ord}(Q) = m^v$, the reduced Tate pairing $T_{m^n}(P, Q)$ is a primitive m^n-th root of unity. Furthermore, for a fixed P, the pairing $T_{m^n}(P, \cdot)$ is constant for all Q with $\mathrm{ord}(Q) = m^v$ and $m^{v-n}Q = P$.

Proof. Assume that $T_{m^n}(P, Q)$ is not a primitive m^n-th root of unity, then $T_{m^n}(P, Q) \in \mu_{m^{n-1}}$, and in particular

$$1 = T_{m^n}(P, Q)^{m^{n-1}} = T_{m^n}(m^{n-1}P, Q).$$

Since P has order m^n, the point $m^{n-1}P$ is not the identity element $\mathbf{0}$. Further, since Q generates $E_0(\mathbb{F}_q)[m^\infty]$, we conclude that $T_{m^n}(m^{n-1}P, \cdot)$ is degenerate on the whole of $E_0(\mathbb{F}_q)/m^n E_0(\mathbb{F}_q)$, which contradicts the non-degeneracy of the Tate pairing. Thus we conclude that $T_{m^n}(P, Q)$ is a primitive m^n-th root of unity. The solutions to $m^{v-n}X = P$ are given by $Q + R$ with $\mathrm{ord}(R)|m^{v-n}$. But then $R \in m^n E_0(\mathbb{F}_q)$ and so $T_m(P, R) = 1$, which shows that $T_{m^n}(P, Q)$ is independent of the choice of Q.

Character δ Recall that the character δ exists when $n \equiv 0, 1, 4, 5 \bmod 8$. By taking a field extension if needed, we can assume without loss of generality that $v = \mathrm{val}_2(\#E(\mathbb{F}_q)) \geq 2$ and that $4 \mid (q-1)$. As before, by walking down the volcano we reach a curve E_0 on the floor (and similarly E_0') satisfying $E_0(\mathbb{F}_q)[2^\infty] = \mathbb{Z}/(2^v)$. We can now apply Theorem 10 for $m = 2$ and $n = 2$, and if $\mathfrak{b}$ is an ideal connecting E_0 and E_0', we can compute the exact value

$$\mathrm{N}(\mathfrak{b}) \bmod 4 = \log_{T_4(P,Q)} T_4(P', Q') \tag{2}$$

for appropriately chosen points $P, Q \in E_0(\mathbb{F}_q)[2^\infty]$ and $P', Q' \in E_0'(\mathbb{F}_q)[2^\infty]$. Indeed, recall that the points P' and Q' are only determined by P and Q up to a scalar $k \in (\mathbb{Z}/(4))^*$, i.e. $k \equiv 1, 3 \bmod 4$, and so $k^2 \equiv 1 \bmod 4$.

A similar reasoning as before then shows that $[\mathfrak{b}\mathcal{O}] = [\mathfrak{a}]$, where we can assume $\mathrm{N}(\mathfrak{b}\mathcal{O}) = \mathrm{N}(\mathfrak{b})$, so we find that

$$\delta([\mathfrak{a}]) = \delta([\mathfrak{b}\mathcal{O}]) = (-1)^{(\mathrm{N}(\mathfrak{b}\mathcal{O})-1)/2} = (-1)^{(\log_{T_4(P,Q)} T_4(P',Q')-1)/2},$$

or, equivalently, we recover $\mathrm{N}(\mathfrak{a}) \bmod 4$ by the same formula as in (2).

Characters $\delta\epsilon$ and ϵ Recall that the character $\delta\epsilon$ exists when $n \equiv 0, 2 \bmod 8$ and the character ϵ exists when $n \equiv 0, 6 \bmod 8$. Again, by taking a field extension if needed, we can assume without loss of generality that $v = \mathrm{val}_2(\#E(\mathbb{F}_q)) \geq 3$ and that $8 \mid (q-1)$. Notice that, if δ and ϵ do not exist simultaneously, then we are necessarily on the surface of the 2-volcano, hence it takes at least one step to go to curves E_0 and E_0' on the floor. During this step the discriminant becomes multiplied by a factor of 4. Hence, on the floor, we are certain that both characters exist.

Now applying Theorem 10 for $m = 2$ and $n = 3$, and using the fact that for $k \equiv 1, 3, 5, 7 \bmod 8$ we have $k^2 \equiv 1 \bmod 8$, we know that the norm of an ideal $\mathfrak{b}$ connecting E_0 and E_0' satisfies

$$\mathrm{N}(\mathfrak{b}) \bmod 8 = \log_{T_8(P,Q)} T_8(P', Q'), \tag{3}$$

for appropriately chosen points $P, Q \in E_0(\mathbb{F}_q)[2^\infty]$ and $P', Q' \in E_0'(\mathbb{F}_q)[2^\infty]$. The same reasoning as before then shows that $[\mathfrak{b}\mathcal{O}] = [\mathfrak{a}]$, where we can assume $\mathrm{N}(\mathfrak{b}\mathcal{O}) = \mathrm{N}(\mathfrak{b})$, hence we find

$$\epsilon([\mathfrak{a}]) = \epsilon([\mathfrak{b}\mathcal{O}]) = (-1)^{(\mathrm{N}(\mathfrak{b}\mathcal{O})^2-1)/8} = (-1)^{((\log_{T_8(P,Q)} T_8(P',Q'))^2-1)/8},$$

and similarly for $\delta\epsilon$. However, in general, we cannot conclude that $\mathrm{N}(\mathfrak{a}) \bmod 8$ can be recovered by the same formula as in (3). E.g., if $n \equiv 6 \bmod 8$, in the presence of ϵ but in the absence of δ, an ideal class containing ideals having norm 1 mod 8 will also contain ideals having norm 7 mod 8. It is during the first step down the volcano that both congruence classes become separated.

4 Computing the characters for supersingular curves

We now turn our attention to supersingular elliptic curves over prime fields $\mathbb{F}_p$ with $p > 3$. Recall that any such curve $E/\mathbb{F}_p$ has exactly $p+1$ rational points and its Frobenius satisfies $\pi^2 + p = 0$, therefore $\mathcal{O} = \mathrm{End}_p(E)$ has discriminant

$$\Delta_{\mathcal{O}} = \begin{cases} -4p & \text{if } p \equiv 1 \bmod 4, \\ -p \text{ or } -4p & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

From genus theory, we see that $\mathrm{cl}(\mathcal{O})$ has non-trivial 2-torsion only in the former case. So we will restrict our attention to $p \equiv 1 \bmod 4$, in which case $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$. There are two assigned characters: the Legendre character associated with p, and δ. From the character relation (1) (see also Example 6), we see that these coincide on $\mathrm{cl}(\mathcal{O})$, therefore it suffices to compute δ. Unfortunately, due to the peculiar behaviour of supersingular elliptic curves over $\mathbb{F}_{p^2}$, we cannot apply our strategy of "extending the base field and going down the volcano".

Instead, we can compute δ directly on the input curves, i.e. not involving vertical isogenies. This is handled by the following theorem, which can be used to compute δ in many ordinary cases, too. The proof is entirely self-contained, although its flavour is similar to that of Section 3.

Theorem 11. *Let $q \equiv 1 \bmod 4$ be a prime power and let $E, E'/\mathbb{F}_q$ be elliptic curves with endomorphism ring $\mathcal{O}$ and trace of Frobenius $t \equiv 0 \bmod 4$, connected by an ideal class $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$. Then δ is an assigned character of $\mathcal{O}$, and if we write*

$$E : y^2 = x^3 + ax^2 + bx \quad \textit{resp.} \quad E' : y^2 = x^3 + a'x^2 + b'x \tag{4}$$

then $\delta([\mathfrak{a}]) = (b'/b)^{(q-1)/4}$.

Proof. As $t \equiv 0 \bmod 4$, we have $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q) = q + 1 - t \equiv 2 \bmod 4$, and therefore both curves contain a unique rational point of order 2. When positioned at $(0,0)$, we indeed obtain models of the form (4). We point out that $b^{(q-1)/4}$ does not depend on the specific choice of such a model: it is easy to check that the only freedom left is scaling a by u^2 and b by u^4 for some $u \in \mathbb{F}_q^*$. Then, of course, the same remark applies to $b'^{(q-1)/4}$.

On E, the points (x_0, y_0) doubling to $P = (0,0)$ satisfy the condition

$$\frac{3x_0^2 + 2ax_0 + b}{2y_0} = \frac{y_0}{x_0},$$

which can be rewritten as $x_0(x_0^2 - b) = 0$. Therefore these points are

$$\left(\sqrt{b}, \pm\sqrt{b(a+2\sqrt{b})}\right) \quad \text{and} \quad \left(-\sqrt{b}, \pm\sqrt{b(a-2\sqrt{b})}\right),$$

from which we see that b is a non-square. Indeed, if we would have $\sqrt{b} \in \mathbb{F}_q$, then one of $a \pm 2\sqrt{b}$ would be a square in $\mathbb{F}_q$ because their product $a^2 - 4b$ is not (since there is only one $\mathbb{F}_q$-rational point of order 2). This would imply the existence of an $\mathbb{F}_q$-rational point of order 4, contradicting $\#E(\mathbb{F}_q) \equiv 2 \bmod 4$. As a consequence, we can characterize b as $-x(Q) \cdot x(\pi_q(Q))$, where Q denotes any of the four halves of P. The same reasoning shows that b' is a non-square, and that it can be rewritten as $-x(Q') \cdot x(\pi_q(Q'))$ with Q' any of the four halves of $P' = (0,0) \in E'$.

Now let $\varphi : E \to E'$ be the isogeny corresponding to a representative $\mathfrak{a}$ of $[\mathfrak{a}]$ having odd norm (coprime to q). Denote by $\pm K_1, \pm K_2, \ldots, \pm K_{(\mathrm{N}(\mathfrak{a})-1)/2}$ the non-trivial points in $\ker \varphi$, say with x-coordinates $x_1, x_2, \ldots, x_{(\mathrm{N}(\mathfrak{a})-1)/2} \in \overline{\mathbb{F}}_q$. Since φ is defined over $\mathbb{F}_q$, we see that $\varphi(P) = P'$. The other points mapping to P' are $P \pm K_1, P \pm K_2, \ldots, P \pm K_{(\mathrm{N}(\mathfrak{a})-1)/2}$, and an easy calculation shows that the x-coordinates of these points are $b/x_1, b/x_2, \ldots, b/x_{(\mathrm{N}(\mathfrak{a})-1)/2}$. This implies that the function

$$x \left(\prod_{i=1}^{(\mathrm{N}(\mathfrak{a})-1)/2} \frac{x - \frac{b}{x_i}}{x - x_i} \right)^2$$

viewed on E has the same divisor as $x \circ \varphi$, therefore both functions are proportional. To determine the constant involved, we can assume that our curve E' is obtained through an application of Vélu's formulae [14, Prop. 38], composed with a translation along the x-axis that positions P' at $(0,0)$. From [14, Cor. 39] we then see that the leading coefficient of the numerator of $x \circ \varphi$ equals $\mathrm{N}(\mathfrak{a}) - 3(\mathrm{N}(\mathfrak{a}) - 1) + 2(\mathrm{N}(\mathfrak{a}) - 1) = 1$. So the involved constant is just 1, i.e. equality holds.

Let $Q \in E$ be one of the halves of P, then $\varphi(Q)$ is a half of $\varphi(P) = P'$, so we can write

$$\begin{aligned}
b' &= -x(\varphi(Q)) \cdot x(\pi_q(\varphi(Q))) \\
&= -(x \circ \varphi)(Q) \cdot (x \circ \varphi)(\pi_q(Q)) \\
&= b \left(\prod_{i=1}^{(\mathrm{N}(\mathfrak{a})-1)/2} \frac{(\sqrt{b} - \frac{b}{x_i})(-\sqrt{b} - \frac{b}{x_i})}{(\sqrt{b} - x_i)(-\sqrt{b} - x_i)} \right)^2 \\
&= \frac{b^{\mathrm{N}(\mathfrak{a})}}{\left(\prod_{i=1}^{(\mathrm{N}(\mathfrak{a})-1)/2} x_i\right)^4}.
\end{aligned}$$

The theorem then follows by raising both sides to the power $(q-1)/4$ and using that we end up with primitive fourth roots of unity (indeed, recall that b and b' are non-square), whose ratio is either 1 or -1. □

Note that we can rewrite

$$b^{\frac{q-1}{4}} = (-x(Q) \cdot x(\pi_q(Q)))^{\frac{q-1}{4}} = \left(-f_{2,P}(Q)^{1+q}\right)^{\frac{q-1}{4}} = (-1)^{\frac{q-1}{4}} f_{2,P}(Q)^{\frac{q^2-1}{4}},$$

so the above proof can be seen to rely on a disguised, non-fully reduced 2-Tate pairing.

5 Impact on DDH and countermeasures

5.1 Impact on decisional Diffie–Hellman for class group actions

It is clear that any non-trivial character χ (or δ, ϵ, $\delta\epsilon$) can be used to determine whether a sample $(E' = [\mathfrak{a}]\star E, E'' = [\mathfrak{b}]\star E, E''')$ is a true Diffie-Hellman sample, i.e. whether $E''' = [\mathfrak{a}\cdot\mathfrak{b}]\star E$ or not. For instance, one could compute $\chi([\mathfrak{a}])$ in two different ways, e.g. namely as $\chi(E, E')$ and compare with $\chi(E'', E''')$. Similarly, one could compute $\chi([\mathfrak{b}])$ as $\chi(E, E'')$ as well as $\chi(E', E''')$. If the sample is not a true Diffie-Hellman sample this will be detected with probability $1/2$. In many cases we have more than one character available, so if we assume that $s < \mu$ linearly independent characters are computable (see below for the complexity of a single character), this probability increases to $1 - 1/2^s$.

Supersingular curves For supersingular curves over $\mathbb{F}_p$ with $p \equiv 1 \bmod 4$, the character δ exists and is always non-trivial (see Example 6). As shown in Section 4, computing this character requires computing a 2-torsion point, one inversion and one exponentiation in $\mathbb{F}_p$, so in this case, DDH can be broken in time $O(\log p \cdot M_p)$ with M_p the cost of a multiplication in $\mathbb{F}_p$.

Ordinary curves For ordinary curves, we will order the characters (if they exist) according to their complexity: δ, ϵ, $\delta\epsilon$, χ_{m_i} for $i = 1, \ldots, r$. From genus theory, it follows that at most one of the μ characters is trivial (since $\#\operatorname{cl}(\mathcal{O})[2] = 2^{\mu-1}$), so if the easiest to compute character is trivial, we immediately conclude that the second easiest to compute character is non-trivial. To determine the complexity, assume that m is an odd prime divisor of $\Delta_\mathcal{O}$. To be able to apply our attack, we first need to find the smallest extension $\mathbb{F}_{q^k}$ such that $\operatorname{val}_m(\#E(\mathbb{F}_{q^k})) > 0$. Since $m \mid \Delta_\mathcal{O} \mid t^2 - 4q$, we conclude that the matrix of Frobenius on $E[m]$ is of the form

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},$$

with $\lambda^2 \equiv q \bmod m$. In both cases, for $k = \operatorname{ord}(\lambda) \in \mathbb{Z}/(m)^*$, we conclude that $\operatorname{val}_m(\#E(\mathbb{F}_{q^k})) > 0$. Furthermore, since the determinant of the k-th power equals $q^k \equiv \lambda^{2k} \equiv 1 \bmod m$, we conclude that $\mu_m \subset \mathbb{F}_{q^k}$ and thus the m-Tate pairing is defined over $\mathbb{F}_{q^k}$. We see that in the worst case, we have $k = m - 1$. Computing the m-Tate pairing requires $O(\log m \cdot M_{q^k})$ which is $O(m^{1+\varepsilon} \cdot M_q)$ assuming

fast polynomial arithmetic and using $k < m$. The cost of walking down the volcano [31] over $\mathbb{F}_{q^k}$ in the worst case is given by $O(h \cdot (m^{3+\varepsilon} \cdot \log q) \cdot M_q)$ assuming fast polynomial arithmetic (and $k < m-1$), with h a bound on the height of the volcano. Once we reached the floor of the volcano, we need to solve the equation $m^{v-1}Q = P$, with P an m-torsion point, and $v = \mathrm{val}_m(\#E(\mathbb{F}_{q^k}))$. This can be computed deterministically using division polynomials, or probabilistically as follows: first generate a point Q_1 of order m^v, and compute $P_1 = m^{v-1}Q_1$. Since we are on the floor, $E(\mathbb{F}_q)[m]$ is cyclic, so there exists a k with $P = kP_1$. Then $Q = kQ_1$ is a solution. This randomized approach can be done in expected time $O(m^{3+\varepsilon} \cdot \log q \cdot M_q)$.

As remarked before, we note that in the majority of cases (probability roughly $1 - 1/m$), the height of the m-volcano is zero and the complexity of the attack is solely determined by the computation of the Tate pairing.

Computing the exact coset modulo $\mathbf{cl}(\mathcal{O})^2$ Genus theory shows that $\mathrm{cl}(\mathcal{O})^2$ equals the intersection of the kernels of the assigned characters. Thanks to the class group relation (1), we are allowed to omit one character. If all remaining characters have a manageable complexity, this allows to determine completely the coset of $\mathrm{cl}(\mathcal{O})^2$ inside $\mathrm{cl}(\mathcal{O})$ to which our secret ideal class $[\mathfrak{a}]$ belongs.

5.2 Implementation results

We implemented our attack in the Magma computer algebra system [5] and the code is given in Appendix B. The main functions are `ComputeEvenCharacters`, `ComputeOddCharacter` and `ComputeSupersingularDelta`. We also use a very simple randomized method to walk to the floor of the volacano in function `ToFloor`. A more efficient approach can be found in [31].

To illustrate the code, we apply it to an example found in [15, Section 4]. In particular, let

$$p = 7 \left(\prod_{2 \leq \ell \leq 380, \ell \text{prime}} \ell \right) - 1$$

and consider the elliptic curve $E : y^2 = x^3 + Ax^2 + x$ with

$$\begin{aligned} A = &10861338504649280383859950140772947007703646408372 \\ &83193432466056688873279777893214248825356514560367 25 \\ &91944602210571423767689240032829444439469242521864171 \end{aligned},$$

then $\mathrm{End}(E)$ is the maximal order and E lies on the surface of a volcano of height 2. By construction, the curve has $\mathbb{F}_p$-rational subgroups of order ℓ with $\ell \in [3, 5, 7, 11, 13, 17, 103, 523, 821, 947, 1723]$. The discriminant is of the form $-4n$ with $n \equiv 2 \bmod 8$, so we will be able to compute the character $\delta\epsilon$.

The code first computes a random isogeny of degree 523 (easy to compute since it is rational), to obtain the "challenge" $E' = [\mathfrak{a}] \star E$. After going to a degree 2 extension, it then descends the volcano to the floor, and on the floor,

it computes both δ as well as ϵ, from which it derives that $\delta\epsilon(E, E') = 1$, which is consistent with the fact that $\delta\epsilon([\mathfrak{a}]) = \delta\epsilon(523) = 1$.

5.3 Countermeasures

Since the attack crucially relies on the existence of 2-torsion in $\mathrm{cl}(\mathcal{O})$, the simplest countermeasure is to restrict to a setting where $\mathrm{cl}(\mathcal{O})[2]$ is trivial, e.g. supersingular elliptic curves over $\mathbb{F}_p$ with $p \equiv 3 \bmod 4$. This corresponds precisely to the CSIDH setting [8], so our attack does not impact CSIDH.

Another standard approach is to work with co-factors: since all characters become trivial on $\mathrm{cl}(\mathcal{O})^2$ we can simply restrict to elements which are squares, i.e. in the Diffie-Hellman protocol one would sample $[\mathfrak{a}]^2$ and $[\mathfrak{b}]^2$.

Warning We advise to be much more cautious than simply squaring. Genus theory gives the structure of $\mathrm{cl}(\mathcal{O})[2]$, but one can also derive the structure of the 2-Sylow subgroup $\mathrm{cl}(\mathcal{O})[2^\infty]$ using an algorithm going back to Gauss and analyzed in detail by Bosma and Stevenhagen [6]. Although our attack is currently not refined enough to also exploit this extra information, we expect that a generalization of our attack will be able to do so. As such, instead of simply squaring, we advise to use as cofactor an upper bound on the exponent of the 2-Sylow subgroup.

6 Conclusion

We showed how the characters defined by genus theory for the class group $\mathrm{cl}(\mathcal{O})$ can be computed from the group action of $\mathrm{cl}(\mathcal{O})$ on $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$, knowing only the equations of two elliptic curves E and $E' = [\mathfrak{a}] \star E$, for an unknown ideal class $[\mathfrak{a}]$. For a character χ associated to the prime divisor $m \mid \Delta_{\mathcal{O}}$, the complexity is exponential in the size of m, and it is thus efficiently computable only for smallish m. However, since only one such character is required to break DDH for class group actions, we conclude that for a subset of density 1 of ordinary curves, and for all supersingular curves over $\mathbb{F}_p$ with $p \equiv 1 \bmod 4$, DDH (without appropriate countermeasures) is broken. Note that CSIDH [8] is not affected, since it relies on supersingular elliptic curves over $\mathbb{F}_p$ with $p \equiv 3 \bmod 4$.

The main, quite surprising, insight of this paper is that the structure of the class group $\mathrm{cl}(\mathcal{O})$ does actually matter, and cannot be assumed to be fully hidden when represented as $\mathcal{E}\ell\ell_q(\mathcal{O}, t)$ under the class group action $\star$. Philosophically, one might argue that this is inherently caused by the fact that the structure of $\mathrm{cl}(\mathcal{O})[2]$ is easily computable. As such, it is imperative to analyze the following two cases which also give partial information about the class group $\mathrm{cl}(\mathcal{O})$:

- As already mentioned in Section 5.3, the algorithm described by Bosma and Stevenhagen [6] determines the structure of the 2-Sylow group $\mathrm{cl}(\mathcal{O})[2^\infty]$. Can our attack be extended to take this extra information into account?

– The class number formula expressing the class number of a suborder $\mathcal{O}$ in terms of the class number of the maximal order $\mathcal{O}_K$ and the conductor c

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)c}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|c} \left(1 - \left(\frac{\Delta_{\mathcal{O}_K}}{p}\right)\frac{1}{p}\right),$$

can be used to derive certain prime factors of $h(\mathcal{O})$ without knowing $h(\mathcal{O}_K)$. For instance, in the case of CSIDH with $p \equiv 3 \bmod 8$ where $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$, the above formula implies that $h(\mathcal{O})$ is divisible by 3. Can an attack be devised where such factors are exploited?

Finally, we note that in most settings the exact structure of $\mathrm{cl}(\mathcal{O})$ is unknown, so the usual approach of restricting to a large prime order subgroup does not apply. As a precaution, we therefore advise to work with supersingular curves $E/\mathbb{F}_p$ with $p \equiv 3 \bmod 4$, such that $\mathrm{End}(E) = \mathcal{O}_K$, i.e. restrict to curves on the surface as was done in the recent CSURF construction [7].

References

[1] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In *ASIACRYPT (1)*, volume 11921 of *Lecture Notes in Computer Science*, pages 227–247. Springer, 2019. https://ia.cr/2018/485.

[2] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, editors. *Advances in elliptic curve cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2005.

[3] Dan Boneh. The decision diffie-hellman problem. In *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 48–63. Springer, 1998.

[4] Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. Circular-secure encryption from decision diffie-hellman. In *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 108–125. Springer, 2008.

[5] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[6] Wieb Bosma and Peter Stevenhagen. On the computation of quadratic 2-class groups. *Journal de Théorie des Nombres de Bordeaux*, 8(2):283–313, 1996.

[7] Wouter Castryck and Thomas Decru. CSIDH on the surface. *IACR Cryptology ePrint Archive*, 2019:1404, 2019.

[8] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *ASIACRYPT (3)*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018. https://ia.cr/2018/383.

[9] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs, 2019. Available at http://nutmic2019.imj-prg.fr/confpapers/OrientIsogGraph.pdf.

[10] Jean-Marc Couveignes. Hard homogeneous spaces, 1997. IACR Cryptology ePrint Archive 2006/291, https://ia.cr/2006/291.

[11] David A. Cox. *Primes of the form x^2+ny^2: Fermat, class field theory, and complex multiplication*. Pure and Applied Mathematics. Wiley, second edition, 2013.

[12] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *CRYPTO*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25. Springer, 1998.
[13] ECRYPT – CSA. Algorithms, key size and protocols report (2018), 2018. Available at https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.
[14] Luca De Feo. Mathematics of isogeny based cryptography, 2017.
[15] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. In *ASIACRYPT (3)*, volume 11274 of *Lecture Notes in Computer Science*, pages 365–394. Springer, 2018. https://ia.cr/2018/485.
[16] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, 2016. https://arxiv.org/abs/1310.7789.
[17] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.
[18] Mireille Fouquet and François Morain. Isogeny volcanoes and the SEA algorithm. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory*, pages 276–291, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.
[19] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *CRYPTO*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18. Springer, 1984.
[20] James L. Hafner and Kevin S. McCurley. A rigorous subexponential algorithm for computation of class groups. *Journal of the American Mathematical Society*, 2:837–850, 1989.
[21] Sorina Ionica and Antoine Joux. Pairing the volcano. *Math. Comp.*, 82(281):581–603, 2013.
[22] David R. Kohel. Endomorphism rings of elliptic curves over finite fields. 1996.
[23] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields. *Appl. Math. Comput.*, 176(2):739–750, 2006.
[24] Josep M. Miret Biosca, Daniel Sadornil Renedo, Juan Tena Ayuso, Rosana Tom'as, and Magda Valls Marsal. Volcanoes of ℓ-isogenies of elliptic curves over finite fields: The case $\ell = 3$. *Publicacions Matemàtiques*, 51:165–180, 2007.
[25] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. In *FOCS*, pages 458–467. IEEE Computer Society, 1997.
[26] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 554–571. Springer, 2008.
[27] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptology ePrint Archive*, 2006:145, 2006.
[28] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–483, May 1985.
[29] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. https://arxiv.org/abs/quant-ph/9508027.
[30] Anton Stolbunov. *Cryptographic Schemes Based on Isogenies*. PhD thesis, 01 2012.
[31] Andrew V. Sutherland. Isogeny volcanoes. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 507–530. Math. Sci. Publ., Berkeley, CA, 2013.

[32] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2(2):134–144, 1966.
[33] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.
[34] William C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure*, 2:521–560, 1969.

A Not walking to the floor

As explained in Section 3, our approach to computing $\chi(E, E')$ is to take an arbitrary walk to the floor of the respective m-isogeny volcanoes of E and E'. The following modification of Theorem 8 shows that, in fact, it suffices to stop walking down as soon as one reaches a level where the m^∞-torsion is sufficiently unbalanced. In some cases, this leads to a slight speed-up.

Theorem 12. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with endomorphism ring $\mathcal{O}$, let m be a prime divisor of $\Delta_\mathcal{O}$, and assume that E is not located on the crater of its m-volcano. Assume that*

$$E(\mathbb{F}_q)[m^\infty] \cong \frac{\mathbb{Z}}{(m^r)} \times \frac{\mathbb{Z}}{(m^s)}$$

for some $r > s + 1$. Let $P \in E(\mathbb{F}_q)[m] \setminus \{\infty\}$ be such that there exists a point $Q \in E(\mathbb{F}_q)$ for which $m^{r-1}Q = P$. Then the reduced Tate pairing

$$T_m(P, \cdot) : E(\mathbb{F}_q)/mE(\mathbb{F}_q) \to \mu_m : X \mapsto T_m(P, X) \tag{5}$$

is trivial if and only if X belongs to $E[m^s] \bmod mE(\mathbb{F}_q)$. In particular, $T_m(P, Q)$ is a primitive m-th root of unity which, for a fixed P, does not depend on the choice of Q.

Proof. As in the proof of Theorem 8, we see that $\mu_m \subseteq \mathbb{F}_q$. As explained in [2, IX.7.1], the kernel of $T_m(P, \cdot)$ is a codimension 1 subspace of $E(\mathbb{F}_q)/mE(\mathbb{F}_q)$, when viewed as a vector space over $\mathbb{F}_m$. Therefore it suffices to prove that $T_m(P, \cdot)$ is trivial on $E[m^s] \bmod mE(\mathbb{F}_q)$, because the latter space indeed has codimension 1. More precisely, it has dimension 0 if $s = 0$ and dimension 1 if $s \geq 1$.

Now, since we are not on the crater, we know that there exists an elliptic curve E'/F_q along with an $\mathbb{F}_q$-rational m-isogeny $\varphi : E' \to E$ such that $E'(\mathbb{F}_q)[m^\infty] \cong \mathbb{Z}/(m^{r-1}) \times \mathbb{Z}/(m^{s+1})$. We note:

- $E[m^s] \subseteq \varphi(E'[m^{s+1}]) \subseteq \varphi(E'(\mathbb{F}_q))$, hence each $X \in E[m^s]$ can be written as $\varphi(X')$ for some $X' \in E'(\mathbb{F}_q)$.
- The kernel of the dual isogeny $\hat{\varphi} : E \to E'$ equals $\langle P \rangle$, otherwise E' would admit $\mathbb{F}_q$-rational m^r-torsion, therefore P is the image of a point $P' \in E'[m] \subseteq E'(\mathbb{F}_q)$.

We conclude that

$$T_m(P,X) = T_m(\varphi(P'),\varphi(X')) = T_m(P',X')^{\deg(\varphi)} = T_m(P',X')^m = 1,$$

as wanted. □

Along the same lines of thought, one can give a similar modification of Theorem 10. We actually believe that the assumptions in Theorem 12 can be weakened to include the cases where $r = s+1$ and/or where E is located on the crater; a proof of this generalization is in progress.

B Magma code

```
// Returns factors with multiplicity up to bound B

function SimpleTrialDivision(a, B)
  facs := TrialDivision(a, B);
  if (#facs gt 0 and facs[#facs][1] gt B) then
     // removing last factor if too large
     Remove(~facs, #facs);
  end if;
  return facs;
end function;

// The next four functions allow us to walk to the floor
// They also return the distance to the floor

function OnFloor(E, m, numpts)
  v := Valuation(numpts, m);
  onfloor := false;
  for i in [1..80] do
    if m^(v-1)*(numpts div m^v)*Random(E) ne E ! 0 then
      onfloor := true;
      break i;
    end if;
  end for;
  return onfloor;
end function;

// Random point of order m whose Weil pairing with Q is
// non-trivial assumes m-torsion is fully rational

function FindIndependentOrdermPoint(E, Q, m)
  Fq := BaseField(E);
  R<X> := PolynomialRing(Fq);
  coeffs := Eltseq(E);
  defpol := X^3 + coeffs[2]*X^2 + coeffs[4]*X + coeffs[5];
  xcoords := [rt[1] : rt in Roots(DivisionPolynomial(E,m))];
```

```
  repeat
    x := Random(xcoords);
    y := Sqrt(Evaluate(defpol,x));
    P := E ! [x,y,1];
  until WeilPairing(P,Q,m) ne 1;
  return P;
end function;

// Random point of order m

function FindOrdermPoint(E, m)
  Fq := BaseField(E);
  R<X> := PolynomialRing(Fq);
  coeffs := Eltseq(E);
  defpol := X^3 + coeffs[2]*X^2 + coeffs[4]*X + coeffs[5];
  xcoords := [rt[1] : rt in Roots(DivisionPolynomial(E,m))];
  x := Random(xcoords);
  y := Sqrt(Evaluate(defpol,x));
  return E ! [x,y,1];
end function;

// Walking to the floor of the volcano
// Returns height and distance to the floor
// Assumes existence of point of order m

function ToFloor(E, m, numpts)
  Fq := BaseField(E);
  q := #Fq;
  t := q + 1 - numpts;
  disc_frob := t^2 - 4*q;
  h := Floor(Valuation(disc_frob,m)/2); // height of the
    volcano
  if m eq 2 and (disc_frob div 4^h) mod 4 in {2,3} then
     h -:= 1;
  end if;
  if OnFloor(E, m, numpts) then
    return E, h, 0;
  else
    R<X> := PolynomialRing(Fq);
    repeat
      pathtofloor := 0;
      Efloor := E;
      Q := FindOrdermPoint(Efloor, m);
      repeat
        P := FindIndependentOrdermPoint(Efloor, Q, m);
        if m eq 2 then
          Efloor, phi := IsogenyFromKernel(Efloor, X - P[1]);
        else
          Efloor, phi := IsogenyFromKernel(Efloor, &*[X - (i*
   P)[1] : i in [1..(m-1) div 2]]);
```

```
        end if;
        Q := phi(Q);
        pathtofloor +:= 1;
      until pathtofloor gt h or OnFloor(Efloor, m, numpts);
    until pathtofloor le h; // otherwise we passed through surface
    return Efloor, h, pathtofloor;
  end if;
end function;

// Computes minimal extension such that m-torsion is rational
// Returns extension degree and number of points over extension

function MinimalExtensionmTorsion(m, p, numpts)
  t := p+1-numpts;
  Ts := [t, t^2 - 2*p];
  Ns := [numpts, p^2 + 1 - Ts[2]];
  for i := 3 to m-1 do
    Append(~Ts, t*Ts[i-1] - p*Ts[i-2]);
  end for;
  for d in Divisors(m-1) do
    if (Valuation(p^d + 1 - Ts[d], m) ge 1) then
     return d, p^d + 1 - Ts[d];
  end if;
  end for;
  return 0, 0;
end function;

// Listing available characters smaller than bound B
// Odd primes m appearing in t^2 - 4*p to an even power,
// or for which we need to go to a large extension to see
// some m-torsion are currently ignored.

function ListCharacters(E, B, numpts)

  p := #BaseField(E);
  t := p+1-numpts;
  disc_frob := t^2 - 4*p;

  factors := SimpleTrialDivision(disc_frob, B);

  even_chars := [];
  odd_chars := [];
  for fac in factors do
    if fac[1] ne 2 then
      if IsOdd(fac[2]) then // prime definitely divides Delta_0
        m := fac[1];
```

```
        if (MinimalExtensionmTorsion(m, p, numpts) lt 50)
    then
          odd_chars cat:= [m];
        end if;
      end if;
    else
      ext, numpts_ext := MinimalExtensionmTorsion(2, p,
    numpts);
      q := p^ext;
      Fq := GF(p, ext);
      E_ext := BaseChange(E, Fq);
      _, h, pathtofloor := ToFloor(E_ext, 2, numpts_ext);
      real_disc := disc_frob div 4^pathtofloor; // locally
    around 2, but enough
      if IsEven(real_disc) then
        if (-real_disc div 4) mod 4 le 1 then
          even_chars := ["delta"];
        end if;
        case (-real_disc div 4) mod 8:
          when 0, 6: Append(~even_chars, "epsilon");
          when 2: Append(~even_chars, "delta*epsilon");
        end case;
      end if;
    end if;
  end for;

  return even_chars, odd_chars;
end function;

// This function computes characters associated to odd prime

function ComputeOddCharacter(m, E, Eisog, numpts)

  print "Computing character associated with odd prime m =",
    m;

  p := #BaseField(E);
  t := p+1-numpts;

  ext, numpts_ext := MinimalExtensionmTorsion(m, p, numpts);
  v := Valuation(numpts_ext, m);
  q := p^ext;
  print "    (constructing field Fq of degree", ext,"over Fp)
    ";
  Fq := GF(p, ext);

  Tm := [];
  if v eq 1 then
    print "    Base case using self-pairing";
    for ell_curve in [E, Eisog] do
```

```
      ell_ext := BaseChange(ell_curve, Fq);
      repeat
        P := (numpts_ext div m)*Random(ell_ext);
      until P ne ell_ext ! 0;
      Tm cat:= [TatePairing(P,P,m)^((q-1) div m)];
    end for;
  else
    for ell_curve in [E, Eisog] do
      ell_ext := BaseChange(ell_curve, Fq);
    print " Walking to floor...";
      Efloor, h := ToFloor(ell_ext, m, numpts_ext);
    print " Heigth of volcano is ", h;
      repeat
        P := (numpts_ext div m)*Random(Efloor);
      until P ne Efloor ! 0;
      repeat
        Q := (numpts_ext div m^v)*Random(Efloor);
      until m^(v-1)*Q eq P;
      Tm cat:= [TatePairing(P,Q,m)^((q - 1) div m)];
    end for;
  end if;

  // Computing discrete log naively

  for expo in [1..m-1] do
    if Tm[2] eq Tm[1]^expo then
      return LegendreSymbol(expo, m);
    end if;
  end for;

  return 0;

end function;

// This procedure computes characters associated to prime 2

function ComputeEvenCharacters(even_chars, E, Eisog, numpts)

  print "Computing characters associated with m = 2:";

  p := #BaseField(E);
  t := p+1-numpts;
  S<X> := PolynomialRing(Integers());

  ext := 0;
  repeat
    ext +:= 1;
    numpts_ext := Resultant(1 - X^ext, X^2 - t*X + p);
    v := Valuation(numpts_ext, 2);
    q := p^ext;
```

```
  until q mod 8 eq 1 and v ge 3; // v ge 2 would have
    sufficed for delta
  q := p^ext;
  print "    Constructing field Fq of degree", ext,"over Fp";
  Fq := GF(p, ext);

  T8 := [];

  for ell_curve in [E, Eisog] do
    ell_ext := BaseChange(ell_curve, Fq);
  print "    Walking to floor...";
    Efloor, h := ToFloor(ell_ext, 2, numpts_ext);
  print "    Heigth of volcano is ", h;
    repeat
      P := (numpts_ext div 2^3)*Random(Efloor);
    until 4*P ne Efloor ! 0;
    repeat
      Q := (numpts_ext div 2^v)*Random(Efloor);
    until 2^(v-3)*Q eq P;
    T8 cat:= [TatePairing(P,Q,8)^((q-1) div 8)];
  end for;

  for e in [1,3,5,7] do
    if T8[2] eq T8[1]^e then
      expo := e;
    end if;
  end for;

  delta := (-1)^((expo - 1) div 2);
  epsilon := (-1)^((expo^2 - 1) div 8);
  result := [];
  for char in even_chars do
    case char:
      when "delta": Append(~result, delta);
      when "epsilon": Append(~result, epsilon);
      when "delta*epsilon": Append(~result, delta*epsilon);
    end case;
  end for;

  return result;
end function;

// Computes character delta for supersingular curve
// over F_p with p = 1 mod 4

function ComputeSuperingularDelta(E, Eisog)

  Fpx<x> := PolynomialRing(BaseField(E));
  Ew := WeierstrassModel(E);
  Eisogw := WeierstrassModel(Eisog);
```

```
  a := Coefficients(Ew)[4];
  r := Roots(x^3 + Fpx ! Reverse(Coefficients(Ew)), BaseField
    (E))[1][1];
  aiso := Coefficients(Eisogw)[4];
  riso := Roots(x^3 + Fpx ! Reverse(Coefficients(Eisogw)),
    BaseField(E))[1][1];

  char := ((aiso + 3*riso^2)/(a + 3*r^2))^((#BaseField(E) -
    1) div 4);
  if (char ne 1) then char := -1; end if;

  return char;

end function;

// Computes even character given degree ell

function ComputeEvenChar(cha, ell)
  case cha:
    when "delta": return (-1)^((ell-1) div 2);
    when "epsilon": return (-1)^((ell^2-1) div 8);
    when "delta*epsilon": return (-1)^( ((ell-1) div 2) + ((
    ell^2-1) div 8));
  end case;
  return 0;
end function;

// Defining Kieffer-de Feo-Smith example

p := 120373407382088450343833839782228011370920294512701979\
230713977354082515866699382915878575603568905160699619047 54\
171956588530344066457839297755929645858769;
A := 108613385046492803838599501407729470077036464083728319 3\
432466056688873279777893214248825356514560367259194460221057\
142376768924003282944443946924252186417 1;
ell := 523;
N := 120373407382088450343833839782228011370920294512701979 2\
307139773540825158667008548113803008846179093820187417165277\
134414404326829821994702618847159883806 0;
Fp := GF(p);
R<x> := PolynomialRing(Fp);
E := EllipticCurve([0, Fp ! A, 0, 1, 0]);

// constructing isogeneous curve

repeat
  P := (N div ell)*Random(E);
until (P ne E ! 0);
Eisog := IsogenyFromKernel(E, &*[x - (i*P)[1] : i in [1..
    Floor(ell/2)]]);
```

```
even_chars, odd_chars := ListCharacters(E, 1000, N);  // bound 1000 on character

if #even_chars ne 0 then
  r_even := ComputeEvenCharacters(even_chars, E, Eisog, N);
  ind := 0;
  for char in even_chars do
    ind := ind+1;
  print "Computed char ", char, " = ", r_even[ind], "vs ", char, " = ", ComputeEvenChar(char, ell);
  end for;
end if;

for m in odd_chars do
  char_m := ComputeOddCharacter(m, E, Eisog, N);
  print "Computed char = ", char_m, "vs Leg(ell, m) = ", LegendreSymbol(ell, m);
end for;
```