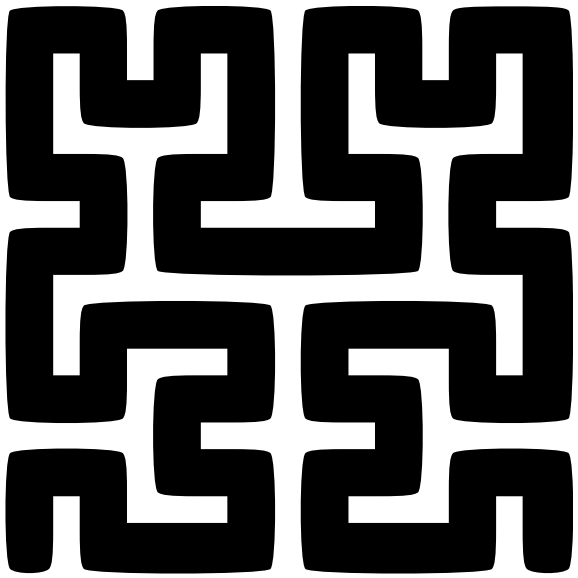

Polynesian Journal of Mathematics

Volume 4, Issue 4

Special volume AJAX in honor of René Schoof

Distortion maps for elliptic curves over finite fields

Nikita Andrusov
Sevag Büyüksimkeşyan
Dimitrios Noulas
Fabien Pazuki
Mustafa Umut Kazancioğlu
Jordi Vilà-Casadevall

Received 14 Jan 2026
Revised 8 Apr 2026
Accepted 19 Apr 2026
Published 28 Sep 2026
Communicated by Elisa Lorenzo García
DOI: 10.69763/polyjmath.4.4

Polynesian Journal of Mathematics
Volume 4, Issue 4 (Sept. 2026)
Special volume AJAX in honor of René Schoof

Distortion maps for elliptic curves over finite fields

Nikita Andrusov[1] Sevag Büyüksimkeşyan[2] Dimitrios Noulas[3]
Fabien Pazuki[4] Mustafa Umut Kazancıoğlu[5]
Jordi Vilà-Casadevall[6]

[1]School of Applied Mathematics and Computer Science,
Moscow Institute of Physics and Technology, Russia
[2]Mathematical Institute, University of Münster, Germany
[3]Department of Mathematics, National and Kapodistrian University of Athens, Greece
[4]Department of Mathematical Sciences, University of Copenhagen, Denmark
[5]Bernoulli Institute, Rijksuniversiteit Groningen, The Netherlands
[5]Faculty of Engineering and Natural Sciences, Sabancı University, İstanbul, Turkey
[6]School of Mathematics, University of Bristol, United Kingdom

Abstract

The Weil pairing on elliptic curves has deep links with discrete logarithm problems, as can be seen, for instance, in [33, 24]. In practice, to better suit the functionalities of cryptosystems, one often needs to modify the original Weil pairing via what is called a distortion map. We propose a study on the question of the existence of distortion maps for elliptic curves over finite fields. We revisit results from the literature and provide detailed proofs. We also propose new perspectives at times.

Keywords: Elliptic curves, Weil pairings, distortion maps.

1 Introduction

Elliptic curves over finite fields are a cornerstone of modern public-key cryptography. Their main advantage over classical cryptographic systems, which use multiplicative groups of finite fields, lies in the apparent difficulty of the Elliptic Curve Discrete Logarithm Problem (DLP). Because no sub-exponential algorithm is known for solving the DLP in most cases, elliptic curve cryptography (ECC) achieves a comparable level of security with much smaller key sizes. This efficiency makes ECC particularly appealing for applications with limited computational or storage resources.

Beyond the DLP, many cryptographic protocols, such as the Diffie–Hellman key exchange, rely on the hardness of the related Decision Diffie–Hellman (DDH) problem. For a cyclic group $G = \langle P \rangle$ of order m, the DDH problem is to computationally distinguish tuples of the form (aP, bP, abP) from random tuples of the form (aP, bP, cP), where

a, b, c are natural integers. For an elliptic curve E over a finite field $\mathbb{F}_q$, the mathematical framework for analyzing the DDH problem relies on the Weil pairing. The Weil pairing $e_m : E[m] \times E[m] \to \mu_m$ is a bilinear, non-degenerate map, where $E[m]$ stands for the m-torsion subgroup of the rational points of the curve $E(\overline{\mathbb{F}}_q)$, and where μ_m is the group of m^{th} roots of unity. We refer the reader to [36, Chapter III.8] for the definition and for the basic properties of this pairing, and to [5] for links between the Weil pairing and identity-based encryption protocols.

A critical property of the Weil pairing is that it is alternating, meaning $e_m(Q, Q) = 1$ for any point $Q \in E[m]$. This property renders the Weil pairing useless for solving the DDH problem within the cyclic subgroup $\langle P \rangle$. We have $e_m(aP, bP) = e_m(P, P)^{ab} = 1$ and $e_m(P, cP) = e_m(P, P)^c = 1$, so the pairing is incapable of distinguishing the valid Diffie–Hellman tuple. This limitation motivates the central question of this paper. The concept of *distortion map* serves to overcome this problem. A distortion map is an endomorphism $\phi : E \to E$ with the property that for a point P of order m, its image $\phi(P)$ does not lie in the cyclic subgroup generated by P; that is, $\phi(P) \notin \langle P \rangle$. We say that a map is a distortion map for $E[m]$ if it is a distortion map for each point in $E[m] \setminus \{O\}$.

The existence of such a map allows for the construction of a modified, non-degenerate pairing $e_{m,\phi}$ defined by $e_{m,\phi}(P, Q) = e_m(P, \phi(Q))$ for all $P, Q \in E[m]$. The bilinearity of the Weil pairing, combined with the fact that $\{P, \phi(P)\}$ can form a basis for $E[m]$, ensures that $e_{m,\phi}(P, P)$ can be a primitive m^{th} root of unity. This modified pairing can be used to efficiently solve the DDH problem in $\langle P \rangle$ by simply checking if $e_{m,\phi}(aP, bP) \stackrel{?}{=} e_{m,\phi}(P, cP)$. Given their critical role in determining the hardness of the DDH problem, a complete characterization of when distortion maps exist is a fundamental question of both theoretical and practical importance.

The Weil pairing on elliptic curves and abelian varieties and its relation to isogenies is also used crucially in outstanding attacks against isogeny-based protocols, as witnessed in [7, Paragraph 4.1, page 427], [23, Lemma 1, page 454], and [29, page 484].

This paper provides cumulative information from the literature related to the existence of distortion maps and their properties. In addition to surveying known results, it provides explicit examples, clarified proofs, and offers new perspectives on several key phenomena; for instance, how distortion maps transfer via isogenies from one curve to another, as well as how to find some criteria for determining when a given isogeny is a distortion map.

The existence of a distortion map is fundamentally an algebraic question about the structure of the curve's endomorphism ring, $\mathrm{End}(E)$. As such, it links to properties of its Frobenius endomorphism, given on affine coordinates by $\pi_q : (x, y) \mapsto (x^q, y^q)$, with classical notions from algebraic number theory: orders in quadratic number fields, quaternions, splitting properties of ideals, etc. There is a deep connection between the study of $\mathrm{End}(E)$ and René Schoof's work, we refer to [31, 32, 33] for some explicit links. In algorithmic number theory, we notably have Schoof's algorithm [32]. It computes efficiently the number of points on an elliptic curve $E/\mathbb{F}_q$. Its primary computation is finding the trace of the Frobenius endomorphism, denoted t. The number of points is then derived from this trace by Hasse's theorem, which reads $\#E(\mathbb{F}_q) = q + 1 - t$. In

most successful implementations of protocols involving elliptic curves, accessing the cardinality of the abelian group $E(\mathbb{F}_q)$ is crucial.

The cryptographic consequences of distortion maps are profound. On one hand, for any cryptographic system whose security relies on the hardness of the DDH problem in a subgroup $\langle P \rangle$, the existence of a distortion map for $\langle P \rangle$ is a weakness, as it renders the problem easier. For these applications, one must specifically choose curves that strictly lack distortion maps. On the other hand, the entire field of pairing-based cryptography, which enables advanced constructions such as identity-based encryption, short signatures, and attribute-based encryption, requires an efficiently computable, non-degenerate bilinear pairing. Distortion maps are one of the primary mechanisms used to construct these necessary pairings. Therefore, understanding the existence of distortion maps is essential for both the construction of cryptographic schemes and for cryptographic security analysis.

The article is divided into sections. Section 2 establishes the mathematical foundation by introducing distortion maps, alongside some of the key concepts for their study. It provides a criterion in Proposition 2.6 for determining for which points a given isogeny is a distortion map, it details the properties of the modified Weil pairing in Proposition 2.16 and it demonstrates how isogenies can be used to transfer distortion maps between elliptic curves in Proposition 2.19. Following this, Section 3 investigates the case of ordinary elliptic curves, introducing Verheul's theorem and applying the criterion from the previous section to characterize the existence of distortion maps. Section 4 turns to the supersingular case: using a theorem of Tate, we give a proof of Theorem 4.4, ensuring the existence of distortion maps for $E[m]$. Some arguments in the proof are inspired by Verheul's paper [41], who himself credits Schoof[1]. Section 5 reviews algorithmic constructions, specifically those relying on isogeny cycles and the constructive Deuring correspondence, while also summarizing known distortion maps for both supersingular and ordinary curves. Finally, Section 6 extends the framework to higher dimensions, examining briefly distortion maps on Jacobians of curves and supersingular abelian varieties.

Acknowledgments

The authors are indebted to the anonymous referees for suggestions and comments that helped improve the exposition. They thank CIMPA for the summer school "Elliptic curves and their applications" in Yerevan during the period 14–26 July 2025. This is where they started working on the topic of distortion maps. They are grateful to the Institute of Mathematics of the National Academy of Sciences of the Republic of Armenia for hosting the school. Many thanks to Diana Davidova, Tigran Hakobyan, Valentijn Karemaker, Mihran Papikian, and also to Erenay Boyalı, Mahabba El Sahili, and Rahim Rahmati-Asghar, for nice mathematical discussions during the CIMPA school.

[1]It is therefore only fair to thank René Schoof for long-term inspiring mathematics!

Jordi Vilà-Casadevall received the support of a fellowship from the "la Caixa" Foundation (ID 100010434). The fellowship code is LCF/BQ/EU24/12060082. Fabien Pazuki was supported by ANR JINVARIANT (ANR-20-CE40-0003).

2 Distortion maps and modified Weil pairing

2.1 Distortion maps

Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$, where $q = p^n$, p is a prime and $n \geqslant 1$ is an integer. We denote by $\mathrm{End}(E)$ the (geometric) endomorphism ring of E, i.e., the ring of isogenies $E \to E$ defined over $\overline{\mathbb{F}}_q$. This ring can have two possible structures:

- $\mathrm{End}(E)$ is an order in an imaginary quadratic field.
- $\mathrm{End}(E)$ is an order in a definite quaternion algebra over $\mathbb{Q}$.

In the first case, we say that E is *ordinary*. In the second case, we say that E is *supersingular*. For the structure theorem of $\mathrm{End}(E)$, see [36, Chapter III.9] and for the foundational properties of quaternion algebras, see [42].

Throughout this paper, we denote the order of a point $P \in E(\overline{\mathbb{F}}_q)$ in the group of rational points by $\mathrm{ord}_E(P)$. Similarly, for an integer $m > 1$ coprime to p, we denote the group of m^{th} roots of unity in $\overline{\mathbb{F}}_q^\times$ by μ_m and the multiplicative order of $\zeta \in \mu_m$ by $\mathrm{ord}_{\mu_m}(\zeta)$.

Definition 2.1. *Let $P \in E(\overline{\mathbb{F}}_q)$ be a point of order $m > 1$ coprime to p. A distortion map for P (or, equivalently, for the cyclic group $\langle P \rangle$ when m is prime) is an isogeny $\phi \in \mathrm{End}(E)$ such that $\phi(P) \notin \langle P \rangle$. A distortion map for $E[m]$ is an isogeny $\phi \in \mathrm{End}(E)$ such that $\phi(P) \notin \langle P \rangle$ for every $P \in E[m] \setminus \{O\}$.*

The structure of the endomorphism ring of E thus plays a crucial role when studying the existence of distortion maps on E. Another important notion when working with distortion maps for a point $P \in E(\mathbb{F}_q)$ of prime order ℓ is what we call the embedding degree:

Definition 2.2. *For a prime $\ell \neq p$, the embedding degree $k(q, \ell)$ is defined to be the order of q in the multiplicative group $(\mathbb{Z}/\ell\mathbb{Z})^\times$.*

Remark 2.3. The embedding degree $k(q, \ell)$ is the smallest $k \geqslant 1$ for which $\mu_\ell \subseteq \mathbb{F}_{q^k}^\times$. If $E[\ell] \subseteq E(\mathbb{F}_q)$ for some prime $\ell \neq p$, since the Weil pairing is Galois-invariant, $\mu_\ell \subseteq \mathbb{F}_q^\times$, and hence $k(\ell, q) = 1$. On the other side, if $\ell \mid \#E(\mathbb{F}_q)$ and $k(\ell, q) > 1$, a theorem of Balasubramanian and Koblitz [2, Theorem 1] states that $k(\ell, q)$ is the minimal k such that $E[\ell] \subseteq E(\mathbb{F}_{q^k})$.

Any isogeny $\phi \in \mathrm{End}(E)$ induces a $\mathbb{Z}/\ell\mathbb{Z}$-linear endomorphism of $E[\ell]$ by restriction, which we denote by $\phi|_{E[\ell]}$. For a point $P \in E[\ell]$, the condition $\phi(P) \notin \langle P \rangle$ is equivalent to saying that P is not an eigenvector of $\phi|_{E[\ell]}$. Charles [8] used this idea

and the ramification of primes in imaginary quadratic fields to study the existence of distortion maps for ordinary elliptic curves. His methods can be extended to the case of supersingular elliptic curves. To present these, we recall the definition of the Kronecker symbol, which extends the usual Legendre symbol to include the special case of the prime 2:

Definition 2.4. *Let D be an integer and ℓ a prime. For $\ell > 2$, we define the Kronecker symbol $\left(\frac{D}{\ell}\right)$ as the usual Legendre symbol, i.e.,*

$$\left(\frac{D}{\ell}\right) = \begin{cases} 1 & \text{if } D \text{ is a quadratic residue modulo } \ell, \text{ and } \ell \nmid D, \\ -1 & \text{if } D \text{ is a quadratic non-residue modulo } \ell, \\ 0 & \text{if } \ell \mid D. \end{cases}$$

For $\ell = 2$, we set $\left(\frac{D}{2}\right) = 1$ for $D \equiv \pm 1 \bmod 8$, $\left(\frac{D}{2}\right) = -1$ for $D \equiv \pm 3 \bmod 8$, and $\left(\frac{D}{2}\right) = 0$ if $2 \mid D$.

Remark 2.5. If K is a quadratic imaginary number field with fundamental discriminant D_K, then a prime ℓ splits in K if $\left(\frac{D_K}{\ell}\right) = 1$, ramifies in K if $\left(\frac{D_K}{\ell}\right) = 0$, and remains inert in K if $\left(\frac{D_K}{\ell}\right) = -1$ (see [10, Proposition 5.16]). In particular, since it always holds that $D_K \equiv 0, 1 \bmod 4$, the prime $\ell = 2$ is split if $D_K \equiv 1 \bmod 8$, is inert if $D_K \equiv 5 \bmod 8$ and ramifies if $4 \mid D_K$.

Let $B = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ be the endomorphism algebra of E, which is either an imaginary quadratic field or a definite quaternion algebra over $\mathbb{Q}$. In both cases, for a given isogeny $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$, one has that $\mathbb{Z}[\phi] \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic subfield of B, which we denote by K_ϕ. Then $\mathbb{Z}[\phi]$ is an order in K_ϕ.

Proposition 2.6. *Let $\ell \neq p$ be a prime and $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$ be an isogeny. Let D_ϕ be the discriminant of $\mathbb{Z}[\phi] \subseteq K_\phi$. If $\ell \mid \left[\mathrm{End}(E) \cap K_\phi : \mathbb{Z}[\phi]\right]$, then ϕ is not a distortion map for any $P \in E[\ell] \setminus \{O\}$. Otherwise,*

1. *$\left(\frac{D_\phi}{\ell}\right) = 1$ if and only if ϕ is a distortion map for all but two cyclic subgroups of $E[\ell]$.*
2. *$\left(\frac{D_\phi}{\ell}\right) = -1$ if and only if ϕ is a distortion map for $E[\ell]$.*
3. *$\left(\frac{D_\phi}{\ell}\right) = 0$ if and only if ϕ is a distortion map for all but one cyclic subgroup of $E[\ell]$.*

Proof. Let $\mathcal{O}_{K_\phi}$ be the ring of integers of K_ϕ and consider the inclusion of orders $\mathbb{Z}[\phi] \subseteq \mathrm{End}(E) \cap K_\phi \subseteq \mathcal{O}_{K_\phi}$. Let $f = \left[\mathrm{End}(E) \cap K_\phi : \mathbb{Z}[\phi]\right]$ and $f' = \left[\mathcal{O}_{K_\phi} : \mathrm{End}(E) \cap K_\phi\right]$. Then $ff' = \left[\mathcal{O}_{K_\phi} : \mathbb{Z}[\phi]\right]$. We denote the fundamental discriminant of $\mathcal{O}_{K_\phi}$ by D_{K_ϕ}, so $D_\phi = (ff')^2 D_{K_\phi}$.

Assume first that $\ell \mid f$ and let $\beta \in \mathrm{End}(E) \cap K_\phi$ be generator of this order, i.e., $\mathrm{End}(E) \cap K_\phi = \mathbb{Z}[\beta]$. Then, $\mathbb{Z}[\phi] = \mathbb{Z}[f\beta]$. Hence, after changing the sign of β if necessary, we can write $\phi = a + f\beta$ for some $a \in \mathbb{Z}$. Since multiplication by f induces the 0 map on $E[\ell]$, we have that $\phi|_{E[\ell]} = a|_{E[\ell]}$, so ϕ is not a distortion map for any $P \in E[\ell] \setminus \{O\}$.

From now on, we assume that $\ell \nmid f$. The rest of the proof relies on the splitting properties of the characteristic polynomial of ϕ, which we denote by χ_ϕ. We link these properties with the distorsion property on the one hand, and link the same properties with the Kronecker symbol on the other hand, which will be enough to conclude.

Observe that the characteristic polynomial of $\phi|_{E[\ell]}$ as a linear map on $E[\ell]$ is the reduction $\bar{\chi}_\phi$ of χ_ϕ modulo ℓ. Three possible situations may occur:

(i) $\bar{\chi}_\phi(x) \in \mathbb{F}_\ell[x]$ is irreducible,

(ii) $\bar{\chi}_\phi(x) = (x - \bar{a})(x - \bar{b})$ for two different $\bar{a}, \bar{b} \in \mathbb{F}_\ell$,

(iii) $\bar{\chi}_\phi(x) = (x - \bar{a})^2$ for some $\bar{a} \in \mathbb{F}_\ell$.

In Situation (i), since $\bar{\chi}_\phi$ doesn't have roots in $\mathbb{F}_\ell$, the map $\phi|_{E[\ell]}$ doesn't have eigenvectors, so ϕ is a distortion map for $E[\ell]$. In Situation (ii), $\phi|_{E[\ell]}$ has two different eigenvalues, and hence two different one-dimensional eigenspaces. Thus ϕ is a distortion map for a point P if and only if P does not lie in any of the eigenspaces. In Situation (iii), $\phi|_{E[\ell]}$ has a unique eigenvalue. The corresponding eigenspace could be 1 or 2-dimensional. We claim that it is necessarily 1-dimensional. Assume otherwise. Then $\phi|_{E[\ell]} = a|_{E[\ell]}$ for some integer $a \in \mathbb{Z} \subseteq \mathrm{End}(E)$. This implies that $\ker(\ell) \subseteq \ker(\phi - a)$. Since multiplication by ℓ is a separable isogeny, as $\ell \neq p$, there exist some $\psi \in \mathrm{End}(E)$ with $\ell\psi = \phi - a$ (see [36, Corollary III.4.11]). As we have $\mathbb{Z}[\phi] = \mathbb{Z}[\ell\psi]$, we get $\mathbb{Z}[\psi] \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Z}[\phi] \otimes_{\mathbb{Z}} \mathbb{Q} = K_\phi$, and hence $\psi \in \mathrm{End}(E) \cap K_\phi$. Moreover, $\ell = [\mathbb{Z}[\psi] : \mathbb{Z}[\phi]] \mid f$, which contradicts our assumptions. This proves the claim. In Situation (iii), ϕ is a distortion map for all points P not lying in the one-dimensional eigenspace of $\phi|_{E[\ell]}$.

Consider now as a first subcase that $\ell \mid f'$, so $\ell \mid ff'$. Let $\alpha \in \mathcal{O}_{K_\phi}$ be a generator of the ring of integers, i.e., $\mathcal{O}_{K_\phi} = \mathbb{Z}[\alpha]$. Changing the sign of α if necessary, we can write $\phi = a + ff'\alpha$ for some $a \in \mathbb{Z}$. Let $\chi_\alpha(x) = x^2 + bx + c$, with $b, c \in \mathbb{Z}$, be the characteristic polynomial of α. Then $\chi_\phi(x) = (x - a)^2 + bff'(x - a) + c(ff')^2$, and hence $\bar{\chi}_\phi(x) = (x - \bar{a})^2$, i.e., we are in Situation (iii). Since $\ell \mid D_\phi = (ff')^2 D_K$, in this subcase ($\ell \mid f'$), we have $\left(\frac{D_\phi}{\ell}\right) = 0$.

Consider now that $\ell \nmid f'$, so $\ell \nmid ff'$. By the Dedekind–Kummer theorem (see [9, Theorem 1]), Situation (i) occurs precisely when ℓ remains inert in K_ϕ, Situation (ii) when ℓ splits in K_ϕ, and Situation (iii) when ℓ ramifies in K_ϕ. The first case takes place precisely when $\left(\frac{D_K}{\ell}\right) = -1$ and, since D_ϕ and D_K differ by a non-zero square modulo ℓ, this is equivalent to saying that $\left(\frac{D_\phi}{\ell}\right) = -1$. The second case occurs precisely when $\left(\frac{D_K}{\ell}\right) = 1$. Again, this is equivalent to saying that $\left(\frac{D_\phi}{\ell}\right) = 1$. Finally, the third case occurs precisely when $\ell \mid D_K$, which is equivalent to $\ell \mid D_\phi$ and $\left(\frac{D_\phi}{\ell}\right) = 0$. □

One can derive several interesting consequences from the previous proposition. The first one allows us to determine when a given isogeny is a distortion map for $E[m]$ for some integer m. Before stating it, we first show the following fact:

Lemma 2.7. *Let $m > 1$ be an integer coprime to p. An isogeny ϕ is a distortion map for $E[m]$ if and only if ϕ is a distortion map for $E[\ell]$ for all primes $\ell \mid m$. In particular, ϕ is a distortion map for $E[\ell]$ if and only if it is for $E[\ell^n]$, for all integers $n \geqslant 1$.*

Proof. The direct implication is trivial as $E[\ell] \subseteq E[m]$ for all $\ell \mid m$. We prove the inverse implication by contrapositive. Assume ϕ is not a distortion map for $E[m]$ and let $P \in E[m]$ be a non-trivial point with $\phi(P) = aP$ for some $a \in \mathbb{Z}$. Let ℓ be a prime with $\ell \mid \mathrm{ord}_E(P)$. Then $Q \coloneqq \frac{\mathrm{ord}_E(P)}{\ell} P$ is a point of order ℓ. Moreover,

$$\phi(Q) = \phi\left(\frac{\mathrm{ord}_E(P)}{\ell} P\right) = \frac{\mathrm{ord}_E(P)}{\ell} aP = aQ,$$

so ϕ is not a distortion map for $E[\ell]$. □

Corollary 2.8. *Let $m > 1$ be an integer coprime to p, $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$ and $D_\phi = \mathrm{disc}(\mathbb{Z}[\phi])$. Then, ϕ is a distortion map for $E[m]$ if and only if $\left(\frac{D_\phi}{\ell}\right) = -1$ for all $\ell \mid m$.*

Proof. Combine Proposition 2.6 and Lemma 2.7. □

Another consequence of Proposition 2.6 is that there is no universal distortion map:

Corollary 2.9. *There is no $\phi \in \mathrm{End}(E)$ that is a distortion map for every point of E of order coprime to p.*

Proof. Fix $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$ and write $D_\phi = \mathrm{Disc}(\mathbb{Z}[\phi])$. For a given $\ell \neq p$, Proposition 2.6 tells us that ϕ is a distortion map for $E[\ell]$ if and only if $\left(\frac{D_\phi}{\ell}\right) = -1$. Since $D_\phi < -1$, there is at least one prime ℓ with $\left(\frac{D_\phi}{\ell}\right) = 0$, which is enough to conclude. □

Remark 2.10. One can say more using the Chebotarev density theorem (see Serre's book [34, Chapter I, Section 2.2]). The theorem states that for an extension of $\mathbb{Q}$ of degree n, splitting primes have density $\frac{1}{n}$. Therefore in the case of a quadratic extension with discriminant D_ϕ, as only finitely many primes are ramified (the divisors of D_ϕ), one has that $\left(\frac{D_\phi}{\ell}\right) = 1$ for 50% of the primes ℓ and $\left(\frac{D_\phi}{\ell}\right) = -1$ for the remaining 50%. This means that any given ϕ is a distortion map for only half the groups $E[\ell]$, when ℓ grows in the natural sequence of primes.

2.2 The trace map

We saw in the previous section how to determine whether a given isogeny is a distortion map. For any elliptic curve $E/\mathbb{F}_q$, one can always consider the q^{th} power Frobenius endomorphism π_q (see, for instance, [36, Example III.4.6, page 70]). Another isogeny that is sometimes used as a distortion map is the trace map, which we now define. Let us denote by π_q^0 the identity map on E, and for any integer $i \geqslant 0$, consider $\pi_q^{i+1} = \pi_q \circ \pi_q^i$.

Definition 2.11. *Let $n \geqslant 1$ be an integer. The n^{th} trace map is the isogeny*

$$\mathrm{Tr}_n \coloneqq \sum_{i=0}^{n-1} \pi_q^i \in \mathrm{End}(E).$$

Remark 2.12. One can show that for any $n \geqslant 1$ and any point $P \in E(\mathbb{F}_{q^n})$, one has that $\mathrm{Tr}_n(P) \in E(\mathbb{F}_q)$. Moreover, if $P \in E(\mathbb{F}_q)$, then $\mathrm{Tr}_n(P) = nP$.

From now on, in this subsection, we fix a prime $\ell \neq p$ with $\ell \mid \#E(\mathbb{F}_q)$ and denote the embedding degree $k(q, \ell)$ by k. We shall see that, when $k > 1$, the k^{th} trace map allows us to construct a distortion map for certain points.

Lemma 2.13. *Assume $k > 1$. Then $\pi_q|_{E[\ell]}$ has two different eigenspaces, with respective eigenvalues equal to* 1 *and q.*

Proof. As ℓ is a prime dividing $\#E(\mathbb{F}_q)$ by assumption, E has some non-trivial ℓ-torsion point defined over $\mathbb{F}_q$. Such a point is fixed by π_q, and hence the map $\pi_q|_{E[\ell]}$ must have an eigenvector of eigenvalue 1. Let $t = q + 1 - \#E(\mathbb{F}_q)$ denote the trace of π_q. The characteristic polynomial of $\pi_q|_{E[\ell]}$ is the reduction modulo ℓ of the characteristic polynomial of π_q, and hence given by $X^2 - \bar{t}X + \bar{q}$. As $t \equiv q + 1 \bmod \ell$, this polynomial factors as $(X - \bar{1})(X - \bar{q})$. Observe that $\bar{1}$ and $\bar{q}$ are different if and only if $q \not\equiv 1 \bmod \ell$. This is equivalent to saying that $k > 1$ by definition of the embedding degree. □

The eigenspace of $\pi_q|_{E[\ell]}$ of eigenvalue 1 is $E(\mathbb{F}_q)[\ell]$. As explained in Remark 2.12, the points $P \in E(\mathbb{F}_q)[\ell]$ satisfy that $\mathrm{Tr}_k(P) = kP$, and hence Tr_k is not a distortion map for these points. Boneh showed that the eigenspace of $\pi_q|_{E[\ell]}$ of eigenvalue q is precisely the set of points $P \in E[\ell]$ of k^{th} trace 0 (see [4, Lemma 3] or [14, Lemma IX.16]). Hence, Tr_k is not a distortion map for this eigenspace either. The following lemma shows that the k^{th} trace map is a distortion map for all other points:

Lemma 2.14. *Assume $k > 1$. Let $P \in E[\ell]$ be a point not lying in one of the eigenspaces of $\pi_q|_{E[\ell]}$. Then Tr_k is a distortion map for P.*

Proof. Observe that, since k is the order of q in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, we have $k \mid \ell - 1$. In particular, $\ell \nmid k$. Thus, the action of the k^{th} trace map on $E[\ell]$ has two different eigenvalues: k and 0. As explained before, the eigenspaces of $\mathrm{Tr}_k|_{E[\ell]}$ associated with the eigenvalues k and 0 coincide, respectively, with the eigenspaces of $\pi_q|_{E[\ell]}$ of eigenvalues 1 and q. Hence, if P does not lie in an eigenspace of $\pi_q|_{E[\ell]}$, it does not lie in an eigenspace of $\mathrm{Tr}_k|_{E[\ell]}$ either. The result follows. □

2.3 Modified Weil pairing

The interest of distortion maps comes from the fact that they allow us to modify the usual Weil pairing e_m on $E[m]$ to obtain a new pairing that is not skew-symmetric, but preserves all the other interesting properties of e_m. To describe it, let us fix an integer $m > 1$ coprime to p and a distortion map $\phi \in \mathrm{End}(E)$ for $E[m]$.

Recall that the standard Weil pairing $e_m : E[m] \times E[m] \to \mu_m$ is constructed via functions on E with specified divisors (we refer the reader to [36, Chapter III.8] for the formal definition and fundamental properties).

Definition 2.15. *The modified Weil pairing with respect to ϕ on $E[m]$ is the pairing*

$$e_{m,\phi} : \begin{cases} E[m] \times E[m] \longrightarrow \mu_m \\ (P, Q) \longmapsto e_m(P, \phi(Q)) \end{cases}$$

where e_m is the Weil pairing on the m^{th} torsion points.

Proposition 2.16. *The modified Weil pairing satisfies the following properties:*

(1) Bilinearity: for all $P_1, P_2, Q, P, Q_1, Q_2 \in E[m]$,

$$e_{m,\phi}(P_1 + P_2, Q) = e_{m,\phi}(P_1, Q)e_{m,\phi}(P_2, Q),$$
$$e_{m,\phi}(P, Q_1 + Q_2) = e_{m,\phi}(P, Q_1)e_{m,\phi}(P, Q_2).$$

(2) Distortion: let $P \in E[m]$ be a point with $\mathrm{ord}_E(P) = m$. Then,

$$\mathrm{ord}_{\mu_m}\left(e_{m,\phi}(P, P)\right) = m.$$

(3) Nondegeneracy: Fix $Q \in E[m]$.

$$\text{If } e_{m,\phi}(P, Q) = 1 \text{ for all } P \in E[m], \text{ then } Q = O.$$
$$\text{If } e_{m,\phi}(P, Q) = 1 \text{ for all } Q \in E[m], \text{ then } P = O.$$

(4) Compatibility: if $m = dd'$, then

$$e_{m,\phi}(P, Q) = e_{d,\phi}(d'P, Q) \text{ for all } P \in E[m] \text{ and all } Q \in E[d].$$
$$e_{m,\phi}(P, Q) = e_{d,\phi}(P, d'Q) \text{ for all } P \in E[d] \text{ and all } Q \in E[m].$$

(5) Galois invariance: assume ϕ is defined over $\mathbb{F}_{q^k}$. For all $P, Q \in E[m]$,

$$e_{m,\phi}(P^\sigma, Q^\sigma) = e_{m,\phi}(P, Q)^\sigma \text{ for all } \sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^k}).$$

Proof. Properties (1) and (4) follow from the linearity of ϕ and the analogous properties for the Weil pairing (see [36, Proposition III.8.1]). Property (5) follows from the fact that if $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^k})$, then $\phi(P^\sigma) = \phi(P)^\sigma$, and the corresponding property of e_m.

To show Property (3), observe that $\phi|_{E[m]}$ is an isomorphism. Indeed, since $E[m]$ is finite, it suffices to show injectivity. By definition of a distortion map, if $P \neq O$, then $\phi(P) \notin \langle P \rangle$. In particular, $\ker \phi|_{E[m]} = \{O\}$. Property (3) then follows from the analogous property of the Weil pairing.

Finally, to prove Property (2), let P be a point of order m and let Q be a point such that P, Q form a basis of the $\mathbb{Z}/m\mathbb{Z}$-module $E[m]$. If $e_m(P, \phi(P))$ is of order s for some integer $s < m$, then $\phi(P) = aP + \frac{bm}{s}Q$ for some $a, b \in \mathbb{Z}$. Then $\phi(sP) \in \langle P \rangle$ and $sP \neq O$ which contradicts the distortion property of ϕ. Therefore $e_m(P, \phi(P))$ is of order m. □

When m is square-free, the following stronger version of the distortion property for the modified Weil pairing holds:

Corollary 2.17 (strong distortion)**.** *Assume m is square-free, let $n \mid m$, and let $P \in E[m]$ be a point with $\mathrm{ord}_E(P) = n$. Then,*

$$\mathrm{ord}_{\mu_m}\left(e_{m,\phi}(P,P)\right) = n.$$

Proof. Write $m = nn'$. By Proposition 2.16.(4), we have that

$$e_{m,\phi}(P,P) = e_{n,\phi}(n'P,P) = e_{n,\phi}(P,P)^{n'}.$$

By Proposition 2.16.(2), the element $e_{n,\phi}(P,P)$ is a primitive n^{th} root of unity. Moreover, since m is square-free, n and n' are coprime. The result follows. □

Remark 2.18. Corollary 2.17 fails if m is not square-free. Indeed, take $m = \ell^2 m'$ and $P \in E[m]$ a point of order ℓ. It follows from the compatibility property that $e_{m,\phi}(P,P) = 1$, even though $\phi(P) \notin \langle P \rangle$.

2.4 Isogeny transfer

One can use isogenies to transfer distortion maps from one elliptic curve to another. Consider two elliptic curves E_1, E_2 over $\mathbb{F}_q$, and an isogeny $\psi : E_1 \to E_2$ of degree $d = \deg(\psi)$. We denote by $\widehat{\psi} : E_2 \to E_1$ the dual isogeny of ψ.

Proposition 2.19. *Let $P \in E_1(\overline{\mathbb{F}}_q)$ be a point of order m coprime to pd, and assume $\phi \in \mathrm{End}(E_1)$ is a distortion map for P. Then $\psi \circ \phi \circ \widehat{\psi} \in \mathrm{End}(E_2)$ is a distortion map for $\psi(P) \in E_2(\overline{\mathbb{F}}_q)$.*

Proof. Let e_m^1 and e_m^2 denote the Weil pairings on $E_1[m]$ and $E_2[m]$, respectively. By the properties of the Weil pairing, it suffices to show that $e_m^2\big(\psi(P), \psi \circ \phi \circ \widehat{\psi}(\psi(P))\big) \neq 1$. Using [36, Proposition III.8.2], we have that

$$e_m^2\left(\psi(P), (\psi \circ \phi \circ \widehat{\psi} \circ \psi)(P))\right) = e_m^1\left((\widehat{\psi} \circ \psi)(P), (\phi \circ \widehat{\psi} \circ \psi)(P)\right) = e_m^1(P, \phi(P))^{d^2}.$$

Since d is coprime to m and $e_m^1(P, \phi(P)) \neq 1$ by Proposition 2.16.(2), the result follows. □

Corollary 2.20. *Let $m > 1$ be an integer coprime to pd and assume $\phi \in \mathrm{End}(E_1)$ is a distortion map for $E_1[m]$. Then $\psi \circ \phi \circ \widehat{\psi} \in \mathrm{End}(E_2)$ is a distortion map for $E_2[m]$.*

Proof. Since d is coprime to m, ψ induces an isomorphism from $E_1[m]$ to $E_2[m]$. The result follows from the previous proposition. □

Remark 2.21. One can apply the previous results to the dual isogeny to show that these are necessary and sufficient conditions.

The endomorphism rings $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$ are orders of the same endomorphism algebra. Moreover, they satisfy $\psi\,\mathrm{End}(E_1)\widehat{\psi} \subseteq \mathrm{End}(E_2)$ and $\widehat{\psi}\,\mathrm{End}(E_2)\psi \subseteq \mathrm{End}(E_1)$ (see [21, page 7]). Hence, if we denote by $\mathcal{D}_{E,P}$ and $\mathcal{D}_{E,m}$ the sets of distortion maps for $P \in E(\overline{\mathbb{F}}_q)$ and $E[m]$ respectively, we have the following result:

Corollary 2.22. *Let $m > 1$ be an integer coprime to pd, and $P \in E_1(\overline{\mathbb{F}}_q)$ and $Q \in E_2(\overline{\mathbb{F}}_q)$ points of order m. Then,*

- $\psi \mathcal{D}_{E_1,P} \widehat{\psi} \subseteq \mathcal{D}_{E_2,\psi(P)}$ *and* $\widehat{\psi} \mathcal{D}_{E_2,Q} \psi \subseteq \mathcal{D}_{E_1,\widehat{\psi}(Q)}$.
- $\psi \mathcal{D}_{E_1,m} \widehat{\psi} \subseteq \mathcal{D}_{E_2,m}$ *and* $\widehat{\psi} \mathcal{D}_{E_2,m} \psi \subseteq \mathcal{D}_{E_1,m}$.

Example 2.23. By an implementation[2] in SageMath [39], we will transfer via isogenies the distortion map from the third example in Table 1. Let $\mathbb{F}_{101^6} = \mathbb{F}_{101}[X]/(X^6 + 2X^4 + 90X^3 + 20X^2 + 67X + 2)$ and z the image of X in $\mathbb{F}_{101^6}$. Let τ be a root of the polynomial $x^2 - 2$, which is not in $\mathbb{F}_{101}$. Consider the elliptic curve

$$E : y^2 = x^3 + \tau + 1 \ / \ \mathbb{F}_{101^2}.$$

Let r be a root of the polynomial $x^2 - (\tau + 1)$ and ω a root of $x^3 - r$ as specified in Table 1. For instance, in $\mathbb{F}_{101^6} = \mathbb{F}_{101}(z)$, one can take:

$$\begin{aligned} \tau &= 56z^5 + 25z^4 + 79z^3 + 20z^2 + 70z + 9, \\ r &= 69z^5 + 29z^4 + 27z^3 + 3z^2 + 61z + 3, \\ \omega &= 38z^5 + 90z^4 + 19z^3 + 94z^2 + 100z + 69. \end{aligned}$$

One has that $\#E(\mathbb{F}_{101^6}) = 2^2 \cdot 3^4 \cdot 7^2 \cdot 13^2 \cdot 17^2 \cdot 37^2$. We pick a nontrivial point $Q \in E[17]$ which, by Vélu's method [40] will yield an isogeny of degree 17, then transfer the properly distorted points of $E[7]$. Note that it is specified in [20] that the map $\phi(x, y) = \left(\omega \frac{x^p}{r^{(2p-1)/3}}, \frac{y^p}{r^{p-1}}\right)$ is a distortion map for the 6 non-trivial points in $E[7](\mathbb{F}_{101^2})$. In fact, we computed that ϕ distorts all but 12 non-trivial points in $E[7]$.

Pick $Q = (32z^5 + 16z^4 + 91z^3 + 59z^2 + 49z, 90z^5 + 51z^4 + 44z^3 + 61z^2 + 62z + 41)$. This gives a 17-degree isogeny $\psi : E \to E'$, where E' is given by the equation $y^2 = x^3 + (70z^5 + 4z^4 + 88z^3 + z^2 + 12z + 43)x + (6z^5 + 64z^4 + 77z^3 + 31z^2 + 58z + 88)$. The new distortion map for E' is

$$\psi \circ \phi \circ \widehat{\psi}(x, y) = (g_1(x, y), g_2(x, y)),$$

where $g_1(x, y), g_2(x, y)$ are too large to be included in the text, but both are easily computed and have leading terms $(32z^5 + 32z^4 - 49z^3 - 50z^2 + 18z + 14)x^{29189}$ and $(-36z^5 + 20z^4 + 43z^3 + 16z^2 - 45z - 10)x^{43632}y^{101}$, respectively.

We check that $\psi \circ \phi \circ \widehat{\psi}$ distorts all but 12 non-trivial points of $E'[7]$. For instance, let $P = (83z^5 + 30z^4 + 59z^3 + 26z^2 + 46z + 100, 36z^5 + 81z^4 + 56z^3 + 23z^2 + 32z + 56) \in E'[7]$, then the modified Weil pairing of $E'[7]$ with respect to $\psi \circ \phi \circ \widehat{\psi}$ maps P to the 7^{th} root of unity $52z^5 + 11z^4 + 12z^3 + 57z^2 + 81z + 72$. However, $P' = (23z^4 + 33z^3 + 89z^2 + 66z + 46, 22z^5 + 30z^4 + 82z^3 + 4z^2 + 75z + 42) \in E'[7]$ is sent to 1.

Remark 2.24. In the previous example, we verified computationally that ϕ and $\psi \circ \phi \circ \widehat{\psi}$ distort all but 2 cyclic subgroups of $E[7]$ and $E'[7]$, respectively. This is consistent with

[2] Code for all the examples is available at: `https://github.com/noulasd/distortion`

the fact that $\phi|_{E[7]}$ has two distinct eigenvalues, which we computed to be 2 mod 7 and 5 mod 7. Indeed, $\phi^2(x,y) = \left(\zeta \cdot x^{101^2}, y^{101^2}\right)$, where $\zeta = r^{-2(101^2-1)/3}$. The element ζ is a primitive cubic root of unity, as $r \in \mathbb{F}_{101^2}$ and is not a cube. We verify that $\phi^2 = [\zeta] \circ \pi_{101^2}$ acts on $E[7]$ as multiplication by 4, yielding the characteristic polynomial $X^2 - 4 \equiv (X-2)(X-5) \bmod 7$.

3 Distortion maps for ordinary elliptic curves

In this section we assume that E is an ordinary elliptic curve defined over $\mathbb{F}_q$ and $\ell \neq p$ is a prime. In this situation, all the endomorphisms of E are defined over $\mathbb{F}_q$ (see, for example, [44, Corollary 2.2]). The following theorem of Verheul shows that points with an embedding degree greater than 1 do not admit a distortion map:

Theorem 3.1 ([41, Theorem 6])**.** *Assume $\ell \mid \#E(\mathbb{F}_q)$ and let $P \in E(\mathbb{F}_q)$ be a point of order ℓ. If $E[\ell]$ is not defined over $\mathbb{F}_q$ (in particular, if the embedding degree $k(q,\ell) > 1$), then there exist no distortion maps for P.*

Proof. We have that $E[\ell] \cap E(\mathbb{F}_q) = \langle P \rangle$. Let $\phi \in \mathrm{End}(E)$ be any isogeny, and $\pi_q \in \mathrm{End}(E)$ be the q^{th} power Frobenius. Recall that a point Q is defined over $\mathbb{F}_q$ if and only if it is fixed by π_q. Observe that $\phi(P) \in E[\ell]$ and, since $\mathrm{End}(E)$ is commutative,

$$\pi_q(\phi(P)) = \phi(\pi_q(P)) = \phi(P),$$

so $\phi(P) \in \langle P \rangle$. Hence, ϕ is not a distortion map for P. □

Since $\mathrm{End}(E)$ is an order in a quadratic imaginary number field, one can apply Proposition 2.6 to its generator to determine the existence of a distortion map for different points of E:

Theorem 3.2. *Let $D = \mathrm{Disc}(\mathrm{End}(E))$. Then,*

1. *If $\left(\frac{D}{\ell}\right) = 1$, all but two cyclic subgroups of $E[\ell]$ admit a distortion map.*
2. *If $\left(\frac{D}{\ell}\right) = -1$, then $E[\ell]$ admits a distortion map.*
3. *If $\left(\frac{D}{\ell}\right) = 0$, then all but one cyclic subgroup of $E[\ell]$ admit a distortion map.*

Proof. Let ω be a generator of $\mathrm{End}(E)$, i.e., $\mathrm{End}(E) = \mathbb{Z}[\omega]$. Then any isogeny $\phi \in \mathrm{End}(E)$ can be written as $\phi = a + b\omega$ for some $a, b \in \mathbb{Z}$. For a given point $P \in E[\ell]$, if ϕ is a distortion map for P, then so is ω. Indeed by contrapositive, one clearly sees that if $\omega(P) \in \langle P \rangle$, then $\phi(P) \in \langle P \rangle$. Hence, a given point P admits a distortion map if and only if ω is a distortion map for P.

Let $K = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ be the endomorphism algebra of ω. Then, using the notation of Proposition 2.6, we have that $K_\omega = K$ and $D_\omega = D$. Since $[\mathrm{End}(E) \cap K_\omega : \mathbb{Z}[\omega]] = 1$ in this setting, the result follows from Proposition 2.6. □

Remark 3.3. Charles [8, Examples 3.1, 3.2, 3.3 and 3.4] gave examples satisfying the different cases from the previous theorem. Theorem 3.2 is a reformulation of Charles' [8, Theorem 2.1]. However, the statement is slightly different from Charles', as we corrected some imprecision: Charles' Theorem 2.1 states that there are no points of $E[\ell]$ that admit a distortion map when $\ell \mid [\mathcal{O}_K : \mathrm{End}(E)]$. Theorem 3.2 shows that, when $\ell \mid [\mathcal{O}_K : \mathrm{End}(E)]$, all but one cyclic subgroup of $E[\ell]$ admit a distortion map. Let us now provide a computational example, extending the idea of Example 3.4 in Charles', where this case has been tested.

Example 3.4 (a case where $\ell \mid [\mathcal{O}_K : \mathrm{End}(E)]$). Let $\mathbb{F}_{13^3} = \mathbb{F}_{13}[X]/(X^3 + 2X + 11)$ and consider the curve $E : y^2 = x^3 + x + 5$ over $\mathbb{F}_{13^3}$. Using SageMath, we compute that $\#E(\mathbb{F}_{13^3}) = 2^2 \cdot 3^4 \cdot 7$, and therefore the trace of the $(13^3)^{\text{th}}$ power Frobenius π_{13^3} is $t = -70$ and the order $\mathbb{Z}[\pi_{13^3}]$ has discriminant $D_{\pi_{13^3}} = -3888$. Observe that E is ordinary. Observe also that $K = \mathbb{Z}[\pi_{13^3}] \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-3})$, which has fundamental discriminant $D_K = -3$. We argue that the conductor $[\mathcal{O}_K : \mathrm{End}(E)]$ is 3 as follows. Let $E'/\mathbb{Q}$ be given by the equation

$$E' : y^2 = x^3 - \frac{120000000}{64009}x + \frac{2000000000}{64009},$$

which reduces to E mod 13. It holds that the j-invariant $j(E') = -12288000$ is a root of the Hilbert class polynomial $H_{-27} = H_{\mathcal{O}}$, for $\mathcal{O}$ being the order of conductor 3 in the maximal order $\mathbb{Z}[(1 + \sqrt{-3})/2]$, as $-27 = 3^2 \cdot D_K$. Therefore $\mathcal{O} \cong \mathrm{End}(E')$. We refer to [37, 10] for the theory regarding the Hilbert class polynomial. Since 13 splits in K, the Deuring reduction theorem [22, Chapter 13, Theorem 12] asserts that $\mathrm{End}(E) \cong \mathrm{End}(E') \cong \mathcal{O}$.

We now construct the distortion map. Pick the 9-torsion point $(3, 3)$ of E, which by Vélu's method [40], induces a 9-degree isogeny $\phi : E \to E$, given by the rational map

$$\phi(x, y) = \left(\frac{f_1(x)}{f_2(x)}, \frac{g_1(x, y)}{g_2(x, y)}\right),$$

where

$$\begin{aligned}
f_1(x) &= x^9 + x^8 + 4x^7 + x^6 - 6x^5 - x^4 + 5x^3 - 6x^2 - 5,\\
f_2(x) &= x^8 + x^7 + 4x^6 + x^5 - 6x^4 - x^3 + 3x^2 + 5x + 4,\\
g_1(x, y) &= x^{12}y - 5x^{11}y - 5x^{10}y + 2x^9y + 2x^8y - x^7y\\
&\quad - 2x^6y + 5x^4y - 4x^3y - 2x^2y + 3xy - 6y,\\
g_2(x, y) &= x^{12} - 5x^{11} - 5x^{10} + 2x^9 + 2x^8 - x^7 - 5x^6\\
&\quad + 2x^5 + x^4 - 5x^3 + 5x^2 - 2x + 5.
\end{aligned}$$

Let $P = (12, 4)$ be a 3-torsion point which is defined over $\mathbb{F}_{13}$, then it holds that $E[3] \cap E(\mathbb{F}_{13}) = \langle P \rangle$. We verify that ϕ maps $\langle P \rangle$ to the point at infinity of E, while it distorts the points $Q \in E[3] \setminus E(\mathbb{F}_{13})$, as we compute that $\phi(Q) \in \langle P \rangle$. For $\ell = 3$, this example showcases the $\mathbb{F}_\ell[x]/(x^2)$ structure of the action of $\mathrm{End}(E)$ on $E[\ell]$, as was determined in the proof of Proposition 2.6 in the case of ℓ dividing the conductor f'.

Remark 3.5. Since E is ordinary, the trace t of π_q is not divisible by p, and in particular is non-zero (see, for example, [43, Proposition 4.31]). Hence, Hasse's theorem tells us that $t^2 - 4q < 0$, which implies that $\pi_q \notin \mathbb{Z}$. Thus, one can apply Corollary 2.8 to find a suitable m for which π_q is a distortion map for $E[m]$. We illustrate this with an example:

Example 3.6. Let $\mathbb{F}_{19^2} \coloneqq \mathbb{F}_{19}[X]/(X^2 + 18X + 2)$ and let a be the image of X in $\mathbb{F}_{19^2}$. Consider the elliptic curve $E : y^2 = x^3 + a$ over $\mathbb{F}_{19^2}$. Let π_{19^2} be the $(19^2)^{\text{th}}$ power Frobenius endomorphism. Using a computer algebra system, one finds that $\#E(\mathbb{F}_{19^2}) = 325$. Its norm is $n = 19^2$ and its trace is $t = 19^2 + 1 - \#E(\mathbb{F}_{19^2}) = 37$. Observe that E is ordinary. The discriminant of $\mathbb{Z}[\pi_{19^2}]$ is $D_{\pi_{19^2}} = t^2 - 4n = -75$. The smallest two primes ℓ with $\left(\frac{-75}{\ell}\right) = -1$ are 2 and 11. Hence, π_{19^2} is a distortion map for $E[22]$.

One can computationally check that the smallest n for which $\#E(\mathbb{F}_{19^{2n}})$ is divisible by 22 is 60, so $\mathbb{F}_{19^{120}}$ is the smallest field over which there is a point P of order 22. By Theorem 3.1 we know that, in fact, $E[22]$ must be defined over $\mathbb{F}_{19^{120}}$. Indeed, since $E[2]$ admits a distortion map, the smallest field $\mathbb{F}_q$ with a 2-torsion point must also be the minimal field of definition of $E[2]$. The same reasoning holds for $E[11]$. Hence, both $E[2]$ and $E[11]$ are defined over $\mathbb{F}_{19^{120}}$, and thus so is $E[22]$.

Example 3.7 (isogeny transfer of [8, Example 3.2]). The ordinary elliptic curve in question is $E : y^2 = x^3 - 35x + 98$ over $\mathbb{F}_{701}$, with endomorphism ring $\mathrm{End}(E) = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$. Observe that the discriminant D of $\mathrm{End}(E)$ is -7, and that $\left(\frac{-7}{5}\right) = -1$, so Theorem 3.2 tells us that $E[5]$ admits a distortion map. The distortion map ϕ for $E[5]$ given in [8] corresponding to multiplication by $\alpha = \frac{1+\sqrt{-7}}{2}$ is the rational map

$$\phi(x, y) = \left(\alpha^{-2}\left(x - \frac{7(x-\alpha)^4}{x + \alpha^2 - 2}\right), \alpha^{-3} y\left(1 + \frac{7(1-\alpha)^4}{(x + \alpha^2 - 2)^2}\right)\right),$$

and α reduces to $386 \in \mathbb{F}_{701}$. Pick the 2-torsion point $P = (319, 0)$ on E, then the group theoretic quotient $E \longrightarrow E/\langle P\rangle$ corresponds to a degree-2 isogeny of elliptic curves

$$\psi : \begin{cases} E \longrightarrow E' \\ (x, y) \longmapsto \left(\frac{x^2 - 319x + 313}{x - 319}, \frac{x^2 y + 63xy - 197y}{x^2 + 63x + 116}\right), \end{cases}$$

where E' is given by the equation $y^2 = x^3 + 503x + 66$ over $\mathbb{F}_{701}$. We computed this equation using SageMath, but the procedure can be found in Vélu's paper [40]. The dual isogeny is given by

$$\widehat{\psi} : \begin{cases} E' \longrightarrow E \\ (x, y) \longmapsto \left(\frac{-175x^2 - 191x - 52}{x - 63}, \frac{263x^2 y - 191xy + 84y}{x^2 - 126x - 237}\right). \end{cases}$$

Now Corollary 2.20 gives that $\phi' \coloneqq \psi \circ \phi \circ \widehat{\psi}$ is an appropriate distortion map for $E'[5]$, which we also verify by computation for all points $E'[5]$. For instance, pick $Q = (675, 16)$ a 5-torsion point on E'. By computation, we have that $e_5(Q, \phi'(Q)) = 638 \neq 1$, which is a fifth root of unity in $\mathbb{F}_{701}$.

4 Distortion maps for supersingular elliptic curves

In Verheul's paper [41], Theorem 5 proves the existence of distortion maps for any point P of a supersingular elliptic curve. Interestingly, Theorems 5 and 7 were absent from the original preprint, and for these Verheul acknowledges the help of René Schoof in the published article. Their proof is based on the following theorem of Tate, which relates the endomorphism ring of E with the endomorphism ring of its Tate module $T_\ell(E)$:

Theorem 4.1 ([38, Main Theorem, page 134])**.** *Let K be a finite field and E/K be an elliptic curve. Fix a prime $\ell \neq \mathrm{char}(K)$. Let $\mathrm{End}_K(T_\ell(E))$ denote the ring of $\mathrm{Gal}(\overline{K}/K)$-equivariant $\mathbb{Z}_\ell$-linear endomorphisms of $T_\ell(E)$ and let $\mathrm{End}_K(E)$ denote the ring of isogenies $E \to E$ defined over K. The canonical map*

$$\begin{cases} \mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{End}_K(T_\ell(E)) \\ \qquad\qquad \phi \otimes a \longmapsto a \cdot \phi_\ell, \end{cases}$$

where ϕ_ℓ is the $\mathbb{Z}_\ell$-linear map induced by ϕ on the Tate module defined as in [36, Chapter III.7], is an isomorphism of rings.

We shall extend Verheul and Schoof's argument to prove the existence of a distortion map for $E[m]$, for any m coprime to p.

Remark 4.2. Given a supersingular elliptic curve $E/\mathbb{F}_q$, its endomorphism algebra $B = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$. By definition, such algebras are central $\mathbb{Q}$-algebras, which means that the center of B is precisely $\mathbb{Q}$. The center of $\mathrm{End}(E)$ clearly contains $\mathbb{Z}$ and, since $\mathrm{End}(E) \subseteq B$ is a $\mathbb{Z}$-lattice, $\mathrm{End}(E) \cap \mathbb{Q} = \mathbb{Z}$. This implies that the center of $\mathrm{End}(E)$ is precisely $\mathbb{Z}$.

Let $E/\mathbb{F}_q$ be a supersingular elliptic curve and $m > 1$ coprime to p. Given an isogeny $\phi \in \mathrm{End}(E)$, its restriction to $E[m]$ defines a $\mathbb{Z}/m\mathbb{Z}$-linear endomorphism of $E[m]$. We denote the ring of $\mathbb{Z}/m\mathbb{Z}$-linear endomorphism of $E[m]$ by $\mathrm{End}_{\mathbb{Z}/m\mathbb{Z}}(E[m])$. This yields a ring homomorphism

$$\mathrm{res}_m : \begin{cases} \mathrm{End}(E) \longrightarrow \mathrm{End}_{\mathbb{Z}/m\mathbb{Z}}(E[m]) \\ \qquad \phi \longmapsto \phi|_{E[m]}. \end{cases}$$

Lemma 4.3. *The map res_m is surjective.*

Proof. Let $\ell \neq p$ be a prime and let $K = \mathbb{F}_{q^k}$ be the minimal field of definition of $\mathrm{End}(E)$, so that $\mathrm{End}_K(E) = \mathrm{End}(E)$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^k})$ be the $(q^k)^{\text{th}}$ power arithmetic Frobenius automorphism, and $\pi_{q^k} \in \mathrm{End}(E)$ be the $(q^k)^{\text{th}}$ power Frobenius endomorphism. Then, for any isogeny $\phi \in \mathrm{End}(E)$, since ϕ is defined over K, it commutes with the action of σ. Moreover, since σ and π_{q^k} act in the same way on $E(\overline{\mathbb{F}}_q)$, ϕ commutes with π_{q^k} as well. Hence, π_{q^k} lies in the center of $\mathrm{End}(E)$. As explained in Remark 4.2, since E is supersingular, the center of $\mathrm{End}(E)$ is $\mathbb{Z}$, so $\pi_{q^k} \in \mathbb{Z}$. Consequently, the induced map $(\pi_{q^k})_\ell$ on the Tate module lies in the center of $\mathrm{End}(T_\ell(E))$. As $(\pi_{q^k})_\ell$ acts on $T_\ell(E)$ in

the same way as σ, then any endomorphism of $T_\ell(E)$ is $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^k})$-equivariant. Thus, applying Theorem 4.1 for E/K establishes an isomorphism

$$\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{End}(T_\ell(E)).$$

Hence, the canonical surjection

$$\begin{cases} \mathrm{End}(T_\ell(E)) \longrightarrow \mathrm{End}_{\mathbb{Z}/\ell^n\mathbb{Z}}(E[\ell^n]) \\ \psi \longmapsto \psi|_{E[\ell^n]} \end{cases}$$

induces then a surjection

$$\begin{cases} \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{End}_{\mathbb{Z}/\ell^n\mathbb{Z}}(E[\ell^n]) \\ \phi \otimes a \longmapsto \bar{a} \cdot \phi|_{E[\ell^n]}, \end{cases}$$

where $\bar{a}$ is the reduction of a modulo ℓ^n. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_\ell$, any ℓ-adic integer is congruent to some integer modulo ℓ^n, so the restriction map

$$\mathrm{res}_{\ell^n} : \begin{cases} \mathrm{End}(E) \longrightarrow \mathrm{End}_{\mathbb{Z}/\ell^n\mathbb{Z}}(E[\ell^n]) \\ \phi \longmapsto \phi|_{E[\ell^n]} \end{cases}$$

is again surjective.

Consider the prime factorization $m = \ell_1^{n_1} \cdots \ell_r^{n_r}$. By the Chinese remainder theorem,

$$E[m] \cong \prod_{i=1}^{r} E[\ell_i^{n_i}],$$

which induces a ring isomorphism

$$\mathrm{End}_{\mathbb{Z}/m\mathbb{Z}}(E[m]) \cong \prod_{i=1}^{r} \mathrm{End}_{\mathbb{Z}/\ell_i^{n_i}\mathbb{Z}}(E[\ell_i^{n_i}]). \tag{1}$$

We claim that the map

$$\prod_{i=1}^{r} \mathrm{res}_{\ell_i^{n_i}} : \mathrm{End}(E) \longrightarrow \prod_{i=1}^{r} \mathrm{End}_{\mathbb{Z}/\ell_i^{n_i}\mathbb{Z}}(E[\ell_i^{n_i}])$$

is surjective. Indeed, given $(\lambda_1, \ldots, \lambda_r)$ in the codomain, take $\phi_i \in \mathrm{End}(E)$ with $\mathrm{res}_{\ell_i^{n_i}}(\phi_i) = \lambda_i$, and integers a_i congruent to 1 modulo $l_i^{n_i}$ and to 0 modulo $l_j^{n_j}$ for $j \neq i$. Then, the isogeny $\sum_{i=1}^{r} a_i\phi_i$ restricts to $(\lambda_1, \ldots, \lambda_r)$. Since the isomorphism (1) respects the restriction maps, the result follows. □

A consequence of the previous lemma is that any point P of order coprime to p admits a distortion map. In fact, the following stronger statement holds:

Theorem 4.4. *Let E be a supersingular elliptic curve over a finite field $\mathbb{F}_q$ and let $m > 1$ be an integer coprime to q. Then $E[m]$ admits a distortion map.*

Proof. Fix a basis of $E[m]$, so any $\mathbb{Z}/m\mathbb{Z}$-linear endomorphism of $E[m]$ is given by a matrix $A \in \mathrm{M}_2(\mathbb{Z}/m\mathbb{Z})$. We claim that A has no eigenvectors $v \in (\mathbb{Z}/m\mathbb{Z})^2 \setminus \{0\}$ if and only if

$$\det(\lambda I - A) \in (\mathbb{Z}/m\mathbb{Z})^\times$$

for all $\lambda \in \mathbb{Z}/m\mathbb{Z}$. For the necessary condition, fix $\lambda \in \mathbb{Z}/m\mathbb{Z}$ and assume that we have $\det(\lambda I - A) \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then, $\lambda I - A$ is invertible. If $Av = \lambda v$ for some $v \in (\mathbb{Z}/m\mathbb{Z})^2$, then $(\lambda I - A)v = 0$ and, by multiplying with $(\lambda I - A)^{-1}$, we obtain that $v = 0$. This shows that A has no eigenvector. For the sufficient condition, observe that, for any $\lambda \in \mathbb{Z}/m\mathbb{Z}$, the linear map

$$\lambda I - A : (\mathbb{Z}/m\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/m\mathbb{Z})^2$$

is injective, as it has trivial kernel. Since $(\mathbb{Z}/m\mathbb{Z})^2$ is finite, it is also surjective. If $e_1 = (1, 0)$ and $e_2 = (0, 1)$, there are vectors $v_i \in (\mathbb{Z}/m\mathbb{Z})^2$ with $(\lambda I - A)v_i = e_i$ for $i = 1, 2$. The matrix with columns v_1, v_2 is then the inverse of $\lambda I - A$, so $\det(\lambda I - A) \in (\mathbb{Z}/m\mathbb{Z})^\times$.

By Lemma 4.3, the statement of the theorem reduces to finding $A \in \mathrm{M}_2(\mathbb{Z}/m\mathbb{Z})$ for which $\det(\lambda I - A)$ is invertible for every $\lambda \in \mathbb{Z}/m\mathbb{Z}$. By the Chinese remainder theorem, it suffices to do this for $A \in M_2(\mathbb{Z}/\ell^n\mathbb{Z})$. If $\ell \neq 2$, let a be a quadratic non-residue modulo ℓ. Then, the polynomial $x^2 - \bar{a} \in (\mathbb{Z}/\ell^n\mathbb{Z})[x]$ takes values in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ for all $\lambda \in (\mathbb{Z}/\ell^n\mathbb{Z})$. Hence, the matrix

$$A = \begin{pmatrix} 0 & \bar{a} \\ 1 & 0 \end{pmatrix}$$

satisfies the desired property. For $\ell = 2$, one can take the matrix

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

with characteristic polynomial $x^2 - x - 1$, which also satisfies the desired property. □

5 Algorithms and known distortion maps

Having discussed properties and the question of existence of a distortion map $\phi \in \mathrm{End}(E)$ in the previous sections, we now turn to the literature to list specific algorithms for obtaining the rational coordinates of ϕ. We also list some known distortion maps in Tables 1 and 2. Furthermore, we restrict our attention to maps where ϕ is not the Frobenius endomorphism, as this case is well-known. The algorithms discussed will thus focus on finding distortion maps on the eigenspaces of the Frobenius endomorphism. This approach is advantageous for applications: it allows for the distortion of $\mathbb{F}_q$-points without requiring further field extensions.

The main backbone of the algorithms for computing distortion maps on a curve E is that they rely on finding a finite sequence of isogenies ψ_i, $i = 1, \ldots, c$ until the target

space E' is an elliptic curve isomorphic to E, as follows:

$$E = E_0 \xrightarrow{\psi_1} E_1 \xrightarrow{\psi_2} \cdots \xrightarrow{\psi_{c-1}} E_{c-1} \xrightarrow{\psi_c} E_c = E' \overset{\gamma}{\cong} E. \tag{2}$$

Denote $\psi \coloneqq \psi_c \circ \cdots \circ \psi_1$. Then, the candidate distortion map is defined as

$$\phi \coloneqq \gamma \circ \psi : E \to E.$$

In general, the primary computational cost of constructing ϕ lies in computing a suitable isogeny chain ψ which will correctly yield a distortion map. In contrast, determining the isomorphism γ is typically the easier part. The isogenies ψ_i are computed using Vélu's formulas [40] by considering quotients of elliptic curves by finite cyclic subgroups. Assuming one has the information of the order $\mathrm{End}(E)$ and its discriminant D, the strategy for ψ is then to be an isogeny of degree $|D|$, relating the intermediate isogenies ψ_i with the prime divisors of D.

5.1 Algorithms for supersingular elliptic curves

In the supersingular setting, the assumption that one understands $\mathrm{End}(E)$ is not particularly restrictive in practice, as Galbraith and Rotger explain [17, Section 6]. Indeed, the only known method for constructing a supersingular elliptic curve is via the Complex Multiplication method in characteristic zero paired with the Deuring reduction theorem. Consequently, one understands $\mathrm{End}(E)$ when constructing E. On the other hand, determining the endomorphism ring from the supersingular curve E alone is a computationally hard problem, which typically underpins the security of cryptosystems built on isogenies of supersingular curves. Although Kohel's algorithm [21] can compute a basis for $\mathrm{End}(E)$, it runs in exponential time.

We list below the primary references in the literature that have detailed algorithms for constructing distortion maps. From the previous discussion, these require as input the field $\mathbb{Q}(\sqrt{-d})$ by which the characteristic-zero elliptic curve has complex multiplication, before the reduction to $\mathbb{F}_q$. As these algorithms aim to distort points P from Frobenius eigenspaces, their correctness rely on P not being in $\ker\left(\phi\pi_q - \pi_q\phi\right)$, where π_q is the q^{th} power Frobenius, see [17, Lemma 5.1]. Additionally, Algorithms (1) and (2) rely also on [17, Proposition 6.1]. Here is the list:

(1) Moody's algorithm [26, Algorithm 2].

(2) Galbraith and Rotger's algorithm [17, Algorithm 1].

(3) Constructive Deuring Correspondence by Eriksen, Panny, Sotáková, and Veroni [11].

Despite sharing the structural approach of Diagram (2), the algorithms employ distinct methods to find the isogeny ψ. Moody utilizes the Weierstrass $\wp$-function up to a certain precision alongside Vélu's formulas. It is important to note that the streamlined description of the algorithm in the journal version [26] may hide this fact, but the idea is described in greater detail in his PhD thesis [27, Algorithm 3].

Galbraith and Rotger [17, Theorem 5.2] gave an alternative constructive proof for the existence of a distortion map for the points $P \in E[\ell]$ laying in an eigenspace of $\pi_q|_{E[\ell]}$ when $k(q,\ell) > 1$, which does not rely on the Tate module. Their algorithm is derived from this constructive proof. In order to arrive at a suitable ψ in Diagram (2), the algorithm performs a walk on an isogeny graph that is defined as a tree of j-invariants connected by prime degree isogenies. The tree is built using a separate algorithm by Galbraith [13].

Notation 5.1. We denote by $B = (\alpha, \beta \mid \mathbb{Q})$ the quaternion algebra over $\mathbb{Q}$ with basis $\{1, i, j, k\}$, subject to the multiplication rules $i^2 = \alpha$, $j^2 = \beta$, and $ij = -ji = k$, where $\alpha, \beta \in \mathbb{Q}^\times$.

The goal of the constructive Deuring correspondence is to find a supersingular elliptic curve E such that $\mathrm{End}(E) \cong \mathcal{O}$ for a given maximal order $\mathcal{O}$ in $B_{p,\infty}$, the unique (up to isomorphism) quaternion algebra ramified at p and ∞. For details on the entire correspondence algorithm and its implementation, see [11]. For background on the Hilbert modular polynomial, we refer to [37, 10]. We focus here on the curves and the distortion maps it constructs.

- Case $p \equiv 3 \pmod 4$: The curve is $E_0 : y^2 = x^3 + x$. The endomorphism ring is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\frac{i+j}{2} \oplus \mathbb{Z}\frac{1+k}{2}$ in the algebra $B_{p,\infty} = (-1, -p \mid \mathbb{Q})$.
- Case $p \equiv 2 \pmod 3$: The curve is $E_0 : y^2 = x^3 + 1$. The endomorphism ring corresponds to the maximal order $\mathcal{O}_0 = \mathbb{Z} \oplus \mathbb{Z}\frac{1+i}{2} \oplus \mathbb{Z}\frac{j+k}{2} \oplus \mathbb{Z}\frac{i+k}{3}$ in $B_{p,\infty} = (-3, -p \mid \mathbb{Q})$. The basis elements rely on generators satisfying $i^2 = -3$ and $j^2 = -p$, where the element $(i-1)/2$ corresponds to the order-3 automorphism of E_0.
- Case $p \equiv 1 \pmod 4$: This case is more complex. The algorithm finds the smallest prime $\alpha \equiv 3 \pmod 4$ such that p is inert in $\mathbb{Q}(\sqrt{-\alpha})$. It then computes the Hilbert class polynomial $H_{-\alpha}$ to find a rational root $j \in \mathbb{F}_p$, constructing E_0 with this j-invariant. An isomorphism allows mapping the provided order $\mathcal{O}$ into the specific algebra representation used by $\mathcal{O}_0$ defined as [11, Equation (1)].

Following the approach in [11], for primes $p \equiv 1 \pmod 4$, one can construct a supersingular elliptic curve E_0 such that its endomorphism ring contains an explicitly known endomorphism ϕ suitable for distortion. The construction proceeds as follows.

1. Find the smallest prime $\alpha \equiv 3 \pmod 4$ such that p remains inert in $\mathbb{Q}(\sqrt{-\alpha})$ (i.e., $\left(\frac{-\alpha}{p}\right) = -1$).
2. Compute the Hilbert class polynomial $H_{-\alpha}(X)$ and find a rational root $j_0 \in \mathbb{F}_p$. Construct E_0 with $j(E_0) = j_0$.
3. The endomorphism ring $\mathrm{End}(E_0)$ is isomorphic to a maximal order $\mathcal{O}_0$ in the quaternion algebra $B_{p,\infty} = (-\alpha, -p \mid \mathbb{Q})$. The algebra is generated by $1, i, j, k$ with $i^2 = -\alpha$, $j^2 = -p$, and $ij = -ji = k$.

Field	Curve	Morphism	Conditions	Group order	Reference
$\mathbb{F}_p$	$y^2 = x^3 + ax$	$(x, y) \mapsto (-x, iy)$ $i^2 = -1$	$p \equiv 3 \pmod 4$	$p + 1$	[20], [11]
$\mathbb{F}_p$	$y^2 = x^3 + a$	$(x, y) \mapsto (\zeta x, y)$ $\zeta^3 = 1$	$p \equiv 2 \pmod 3$	$p + 1$	[20], [11]
$\mathbb{F}_{p^2}$	$y^2 = x^3 + a$ $a \notin \mathbb{F}_p$	$(x, y) \mapsto \left(\omega \frac{x^p}{r^{(2p-1)/3}}, \frac{y^p}{r^{p-1}}\right)$ $r^2 = a, r \in \mathbb{F}_{p^2}$ $\omega^3 = r, \omega \in \mathbb{F}_{p^6}$	$p \equiv 2 \pmod 3$	$p^2 - p + 1$	[20]
$\mathbb{F}_p$	$y^2 = x^3 + ax + b$ (via root of $H_{-\alpha}$)	$\phi^2 = [-q]$, $\phi\pi = -\pi\phi$	$p \equiv 1 \pmod 4$, $\alpha \equiv 3 \pmod 4$, minimal $\left(\frac{-\alpha}{p}\right) = -1$	$p + 1$	[11]
$\mathbb{F}_{2^d}$	$y^2 + y = x^3 + x$	$(x, y) \mapsto (x + s^2, y + sx + t)$ $s^2 + s + 1 = 0$, $t^2 + t + s = 0$		$2^d + 1 \pm 2^{(d+1)/2}$	[27], [17]
$\mathbb{F}_{3^d}$	$y^2 = x^3 + x + 1$	$(x, y) \mapsto (-x + s, iy)$ $s^3 + 2s + 2 = 0$, $i^2 = -1$		$3^d + 1 \pm 3^{(d+1)/2}$	[27], [17]

Table 1: Distortions in some supersingular curves with respect to the torsion points defined over the ground field on the first column, for $p > 3$.

4. The distortion map ϕ corresponds to the element $\sqrt{-\alpha}$ in the algebra. It satisfies $\phi^2 = [-\alpha]$ and $\phi\pi = -\pi\phi$ where π is the Frobenius.

Computationally, ϕ is evaluated by composing a normalized isogeny of degree α with an isomorphism. If $E_0 : y^2 = x^3 + ax + b$, one defines the auxiliary curve $E_0' : y^2 = x^3 + \alpha^2 ax - \alpha^3 b$ and the isomorphism $\tau : E_0 \to E_0'$ defined by $(x, y) \mapsto (-\alpha x, (-\alpha)^{3/2} y)$.

The composition $\phi' = \tau \circ \phi$ is a normalized isogeny $E_0 \to E_0'$ of degree α, which can be computed efficiently by [6]. The target endomorphism is then recovered as

$$\phi = \tau^{-1} \circ \phi'.$$

We list in Table 1 families of distortion maps for supersingular elliptic curves together with their respective reference in the literature. The three cases from the constructive Deuring correspondence are included. See also [27] for nine specific curves and distortion maps with respect to the nine class-number-one imaginary quadratic fields, as well as [15] for more examples.

5.2 Algorithms for ordinary elliptic curves

In 2009, Moody [26] stated that it would be interesting to have algorithms that efficiently compute distortion maps for ordinary elliptic curves in the case of $k(q, \ell) = 1$. To date, no such algorithm appears to exist in the literature; however, recent developments offer some new perspectives, which we discuss below.

In the work of Fouquet, Miret, and Valera [12], distortion maps from isogenies as in Diagram (2) are modeled as closed walks on the crater of an isogeny volcano (for background on isogeny volcanoes, one may also consult [21, 3] for instance). Specifically, consider an ordinary curve E and primes m, ℓ. Let $\phi = \gamma \circ \psi$ arise as in Diagram (2) on the crater of the m-volcano, and let P be an ℓ-torsion point that yields a descending isogeny to a curve E' (within the ℓ-volcano). Under these conditions, ϕ fails to distort P if and only if the m-craters of E and E' have the same cardinality [12, Proposition 5.1]. While this approach does not offer a deterministic algorithm yet, it effectively serves as a volcano analogue to Galbraith and Rotger's strategy of isogeny walks in the supersingular case.

In [18], Hu, Wang, Xu, and Zhang provide an efficient algorithm for generating ordinary elliptic curves of embedding degree 1 via the complex multiplication method. Furthermore, their Theorem 2 establishes that the symmetric reduced Tate pairing $t(P, P)$ is non-degenerate on the curves produced by their Algorithm 1. Depending on the Legendre symbol (as detailed in our Proposition 2.6), this non-degeneracy holds either for all non-trivial points in $E[r]$, where r is prime or for all points excluding two specific eigenspaces. Their construction ensures that r is coprime to the elliptic curve's discriminant, ruling out the single eigenspace case. Thus, the reduced Tate pairing can be used instead of the modified Weil pairing without the cost of explicitly evaluating a distortion map ϕ. However, assuming $\mathrm{End}(E) = \mathbb{Z}[\phi]$, the proof of Theorem 2 reveals that the non-degeneracy is intrinsically linked to the underlying behavior of ϕ: the reduced Tate pairing is non-degenerate precisely when ϕ acts as a distortion map on P.

Furthermore, Hu, Xu, and Zhou [19] present two classes of ordinary elliptic curves that admit computable distortion maps. This result, formulated as Theorem 6, provides a partial generalization of Verheul's theorem [41, Theorem 3] for ordinary curves, regarding the hardness of the DLP on $\mathbb{F}_p^\times$. The necessary conditions and a table of these distortion maps are listed below.

- Type I: Let $\omega = (1 + \sqrt{-3})/2$, and p, r be primes such that $r \equiv 2 \pmod 3$ and $p = r^2 + r + 1$. Let $v = \omega - r\overline{\omega}$ and let $(\cdot)_6$ be the 6^{th} power residue symbol taking values in $\{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$. Assume for the coefficient b that $(\frac{4b}{v})_6 = -\omega$.
- Type II: Let $r \equiv 3 \pmod 4$ and $p = 16r^2 + 1$ be primes.

There are a few more examples, one may for instance use ordinary reduction on the curves in [35, Proposition 2.3.1] as Charles did in [8, Example 3.2].

Remark 5.2. In the case of ℓ dividing the conductor, as in Example 3.4, what worked as a strategy for a distortion map ϕ on some points of $E[\ell]$ was to pick a point of order ℓ^2 for the associated isogeny in (2). This resulted in $\phi^2 = 0$ on $E[\ell]$. We can showcase this similarly, in [8, Example 3.4], contradicting the claim that $\mathrm{End}(E) \pmod 2 \cong \mathbb{Z}/2\mathbb{Z}$. The ordinary curve is $y^2 = x^3+11x+4$ over $\mathbb{F}_{13}$. Let $\mathbb{F}_{13^6} = \mathbb{F}_{13}[X]/(X^6+10X^3+11X^2+11X+2)$

Field	Curve	Morphism	Conditions	Group Order	Reference
$\mathbb{F}_p$	$y^2 = x^3 + b$	$(x, y) \mapsto (r \cdot x, y)$	Type I	r^2	[19]
$\mathbb{F}_p$	$y^2 = x^3 - x$	$(x, y) \mapsto (-x, 4r \cdot y)$	Type II	$16r^2$	[19]

Table 2: Distortion maps for ordinary curves with respect to the entire group $E(\mathbb{F}_p)$.

generated by z. The 4-torsion point $P = (4, 3z^5 + 9z^4 + 7z^3 + 12z + 5)$ in $E(\mathbb{F}_{13^6})$ yields an isogeny $\psi : E \to E' : y^2 = x^3 + 8x + 9$. There is an isomorphism $\gamma : E' \to E$ given by $(x, y) \mapsto (4x, -5y)$. Then, $\phi := \gamma \circ \psi$ distorts the 2-torsion points $(6, 0), (9, 0)$ by mapping them to $(11, 0)$, and maps $(11, 0)$ to the point at infinity.

6 Distortion maps in higher dimension

For higher dimensional abelian varieties in general (see [25]), there is also a notion of a distortion map which has the same properties as in the one-dimensional case. Let A be an abelian variety over $\mathbb{F}_q$ and let $A^\vee$ be its dual. The Weil pairing is a bilinear map

$$e_m : A[m] \times A^\vee[m] \to \mu_m,$$

and, if we are given a principal polarization $\psi : A \longrightarrow A^\vee$, we may define:

$$e_m^\psi : A[m] \times A[m] \to \mu_m,$$

by the formula $e_m^\psi(P, Q) = e_m(P, \psi(Q))$, for $P, Q \in A[m]$.

In the case of Jacobians of higher genus curves, the generalization of distortion maps is, for instance, developed in [16]. Let us consider a smooth projective curve C of genus $g \geqslant 1$ over $\mathbb{F}_q$. Its Jacobian $\mathrm{Jac}(C)$ is an abelian variety of dimension g. The Abel–Jacobi map provides an isomorphism $\psi : \mathrm{Jac}(C) \xrightarrow{\sim} \mathrm{Jac}(C)^\vee$, in other words, a principal polarization for $\mathrm{Jac}(C)$.

Similarly to the elliptic curve case, there is a notion of a distortion map for a Jacobian of a higher genus curve given in the following definition:

Definition 6.1. *Let $m > 1$ be an integer coprime to q. Let $D \in \mathrm{Jac}(C)[m]$. An endomorphism $\varphi \in \mathrm{End}(\mathrm{Jac}(C))$ is said to be a distortion map for D if $e_m^\psi(D, \varphi(D)) \neq 1$.*

The article [16] focuses on Jacobians with the following notion of supersingularity.

Definition 6.2. *An abelian variety $A/\mathbb{F}_q$ of dimension $g \geqslant 1$ is said to be supersingular if it is isogenous (over $\overline{\mathbb{F}}_q$) to E^g for some supersingular elliptic curve $E/\overline{\mathbb{F}}_q$.*

Remark 6.3. There is a common variant of this definition: a principally polarized abelian variety A of dimension $g \geqslant 1$ is said to be supersingular if it is isogenous (over $\overline{\mathbb{F}}_q$) to $E_1 \times \ldots \times E_g$ for some supersingular elliptic curves $E_1, \ldots, E_g$. By [42, Lemma 42.1.11, page 786], any two supersingular elliptic curves are isogenous, so the two notions of supersingularity are equivalent; see [1] and its references to the work of Oort.

Let us also add that there is another important notion in the literature which resembles supersingularity: an abelian variety can be superspecial. Let us give a remark about this notion to clarify the situation:

Remark 6.4. A principally polarized abelian variety $A/\mathbb{F}_q$ of dimension $g \geqslant 1$ is said to be *superspecial* if it is isomorphic (over $\overline{\mathbb{F}}_q$) to $E_1 \times \ldots \times E_g$ for some supersingular elliptic curves $E_1, \ldots, E_g/\overline{\mathbb{F}}_q$, see also [1] and its references. By [28, Theorem 2 and Remark 3], we have that an abelian variety is superspecial if and only if $\dim_{\overline{\mathbb{F}}_q} \mathrm{Hom}(\alpha_p, A[p]) = \dim(A)$, for α_p the kernel of Frobenius on $\mathbb{G}_a$: in particular, supersingular is not equivalent to superspecial, see [28, Remark 3, page 35], where one finds an example of a supersingular abelian surface A isogenous to E^2 but not isomorphic to any $E_1 \times E_2$ with E_1 and E_2 supersingular.

Remark 6.5. Tate shows in [38, Theorem 2, page 140] that when A is isogenous to E^g for E a supersingular elliptic curve, one has that $\mathrm{End}(A) \otimes \mathbb{Q}$ is a central simple algebra over $\mathbb{Q}$ of dimension $(2g)^2$.

Considering that Theorem 4.1 is originally proved by Tate for general abelian varieties over finite fields, the argument used in the proof of Lemma 4.3 can be adapted to the higher dimension case to obtain the following result:

Theorem 6.6 ([16, Theorem 2.1])**.** *Let A be a principally polarized abelian variety of dimension g over $\mathbb{F}_q$, assume that A is isogenous to E^g for E a supersingular elliptic curve, and let ℓ be a prime not equal to the characteristic of $\mathbb{F}_q$. Assume $\psi : A \to A^\vee$ is a principal polarization. For every non-trivial element $D \in A(\mathbb{F}_q)[\ell]$, there exists $\phi \in \mathrm{End}(A)$ such that $e_\ell^\psi(D, \phi(D)) \neq 1$.*

In [30] it is shown that distortion maps in genus $\geqslant 3$ are not useful for applications in cryptography. The case of genus two remains interesting, and Jacobian surfaces isogenous to E^2 for E supersingular are studied in [16] by a case-by-case analysis. In particular, the article [16] provides constructive ways to obtain a distortion map in the case where the embedding degree is $\geqslant 4$.

References

[1] Jeffrey D. Achter and Rachel Pries. Superspecial rank of supersingular abelian varieties and Jacobians. *Journal de Théorie des Nombres de Bordeaux*, 27(3):605–624, 2015. DOI: 10.5802/jtnb.916.

[2] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm. *Journal of Cryptology*, 11:141–145, 1998. DOI: 10.1007/s001459900040.

[3] Henry Bambury, Francesco Campagna, and Fabien Pazuki. Ordinary isogeny graphs over $\mathbb{F}_p$: the inverse volcano problem. *Annali Scuola Normale Superiore - Classe di Scienze*, 33, 2024. DOI: 10.2422/2036-2145.202310_022.

[4] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. On the selection of pairing-friendly groups. In *Selected Areas in Cryptography*, volume 3006 of *Lecture Notes in Computer Science*, pages 17–25. Springer, 2004. DOI: 10.1007/978-3-540-24654-1_2.

[5] Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. In *Advances in cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001. DOI: 10.1007/3-540-44647-8_13.

[6] Alin Bostan, François Morain, Bruno Salvy, and Éric Schost. Fast algorithms for computing isogenies between elliptic curves. *Mathematics of Computation*, 77(263):1755–1778, 2008. DOI: 10.1090/S0025-5718-08-02066-8.

[7] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *Advances in Cryptology – EUROCRYPT 2023*, volume 14008 of *Lecture Notes in Computer Science*, pages 423–447. Springer, 2023. DOI: 10.1007/978-3-031-30589-4_15.

[8] Denis Charles. On the existence of distortion maps on ordinary elliptic curves. Preprint, 2006. DOI: 10.48550/arXiv.math/0603724.

[9] Keith Conrad. Factoring after Dedekind. Notes, 2025. https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf.

[10] David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication.* John Wiley and Sons, 1989. ISBN: 9780471190790.

[11] Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, and Mattia Veroni. Deuring for the people: supersingular elliptic curves with prescribed endomorphism ring in general characteristic. In *LuCaNT: LMFDB, Computation, and Number Theory*, volume 796 of *Contemporary Mathematics*, pages 339–373. American Mathematical Society, 2024. ISBN: 9781470472603.

[12] Mireille Fouquet, Josep M. Miret, and Javier Valera. Distorting the volcano. *Finite Fields and Their Applications*, 49:108–125, 2018. DOI: 10.1016/j.ffa.2017.09.006.

[13] Steven D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, 2:118–138, 1999. DOI: 10.1112/S1461157000000097.

[14] Steven D. Galbraith. Pairings. In *Advances in Elliptic Curve Cryptography*, Chapter IX, pages 183–214. Cambridge University Press, 2009. DOI: 10.1017/CBO9780511546570.011.

[15] Steven D. Galbraith and Alfred Menezes. Algebraic curves and cryptography. *Finite Fields and Their Applications*, 11(3):544–577, 2005. DOI: 10.1016/j.ffa.2005.05.001.

[16] Steven D. Galbraith, Jordi Pujolàs, Christophe Ritzenthaler, and Benjamin Smith. Distortion maps for supersingular genus two curves. *Journal of Mathematical Cryptology*, 3(1):1–18, 2009. DOI: 10.1515/JMC.2009.001.

[17] Steven D. Galbraith and Victor Rotger. Easy decision Diffie–Hellman groups. *LMS Journal of Computation and Mathematics*, 7:201–218, 2004. DOI: 10.1112/S1461157000001108.

[18] Zhi Hu, Lin Wang, Maozhi Xu, and Guoliang Zhang. Generation and Tate pairing computation of ordinary elliptic curves with embedding degree one. In *Information and Communications Security*, volume 8233 of *Lecture Notes in Computer Science*, pages 393–403. Springer, 2013. DOI: 10.1007/978-3-319-02726-5_28.

[19] Zhi Hu, Maozhi Xu, and Zhenghua Zhou. A generalization of Verheul's theorem for some ordinary curves. In *Information Security and Cryptology*, volume 6584 of *Lecture Notes in Computer Science*, pages 105–114. Springer, 2011. DOI: 10.1007/978-3-642-21518-6_8.

[20] Antoine Joux and Kim Nguyen. Separating decision Diffie–Hellman from computational Diffie–Hellman in cryptographic groups. *Journal of Cryptology*, 16(4):239–247, 2003. DOI: 10.1007/s00145-003-0052-4.

[21] David R. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996.

[22] Serge Lang. *Elliptic functions*. Volume 112 of *Graduate Texts in Mathematics*. Springer, 1987. ISBN: 9780387965086.

[23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In *Advances in cryptology – EUROCRYPT 2023*, volume 14008 of *Lecture Notes in Computer Science*, pages 448–471. Springer, 2023. DOI: 10.1007/978-3-031-30589-4_16.

[24] Alfred Menezes, Tatsuaki Okamoto, and Scott Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993. DOI: 10.1109/18.259647.

[25] James S. Milne. Abelian Varieties. In *Arithmetic Geometry*, pages 103–150. Springer, 1986. DOI: 10.1007/978-1-4613-8655-1_5.

[26] Dustin Moody. The Diffie–Hellman problem and generalization of Verheul's theorem. *Designs, Codes and Cryptography* , 52(3):381–390, 2009. DOI: 10.1007/s10623-009-9287-x.

[27] Dustin Moody. *The Diffie–Hellman problem and generalization of Verheul's theorem*. PhD thesis, University of Washington, 2009.

[28] Frans Oort. Which abelian surfaces are products of elliptic curves? *Mathematische Annalen*, 214:35–47, 1975. DOI: 10.1007/BF01428253.

[29] Damien Robert. Breaking SIDH in polynomial time. In *Advances in cryptology – EUROCRYPT 2023*, volume 14008 of *Lecture Notes in Computer Science*, pages 472–503. Springer, 2023. DOI: 10.1007/978-3-031-30589-4_17.

[30] Karl Rubin and Alice Silverberg. Supersingular abelian varieties in cryptology. In *Advances in Cryptology – CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 336–353. Springer, 2002. DOI: 10.1007/3-540-45708-9_22.

[31] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, 1985. DOI: 10.1090/S0025-5718-1985-0777280-6.

[32] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1):219–254, 1995. DOI: 10.5802/jtnb.142.

[33] René Schoof. The discrete logarithm problem. In *Open Problems in Mathematics*, pages 403–416. Springer, 2016. ISBN: 9783319321608.

[34] Jean-Pierre Serre. *Abelian l-Adic Representations and Elliptic Curves*. CRC Press, 1997. ISBN: 9780429063015.

[35] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Volume 151 of *Graduate Texts in Mathematics*. Springer, 1994. DOI: 10.1007/978-1-4612-0851-8.

[36] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Volume 106 of *Graduate Texts in Mathematics*. Springer, 2009. DOI: 10.1007/978-0-387-09494-6.

[37] Andrew V. Sutherland. Elliptic Curves. Lecture notes, Massachussets Institute of Technology, 2023. https://math.mit.edu/classes/18.783/2023/LectureNotes20.pdf.

[38] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2:134–144, 1966. DOI: 10.1007/BF01404549.

[39] The Sage Developers. *SageMath, the Sage Mathematics Software System*. https://www.sagemath.org/.

[40] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes rendus de l'académie des sciences de Paris*, 273:238–241, 1971.

[41] Eric R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *Journal of Cryptology*, 17:277–296, 2004. DOI: 10.1007/s00145-004-0313-x.

[42] John Voight. *Quaternion Algebras*. Volume 288 of *Graduate Texts in Mathematics*. Springer, 2021. DOI: 10.1007/978-3-030-56694-4.

[43] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC, 2008. ISBN: 9781584883654.

[44] Christian Wittmann. Group structure of elliptic curves over finite fields. *Journal of Number Theory*, 88(2):335–344, 2001. DOI: 10.1006/jnth.2000.2622.