Computational aspects of class group actions and applications to post-quantum cryptography

Houben, M.R.

Chapter 4

On the decisional Diffie–Hellman problem for class group actions on oriented elliptic curves

This chapter consists of a paper written together with Wouter Castryck, Frederik Vercauteren, and Benjamin Wesolowski. It has been published as

Wouter Castryck, Marc Houben, Frederik Vercauteren, and Benjamin Wesolowski. On the decisional Diffie-Hellman problem for class group actions on oriented elliptic curves. *Res. Number Theory*, 8(4):Paper No. 99, 18, 2022. `https://doi.org/10.1007/s40993-022-00399-6`.

All authors of this paper contributed equally to the work.

Compared to the published version, we have fixed a few minor typographical and mathematical errors. We also improved the complexity estimate of the second step in Algorithm 1 based on a suggestion by Marco Streng. Additionally, we more concretely specified the input size in the complexity statements of Section 4.5, following a suggestion by Chloe Martindale. The numbering (of e.g. theorems and definitions) in the published version is different.

Acknowledgements

We thank the anonymous reviewers for several helpful comments, and Daniel J. Bernstein for suggesting to use Kedlaya–Umans factorization in the proof of Theorem 4.4.1.

Abstract

We show how the Weil pairing can be used to evaluate the assigned characters of an imaginary quadratic order $\mathcal{O}$ in an unknown ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ that connects two given $\mathcal{O}$-oriented elliptic curves (E, ι) and $(E', \iota') = [\mathfrak{a}](E, \iota)$. When specialized to ordinary elliptic curves over finite fields, our method is conceptually simpler and often somewhat faster than a recent approach due to Castryck, Sotáková and Vercauteren, who rely on the Tate pairing instead. The main implication of our work is that it breaks the decisional Diffie–Hellman problem for practically all oriented elliptic curves that are acted upon by an even-order class group. It can also be used to better handle the worst cases in Wesolowski's recent reduction from the vectorization problem for oriented elliptic curves to the endomorphism ring problem, leading to a method that always works in sub-exponential time.

4.1 Introduction

This paper is primarily concerned with the Decisional Diffie–Hellman problem (DDH) for ideal class groups acting on oriented elliptic curves through isogenies. In order to state this problem precisely, we fix an order $\mathcal{O}$ in an imaginary quadratic number field K along with an algebraically closed field k. A (primitive) $\mathcal{O}$-*orientation* on an elliptic curve E over k is an injective ring homomorphism $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$ that cannot be extended to a superorder $\mathcal{O}' \supsetneq \mathcal{O}$ in K. The set

$$\mathcal{Ell}_{\mathcal{O}}(k) = \{\, (E, \iota) \,|\, E \text{ an elliptic curve over } k \text{ and } \iota \text{ an } \mathcal{O}\text{-orientation on } E \,\}/\cong,$$

if non-empty, comes equipped with a free action

$$\mathrm{Cl}(\mathcal{O}) \times \mathcal{Ell}_{\mathcal{O}}(k) \longrightarrow \mathcal{Ell}_{\mathcal{O}}(k) : ([\mathfrak{a}], (E, \iota)) \longmapsto [\mathfrak{a}](E, \iota) \tag{4.1}$$

by the ideal class group of $\mathcal{O}$, see Section 4.2 for details (including what it means for two $\mathcal{O}$-oriented elliptic curves (E, ι) and (E', ι') to be isomorphic). Now assume that a party, say Eve, has unlimited access to samples from $\mathcal{Ell}_{\mathcal{O}}(k)^3$ that are consistently of either of the following two forms:

$$\begin{aligned} &\big(\, [\mathfrak{a}](E,\iota),\ [\mathfrak{b}](E,\iota),\ [\mathfrak{a}][\mathfrak{b}](E,\iota) \,\big) && [\mathfrak{a}], [\mathfrak{b}] \xleftarrow{\$} \mathrm{Cl}(\mathcal{O}), \\ &\big(\, [\mathfrak{a}](E,\iota),\ [\mathfrak{b}](E,\iota),\ [\mathfrak{c}](E,\iota) \,\big) && [\mathfrak{a}], [\mathfrak{b}], [\mathfrak{c}] \xleftarrow{\$} \mathrm{Cl}(\mathcal{O}), \end{aligned}$$

for some fixed and publicly known (E, ι). Then Eve successfully solves DDH if she can guess, with non-negligible advantage, from which of these two distributions her triples were sampled.

The hardness of the decisional Diffie–Hellman problem is a natural security foundation for cryptographic constructions based on ideal class group actions, which can be traced back to the works of Couveignes [11] and Rostovtsev–Stolbunov [24, 28] and which have attracted much attention lately, in the context of post-quantum cryptography. Here, one lets k be an algebraic closure of a finite field, in which case all curves in $\mathcal{Ell}_{\mathcal{O}}(k)$ can be defined over a common finite subfield $F \subseteq k$. While the initial focus was on ordinary elliptic curves, whose orientations ι are just ring isomorphisms, most of the latest work is concerned with supersingular elliptic curves, whose endomorphism rings are orders in a quaternion algebra and therefore leave room for a wide range of orientations. Here, we highlight supersingular elliptic curves defined over a finite prime field $\mathbf{F}_p$, which are naturally oriented by an order in $\mathbf{Q}(\sqrt{-p})$. The corresponding ideal class group actions underpin CSIDH [6] and spin-offs such as [1, 15, 2, 20], and tend to yield more practical cryptosystems than in the ordinary case. More generally oriented supersingular elliptic curves made their first cryptographic appearance in the OSIDH protocol due to Colò and Kohel [10]. To date, this protocol remains largely theoretical, but it has attracted a good amount of recent interest, see e.g. [13, 22, 31].

Our paper revisits the recent work [8], which presents an efficient solution to DDH for essentially all ordinary elliptic curves over finite fields whose endomorphism ring has an even class number. In more detail, as soon as there exists a non-trivial assigned

character $\chi : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\}$ of sufficiently small modulus m, the attack from [8] allows Eve to compute $\chi([\mathfrak{a}])$ merely from the knowledge of (E, ι) and $(E', \iota') = [\mathfrak{a}](E, \iota)$, i.e., without knowing $[\mathfrak{a}]$ itself. This indeed suffices to break DDH, since it allows her to check whether $\chi([\mathfrak{c}]) = \chi([\mathfrak{a}])\chi([\mathfrak{b}])$, which is true for $[\mathfrak{c}] = [\mathfrak{a}][\mathfrak{b}]$, but for uniformly random $[\mathfrak{c}]$ it fails with probability $1/2$.

Unfortunately, the method from [8] is specific to ordinary curves: the attack proceeds by extending the base field and navigating to the floors of the m-isogeny volcanoes[1] of (E, ι) and (E, ι'), with the goal of enforcing non-trivial cyclic rational m^∞-torsion, and then recovering the character value using two Tate pairing computations. Beyond ordinary curves, it is generally impossible to turn the rational m^∞-torsion cyclic using an isogeny walk, so this strategy fails. For supersingular elliptic curves over $\mathbf{F}_p$ with $p \equiv 1 \bmod 4$ equipped with their natural $\mathbf{Z}[\sqrt{-p}]$-orientation, where it suffices to consider the assigned character of modulus $m = 4$, an ad-hoc fix was given in [8, Thm. 10], but it is unclear how this fix would generalize.

Contribution

We give an alternative method for computing assigned character values $\chi([\mathfrak{a}])$ purely from (E, ι) and $(E', \iota') = [\mathfrak{a}](E, \iota)$, using the Weil pairing rather than the Tate pairing. Our approach deals with arbitrary orientations and works over arbitrary fields. Moreover, it simplifies and often speeds up the attack from [8] in the case of ordinary elliptic curves over finite fields, as it avoids the need for navigating through isogeny volcanoes. It also naturally incorporates the previously ad-hoc case of supersingular elliptic curves over prime fields.

The main result is easy enough to be stated right away; we recall that for an odd prime divisor $m \mid \mathrm{Disc}(\mathcal{O})$, the assigned character of modulus m is defined as

$$\chi_m : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\} : [\mathfrak{a}] \mapsto \left(\frac{N(\mathfrak{a})}{m}\right) \tag{4.2}$$

where it is assumed that $[\mathfrak{a}]$ is represented by an ideal $\mathfrak{a}$ of norm coprime to m (see our conventions further down) and $\left(\frac{\cdot}{m}\right)$ is the Legendre symbol.

Theorem 4.1.1 *Let $\mathcal{O}$ be an imaginary quadratic order and let $(E, \iota), (E', \iota')$ be $\mathcal{O}$-oriented elliptic curves connected by an ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$. Let $m \mid \mathrm{Disc}(\mathcal{O})$ be an odd prime divisor different from $\operatorname{char} k$ and consider the assigned character $\chi_m : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\}$ of modulus m. Then $\mathcal{O}$ admits a generator σ (i.e. $\mathcal{O} = \mathbf{Z}[\sigma]$) of norm coprime to m, and for any such σ there exist points $P \in E[m]$, $P' \in E'[m]$ such that $\iota(\sigma)(P)$ is not a multiple of P, and likewise for P'. Moreover*

$$\chi_m([\mathfrak{a}]) = \left(\frac{a}{m}\right)$$

with $a = \log_{e_m(P, \iota(\sigma)(P))} e_m(P', \iota'(\sigma)(P'))$, regardless of the choice of such σ, P, P'.

[1] Or rather 2-isogeny volcanoes in case $m \in \{4, 8\}$.

The condition that σ be a generator of $\mathcal{O}$ can be relaxed to $\sigma \in \mathcal{O} \setminus (\mathbf{Z} + m\mathcal{O})$. A proof of Theorem 4.1.1, along with its adaptations covering assigned characters with even modulus, can be found in Section 4.3. Since these results apply to arbitrary fields, they may be of independent theoretical interest.

Applications and implications

From a cryptographic viewpoint, the most important consequence is that DDH should be considered broken by classical computers for essentially all elliptic curves over finite fields that are oriented by an imaginary quadratic order $\mathcal{O}$ with even class number; see Section 4.4 for a more in-depth discussion.

As a more surprising application, we prove in Section 4.5 that the new method allows to significantly improve reductions between computational problems underlying isogeny-based cryptography. On one hand, we have the problem of computing endomorphism rings of supersingular elliptic curves. It is of foundational importance to the field, as its presumed hardness is necessary for the security of essentially all isogeny-based cryptosystems [17, 7, 16]. Oriented versions of this Endomorphism Ring Problem were introduced in [31]. On the other hand, many cryptosystems relate directly to the presumably hard inversion problem for the action of the class group $\mathrm{Cl}(\mathcal{O})$ on oriented supersingular curves: the Vectorization Problem. It was proved in [31] that the vectorization problem reduces to the endomorphism ring problem in polynomial time in the length of the instance and in $\#(\mathrm{Cl}(\mathcal{O})[2])$. Unfortunately, the dependence on $\#(\mathrm{Cl}(\mathcal{O})[2])$ means that the reduction is, in the worst case, exponential in the size of the input, since $\#(\mathrm{Cl}(\mathcal{O})[2])$ could be as large as $D^{1/\log\log D}$, where $D = |\operatorname{Disc}(\mathcal{O})|$. We improve this result, by proving in Section 4.5 that there is a reduction from the vectorization problem to the endomorphism ring problem that, in the worst case, is sub-exponential in the length of the input.

Conventions

Throughout, all ideal classes $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ are assumed to be represented by an ideal $\mathfrak{a}$ of norm coprime to $p \operatorname{Disc}(\mathcal{O})$, where $p = \max\{1, \operatorname{char} k\}$. Such a representative always exists, see e.g. [12, Cor. 7.17]. For an $\mathcal{O}$-oriented elliptic curve (E, ι) and a point $P \in E$, we will sometimes write $\sigma(P)$ instead of $\iota(\sigma)(P)$ if ι is clear from the context. Likewise, for $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ we will sometimes write $[\mathfrak{a}]E$ for the first component of $[\mathfrak{a}](E, \iota)$.

Paper organization

Section 4.2 provides background: it gives the full list of assigned characters of an imaginary quadratic order and it recalls how its ideal class group acts on oriented elliptic curves. Our main Section 4.3 contains a proof of Theorem 4.1.1, as well as statements and proofs for the even-modulus counterparts. Section 4.4 discusses the algorithmic aspects of these results, along with their implications for the decisional Diffie–Hellman problem. Finally, in Section 4.5 we present our improved reduction

from the vectorization problem for oriented elliptic curves to the endomorphism ring problem.

4.2 Background

4.2.1 Assigned characters

The following is a very brief summary of the relevant parts of [12, I.§3 & II.§7], to which we refer for more details. From genus theory, we know that each order $\mathcal{O}$ in an imaginary quadratic field comes equipped with an explicit list of group homomorphisms $\mathrm{Cl}(\mathcal{O}) \to \{\pm 1\}$, called the *assigned characters*, whose joint kernel is $\mathrm{Cl}(\mathcal{O})^2$. Writing

$$\mathrm{Disc}(\mathcal{O}) = -2^f d = -2^f m_1^{f_1} m_2^{f_2} \cdots m_r^{f_r}$$

for distinct odd prime numbers $m_1, \ldots, m_r$ and exponents $f \geq 0$, $f_1, \ldots, f_r \geq 1$, this list consists of

$$\begin{array}{ll}
\chi_{m_1}, \ldots, \chi_{m_r} & \text{if } f = 0, \\
\chi_{m_1}, \ldots, \chi_{m_r}, \delta & \text{if } f = 2 \text{ and } d \equiv 1 \bmod 4, \\
\chi_{m_1}, \ldots, \chi_{m_r} & \text{if } f = 2 \text{ and } d \equiv 3 \bmod 4, \\
\chi_{m_1}, \ldots, \chi_{m_r}, \delta\epsilon & \text{if } f = 3 \text{ and } d \equiv 1 \bmod 4, \\
\chi_{m_1}, \ldots, \chi_{m_r}, \epsilon & \text{if } f = 3 \text{ and } d \equiv 3 \bmod 4, \\
\chi_{m_1}, \ldots, \chi_{m_r}, \delta & \text{if } f = 4, \\
\chi_{m_1}, \ldots, \chi_{m_r}, \delta, \epsilon & \text{if } f \geq 5.
\end{array}$$

Here χ_{m_i} is defined as in (4.2) and

$$\delta : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\} : [\mathfrak{a}] \mapsto (-1)^{\frac{N(\mathfrak{a})-1}{2}}, \quad \epsilon : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\} : [\mathfrak{a}] \mapsto (-1)^{\frac{N(\mathfrak{a})^2-1}{8}}.$$

Observe that $\delta\epsilon$ can be described in one go as

$$\delta\epsilon : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\} : [\mathfrak{a}] \mapsto (-1)^{\frac{(N(\mathfrak{a})+2)^2-9}{8}}.$$

We write $\mu \in \{r, r+1, r+2\}$ for the total number of assigned characters.[2]

Because the joint kernel is $\mathrm{Cl}(\mathcal{O})^2$, any character of $\mathrm{Cl}(\mathcal{O})$ whose order divides 2 can be written as a product of pairwise distinct assigned characters. As it turns out, there is a unique non-trivial combination that produces the trivial character:

$$\chi_{m_1}^{f_1 \bmod 2} \chi_{m_2}^{f_2 \bmod 2} \cdots \chi_{m_r}^{f_r \bmod 2} \delta^{\frac{d+1}{2} \bmod 2} \epsilon^{f \bmod 2} = 1. \tag{4.3}$$

Therefore, by combining assigned characters we obtain $2^{\mu-1}$ distinct characters. Necessarily, this quantity equals the cardinality of $\mathrm{Cl}(\mathcal{O})/\mathrm{Cl}(\mathcal{O})^2 \cong \mathrm{Cl}(\mathcal{O})[2]$.

[2]Note that two different assigned characters may define the same map $\mathrm{Cl}(\mathcal{O}) \to \{\pm 1\}$. Thus, formally, the definition of an assigned character should include its symbol (e.g. χ_{m_1}) as appearing in the list above.

Example 4.2.1 For a prime number $p \equiv 1 \bmod 4$, the ring $\mathbf{Z}[\sqrt{-p}]$ has two assigned characters: δ and χ_p. By (4.3) these are in fact equal to each other, and non-trivial. If $p \equiv 3 \bmod 4$ then $\mathbf{Z}[\sqrt{-p}]$ has only one assigned character, namely χ_p, and it is trivial. ☆

We often make reference to the *modulus* m of an assigned character χ, which is an important complexity parameter for our attack. This is simply defined to be

$$\begin{cases} m_i & \text{if } \chi = \chi_{m_i}, \\ 4 & \text{if } \chi = \delta, \\ 8 & \text{if } \chi = \epsilon, \delta\epsilon. \end{cases}$$

Note that $\chi([\mathfrak{a}]) = \chi([\mathfrak{a}'])$ as soon as $N(\mathfrak{a}) \equiv N(\mathfrak{a}') \bmod m$. Typically m is the smallest positive integer with this property, but not always (e.g., as in the case of $m_i = p$ in both examples above).

4.2.2 Class group action

We now recall how the ideal class group of $\mathcal{O}$ acts on $\mathcal{Ell}_{\mathcal{O}}(k)$. This is part of the theory of complex multiplication, which is classical for $k = \mathbf{C}$, while for k an algebraic closure of a finite field this was elaborated in [30, §3.9-12]; see also [22] for the specifics of the supersingular case. For arbitrary k, we refer to Milne's course notes [21, §7].

If ι is an $\mathcal{O}$-orientation on an elliptic curve E over k, then we can linearly extend it to a map $K \hookrightarrow \mathrm{End}^0(E)$, where $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbf{Z}} \mathbf{Q}$ denotes the endomorphism algebra. To each isogeny $\varphi : E \to E'$ we can naturally attach an embedding

$$\iota_{\mathbf{Q}} : K \hookrightarrow \mathrm{End}^0(E') : \sigma \mapsto \frac{1}{\deg \varphi} \varphi \circ \iota(\sigma) \circ \hat{\varphi},$$

whose restriction to the preimage $\mathcal{O}'$ of $\mathrm{End}(E')$ is an orientation that is called the *induced orientation*, denoted by $\varphi_* \iota$. We are primarily interested in isogenies φ for which $\mathcal{O}' = \mathcal{O}$, in which case φ is said to be *horizontal* with respect to ι. Two $\mathcal{O}$-oriented elliptic curves $(E, \iota), (E', \iota')$ are called *isomorphic*, denoted $(E, \iota) \cong (E', \iota')$, if there exists an isomorphism $\varphi : E \to E'$ such that $\iota' = \varphi_* \iota$.

The default way to construct a horizontal isogeny is by considering an invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ of norm coprime to $\max\{1, \mathrm{char}\, k\}$ and attaching to it the finite subgroup

$$E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker \iota(\alpha).$$

Then the separable degree-$N(\mathfrak{a})$ isogeny $\varphi_{\mathfrak{a}} : E \to E'$ with kernel $E[\mathfrak{a}]$ is horizontal. In particular E' comes naturally equipped with an $\mathcal{O}$-orientation $\iota' = \varphi_{\mathfrak{a}*} \iota$. The pair (E', ι') is well-defined up to isomorphism and only depends on the class of $\mathfrak{a}$ inside $\mathrm{Cl}(\mathcal{O})$; we write $[\mathfrak{a}](E, \iota) := (E', \iota')$. This defines the map (4.1), which turns out to be a free group action.

Remark 4.2.2 In general the action is not transitive, where one subtlety is reflected in [22, Prop. 3.3]; see also the example in [22, §3.1] and the proof of [26, Thm. 4.5]. This has no consequences for the current paper, since we are working in a single orbit, namely that of the starting curve (E, ι). ◊

4.3 Evaluating characters using the Weil pairing

In this section we prove Theorem 4.1.1 and discuss its analogues for the assigned characters $\delta, \epsilon, \delta\epsilon$. In all cases it is assumed that $p = \max\{1, \operatorname{char} k\}$ is coprime to the modulus of the character under consideration. If p is an odd prime then χ_p, if it appears in the list of assigned characters, can be computed from the other characters using the relation (4.3); see for instance Example 4.2.1 where we had $\chi_p = \delta$. If $p = 2$ then the same conclusion holds for δ, ϵ or $\delta\epsilon$, because in even characteristic at most one of these three characters can appear in the list of assigned characters.[3]

4.3.1 Preliminaries

Lemma 4.3.1 *Let $\mathcal{O}$ be an imaginary quadratic order and let m be an odd prime number. Then $\mathcal{O} = \mathbf{Z}[\sigma]$ for some $\sigma \in \mathcal{O}$ of norm coprime to m.*

Proof. Let $\tau \in \mathcal{O}$ be a generator of $\mathcal{O}$, suppose of norm divisible by m. Then for any $k \in \mathbf{Z}$,

$$N(\tau + k) = N(\tau) + k(\operatorname{tr}(\tau) + k) \equiv k(\operatorname{tr}(\tau) + k) \bmod m.$$

Since $m \geq 3$ we can thus always find $k \in \mathbf{Z}$ such that $m \nmid N(\tau + k)$. □

Lemma 4.3.2 *Let $\mathcal{O}$ be an imaginary quadratic order of even discriminant. Then $\mathcal{O} = \mathbf{Z}[\sigma]$ for some $\sigma \in \mathcal{O}$ of odd norm.*

Proof. Let $\tau \in \mathcal{O}$ be a purely imaginary generator of $\mathcal{O}$, e.g. $\tau = \sqrt{\operatorname{Disc}(\mathcal{O})/4}$, where $\operatorname{Disc}(\mathcal{O})$ is the discriminant of $\mathcal{O}$. Then $N(\tau + 1) = N(\tau) + \operatorname{tr}(\tau) + 1 = N(\tau) + 1$, hence we can take $\sigma = \tau$ or $\sigma = \tau + 1$. □

Lemma 4.3.3 *Let $\mathcal{O}$ be an imaginary quadratic order, let (E, ι) be an $\mathcal{O}$-oriented elliptic curve over k, let $m \neq \operatorname{char} k$ be a prime number, and let $\sigma \in \mathcal{O}$ be a generator. Then there exists a $P \in E[m]$ such that $\iota(\sigma)(P)$ is not a multiple of P.*

Proof. The endomorphism $\iota(\sigma)$ of E induces an $\mathbf{F}_m$-linear map $E[m] \to E[m]$. Suppose to the contrary that every $P \in E[m]$ is an eigenvector. This can only happen if the map has the full m-torsion $E[m]$ as an eigenspace. Thus there exists $\lambda \in \mathbf{Z}$ such

[3] If (E, ι) is an $\mathcal{O}$-oriented elliptic curve over an algebraically closed field k with $\operatorname{char} k = 2$, then $2^5 \nmid \operatorname{Disc}(\mathcal{O})$. Indeed, if we would have $2^5 \mid \operatorname{Disc}(\mathcal{O})$ then E is necessarily supersingular, hence it concerns $y^2 + y = x^3$, the unique supersingular elliptic curve in characteristic 2. Its endomorphism ring is isomorphic to the ring of Hurwitz quaternions H, and it is easy to check that every embedding $\mathcal{O} \hookrightarrow H$ can be extended to an embedding $\mathcal{O}' \hookrightarrow H$ with $\operatorname{Disc}(\mathcal{O}') = \operatorname{Disc}(\mathcal{O})/4$. See [22, Prop. 3.2] for a generalization of this observation.

that $E[m] \subseteq \ker(\iota(\sigma - \lambda))$. It then follows that $\iota_{\mathbf{Q}}((\sigma - \lambda)/m) \in \mathrm{End}(E)$, and hence that $\sigma - \lambda \in m\mathcal{O}$ by the fact that ι is a primitive embedding, i.e. it cannot be extended to a strict superorder of $\mathcal{O}$. Since $\mathbf{Z} + m\mathcal{O} \subsetneq \mathcal{O}$ this contradicts the assumption that σ generates $\mathcal{O}$. □

4.3.2 Evaluating the characters χ_m

We now prove Theorem 4.1.1.

Proof of Theorem 4.1.1. The existence of σ, P, P' follows from Lemma 4.3.1 combined with Lemma 4.3.3. The endomorphism $\iota(\sigma)$ of E induces an $\mathbf{F}_m$-linear map $E[m] \to E[m]$. Since $m \mid \mathrm{Disc}(\mathcal{O}) = \mathrm{tr}(\sigma)^2 - 4N(\sigma)$ and $m \nmid N(\sigma)$, its characteristic polynomial has a nonzero double root, say $\alpha \in \mathbf{F}_m^\times$. Consequently, we can extend to a basis P_0, P of $E[m]$ for which the matrix of σ is in upper-triangular form $\left(\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha \end{smallmatrix}\right)$ for some $\beta \in \mathbf{F}_m^\times$. With respect to this basis any $Q \in E[m]$ that is not an eigenvector of σ is of the form $Q = \lambda P_0 + \mu P$ where $\mu \neq 0$. We see that

$$e_m(Q, \sigma(Q)) = e_m(\lambda P_0 + \mu P, (\alpha\lambda + \beta\mu)P_0 + \alpha\mu P) = e_m(P, \beta P_0)^{\mu^2} = e_m(P, \sigma(P))^{\mu^2},$$

showing that $e_m(P, \sigma(P))$ is independent of the choice of P, up to raising to powers that are nonzero squares modulo m. Then, of course, the same conclusion applies to $e_m(P', \sigma(P'))$.

Recall our convention from the introduction, namely that we assume that the norm of $\mathfrak{a}$, which equals the degree of the corresponding isogeny $\varphi = \varphi_{\mathfrak{a}} : E \to E'$, is coprime to m. In particular, $P_0 \notin \ker \varphi$. By definition of the class group action, $\iota' = \varphi_* \iota$ satisfies

$$\iota'(\sigma)(\varphi(P)) = \left(\frac{1}{\deg \varphi} \varphi \iota(\sigma) \hat{\varphi}\right)(\varphi(P)) = \varphi(\iota(\sigma)(P)) = \beta\varphi(P_0) + \alpha\varphi(P),$$

showing that $\varphi(P)$ is not an eigenvector for $\iota'(\sigma)$ acting on $([\mathfrak{a}]E)[m]$. So we see that $e_m(\varphi(P), \iota'(\sigma)(\varphi(P)))$ is obtained from $e_m(P', \iota'(\sigma)(P'))$ by raising it to a nonzero square mod m. To conclude, we observe that

$$e_m(\varphi(P), \iota'(\sigma)(\varphi(P))) = e_m(\varphi(P), \varphi(\iota(\sigma)(P))) = e_m(P, \iota(\sigma)(P))^{\deg \varphi}.$$ □

4.3.3 Evaluating δ, ϵ or $\delta\epsilon$

We now present the analogues of Theorem 4.1.1 for the even-modulus characters δ, ϵ and $\delta\epsilon$. We first focus on δ, which, as we saw in Section 4.2.1, is an assigned character if and only if we can write $\mathrm{Disc}(\mathcal{O}) = -4 \cdot d$ for some $d \equiv 0, 1 \bmod 4$.

Proposition 4.3.4 *Assume* $\mathrm{char}\, k \neq 2$. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $-4 \cdot d$ where $d \equiv 0, 1 \bmod 4$, and let (E, ι), (E', ι') be $\mathcal{O}$-oriented elliptic curves over k connected by an ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$. Then $\mathcal{O}$ admits an odd-norm*

generator σ, and for any such σ there exist points $P \in E[4]$, $P' \in E'[4]$ such that $\iota(\sigma)(2P) \neq 2P$ and $\iota'(\sigma)(2P') \neq 2P'$. Moreover

$$\delta([\mathfrak{a}]) = (-1)^{\frac{a-1}{2}},$$

with $a = \log_{e_4(P,\iota(\sigma)(P))} e_4(P', \iota'(\sigma)(P'))$, for any such choice of σ, P, P'.

Proof. The existence of σ, P, P' follows from Lemma 4.3.2 and Lemma 4.3.3. Note that the assumption on the discriminant of $\mathcal{O}$ shows that the character δ indeed exists, and that this implies that $N(\sigma) \equiv 1 \bmod 4$ (since the principal ideal class $[(\sigma)]$ lies in the kernel of δ). By upper-triangularizing the action of σ on $E[2]$ as in the proof of Theorem 4.1.1, we see that there exists a $P_0 \in E[4]$ such that the matrix M_σ of σ acting on $E[4]$ with respect to the basis P_0, P is of the form

$$M_\sigma \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \bmod 2.$$

Since $N(\sigma) \equiv 1 \bmod 4$ this means that M_σ is of the form either $\left(\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} \alpha & \beta \\ 2 & -\alpha \end{smallmatrix}\right)$, with α, β odd. Any Q with the property that $\sigma(2Q) \neq 2Q$ is of the form $\lambda P_0 + \mu P$ where μ is odd. If M_σ is of the first form we get

$$e_4(Q, \sigma(Q)) = e_4(\lambda P_0 + \mu P, (\alpha\lambda + \beta\mu)P_0 + \alpha\mu P) = e_4(P, \beta P_0)^{\mu^2} = e_4(P, \sigma(P))^{\mu^2}.$$

If M_σ is of the second form we again get

$$\begin{aligned} e_4(Q, \sigma(Q)) &= e_4(\lambda P_0 + \mu P, (\alpha\lambda + \beta\mu)P_0 + (2\lambda - \alpha\mu)P) \\ &= e_4(P, \beta P_0)^{\mu^2} e_4(P, P_0)^{2(\lambda\alpha\mu - \lambda^2)} = e_4(P, \sigma(P))^{\mu^2} \end{aligned}$$

where the last equality uses that λ, μ, α are odd. From $\mu^2 \equiv 1 \bmod 4$ it follows that $e_4(P, \sigma(P))$ does not depend on the choice of P. Then, of course, the same is true for $e_4(P', \sigma(P'))$.

By our convention we assume that the norm of $\mathfrak{a}$, and hence the degree of the corresponding isogeny $\varphi = \varphi_{\mathfrak{a}} : E \to E'$, is odd. In particular, $2P_0 \notin \ker \varphi$ and

$$\iota'(\sigma)(\varphi(2P)) = \left(\frac{1}{\deg \varphi} \varphi\iota(\sigma)\hat{\varphi}\right)(\varphi(2P)) = \varphi(\iota(\sigma)(2P)) = \varphi(2P_0) + \varphi(2P)$$

is different from $\varphi(2P)$. Thus we find that $e_4(P', \sigma(P'))$ equals

$$e_4(\varphi(P), \iota'(\sigma)(\varphi(P))) = e_4(\varphi(P), \varphi(\iota(\sigma)(P))) = e_4(P, \iota(\sigma)(P))^{\deg \varphi},$$

which concludes the proof. □

Next, we discuss the modulus-8 characters ϵ and $\delta\epsilon$. Note that by Section 4.2.1, we have that ϵ is an assigned character if and only if either $2^5 \mid \mathrm{Disc}(\mathcal{O})$ or $\mathrm{Disc}(\mathcal{O}) = -2^3 \cdot d$ with $d \equiv 3 \bmod 4$. Similarly, $\delta\epsilon$ is an assigned character if and only if either $2^5 \mid \mathrm{Disc}(\mathcal{O})$ or $\mathrm{Disc}(\mathcal{O}) = -2^3 \cdot d$ with $d \equiv 1 \bmod 4$.

Proposition 4.3.5 *Assume* $\operatorname{char} k \neq 2$*, let* $\mathcal{O}$ *be an imaginary quadratic order of discriminant* $\operatorname{Disc}(\mathcal{O}) \equiv -2^f d$ *with* d *odd and* $f \geq 3$*, and consider* $\mathcal{O}$*-oriented elliptic curves* (E, ι)*,* (E', ι') *over* k *connected by an ideal class* $[\mathfrak{a}] \in \operatorname{Cl}(\mathcal{O})$*. Assume that* ϵ*, resp.* $\delta\epsilon$*, appears among the assigned characters of* $\mathcal{O}$*. Then* $\mathcal{O}$ *admits an odd-norm generator* σ*, and for any such* σ *there exist points* $P \in E[8]$*,* $P' \in E'[8]$ *such that* $\iota(\sigma)(4P) \neq 4P$ *and* $\iota'(\sigma)(4P') \neq 4P'$*. Moreover* $\epsilon([\mathfrak{a}])$*, resp.* $\delta\epsilon([\mathfrak{a}])$*, can be computed as*

$$\epsilon([\mathfrak{a}]) = (-1)^{\frac{a^2-1}{8}}, \quad \textit{resp.} \quad \delta\epsilon([\mathfrak{a}]) = (-1)^{\frac{(a+2)^2-9}{8}},$$

with

$$a = \log_{e_8(P,\iota(\sigma)(P))} e_8(P', \iota'(\sigma)(P')),$$

and for any such choice of σ, P, P'*.*

Proof. As in the previous proof, the existence of σ, P, P' follows from Lemma 4.3.2 and Lemma 4.3.3. The main difference with the foregoing proofs is that if $Q \in E[8]$ is another point satisfying $\sigma(4Q) \neq 4Q$, then $e_8(Q, \sigma(Q))$ relates more subtly to $e_8(P, \sigma(P))$. Namely, we will argue that

$$e_8(Q, \sigma(Q)) \in \left\{ e_8(P, \sigma(P)), e_8(P, \sigma(P))^{N(\sigma)} \right\}, \tag{4.4}$$

and then of course the same again applies to $e_8(P', \sigma(P'))$. This will then lead to the conclusion that

$$e_8(P', \sigma(P')) \in \left\{ e_8(P, \sigma(P))^{\deg \varphi}, e_8(P, \sigma(P))^{N(\sigma) \deg \varphi} \right\},$$

which is indeed sufficient, since the principal ideal class $[(\sigma)]$ has trivial character values. More explicitly, if ϵ exists then we must have $N(\sigma) \bmod 8 \in \{1, 7\}$, while if $\delta\epsilon$ exists then we have $N(\sigma) \bmod 8 \in \{1, 3\}$.

In order to prove (4.4), note that, since $N(\sigma) \equiv 1 \bmod 2$,

$$\operatorname{tr}(\sigma)^2 + 4 \equiv \operatorname{tr}(\sigma)^2 - 4 \cdot N(\sigma) = \operatorname{Disc}(\mathcal{O}) \equiv 0 \bmod 8,$$

so that $\operatorname{tr}(\sigma) \equiv 2 \bmod 4$. It follows that the characteristic polynomial of σ modulo 4 is $X^2 + 2X + N(\sigma)$, hence we can extend to a basis P_0, P of $E[8]$ such that the matrix of $\iota(\sigma)$ acting on $E[8]$ is of the form

$$M_\sigma \equiv \begin{cases} \begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix} \bmod 4 & \text{if } N(\sigma) \equiv 1 \bmod 4, \\ \begin{pmatrix} \alpha & \beta \\ 2 & \alpha \end{pmatrix} \bmod 4 & \text{if } N(\sigma) \equiv 3 \bmod 4, \end{cases}$$

with α, β odd. It follows that

$$M_\sigma^2 \equiv \begin{cases} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \bmod 4 & \text{if } N(\sigma) \equiv 1 \bmod 4, \\ \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix} \bmod 4 & \text{if } N(\sigma) \equiv 3 \bmod 4. \end{cases}$$

In any case we can record that

$$e_8(P, \sigma^2(P))^2 = e_8(P, P_0)^4 = -1. \tag{4.5}$$

Now, with respect to the basis $P, \sigma(P)$, the matrix of $\iota(\sigma)$ acting on $E[8]$ is congruent to $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ mod 2. Any other $Q = \lambda P + \mu\sigma(P)$ such that $\sigma(4Q) \neq 4Q$ thus has exactly one of λ, μ odd. We now proceed to showing (4.4). If μ is odd then we can write $\sigma(Q) = \lambda' P + \mu'\sigma(P)$ with λ' odd, so since

$$e_8(Q, \sigma(Q))^{N(\sigma)} = e_8(\sigma(Q), \sigma^2(Q))$$

we may reduce to the case where λ is odd (and μ is even). For odd λ, we have

$$e_8(Q, \sigma(Q)) = e_8(\lambda^{-1}Q, \sigma(\lambda^{-1}Q))^{\lambda^2} = e_8(\lambda^{-1}Q, \sigma(\lambda^{-1}Q)),$$

hence we may further reduce to the case where $\lambda = 1$. Now note that

$$\begin{aligned} e_8(P + \mu\sigma(P), \sigma(P) + \mu\sigma^2(P)) &= e_8(P, \sigma(P)) e_8(\sigma(P), \sigma^2(P))^{\mu^2} e_8(P, \sigma^2(P))^{\mu} \\ &= e_8(P, \sigma(P)) e_8(P, \sigma(P))^{4\frac{\mu^2}{4} N(\sigma)} e_8(P, \sigma^2(P))^{2\frac{\mu}{2}} \\ &= e_8(P, \sigma(P)) \cdot (-1)^{\frac{\mu^2}{4}} \cdot (-1)^{\frac{\mu}{2}} \\ &= e_8(P, \sigma(P)), \end{aligned}$$

where in the third equality we used (4.5). □

Remark 4.3.6 If $\mathcal{O}$ is an imaginary quadratic order of discriminant $\mathrm{Disc}(\mathcal{O}) \equiv 0 \bmod 2^5$, then both ϵ and $\delta\epsilon$ and hence $\delta = (\delta\epsilon)\epsilon$ exist, so that $N(\sigma) \equiv 1 \bmod 8$. In this case there is a well-defined group homomorphism $\gamma : \mathrm{Cl}(\mathcal{O}) \to (\mathbf{Z}/8\mathbf{Z})^\times : [\mathfrak{a}] \mapsto N(\mathfrak{a}) \bmod 8$ through which $\delta, \epsilon, \delta\epsilon$ factor. This is the only situation where one can get finer-than-binary modular information about $N(\mathfrak{a})$ modulo a prime power; the above proof shows that we can recover $\gamma([\mathfrak{a}])$ at once as

$$\log_{e_8(P, \iota(\sigma)(P))} e_8(P', \iota'(\sigma)(P').$$

◊

Remark 4.3.7 In the statements of Theorem 4.1.1, Proposition 4.3.4 and Proposition 4.3.5, the condition that σ be a generator of $\mathcal{O}$ can in fact be relaxed to

$\sigma \in \mathcal{O} \setminus (\mathbf{Z} + m\mathcal{O})$ if m is odd and to $\sigma \in \mathcal{O} \setminus (\mathbf{Z} + 2\mathcal{O})$ if m is even, without modifying the proofs. $\Diamond$

Wrapping up, we have given justification for Algorithm 1 below, evaluating an assigned character $\chi : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\}$ of modulus m coprime to $\max\{1, \mathrm{char}\, k\}$ in an unknown ideal class $[\mathfrak{a}]$ connecting two given $\mathcal{O}$-oriented curves (E, ι) and (E', ι'). Here, by the field of definition of (E, ι), (E', ι') we mean any (e.g., the smallest) subfield $F \subseteq k$ over which the curves E, E' and the endomorphisms in $\iota(\mathcal{O}), \iota'(\mathcal{O})$ are defined.

Algorithm 1: Evaluating an assigned character in an unknown ideal class

Input:

$\mathcal{O}$-oriented curves (E, ι), (E', ι') in the same orbit with field of definition F
an assigned character χ of $\mathrm{Cl}(\mathcal{O})$ with modulus m coprime to $\max\{1, \mathrm{char}\, F\}$

Output:

$\chi([\mathfrak{a}]) \in \{\pm 1\}$, where $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ is such that $(E', \iota') = [\mathfrak{a}](E, \iota)$

1: Find a generator σ of $\mathcal{O}$ of norm coprime to m.
2: Base-change to the smallest extension $\mathcal{F} \supseteq F$ over which all points in $E[m]$ are defined; necessarily, then also all of $E'[m]$ is defined over $\mathcal{F}$.
3: Find a point $P \in E(\mathcal{F})$ such that $E[m] = \langle P, \iota(\sigma)(P) \rangle$ and compute $\zeta = e_m(P, \iota(\sigma)(P))$.
4: Likewise, find a point $P' \in E'(\mathcal{F})$ such that $E'[m] = \langle P', \iota'(\sigma)(P') \rangle$ and compute $\zeta' = e_m(P', \iota'(\sigma)(P'))$.
5: Inside $\mu_m \subseteq \mathcal{F}^\times$, compute $a = \log_\zeta \zeta'$.
6: If m is an odd prime then recover $\chi([\mathfrak{a}])$ as $\left(\frac{a}{m}\right)$, else recover $\chi([\mathfrak{a}])$ as

$$(-1)^{\frac{a-1}{2}}, \quad (-1)^{\frac{a^2-1}{8}}, \quad (-1)^{\frac{(a+2)^2-9}{8}},$$

depending on whether $\chi = \delta, \epsilon, \delta\epsilon$, respectively.

4.4 Complexity and consequences for DDH

Running Algorithm 1 in practice comes with challenges that are specific to our field of definition F. Nevertheless, before going into a more detailed analysis of our main case of interest, namely where F is a finite field, let us add some general comments to its six numbered steps:

1. Very easy, by following the proof of Lemma 4.3.1 or Lemma 4.3.2.

2. The degree of $\mathcal{F}/F$ is $O(m^2)$.[4]

[4] Indeed, by going to at most a quadratic extension, we may assume F is such that $\iota(\mathcal{O}) \subseteq \mathrm{End}_F(E)$. The orientation endows $E[m]$ with the structure of an $\mathcal{O}$-module, and $\mathrm{Aut}_{\mathcal{O}}(E[m]) \cong (\mathcal{O}/m\mathcal{O})^\times$. Since endomorphisms coming from $\mathcal{O}$ are defined over F, hence commute with $\mathrm{Gal}(\mathcal{F}/F)$, we thus obtain a group homomorphism $\mathrm{Gal}(\mathcal{F}/F) \to \mathrm{Aut}_{\mathcal{O}}(E[m])$, which is injective by definition of $\mathcal{F}$. The result follows since $\#(\mathcal{O}/m\mathcal{O})^\times = O(m^2)$.

3.–4. For m an odd prime, the proof of Theorem 4.1.1 shows that the set of m-torsion points that are independent of their image under σ has size $m^2 - m$. So it suffices to try $O(1)$ random points $P \in E[m]$, compute $\iota(\sigma)(P)$ and check whether $e_m(P, \iota(\sigma)(P))$ is a primitive mth root of unity (i.e., not 1).[5]

5. Pollard-ρ type algorithms allow us to compute the discrete logarithm using $O(\sqrt{m})$ operations in μ_m.

6. Trivial.

Theorem 4.4.1 *Let $\mathcal{O} = \mathbf{Z}[\sigma]$ be an imaginary quadratic order and consider two $\mathcal{O}$-oriented elliptic curves (E, ι) and (E', ι') that belong to the same orbit under the action of $\mathrm{Cl}(\mathcal{O})$, say given in Weierstrass form and connected by an unknown ideal class $[\mathfrak{a}]$. Assume that $E, E', \iota(\mathcal{O}), \iota'(\mathcal{O})$ are all defined over a finite field $\mathbf{F}_q$. Let χ be an assigned character of $\mathcal{O}$ with modulus m coprime to q. There exists a randomized algorithm for computing $\chi([\mathfrak{a}])$ that is expected to use*

$$\widetilde{O}(m^3 \log^2 q) \tag{4.6}$$

bit operations and $O(1)$ calls to $\iota(\sigma), \iota'(\sigma)$.

Proof. If we write $f_E(x, y)$ for the defining Weierstrass polynomial of E and $\Psi_{E,m}(x)$ for its m-division polynomial, then the field $\mathcal{F}$ can be constructed as (a quadratic extension of) the splitting field of the resultant $r_{E,m}(x) = \mathrm{res}_y(f_E, \Psi_{E,m})$, whose degree is $O(m^2)$. The division polynomial $\Psi_{E,m}(x)$ can be computed recursively and the resultant $r_{E,m}(x)$ can be factored using Kedlaya–Umans [19]. Using fast arithmetic, this takes a combined time of (4.6). Note that we obtain all points in $E[m]$ as a by-product; once we know $\mathcal{F}$ we can sample points from $E'[m]$ faster. The Weil pairings can be computed using Miller's algorithm, taking $O(\log m)$ operations in $\mathcal{F}$, and Pollard-ρ takes an expected $O(\sqrt{m})$ operations in $\mathcal{F}$, so these costs are dominated by (4.6), again assuming fast arithmetic. Finally, while the norm of the given generator σ may not be coprime to m, from the proofs of Lemma 4.3.1 and Lemma 4.3.2 we see that we can instead work with $\sigma + k$, for some positive integer k bounded by m. Since $\iota(\sigma + k) = \iota(\sigma) + [k]$, the overhead this causes is clearly absorbed by (4.6); and similarly for $\iota'(\sigma + k)$. □

The effectivity of this algorithm co-depends on how easy it is to evaluate $\iota(\sigma)$ and $\iota'(\sigma)$, which is a separate discussion that is captured by the notion of *efficient representations*, see Section 4.5.1 and [32] for more details. One special but interesting case is where $\iota(\sigma)$ equals $\pi_{\mathbf{F}_q}$, or is easily derived from it, whose cost is quasi-quadratic in $m \log q$. So, in this case, the overall cost remains estimated by (4.6). This matches with the asymptotic runtime of the Tate pairing attack from [8], as estimated in [8,

[5] Alternatively, one may opt for a more deterministic approach by computing and analyzing a matrix of $\iota(\sigma)$ acting on $E[m]$, in which case two evaluations of $\iota(\sigma)$ will do. Note however that writing down a matrix of $\iota(\sigma)$ comes at the cost of computing some discrete logarithms.

§5.1].[6]

While the Weil pairing attack is conceptually simpler (no descent of the isogeny volcano needed), in general one should expect the Tate pairing attack to run faster in practice. The main reason is that there it suffices to work over a field $\mathcal{F}$ such that E admits an $\mathcal{F}$-rational point of order m, rather than requiring all m-torsion to be $\mathcal{F}$-rational (in turn, this is because the Tate pairing admits non-trivial self-pairing values, in contrast with the Weil pairing). The degree of such an extension field is bounded by $O(m)$, rather than by $O(m^2)$. But the comparison turns in favour of the Weil pairing as soon as $E[m] \subseteq E(\mathbf{F}_q)$, where no field extension is needed. Note that, here, it makes more sense to measure the cost of a call to $\iota(\sigma), \iota'(\sigma)$ by the cost of evaluating $(\pi_{\mathbf{F}_q} - 1)/m^s$, where s is maximal such that $E[m^s] \subseteq E(\mathbf{F}_q)$; see [25, Lem. 1]. For this we need s successive point divisions by m; the cost of such a division is dominated by that of finding a root of a polynomial of degree m^2, which can be done in time

$$\widetilde{O}(m^2 \log^2 q), \tag{4.7}$$

see [23, §2]. This now becomes the dominant cost of the attack. The asymptotic cost of the Tate pairing also drops to (4.7) in this case, but the Weil pairing attack comes with less overhead.

All this aside, let us re-emphasize that the Weil pairing approach works in far greater generality: for arbitrary orientations and over any field admitting explicit computation. A proof-of-concept implementation of the new method can be found at `https://github.com/KULeuven-COSIC/oriented_DDH`. At the time of publication, this implementation handles the case of $\mathbf{Z}[\sqrt{-p}]$-oriented elliptic curves in characteristic $p \equiv 1 \bmod 4$. We intend to extend the repository in due course, by also covering the higher-degree group actions that were described in [9].

Consequences for DDH

If $\mathrm{Cl}(\mathcal{O})$ admits a non-trivial assigned character whose modulus m is sufficiently small, say polynomially bounded by $\log \mathrm{Disc}(\mathcal{O})$, and if it satisfies $\gcd(m, q) = 1$, then we can use this character to distinguish between random triples and Diffie–Hellman triples with probability $1/2$, as explained in the introduction. So, in this case, we can consider the decisional Diffie–Hellman problem broken for $\mathcal{O}$-oriented elliptic curves over $\mathbf{F}_q$. More generally, if $\mathrm{Cl}(\mathcal{O})$ admits $s \geq 1$ independent such characters (meaning that one cannot use the relation (4.3) to rewrite one of the characters in terms of the others), then we can distinguish with probability $1 - 1/2^s$.

A sufficient condition for the existence of such a character is that $\mathrm{Disc}(\mathcal{O})$ has at least two small odd prime factors different from $p = \mathrm{char}\, \mathbf{F}_q$.[7] Heuristically, we expect that this applies to a density 1 subset of all imaginary quadratic orders when ordered

[6] Here and below, for simplicity, the height $h \approx \mathrm{val}_m(\mathrm{tr}(\pi_{\mathcal{F}})^2 - 4\#\mathcal{F})$ of the m-isogeny volcano of E over $\mathcal{F}$ is estimated by $O(1)$.

[7] In serious cryptographic applications, one can ignore the phrase "different from $p = \mathrm{char}\, \mathbf{F}_q$". Indeed, if $p \mid \mathrm{Disc}(\mathcal{O})$ then E and E' are necessarily supersingular, so if moreover p is small then we can compute $\mathrm{End}(E)$ and $\mathrm{End}(E')$ by navigating through all $O(p)$ nodes of the supersingular isogeny graph. As a result, one is skating on very thin ice (see Section 4.5).

by the absolute value of their discriminant. This can be backed up using Mertens' third theorem; or see [29, III.§6] for more dedicated tools.

As discussed in [8, §6], one can thwart the attack by restricting the class-group action to $\mathrm{Cl}(\mathcal{O})^2$, or at least to a subgroup of $\mathrm{Cl}(\mathcal{O})$ on which all assigned characters of small modulus have trivial evaluations. However, this may have practical consequences in terms of key generation and key validation. Moreover, we do not rule out that the attack can be modified to work for characters whose order is a larger power of 2, e.g., in view of [3, 27]. Quantumly, it is known that 2^r-torsion subgroups, for any small fixed value of r, do not contribute to the hardness of the vectorization problem anyway [5]. Therefore, the cleanest way out is to follow the recommendation from [8, §6], namely to only work with orientations by imaginary quadratic orders whose class number is odd. There may be constructive reasons to deviate from this, e.g., as in the OSIDH protocol [10] where one uses orders of large prime power conductor in an imaginary quadratic field with class number one (such orders always have even class number).

Remark 4.4.2 It is interesting to view Theorem 4.4.1 against the *classical* decisional Diffie–Hellman problem, namely for exponentiation in a group $G = \langle g \rangle$ of some large prime order m. Note that exponentiation defines a free and transitive action of $(\mathbf{Z}/m\mathbf{Z})^\times$ on the set of generators of G. The Legendre symbol

$$\chi : (\mathbf{Z}/m\mathbf{Z})^\times \to \{\pm 1\} : a \mapsto \left(\frac{a}{m}\right)$$

is the unique quadratic character, of modulus m, and if one could cook up an efficient classical way for computing $\chi(a)$ merely from the knowledge of g and g^a, then this would break DDH in this setting. This would be a spectacular result; in general, to the best of our knowledge, we cannot do significantly better than computing a using Pollard-ρ and then evaluating χ at a. This should be compared to steps 5. and 6. from Algorithm 1. In other words, one could say that classical DDH is not weakened by the existence of χ because its modulus is large. ◊

4.5 Reductions to endomorphism ring computation

In this section, we prove that our main result Theorem 4.1.1 allows to significantly improve reductions between computational problems underlying isogeny-based cryptography. It was proved in [31] that two such families of problems are tightly connected: there are computational reductions from action inversion problems (called Effective $\mathcal{O}$-Vectorization or Effective $\mathcal{O}$-Uber) to endomorphism ring computation problems (called $\mathcal{O}$-EndRing and $\mathcal{O}$-EndRing*). However, these reductions are exponential in the worst case. In this section, we apply Theorem 4.1.1 to obtain reductions that are sub-exponential in the worst case, and even polynomial in many regimes of interest. All results in this section that start with (ERH), such as Theorem 4.5.7, assume the extended Riemann hypothesis — precisely, the Riemann hypothesis for Hecke L-functions.

4.5.1 The supersingular endomorphism ring problem

In this section, we assume that the field k is an algebraic closure of a finite field of characteristic p, and that p does not split in $\mathcal{O}$, nor does it divide the conductor of $\mathcal{O}$. Then, the set $\mathcal{Ell}_{\mathcal{O}}(k)$ is non-empty and all curves in it are supersingular; this set is often denoted by $\mathrm{SS}_{\mathcal{O}}(p)$ in the literature [22, Prop. 3.2]. Recall that a curve E/k is supersingular if and only if its endomorphism ring $\mathrm{End}(E)$ is isomorphic to a maximal order in the quaternion algebra

$$B_{p,\infty} = \left(\frac{-q, -p}{\mathbf{Q}}\right) = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}ij,$$

with the multiplication rules $i^2 = -q$, $j^2 = -p$, and $ji = -ij$, where q is a positive integer that depends on p.

Given a supersingular elliptic curve E over k, the endomorphism ring problem EndRing consists in computing four endomorphisms that form a basis of $\mathrm{End}(E)$. There is flexibility in how these endomorphisms can be represented, but we always assume that it is an *efficient representation*. As in [32], we say that an isogeny $\varphi : E \to E'$ is given in an efficient representation if there is an algorithm to evaluate $\varphi(P)$ for any $P \in E(\mathbf{F}_{p^r})$ in time polynomial in the length of the representation of φ and in $r\log(p)$. We also assume that an efficient representation of φ has length $\Omega(\log(\deg(\varphi)))$.

This endomorphism ring problem is of foundational importance to isogeny-based cryptography: it is presumed to be hard, and this hardness is *necessary* (and sometimes sufficient) for the security of essentially all isogeny-based protocols [17, 7, 16]. It does not, however, capture well the notion of orientation, which plays an important role in many protocols. Therefore, the following oriented variants were introduced in [31]. Computationally, an $\mathcal{O}$-orientation ι is represented by a generator σ of $\mathcal{O}$ (i.e., $\mathcal{O} = \mathbf{Z}[\sigma]$) together with an efficient representation of the endomorphism $\iota(\sigma)$.

Problem 4.5.1 ($\mathcal{O}$-EndRing) *Given $(E, \iota) \in \mathcal{Ell}_{\mathcal{O}}(k)$, find a basis of* $\mathrm{End}(E)$.

Problem 4.5.2 ($\mathcal{O}$-EndRing*) *Given an $\mathcal{O}$-orientable curve E, find a basis of* $\mathrm{End}(E)$*, and an $\mathcal{O}$-orientation of E expressed in this basis.*

Clearly, $\mathcal{O}$-EndRing reduces to $\mathcal{O}$-EndRing*.

4.5.2 Action inversion problems

Many cryptosystems relate, directly or more subtly, to an inversion problem for the action of $\mathrm{Cl}(\mathcal{O})$ on $\mathcal{Ell}_{\mathcal{O}}(k)$. In essence, given (E, ι) and (E', ι') in $\mathcal{Ell}_{\mathcal{O}}(k)$, find a class $[\mathfrak{a}]$ such that $(E', \iota') \cong [\mathfrak{a}](E, \iota)$ (or decide that it does not exist). This is called the vectorization problem. It is too weak for many practical purposes, because knowledge of the class $[\mathfrak{a}]$ is not sufficient to efficiently apply its action on any other $\mathcal{O}$-oriented curve. Therefore, the following stronger problem was introduced in [31].

Problem 4.5.3 (Effective $\mathcal{O}$-Vectorization) *Given three $\mathcal{O}$-oriented supersingular curves $(E,\iota),(E',\iota'),(F,\jmath) \in \mathcal{Ell}_{\mathcal{O}}(k)$, find an $\mathcal{O}$-ideal $\mathfrak{a}$ (or decide that it does not exist) such that $(E',\iota') \cong [\mathfrak{a}](E,\iota)$, and an efficient representation of $\varphi_{\mathfrak{a}} : (F,\jmath) \to [\mathfrak{a}](F,\jmath)$.*

The security of many cryptosystems directly reduces to this problem, such as CSIDH [6], CSI-FiSh [1], CSURF [4], or other generalizations [9].

One can define a similar problem where no orientation is provided for E'. Then, one cannot require $(E',\iota') \cong [\mathfrak{a}](E,\iota)$ anymore, but one can still ask for $E' \cong [\mathfrak{a}]E$. The resulting *Uber isogeny problem* was introduced in [14].

Problem 4.5.4 (Effective $\mathcal{O}$-Uber) *Given two $\mathcal{O}$-oriented curves $(E,\iota),(F,\jmath) \in \mathcal{Ell}_{\mathcal{O}}(k)$ and an $\mathcal{O}$-orientable curve E', find an $\mathcal{O}$-ideal $\mathfrak{a}$ such that $E' \cong [\mathfrak{a}]E$, and an efficient representation of $\varphi_{\mathfrak{a}} : (F,\jmath) \to [\mathfrak{a}](F,\jmath)$.*

This Effective $\mathcal{O}$-Uber problem is significantly harder than the Effective $\mathcal{O}$-Vectorization problem. In fact, most isogeny-based cryptosystems reduce to an instance of Effective $\mathcal{O}$-Uber [14], even cryptosystems such as SIDH [18] which, at first sight, do not seem to involve any orientation.

4.5.3 Action inversion reduces to endomorphism ring

Strengthening and generalizing a result of [7], it was proved in [31] that Effective $\mathcal{O}$-Vectorization reduces to $\mathcal{O}$-EndRing, and that Effective $\mathcal{O}$-Uber reduces to $\mathcal{O}$-EndRing*. Both reductions are in polynomial time in the length of the instance, and in $\#(\mathrm{Cl}(\mathcal{O})[2])$. Unfortunately, the dependence on $\#(\mathrm{Cl}(\mathcal{O})[2])$ means that the reduction is, in the worst case, exponential in the size of the input, since $\#(\mathrm{Cl}(\mathcal{O})[2])$ could be as large as $D^{1/\log\log D}$, where $D = |\operatorname{Disc}(\mathcal{O})|$. The issue is the following: given two oriented curves (E,ι) and (E',ι') as in the definition of Effective $\mathcal{O}$-Vectorization, the reductions first find a class $[\mathfrak{a}]^2$ such that $(E',\iota') \cong [\mathfrak{a}](E,\iota)$. Finding $[\mathfrak{a}]$ from $[\mathfrak{a}]^2$ is a square root computation. There are $\#(\mathrm{Cl}(\mathcal{O})[2])$ square roots of $[\mathfrak{a}]^2$, but only one is the correct class $[\mathfrak{a}]$. In [31], one simply does an exhaustive search. Now, thanks to Theorem 4.1.1, there is a much more efficient way to find the correct square root, which in the worst case is sub-exponential in $\operatorname{Disc}(\mathcal{O})$. This is the following proposition. Recall the L-notation

$$L_x(\alpha) = \exp\left(O\left((\log x)^{\alpha}(\log\log x)^{1-\alpha}\right)\right)$$

for sub-exponential complexities.

Proposition 4.5.5 (ERH) *Given $\mathcal{O}$ of discriminant $-D$, the factorization $D = \prod_{i=1}^{\omega(D)} \ell_i^{e_i}$ (with $\ell_i < \ell_{i+1}$), two $\mathcal{O}$-oriented elliptic curves $(E,\iota),(E',\iota') \in \mathcal{Ell}_{\mathcal{O}}(k)$, a basis of $\mathrm{End}(E)$, and an $\mathcal{O}$-ideal $\mathfrak{a}$ for which there exists an ideal class $[\mathfrak{c}]$ such that $[\mathfrak{a}] = [\mathfrak{c}]^2$ and $(E',\iota') = [\mathfrak{c}](E,\iota)$, one can find a representative for the ideal class $[\mathfrak{c}]$ in*

probabilistic polynomial time in the length of the input and in[8]

$$\min\left(2^{\omega(D)}, \max_i\left(\ell_i \mid \ell_i \leq 2^{\omega(D)-i}\right)\right) \ll \min\left(L_D(1/2), \#(\mathrm{Cl}(\mathcal{O})[2]), \ell_{\omega(D)}\right).$$

Here, by "probabilistic polynomial time in the length of the input", we mean probabilistic polynomial time in $\log p$, $\log D$, $\log N(\mathfrak{a})$, *the lengths of* ι *and* ι', *and in the length of the basis of* $\mathrm{End}(E)$.

Before proving it, let us recall the following proposition from [31].

Proposition 4.5.6 (ERH, [31, Proposition 9]) *Given* $(E, \iota) \in \mathcal{Ell}_{\mathcal{O}}(k)$, *a basis of* $\mathrm{End}(E)$, *and an* $\mathcal{O}$*-ideal* $\mathfrak{a}$, *one can compute* $[\mathfrak{a}](E, \iota)$ *and an efficient representation of* $\varphi_{\mathfrak{a}} : (E, \iota) \to [\mathfrak{a}](E, \iota)$ *in probabilistic polynomial time in the length of the input. That is, in* $\log|\mathrm{Disc}(\mathcal{O})|$, $\log p$, $\log N(\mathfrak{a})$, *and in the length of* ι *and of the basis of* $\mathrm{End}(E)$.

Proof of Proposition 4.5.5. Let $B > 0$ be a bound to be tuned later. Consider the sets of prime numbers

$$P_1 = \{\ell \mid \ell \text{ is an odd prime factor of } \mathrm{Disc}(\mathcal{O}) \text{ and } \ell \leq B\}, \text{ and}$$
$$P_2 = \{\ell \mid \ell \text{ is an odd prime factor of } \mathrm{Disc}(\mathcal{O}) \text{ and } \ell > B\}.$$

For each $\ell \in P_1$, compute $\chi_\ell([\mathfrak{c}])$ in time $\ell^{O(1)}$ using Theorem 4.4.1 and the fact that $(E', \iota') = [\mathfrak{c}](E, \iota)$. Now, with [3], one can compute square roots in $\mathrm{Cl}(\mathcal{O})$ in polynomial time, so we get an ideal $\mathfrak{a}$ such that $[\mathfrak{a}]$ and $[\mathfrak{c}]$ differ by a two-torsion factor. From [3], one also gets a basis of $\mathrm{Cl}(\mathcal{O})[2]$, so we can ensure that $\chi_\ell([\mathfrak{a}]) = \chi_\ell([\mathfrak{c}])$ for each $\ell \in P_1$. The solution is now of the form $[\mathfrak{c}] = [\mathfrak{a}][\mathfrak{b}]$ where $[\mathfrak{b}]$ is in the subgroup G of $\mathrm{Cl}(\mathcal{O})[2]$ of classes such that $\chi_\ell([\mathfrak{b}]) = 1$ for all $\ell \in P_1$. Therefore, the number of remaining candidates for the class $[\mathfrak{c}]$ is $\#G \leq 2^{\#P_2+1}$. These can be enumerated (from the basis of $\mathrm{Cl}(\mathcal{O})[2]$, deduce a basis of the subgroup G) and checked for correctness in polynomial time using Proposition 4.5.6 and the provided basis of $\mathrm{End}(E)$. Overall, the running time is polynomial in $\log p$, $\log|\mathrm{Disc}(\mathcal{O})|$, B, and $2^{\#P_2}$. The running time follows by choosing $B = \min\left(2^{\omega(D)}, \max_i\left(\ell_i \mid \ell_i \leq 2^{\omega(D)-i}\right)\right)$.

Let us prove the last inequality. First, $2^{\omega(D)} \ll \#(\mathrm{Cl}(\mathcal{O})[2])$, so $B \ll \#(\mathrm{Cl}(\mathcal{O})[2])$. Second, if $\{\ell_i \mid \ell_i \leq 2^{\omega(D)-i}\}$ is empty, then $2^{\omega(D)-1} < \ell_1 \leq \ell_{\omega(D)}$ so $2^{\omega(D)} \ll \ell_{\omega(D)}$. If it is not empty, clearly $\max_i\left(\ell_i \mid \ell_i \leq 2^{\omega(D)-i}\right) \ll \ell_{\omega(D)}$. In both cases, we deduce $B \ll \ell_{\omega(D)}$. Lastly, it remains to see that $B \ll L_D(1/2)$. Suppose there exists j such that $\ell_j = \max_i\left(\ell_i \mid \ell_i \leq 2^{\omega(D)-i}\right)$. We have $\log_2(\ell_j) \leq \omega(D) - j$, and

$$\log_2(D) \geq \sum_{i=j+1}^{\omega(D)} \log_2(\ell_i) \geq (\omega(D) - j)\log_2(\ell_j) \geq \log_2(\ell_j)^2.$$

[8] With the convention that $\max(\emptyset) = +\infty$.

We deduce that $\ell_j \leq 2^{\log_2(D)^{1/2}}$, hence $B \ll L_D(1/2)$. If there exists no such j, then

$$\log_2(D) \geq \sum_{i=1}^{\omega(D)} \log_2(\ell_i) \geq \sum_{i=1}^{\omega(D)} (\omega(D) - i) = \Theta(\omega(D)^2),$$

so $2^{\omega(D)} = L_D(1/2)$, hence $B \ll L_D(1/2)$. □

The main result of this section is the following theorem.

Theorem 4.5.7 (ERH, reduction of Effective $\mathcal{O}$-Vectorization to $\mathcal{O}$-EndRing) *Given an order $\mathcal{O}$ of discriminant $-D$, the factorization $D = \prod_{i=1}^{\omega(D)} \ell_i^{e_i}$ (with $\ell_i < \ell_{i+1}$), three $\mathcal{O}$-oriented elliptic curves (E, ι), (E', ι'), $(F, \jmath) \in \mathcal{Ell}_{\mathcal{O}}(k)$, together with bases of* $\mathrm{End}(E)$, $\mathrm{End}(E')$ *and* $\mathrm{End}(F)$*, one can compute (or assert that it does not exist) an $\mathcal{O}$-ideal $\mathfrak{c}$ such that $(E', \iota') = [\mathfrak{c}](E, \iota)$ and an efficient representation of $\varphi_{\mathfrak{c}} : (F, \jmath) \to [\mathfrak{c}](F, \jmath)$ in probabilistic polynomial time in the length of the input and in*

$$\min\left(2^{\omega(D)}, \max_i \left(\ell_i \mid \ell_i \leq 2^{\omega(D)-i}\right)\right) \ll \min\left(L_D(1/2), \#(\mathrm{Cl}(\mathcal{O})[2]), \ell_{\omega(D)}\right).$$

Here, by "probabilistic polynomial time in the length of the input", we mean probabilistic polynomial time in $\log p$, $\log D$, *the lengths of ι, ι', and $\jmath$, and in the lengths of the bases of* $\mathrm{End}(E)$, $\mathrm{End}(E')$, *and* $\mathrm{End}(F)$.

Remark 4.5.8 This improves the result of [31, Thm. 2] in two ways. First, the worst case is now sub-exponential: when D is primorial, the running time of [31, Thm. 2] could reach about $D^{1/\log\log D}$, while it is now always at most $L_D(1/2)$. Second, Theorem 4.5.7 is now very efficient for a new important family of discriminants: when almost all prime divisors of D are small, no matter how many there are. In particular, primorial numbers (the worst case of [31, Thm. 2]) now benefit from a polynomial time algorithm. ◊

Proof. Thanks to Proposition 4.5.5, the proof is a straightforward adaptation of the proof of [31, Thm. 2]. Suppose we are given $(E, \iota), (E', \iota') \in \mathcal{Ell}_{\mathcal{O}}(k)$, together with $\mathrm{End}(E)$ and $\mathrm{End}(E')$. Consider the involution $\tau_p : \mathcal{Ell}_{\mathcal{O}}(k) \to \mathcal{Ell}_{\mathcal{O}}(k)$ defined in [31, Def. 7] as $\tau_p(E, \iota) = (E^{(p)}, (\phi_p)_* \bar{\iota})$, where $\bar{\iota}$ is the conjugate of ι (i.e., $\bar{\iota}(\alpha) = \iota(\overline{\alpha})$ for any $\alpha \in \mathcal{O}$), and $\phi_p : E \to E^{(p)}$ is the Frobenius isogeny.

Then, per [31, Prop. 11], one can compute $\mathfrak{a}$ and $\mathfrak{b}$ such that $\tau_p(E, \iota) = [\mathfrak{a}](E, \iota)$ and $\tau_p(E', \iota') = [\mathfrak{b}](E', \iota')$ in polynomial time. From [31, Lem. 10], the ideal class of $\mathfrak{c}$ is one of the $\#(\mathrm{Cl}(\mathcal{O})[2])$ square roots of $[\mathfrak{a}\overline{\mathfrak{b}}]$. Therefore, the ideal $\mathfrak{c}$ can be found by Proposition 4.5.5 within the claimed running time. Finally, compute an efficient representation of $\varphi_{\mathfrak{c}} : (F, \jmath) \to [\mathfrak{c}](F, \jmath)$ in polynomial time with Proposition 4.5.6. □

Corollary 4.5.9 (ERH) *Given an order $\mathcal{O}$ of discriminant $-D$, and the factorization $D = \prod_{i=1}^{\omega(D)} \ell_i^{e_i}$ (with $\ell_i < \ell_{i+1}$),* Effective $\mathcal{O}$-Uber *reduces to* $\mathcal{O}$-EndRing* *in*

probabilistic polynomial time in the length of the instance and in

$$\min\left(2^{\omega(D)}, \max_i\left(\ell_i \mid \ell_i \leq 2^{\omega(D)-i}\right)\right) \ll \min\left(L_D(1/2), \#(\mathrm{Cl}(\mathcal{O})[2]), \ell_{\omega(D)}\right).$$

Here, by "probabilistic polynomial time in the length of the instance", we mean probabilistic polynomial time in $\log p$, $\log D$, *and in the lengths of the orientations.*

Proof. Again, this is a straightforward adaptation of [31, Cor. 4]. Suppose we are given $(E, \iota), (F, \jmath) \in \mathcal{Ell}_{\mathcal{O}}(k)$ and an $\mathcal{O}$-orientable elliptic curve E'. Solving $\mathcal{O}$-EndRing*, one can find ε-bases of $\mathrm{End}(E)$, $\mathrm{End}(F)$ and $\mathrm{End}(E')$, and an $\mathcal{O}$-orientation ι' of E'. The result follows from Theorem 4.5.7. □

4.6 Bibliography

[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] Dan Boneh, Dmitry Kogan, and Katharine Woo. Oblivious pseudorandom functions from isogenies. In *Asiacrypt (2)*, volume 12492 of *Lecture Notes in Computer Science*, pages 520–550. Springer, 2020. https://ia.cr/2020/1532.

[3] Wieb Bosma and Peter Stevenhagen. On the computation of quadratic 2-class groups. *J. Théor. Nombres Bordeaux*, 8(2):283–313, 1996.

[4] Wouter Castryck and Thomas Decru. CSIDH on the surface. In Jintai Ding and Jean-Pierre Tillich, editors, *PQCrypto 2020*, volume 12100 of *Lecture Notes in Computer Science*, pages 111–129. Springer, 2020.

[5] Wouter Castryck, Ann Dooms, Carlo Emerencia, and Alexander Lemmens. A fusion algorithm for solving the hidden shift problem in finite abelian groups. In *PQCrypto*, volume 12841 of *Lecture Notes in Computer Science*, pages 133–153. Springer, 2021. https://eprint.iacr.org/2021/562.

[6] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *Asiacrypt 2018 Pt. 3*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

[7] Wouter Castryck, Lorenz Panny, and Frederik Vercauteren. Rational isogenies from irrational endomorphisms. In *Eurocrypt (2)*, volume 12106 of *Lecture Notes in Computer Science*, pages 523–548. Springer, 2020. https://ia.cr/2019/1202.

[8] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the decisional Diffie-Hellman problem for class group actions using genus theory. In *Crypto (2)*, volume 12171 of *Lectures Notes in Computer Science*, pages 92–120. Springer, 2020. https://ia.cr/2020/151.

[9] Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. In *MathCrypt*, J. Math. Cryptol. (to appear), 2021. https://ia.cr/2021/955.

[10] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptolology*, 14(1):414–437, 2020.

[11] Jean-Marc Couveignes. Hard homogeneous spaces, 2006. Unpublished article, available at https://eprint.iacr.org/2006/291.

[12] 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.

[13] Pierrick Dartois and Luca De Feo. On the security of OSIDH. In *PKC (1)*, volume 13177 of *Lecture Notes in Computer Science*, pages 52–81. Springer, 2022. https://ia.cr/2021/1681.

[14] Luca De Feo, Cyprien Delpech de Saint Guilhem, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Christophe Petit, Javier Silva, and Benjamin Wesolowski. Séta: Supersingular encryption from torsion attacks. In *Asiacrypt (4)*, volume 13093 of *Lecture Notes in Computer Science*, pages 249–278. Springer, 2021. https://ia.cr/2019/1291.

[15] Luca De Feo and Michael Meyer. Threshold schemes from isogeny assumptions. In *PKC (2)*, volume 12111 of *Lecture Notes in Computer Science*, pages 187–212. Springer, 2020. https://ia.cr/2019/1288.

[16] Tako Boris Fouotsa, Péter Kutas, Simon-Philipp Merz, and Yan Bo Ti. On the isogeny problem with torsion point information. In *PKC (1)*, volume 13177 of *Lecture Notes in Computer Science*, pages 142–161. Springer, 2022. https://ia.cr/2021/153.

[17] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In *Asiacrypt (1)*, volume 10031 of *Lecture Notes in Computer Science*, pages 63–91. Springer, 2016. https://ia.cr/2016/859.

[18] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *PQCrypto*, volume 7071 of *Lecture Notes in Computer Science*, pages 19–34. Springer, 2011. https://ia.cr/2011/506.

[19] Kiran S. Kedlaya and Christopher Umans. Fast polynomial factorization and modular composition. In *IEEE FOCS 2008*, pages 146–155, 2008. http://users.cms.caltech.edu/~umans/papers/KU08-final.pdf.

[20] Yi-Fu Lai, Steven D. Galbraith, and Cyprien Delpech de Saint Guilhem. Compact, efficient and UC-secure isogeny-based oblivious transfer. In *Eurocrypt (1)*, volume 12696 of *Lecture Notes in Computer Science*, pages 213–241. Springer, 2021. https://ia.cr/2020/1012.

[21] James S. Milne. Complex multiplication (v0.10), 2020. https://www.jmilne.org/math/CourseNotes/cm.html.

[22] Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields Appl.*, 69:Paper No. 101777, 18, 2021.

[23] Michael Rabin. Probabilistic algorithms in finite fields. *SIAM J. Comput.*, 9(2):273–280, 1980. http://publications.csail.mit.edu/lcs/pubs/pdf/MIT-LCS-TR-213.pdf.

[24] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. IACR Cryptology ePrint Archive 2006/145, 2006. https://ia.cr/2006/145.

[25] Hans-Georg Rück. A note on elliptic curves over finite fields. *Math. Comp.*, 49(179):301–304, 1987.

[26] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[27] Peter Stevenhagen. Rédei-matrices and applications. In *Number theory (Paris, 1992–1993)*, volume 215 of *London Math. Soc. Lecture Note Ser.*, pages 245–259. Cambridge Univ. Press, Cambridge, 1995.

[28] Anton Stolbunov. Cryptographic schemes based on isogenies. 2012. PhD thesis. `https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/262577/529395_FULLTEXT01.pdf`.

[29] 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.

[30] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.*, 2:521–560, 1969.

[31] Benjamin Wesolowski. Orientations and the supersingular endomorphism ring problem. In *Eurocrypt (3)*, volume 13277 of *Lecture Notes in Computer Science*, pages 345–371. Springer, 2022.

[32] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *IEEE FOCS 2021*, pages 1100–1111, 2022.