Radical 3-isogenies for the ideal class group actions on $(2, \varepsilon)$-structures

Masaomi Shibata[1], Hiroshi Onuki[1*], Tsuyoshi Takagi[1]

[1] Graduate School of Information Science and Technology, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, 113-8656, Japan .

*Corresponding author(s). E-mail(s): hiroshi-onuki@g.ecc.u-tokyo.ac.jp;
Contributing authors: shibata.omi@gmail.com;
takagi@g.ecc.u-tokyo.ac.jp;

Abstract

Chenu and Smith introduced the notion of (d, ε)-*structures*, pairs consisting of an elliptic curve over $\mathbb{F}_{p^2}$ and an isogeny of degree d from the curve to its Galois conjugate, and defined an ideal class group action on supersingular (d, ε)-structures, inherited from the action on oriented supersingular elliptic curves. They also outlined extensions of the CSIDH key exchange and of the Delfs–Galbraith algorithm for the supersingular isogeny problem. In particular, they suggested that the latter, called the *generalized Delfs–Galbraith algorithm*, may be faster than the original one by a constant factor for small d, provided that the class group action on (d, ε)-structures can be evaluated efficiently.

In this paper, we focus on the case $d = 2$ and present explicit radical 3-isogenies for evaluating the action of the class of a prime ideal above 3. Note that 3 is the norm of the acting ideal, not the degree d of the isogeny defining a structure; a radical 3-isogeny maps a $(2, \varepsilon)$-structure to another. Our approach relies on two representations of $(2, \varepsilon)$-structures, by reductions of degree-2 $\mathbb{Q}$-curves and by Montgomery curves. We show that any $(2, \varepsilon)$-structure can be represented as a pair of a curve coefficient and a single sign, and from these representations we derive radical 3-isogenies that efficiently implement the action. As an application, we give an explicit meet-in-the-middle algorithm for finding an ideal class connecting two given $(2, \varepsilon)$-structures, which is a part of the generalized Delfs–Galbraith algorithm.

Keywords: Isogeny-based cryptography, Supersingular elliptic curves, Radical 3-isogenies, Ideal class group

MSC Classification: 11G20 , 14K02 , 11Y16 , 94A60

1 Introduction

Isogeny-based cryptography is a promising candidate for post-quantum cryptography since it offers relatively small keys and ciphertexts compared to other post-quantum cryptographic schemes. Currently, there are roughly four types of isogeny-based cryptographic schemes: (i) hash functions using random walks in isogeny graphs such as [1, 2], (ii) a signature scheme using the Deuring correspondence called the SQIsign family [3, 4], (iii) public-key encryption schemes using a trapdoor function based on attacks in [5–7] such as [8–10], (iv) cryptographic primitives using the action of an ideal class group on a set of elliptic curves, which we focus on in this paper.

The first cryptographic primitive using the action of an ideal class group on a set of elliptic curves was proposed by Couveignes [11], and independently by Rostovtsev and Stolbunov [12]. This primitive uses ordinary elliptic curves and is not practical due to the high computational cost of evaluating the action. Later, Castryck, Lange, Martindale, Panny, and Renes [13] proposed CSIDH, a practical key exchange protocol using supersingular elliptic curves over $\mathbb{F}_p$ for a prime p. CSIDH uses the ideal class group of the order $\mathbb{Z}[\sqrt{-p}]$ acting on a set of supersingular elliptic curves over $\mathbb{F}_p$. After that, several variants of CSIDH have been proposed; for example, CSURF [14], OSIDH [15], and SCALLOP [16]. The primitives based on the ideal class group action are important because they provide many cryptographic applications, not only key exchange protocols. For example, a signature scheme [17], threshold schemes [18], and a password-authenticated key exchange protocol [19] have been proposed using the ideal class group action.

Chenu and Smith [20] introduced an ideal class group action associated with an order in $\mathbb{Q}(\sqrt{-dp})$, where d is a square-free positive integer. This action is defined on supersingular elliptic curves over $\mathbb{F}_{p^2}$ equipped with a d-isogeny to their Galois conjugates under the p-th power Frobenius map. They called such a pair of an elliptic curve and a d-isogeny a (d, ε)-*structure*, where $\varepsilon \in \{\pm 1\}$ is determined by the relation between the isogeny and the Frobenius map. They also proposed a variant of the CSIDH key exchange protocol based on (d, ε)-structures. This variant is less efficient than CSIDH because it requires arithmetic over $\mathbb{F}_{p^2}$ rather than $\mathbb{F}_p$, so it is not expected to be practical as a cryptographic protocol. Nevertheless, (d, ε)-structures remain important as a theoretical tool for studying isogenies between supersingular elliptic curves. Chenu and Smith also extended the Delfs–Galbraith algorithm [21] to this setting; they called the resulting method the *generalized Delfs–Galbraith algorithm*. Although this extension does not improve the asymptotic complexity of the original algorithm, Chenu and Smith observed that it may yield a constant-factor speedup for a few small d [20, §6.4]. They also noted that this gain is counterbalanced by the cost of walking in the graph of (d, ε)-structures, which is exactly the cost that efficient evaluation of the class group action reduces.

Recently, Wesolowski [22] proposed a new algorithm for the supersingular isogeny problem with time and memory complexity $p^{1/3+o(1)}$, which improves the exponent $1/2$ of the Delfs–Galbraith algorithm. Its high memory requirement, however, does not make Delfs–Galbraith-type algorithms obsolete. The latest SQIsign specification [4] increased its parameters in reaction to this attack, but did so on the basis of a time–memory tradeoff between the two approaches in which $(\text{time})^2 \times (\text{memory}) = \tilde{O}(p)$,

and under realistic memory constraints Delfs–Galbraith-type algorithms remain competitive at higher security levels [23]. Therefore, efficient evaluation of the class group action on (d, ε)-structures remains relevant.

In the generalized Delfs–Galbraith algorithm based on (d, ε)-structures, one needs to find an ideal class in an order of $\mathbb{Q}(\sqrt{-dp})$ whose action maps one given (d, ε)-structure to another. The best known method for this task is the meet-in-the-middle technique for ideal class group actions described in [13, §7.1]. This method requires evaluating the action of many ideal classes on (d, ε)-structures. One promising way to accelerate these evaluations is to use *radical isogenies*, introduced by Castryck, Decru, and Vercauteren [24]. A radical isogeny formula computes a chain of n-isogenies by computing an n-th root at each step, and the choice of root determines the next isogeny in the chain. In CSIDH and CSURF, this choice can be made deterministically. In particular, when n is coprime with $p - 1$, there is a unique n-th root in $\mathbb{F}_p$. However, no comparably efficient method is known for determining the root corresponding to the ideal class action in the setting of (d, ε)-structures.

Contribution.

In this paper, we address this problem in the case $d = 2$ and $n = 3$, where d is the degree of the isogeny defining a (d, ε)-structure and n is the degree of the isogenies between structures that realize the action of ideals of norm n. In particular, we derive explicit radical 3-isogenies together with an efficient rule for selecting the cube root corresponding to the ideal class action on $(2, \varepsilon)$-structures. Our approach uses two representations of $(2, \varepsilon)$-structures: reductions of degree-2 $\mathbb{Q}$-curves by Hasegawa [25], which we call *Hasegawa parameters*, and Montgomery curves. More precisely, we prove the following two facts:

- Any supersingular $(2, \varepsilon)$-structure can be *uniquely* represented as a pair consisting of a Hasegawa parameter and a sign (Corollary 11).
- Any supersingular $(2, \varepsilon)$-structure can be represented as a pair consisting of a Montgomery coefficient and a sign, and two such pairs represent isomorphic $(2, \varepsilon)$-structures if and only if their coefficients are equal up to sign (Theorem 14).

Using these representations, we derive radical 3-isogenies that efficiently compute the action of the class of a prime ideal $\mathfrak{l}$ above 3 in $\mathbb{Q}(\sqrt{-2p})$ on $(2, \varepsilon)$-structures. In particular, we give a deterministic rule for choosing the cube root corresponding to the action of the class of $\mathfrak{l}$.

To the best of our knowledge, this is the first work that gives radical 3-isogenies for an algebraically specified family of isogenies beyond the ideal class actions arising in CSIDH and CSURF. Here, "algebraically specified" means that the isogenies are characterized by explicit algebraic conditions, rather than by random walks in an isogeny graph as in hash functions [26]. We therefore expect that our formulas will be useful in algorithmic number theory beyond the specific application considered here.

As an application of these radical 3-isogenies, we give an explicit meet-in-the-middle algorithm for finding an ideal class connecting two given $(2, \varepsilon)$-structures, which forms a subroutine of the generalized Delfs–Galbraith algorithm.

We use SageMath [27] for deriving some formulas in this paper and for verifying their correctness. Furthermore, we implemented our radical 3-isogenies in SageMath to give concrete examples of the ideal class action on $(2,\varepsilon)$-structures. Our implementation is available at the GitHub repository:

https://github.com/hiroshi-onuki/2epsilon_structure_sagemath

Organization.

The rest of this paper is organized as follows. In Section 2, we review basic facts required for this paper. In Section 3, we present two representations of $(2,\varepsilon)$-structures. In Section 4, we derive radical 3-isogenies for the ideal class action on $(2,\varepsilon)$-structures. The meet-in-the-middle method for finding an ideal class connecting two given $(2,\varepsilon)$-structures is described in Section 5. Finally, we conclude this paper and discuss future work in Section 6.

2 Preliminaries

In this section, we review the concepts and basic facts required for this paper. In particular, we review basic facts about elliptic curves, orientations, (d,ε)-structures, and radical isogenies.

2.1 Basic facts about elliptic curves

We provide basic descriptions of elliptic curves. For more details, we refer the reader to textbooks such as [28, 29].

Elliptic curves and isogenies.

An *elliptic curve* over a field k is a pair (E,O), where E is a nonsingular algebraic curve of genus 1 defined over k and O is a base point on E defined over k. For an extension field k' of k, the set of k'-rational points on E is denoted by $E(k')$. It is known that $E(k')$ forms an abelian group with identity O. Hereafter, we omit O and call E an elliptic curve for simplicity. We denote the multiplication-by-n map on E by $[n]$ for an integer n. The *n-torsion subgroup* of E is the kernel of $[n]$ and is denoted by $E[n]$. The isomorphism class of an elliptic curve E is characterized by its *j-invariant*, which can be represented as a rational function of the coefficients of E. In particular, two elliptic curves over k are isomorphic over $\bar{k}$ if and only if they have the same j-invariant.

Let E_0 and E_1 be elliptic curves over k. An *isogeny* $\varphi : E_0 \to E_1$ is a non-constant morphism that maps the base point of E_0 to that of E_1. An isogeny $\varphi : E_0 \to E_1$ induces an inclusion $\varphi^* : \bar{k}(E_1) \to \bar{k}(E_0)$ of the function fields. The *degree* of φ is the degree of the field extension $\bar{k}(E_0)/\varphi^*(\bar{k}(E_1))$, denoted by $\deg\varphi$. The isogeny φ is *separable* (resp. *inseparable*) if the field extension $\bar{k}(E_0)/\varphi^*(\bar{k}(E_1))$ is separable (resp. inseparable). We call φ a *d-isogeny* if $\deg\varphi = d$. We have $\#\ker\varphi \leq \deg\varphi$, and the equality holds if and only if φ is separable.

Two elliptic curves E_0 and E_1 are *d-isogenous* if there is a d-isogeny $\varphi : E_0 \to E_1$. For an isogeny $\varphi : E_0 \to E_1$, there exists a unique isogeny $\psi : E_1 \to E_0$ such that $\psi \circ \varphi = [\deg \varphi]$. We call ψ the *dual isogeny* of φ and denote it by $\hat{\varphi}$.

Let G be a finite subgroup of $E_0(\bar{k})$. Then there exists a separable isogeny $\varphi : E_0 \to E_1$ with kernel G. This isogeny φ is unique up to isomorphism of the codomain E_1. If G is stable under the action of $\mathrm{Gal}(\bar{k}/k')$ for some extension field k' of k, then there exists such an isogeny φ defined over k' and φ is unique up to isomorphism of the codomain E_1 over k'. We denote by E_0/G the codomain of φ.

An *endomorphism* of an elliptic curve E over k is an isogeny from E to itself or the zero map. The set of endomorphisms of E over $\bar{k}$ forms a ring with addition defined as pointwise addition and multiplication defined as composition. We call it the *endomorphism ring* of E and denote it by $\mathrm{End}(E)$.

Let E be an elliptic curve over a field k of characteristic not equal to 2. Then E is isomorphic over k to an elliptic curve defined by $y^2 = x^3 + ax^2 + bx + c$ for some $a, b, c \in k$. In this paper, we always assume that elliptic curves are given in this form. For $\nu \in \bar{k}^\times$, the curve E' defined by $y^2 = x^3 + a\nu^2 x^2 + b\nu^4 x + c\nu^6$ is isomorphic to E over $\bar{k}$ by an isomorphism defined by $(x, y) \mapsto (\nu^2 x, \nu^3 y)$. We denote this isomorphism by τ_ν. Let $\sqrt{-1}$ be a fixed square root of -1 in $\bar{k}$. We write θ for the isomorphism $\tau_{-\sqrt{-1}} : (x, y) \mapsto (-x, \sqrt{-1}y)$, which maps E to the curve defined by $y^2 = x^3 - ax^2 + bx - c$. If $a = c = 0$, then θ is an automorphism of E of order 4 with $\theta^2 = [-1]$. For a positive integer n, the *n-division polynomial of E* is a polynomial $\Psi_n \in k[x]$ such that the x-coordinate of a point $P \in E(\bar{k}) \setminus \{O\}$ is a root of Ψ_n if and only if $[n]P = O$.

Elliptic curves over finite fields.

Let p be a prime number and k be a finite field of characteristic p. We say an elliptic curve E over k is *ordinary* if $E[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and *supersingular* if $E[p]$ is the trivial group. If two elliptic curves over k are isogenous over $\bar{k}$, then they are both ordinary or both supersingular. Any supersingular elliptic curve over k is isomorphic over $\bar{k}$ to an elliptic curve defined over $\mathbb{F}_{p^2}$.

Let E be an elliptic curve over k. We denote by $E^{(p)}$ the elliptic curve obtained by applying the p-th power to all coefficients of E. Then there exists the *p-th power Frobenius map* $\pi_p : E \to E^{(p)}$, defined by $(x, y) \mapsto (x^p, y^p)$. Let $\varphi : E \to E'$ be an isogeny over k. We denote by $\varphi^{(p)} : E^{(p)} \to E'^{(p)}$ the isogeny obtained by applying the p-th power to all coefficients of φ. Note that it holds that $\varphi^{(p)} \circ \pi_p = \pi_p \circ \varphi$.

Tate pairing.

Let q be a power of a prime, n be a positive integer such that $n \mid q - 1$, and E be an elliptic curve over $\mathbb{F}_q$. The *n-Tate pairing* is a nondegenerate bilinear map

$$\langle \cdot, \cdot \rangle_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^n.$$

For the definition of the Tate pairing, see [29, Chapter 11.3]. In this paper, we use the following property of the Tate pairing.

Lemma 1 *Let q be a power of an odd prime such that $3 \mid q-1$, and E be an elliptic curve defined by $y^2 = x^3 + ax^2 + bx + c$ for $a, b, c \in \mathbb{F}_q$. Assume that $E(\mathbb{F}_q)[3]$ contains a nonzero point $P = (x_P, y_P)$. Then $\langle P, -P\rangle_3 = 2y_P \bmod (\mathbb{F}_q^\times)^3$.*

Proof Let $f(x,y) = y - \lambda(x - x_P) - y_P$ be the tangent line at P on E, i.e., $\lambda = (3x_P^2 + 2ax_P + b)/(2y_P)$. Since the order of P is 3, the divisor of f is $3(P) - 3(O)$. From Proposition XI.9.2 in [28], if $f \circ [3]$ in $(\mathbb{F}_q(E)^\times)^3$, then we have $\langle P, Q\rangle_3 \equiv f(Q) \bmod (\mathbb{F}_q^\times)^3$ for $Q \in E(\mathbb{F}_q) \setminus \{O, P\}$. Since $f(-P) = -2y_P \equiv 2y_P \pmod{(\mathbb{F}_q^\times)^3}$, it suffices to show that $f \circ [3]$ is in $(\mathbb{F}_q(E)^\times)^3$.

By a similar discussion to Section 3.2 in [29] (or an explicit computation), we can show that $f \circ [3]$ is of the form $yf_1(x)/\Psi_3(x)^3$, where $f_1(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree 12 and $\Psi_3(x)$ is the 3-division polynomial of E.

Let D be a divisor on E defined by

$$D = \sum_{[3]R=P} (R) - \sum_{[3]R=O} (R).$$

Since the degree of D is zero and $\sum_{[3]R=P} R - \sum_{[3]R=O} R = O$, there exists a function $g \in \overline{\mathbb{F}_q}(E)^\times$ such that $\mathrm{div}(g) = D$. In addition, since the q-power Frobenius map acts on D trivially, we can take g in $\mathbb{F}_q(E)^\times$.

Let h_1, h_2 be two polynomials in $\mathbb{F}_q[x, y]$ such that $g = h_1/h_2$. Since the divisors of $f \circ [3]$ and g^3 are the same, there exists a constant $c \in \mathbb{F}_q^\times$ such that

$$(h_1 \cdot \Psi_3)^3 = c \cdot yf_1 \cdot h_2^3.$$

By comparing the highest degree terms of both sides, we have $c \in (\mathbb{F}_q^\times)^3$. This shows that $f \circ [3]$ is in $(\mathbb{F}_q(E)^\times)^3$. □

Complex multiplication.

Let E be an elliptic curve over $\mathbb{C}$, and $\mathcal{O}$ be an order of an imaginary quadratic field K. We say E has *complex multiplication (CM) by* $\mathcal{O}$ if $\mathrm{End}(E)$ is isomorphic to $\mathcal{O}$. We say E has *CM by* K if $\mathrm{End}(E)$ is isomorphic to the ring of integers $\mathcal{O}_K$ of K. The j-invariant of an elliptic curve with CM is an algebraic integer. In particular, if $\mathcal{O}$ has class number 1, then the j-invariant is in $\mathbb{Z}$. In particular, we are interested in elliptic curves with CM by $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-7})$, whose j-invariants are 1728, 8000, 0, and -3375, respectively. Note that the imaginary quadratic orders having elements of norm 2 are $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{-2}]$, and $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ whose corresponding j-invariants are 1728, 8000, and -3375, respectively.

Let $\bar{E}$ be an elliptic curve over a number field L with CM by an order $\mathcal{O}$ of an imaginary quadratic field K, and E be the reduction of $\bar{E}$ modulo a prime ideal above p in L. Then E is ordinary if p splits in $\mathcal{O}$, and supersingular otherwise. In addition, $\mathrm{End}(E)$ contains a subring isomorphic to $\mathcal{O}$.

Montgomery curves.

Let k be a field of characteristic not equal to 2 and $A \in k \setminus \{\pm 2\}$. A *Montgomery curve* is an elliptic curve defined by the equation

$$y^2 = x^3 + Ax^2 + x.$$

We denote this Montgomery curve by E_A and call A the *Montgomery coefficient* of E_A. In the parts of this paper where Montgomery curves appear together with the Hasegawa curves introduced in Section 3.2, we write E_A^{M} instead of E_A to distinguish them.

For any Montgomery curve, the point $(0,0)$ has order 2, and the x-coordinate of a point P such that $[2]P = (0,0)$ is 1 or -1. In particular, θ gives an isomorphism $E_A \to E_{-A}$.

The following facts about Montgomery curves are well-known. We provide proofs for the sake of completeness.

Lemma 2 *Let E be a supersingular elliptic curve over a finite field $\mathbb{F}_{p^2}$. Assume that there exists a point $T \in E(\mathbb{F}_{p^2})$ of order 4. Then there exists a Montgomery curve E_A defined over $\mathbb{F}_{p^2}$ and an isomorphism $\eta : E \to E_A$ defined over $\mathbb{F}_{p^2}$ such that $\eta([2]T) = (0,0)$.*

Proof Since $p \neq 2$, we may assume that E is defined by $y^2 = x^3 + a_2x^2 + a_4x + a_6$ for some $a_2, a_4, a_6 \in \mathbb{F}_{p^2}$. Shifting x-coordinate by the x-coordinate of $[2]T$, we may assume that E is defined by $y^2 = x^3 + a'x^2 + b'x$ for some $a', b' \in \mathbb{F}_{p^2}$ and that $[2]T = (0,0)$. Then it is easy to see that the x-coordinate of T is a square root of b'. Let t be the x-coordinate of T.

Let $v \in \overline{\mathbb{F}}_p$ be a square root of t^{-1}. Since there exists an isomorphism $\tau_v : E \to E_{a'/t}$, it suffices to show that t is in $(\mathbb{F}_{p^2}^{\times})^2$ to prove the lemma. This follows by an argument similar to that used in the proof of Theorem 2 in [30].

A similar discussion to the proof of Lemma 1 shows that

$$t^{\frac{p^2-1}{2}} = (\langle [2]T, T\rangle_2)^{\frac{p^2-1}{2}}.$$

Let π_{p^2} be the p^2-th power Frobenius endomorphism on E, let e_2 be the 2-Weil pairing on E, and $T' \in E(\overline{\mathbb{F}}_p)$ be a point satisfying $[2]T' = T$. Then we have $\langle [2]T, T\rangle_2 = e_2([2]T, T' - \pi_{p^2}(T'))$. Since the order of $E(\mathbb{F}_{p^2})$ is divisible by 4, we have the characteristic polynomial of π_{p^2} is given by $X^2 \pm 2X + p^2$. This means that π_{p^2} is equal to $[p]$ or $[-p]$. This and $T' - \pi_{p^2}(T') \in E[2]$ imply that $T' - \pi_{p^2}(T') = 2T$ or O. Therefore, we have $e_2([2]T, T' - \pi_{p^2}(T')) = 1$. This shows that t is in $(\mathbb{F}_{p^2}^{\times})^2$. □

Lemma 3 *Let E_A be a supersingular Montgomery curve over $\mathbb{F}_{p^2}$. Then we have the following:*

1. *$A + 2$ and $A - 2$ are in $(\mathbb{F}_{p^2}^{\times})^4$,*
2. *$E_A[4] \subset E_A(\mathbb{F}_{p^2})$.*

Especially, the p^2-th power Frobenius endomorphism on E_A is equal to the multiplication by $(-1)^{\frac{p-1}{2}}p$.

Proof By the isogeny in Example III.4.5 in [28], E_A is 2-isogenous to the curve defined by $y^2 = x^3 - 2Ax^2 + (A^2 - 4)x$. This curve is isomorphic (over $\overline{\mathbb{F}}_p$) to the Legendre curve $y^2 = x(x-1)(x - \frac{A+2}{A-2})$. Since this Legendre curve is also supersingular, Proposition 3.1 in

[31] implies that $\frac{A+2}{A-2}$ is in $(\mathbb{F}_{p^2}^{\times})^8$. The Legendre curve with parameter $1-\frac{A+2}{A-2}=-\frac{4}{A-2}$ is isomorphic to the previous Legendre curve. Therefore, $-\frac{4}{A-2}$ is also in $(\mathbb{F}_{p^2}^{\times})^8$. From these, $\frac{A+2}{A-2}\cdot\left(-\frac{4}{A-2}\right)^{-1}=(A+2)/(-4)$ is in $(\mathbb{F}_{p^2}^{\times})^8$. Since -4 is in $(\mathbb{F}_{p^2}^{\times})^4$, we have $A+2$ is in $(\mathbb{F}_{p^2}^{\times})^4$. A similar argument shows that $A-2$ is also in $(\mathbb{F}_{p^2}^{\times})^4$.

Let P be a point on E_A with x-coordinate 1. Since the y-coordinate of P is a square root of $A+2$, the above result implies that P is rational over $\mathbb{F}_{p^2}$. Therefore, the order of $E_A(\mathbb{F}_{p^2})$ is divisible by 4 and the characteristic polynomial of the p^2-th power Frobenius endomorphism π_{p^2} on E_A is given by $X^2\pm 2X+p^2$. Since π_{p^2} acts on P trivially, we have $\pi_{p^2}=[(-1)^{\frac{p-1}{2}}p]$. Therefore, π_{p^2} acts on $E_A[4]$ trivially. □

Lemma 4 *Let k be a field of characteristic not equal to 2 and $A\in k\setminus\{\pm 2\}$. Let $v\in\bar{k}$ be a fourth root of A^2-4 and $A'=-2A/v^2$. Then there exists an isogeny $\varphi: E_A\to E_{A'}$ of degree 2 with kernel $\langle(0,0)\rangle$ defined by*

$$(x,y)\mapsto\left(\frac{x^2+Ax+1}{v^2x},\frac{y(1-x^2)}{v^3x^2}\right).$$

The dual isogeny $\hat{\varphi}: E_{A'}\to E_A$ has kernel $\langle(0,0)\rangle$ and is given by

$$(x,y)\mapsto\left(\frac{v^2(x^2+A'x+1)}{4x},\frac{v^3y(1-x^2)}{8x^2}\right).$$

In addition, if E_A is a supersingular elliptic curve over $\mathbb{F}_{p^2}$, then φ is defined over $\mathbb{F}_{p^2}$.

Proof of Lemma 4 The isogeny φ is obtained by composing the 2-isogeny in Example III.4.5 in [28] and the isomorphism $\tau_{v^{-1}}$ from the codomain of this 2-isogeny to $E_{A'}$. The dual isogeny is obtained similarly.

If E_A is a supersingular elliptic curve over $\mathbb{F}_{p^2}$, then Lemma 3 implies that $v\in\mathbb{F}_{p^2}$. Therefore, the isogeny φ is defined over $\mathbb{F}_{p^2}$. □

We denote the isogeny $E_A\to E_{A'}$ in Lemma 4 by φ_v to indicate its dependence on the fourth root v of A^2-4.

2.2 Orientations

Let E be an elliptic curve over $\mathbb{F}_{p^2}$ and K be an imaginary quadratic field. A *K-orientation* on E is a ring homomorphism $K\hookrightarrow\mathrm{End}(E)\otimes_{\mathbb{Z}}\mathbb{Q}$. We call the pair (E,ι) a *K-oriented elliptic curve*. For an order $\mathcal{O}$ of K, we say ι is an *$\mathcal{O}$-orientation* if $\iota(\mathcal{O})\subset\mathrm{End}(E)$. In addition, if $\iota(\mathcal{O})=\mathrm{End}(E)\cap\iota(K)$, then ι is called a *primitive $\mathcal{O}$-orientation*.

Let (E,ι) be a K-oriented elliptic curve over $\mathbb{F}_{p^2}$ and $\varphi: E\to E'$ be an isogeny. Then we can define an orientation $\varphi_*\iota$ on E' by

$$\varphi_*\iota:\alpha\mapsto\frac{1}{\deg\varphi}\varphi\circ\iota(\alpha)\circ\hat{\varphi}.$$

Let ι' be a K-orientation on E'. Then φ is said to be a *K-oriented isogeny* if $\varphi_*\iota=\iota'$. We denote this by $\varphi:(E,\iota)\to(E',\iota')$. Two K-oriented elliptic curves (E,ι) and

(E', ι') are said to be isomorphic if there exists a K-oriented isogeny $\varphi : E \to E'$ that is an isomorphism as an isogeny of elliptic curves.

Let $\mathcal{O}$ be an order of an imaginary quadratic field K. We denote the set of the isomorphism classes of primitive $\mathcal{O}$-oriented supersingular elliptic curves over $\mathbb{F}_{p^2}$ by $\mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$. This set is not empty if p does not split in $\mathcal{O}$ and the conductor of $\mathcal{O}$ is coprime to p. Let (E, ι) be a primitive $\mathcal{O}$-oriented elliptic curve. For an invertible ideal $\mathfrak{a}$ of $\mathcal{O}$, we define a subgroup $E[\iota(\mathfrak{a})]$ of E as

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

When the orientation ι is clear from the context, we simply write $E[\mathfrak{a}]$ for $E[\iota(\mathfrak{a})]$. Let φ be an isogeny with kernel $E[\mathfrak{a}]$ and E' be the codomain of φ. Then the induced oriented elliptic curve $(E', \varphi_*\iota)$ is a primitive $\mathcal{O}$-oriented elliptic curve. This defines an action of the ideal class group $\mathrm{cl}(\mathcal{O})$ on $\mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$. The action is given by

$$\begin{aligned} \mathrm{cl}(\mathcal{O}) \times \mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p) &\to \mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p), \\ ([\mathfrak{a}], (E, \iota)) &\mapsto ([\mathfrak{a}] * (E, \iota) \coloneqq (E/E[\iota(\mathfrak{a})], \varphi_*\iota)), \end{aligned}$$

where $[\mathfrak{a}]$ is the class of an invertible ideal $\mathfrak{a}$ in $\mathrm{cl}(\mathcal{O})$. For the details of the action, see [15, §3] and [32, §3.3].

Let $\mathcal{O}$ be an order of an imaginary quadratic field such that $\mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$ is not empty, and $\mathcal{E}\ell\ell(\mathcal{O})$ be the set of elliptic curves over a number field with complex multiplication by $\mathcal{O}$. Let $\mathcal{E} \in \mathcal{E}\ell\ell(\mathcal{O})$, and $[\cdot]_{\mathcal{E}}$ be the normalized isomorphism $\mathcal{O} \to \mathrm{End}(\mathcal{E})$. We assume that $\mathcal{E}$ has a good reduction at a prime ideal $\mathfrak{p}$ above p. Then the reduction $\tilde{\mathcal{E}}$ of $\mathcal{E}$ modulo $\mathfrak{p}$ is a supersingular elliptic curve over $\mathbb{F}_{p^2}$. In addition, $(\tilde{\mathcal{E}}, [\cdot]_{\tilde{\mathcal{E}}})$ is a primitive $\mathcal{O}$-oriented elliptic curve over $\mathbb{F}_{p^2}$. We denote the map $\mathcal{E}\ell\ell(\mathcal{O}) \to \mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$ induced by this reduction by ρ. Then $\mathrm{cl}(\mathcal{O})$ acts freely and transitively on $\rho(\mathcal{E}\ell\ell(\mathcal{O}))$ [32, Theorem 3.4].

2.3 (d, ε)-structures

Let d be a positive square-free integer. A $\mathbb{Q}$-*curve* is an elliptic curve E over $\bar{\mathbb{Q}}$ that is isogenous over $\bar{\mathbb{Q}}$ to all of its Galois conjugates E^σ, $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. In particular, an elliptic curve E over a quadratic field k that is d-isogenous over $\bar{\mathbb{Q}}$ to its Galois conjugate E^σ, where σ is the nontrivial element of $\mathrm{Gal}(k/\mathbb{Q})$, is a $\mathbb{Q}$-curve; following Hasegawa [25], we call such a curve a $\mathbb{Q}$-*curve of degree* d. Chenu and Smith [20] introduced an analogous concept for elliptic curves over $\mathbb{F}_{p^2}$, which we call a (d, ε)-*structure*.

Let d be a square-free positive integer that is coprime to p, and ε be 1 or -1. A pair (E, ψ) of an elliptic curve E over $\mathbb{F}_{p^2}$ and a d-isogeny $\psi : E \to E^{(p)}$ is called a (d, ε)-*structure* if $\widehat{\psi} = \varepsilon\psi^{(p)}$. An isogeny $\varphi : (E, \psi) \to (E', \psi')$ between two (d, ε)-structures is defined as an isogeny $\varphi : E \to E'$ of elliptic curves over $\mathbb{F}_{p^2}$ satisfying

$$\psi' \circ \varphi = \varphi^{(p)} \circ \psi.$$

Let (E, ψ) be a (d, ε)-structure and (E', ψ') be a (d, ε')-structure. If there exists an isogeny $\varphi : E \to E'$ defined over $\mathbb{F}_{p^2}$ such that $\psi' \circ \varphi = \varphi^{(p)} \circ \psi$, then we have $\varepsilon = \varepsilon'$. Two (d, ε)-structures (E, ψ) and (E', ψ') are said to be isomorphic if there exists an isogeny $(E, \psi) \to (E', \psi')$ that is an isomorphism as an isogeny of elliptic curves $E \to E'$. This is denoted by $(E, \psi) \simeq (E', \psi')$.

Note that (E, ψ) is not isomorphic to $(E, -\psi)$ if $j(E)$ is not equal to 0 or 1728.

Let δ be a non-square element in $\mathbb{F}_{p^2}$ and $\sqrt{\delta}$ a square root of δ in $\mathbb{F}_{p^4}$. For an elliptic curve $E : y^2 = x^3 + ax^2 + bx + c$ over $\mathbb{F}_{p^2}$, we denote by E^{tw} the quadratic twist $y^2 = x^3 + a\delta x^2 + b\delta^2 x + c\delta^3$ of E, so that $\tau_{\sqrt{\delta}} : E \to E^{\mathrm{tw}}$ is an isomorphism defined over $\mathbb{F}_{p^4}$. For a (d, ε)-structure (E, ψ), we define its *quadratic twist* by

$$(E, \psi)^{\mathrm{tw}} := \left(E^{\mathrm{tw}},\ \tau_{\sqrt{\delta}}^{(p)} \circ \psi \circ \tau_{\sqrt{\delta}}^{-1}\right).$$

It is a $(d, -\varepsilon)$-structure, and its isomorphism class does not depend on the choice of δ [20, §2].

Let (E, ψ) be a (d, ε)-structure and π_p be the p-th power Frobenius map $E^{(p)} \to E$. Then $\mu := \pi_p \circ \psi$ is an endomorphism of E defined over $\mathbb{F}_{p^2}$. We call μ the *associated endomorphism* of (E, ψ).

Our main focus is the case that E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$. In this case, we have the following properties of (E, ψ).

Proposition 5 ([20, Proposition 2]) *Let d be a square-free positive integer coprime to p, and ε be 1 or -1. Let (E, ψ) be a (d, ε)-structure over $\mathbb{F}_{p^2}$ such that E is supersingular. Then the following hold:*

1. $\mu^2 = [-dp]$.
2. $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p + \varepsilon)\mathbb{Z})^2$.

From this proposition, if (E, ψ) is a supersingular (d, ε)-structure, then the associated endomorphism μ induces a $\mathbb{Z}(\sqrt{-dp})$-orientation on E defined by $\sqrt{-dp} \mapsto \mu$. We call this orientation the *natural orientation* of (E, ψ) and denote it by ι_ψ.

The converse of Proposition 5 is also true.

Lemma 6 ([20, Lemma 1]) *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ such that $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p+\varepsilon)\mathbb{Z})^2$, and ι be a $\mathbb{Z}(\sqrt{-dp})$-orientation on E. Then there exists an isogeny $\psi : E \to E^{(p)}$ such that (E, ψ) is a (d, ε)-structure and ι is the natural orientation of (E, ψ).*

In addition, isogenies between (d, ε)-structures are also $\mathbb{Z}(\sqrt{-dp})$-oriented isogenies. More precisely, we have the following lemma.

Lemma 7 ([20, Lemma 2]) *Let (E_0, ψ_0) and (E_1, ψ_1) be (d, ε)-structures over $\mathbb{F}_{p^2}$ such that E_0 and E_1 are supersingular. Let $\varphi : E_0 \to E_1$ be an isogeny. Then φ is an isogeny (resp. isomorphism) of (d, ε)-structures $(E_0, \psi_0) \to (E_1, \psi_1)$ if and only if φ is a $\mathbb{Z}(\sqrt{-dp})$-oriented isogeny (resp. isomorphism) $(E_0, \iota_{\psi_0}) \to (E_1, \iota_{\psi_1})$.*

Let $\mathcal{O}$ be an order of $\mathbb{Q}(\sqrt{-dp})$ such that ι_ψ is a primitive $\mathcal{O}$-orientation. Then $\mathcal{O}$ contains $\sqrt{-dp}$. This means that $\mathcal{O}$ is the ring of integers of $\mathbb{Q}(\sqrt{-dp})$ or the order of conductor 2 in $\mathbb{Q}(\sqrt{-dp})$. From this fact, we define a set $\mathcal{D}_{d,\varepsilon}(p)$ and its subsets as follows.

Definition 1 Let d be a square-free positive integer coprime with p, and ε be 1 or -1. Let $\mathcal{O}_1$ be the ring of integers of $\mathbb{Q}(\sqrt{-dp})$ and $\mathcal{O}_2$ be the order of conductor 2 in $\mathbb{Q}(\sqrt{-dp})$. We define the set $\mathcal{D}_{d,\varepsilon}(p)$ as the set of the isomorphism classes of (d,ε)-structures over $\mathbb{F}_{p^2}$.

- $\mathcal{D}^{\max}_{d,\varepsilon}(p)$ is the subset of $\mathcal{D}_{d,\varepsilon}(p)$ consisting of the classes of (d,ε)-structures such that the natural orientation is a primitive $\mathcal{O}_1$-orientation.
- $\mathcal{D}^{\mathrm{sub}}_{d,\varepsilon}(p)$ is the subset of $\mathcal{D}_{d,\varepsilon}(p)$ consisting of the classes of (d,ε)-structures such that the natural orientation is a primitive $\mathcal{O}_2$-orientation.

We define an action of the ideal class group $\mathrm{cl}(\mathcal{O}_1)$ (resp. $\mathrm{cl}(\mathcal{O}_2)$) on $\mathcal{D}^{\max}_{d,\varepsilon}(p)$ (resp. $\mathcal{D}^{\mathrm{sub}}_{d,\varepsilon}(p)$) as the action induced by the natural orientation. We denote this action in the same manner as the action of the ideal class group on $\mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$. Then we have the following proposition.

Proposition 8 ([20, Theorem 2]) *Let d be a square-free positive integer coprime with p, and ε be 1 or -1. Let $\mathcal{O}_1$ be the ring of integers of $\mathbb{Q}(\sqrt{-dp})$ and $\mathcal{O}_2$ be the order of conductor 2 in $\mathbb{Q}(\sqrt{-dp})$.*

- *The class group $\mathrm{cl}(\mathcal{O}_1)$ acts freely and transitively on $\mathcal{D}^{\max}_{d,\varepsilon}(p)$.*
- *If $\mathcal{D}^{\mathrm{sub}}_{d,\varepsilon}(p) \neq \emptyset$, then $\mathrm{cl}(\mathcal{O}_2)$ acts freely and transitively on $\mathcal{D}^{\mathrm{sub}}_{d,\varepsilon}(p)$.*

2.4 Radical isogenies

Let n be a positive integer, let k be a field with $\mathrm{char}(k) \nmid n$, let E be an elliptic curve over k, and let P be a point in $E(k)$ of order n. Then there exists an isogeny $\varphi : E \to E/\langle P \rangle$ over k with kernel $\langle P \rangle$. We denote the codomain $E/\langle P \rangle$ of φ by E'. Let P' be a point on E' such that $\hat{\varphi}(P') = P$. Castryck, Decru, and Vercauteren [24] showed that P' is defined over $k(\sqrt[n]{\gamma})$, where γ is a representative of the n-Tate pairing $\langle P, -P \rangle_n$. The n choices of an n-th root of γ correspond to the n-isogenies ψ such that the kernel of $\psi \circ \varphi$ is cyclic.

By taking models of E and $E/\langle P \rangle$ such that P and P' are $(0,0)$, they gave explicit formulas to compute $E/\langle P \rangle$ from E, and called these *radical isogenies*. For curve models, they used Tate normal forms [33] for $N \geq 4$.

As an application of radical isogenies, they proposed an efficient method to compute the ideal class group action in an isogeny-based key-exchange protocol CSURF [14], which is a variant of CSIDH [13].

We briefly recall CSIDH and CSURF. Let p be a prime number such that $p \equiv 3 \bmod 4$, and E be a supersingular elliptic curve over $\mathbb{F}_p$. Then the subring $\mathrm{End}_p(E)$ of $\mathrm{End}(E)$ consisting of endomorphisms defined over $\mathbb{F}_p$ is isomorphic to an order in $\mathbb{Q}(\sqrt{-p})$ by mapping the p-th power Frobenius endomorphism to $\sqrt{-p}$. We denote

this orientation by ι_E. Then two oriented elliptic curves (E, ι_E) and $(E', \iota_{E'})$ over $\mathbb{F}_p$ are isomorphic if and only if E and E' are isomorphic as elliptic curves over $\mathbb{F}_p$. Let $\mathcal{O}$ be $\mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$. Then the ideal class group $\mathrm{cl}(\mathcal{O})$ acts freely and transitively on the set of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ whose endomorphism rings are isomorphic to $\mathcal{O}$ [13, Theorem 7]. CSIDH uses $\mathbb{Z}[\sqrt{-p}]$ as $\mathcal{O}$, and CSURF uses $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ as $\mathcal{O}$. In addition, CSURF uses the prime p such that $p \equiv 7 \bmod 8$, so that the prime 2 in $\mathbb{Z}$ splits in $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$.

Radical isogenies can be used to efficiently compute the actions of $\mathrm{cl}(\mathcal{O})$ in CSIDH and CSURF. Let ℓ be a prime number that splits in $\mathcal{O}$, and $\mathfrak{l}$ be a prime ideal of $\mathcal{O}$ above ℓ. Given a primitively $\mathcal{O}$-oriented elliptic curve (E, ι_E) over $\mathbb{F}_p$, a positive integer n, the action of $\mathfrak{l}^n$ on (E, ι_E) can be computed by iteratively applying radical isogenies as follows:

1. Find a point $P \in E(\mathbb{F}_p)$ generating $E[\iota_E(\mathfrak{l})]$.
2. Transform E into a model such that $P = (0, 0)$.
3. Compute the codomain E' of the isogeny with kernel $\langle P \rangle$ using a radical isogeny. Iterate this n times to obtain the curve E''.
4. Transform E'' back to the original model if necessary.

In step 3 above, each radical isogeny requires the computation of an ℓ-th root in $\mathbb{F}_p$. In CSURF setups, there exists a unique ℓ-th root in $\mathbb{F}_p$ for odd primes ℓ, and this unique root induces the isogeny corresponding to the ideal $\mathfrak{l}$. For $\ell = 2$, they use 4-radical isogenies instead of 2-radical isogenies, and give a method to choose the correct 4-th root[1].

The initial paper [24] on radical isogenies gave radical isogenies for $n \leq 13$. Later, radical isogenies for all n up to the point where the square-root Vélu formulas (√élu) [35] outperform them were given in [36, 37].

3 Representing $(2, \varepsilon)$-structures

In the rest of this paper, we use the following notation. Let p be a prime number greater than 7. We fix square roots of -1 and -2 in $\mathbb{F}_{p^2}$, and denote them by $\sqrt{-1}$ and $\sqrt{-2}$, respectively. We choose a non-square $\Delta \in \mathbb{F}_p^\times$ and fix a square root $\sqrt{\Delta}$ of Δ in $\mathbb{F}_{p^2}$. Furthermore, we denote by N_{p^2} the norm on $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$, i.e., $\mathrm{N}_{p^2}(\alpha) = \alpha^{p+1}$ for $\alpha \in \mathbb{F}_{p^2}$.

The assumption $p > 7$ is for ensuring that the CM j-invariants 8000 and -3375 are not equal to 0 or 1728 modulo p. In particular, an elliptic curve over $\mathbb{F}_{p^2}$ with j-invariant 0 never has $(2, \varepsilon)$-structure since the ring of integers of $\mathbb{Q}(\sqrt{-3})$ does not contain elements of norm 2.

3.1 Intuition from modular curves

As mentioned in §3 of [20], relating $(2, \varepsilon)$-structures to modular curves suggests that a $(2, \varepsilon)$-structure can be represented by a pair of a point in $\mathbb{P}^1(\mathbb{F}_p)$ and a sign. Here

[1] The method to choose the correct 4-th root was given as a conjecture in [14], and later proved in [34].

and in what follows, we write u for the point $(u : 1) \in \mathbb{P}^1(\mathbb{F}_p)$ with $u \in \mathbb{F}_p$, and ∞ for the point $(1 : 0)$, so that $\mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\}$. More precisely, we have the following correspondence.

Let $X_0(2)$ be the modular curve of level 2, whose non-cuspidal points over $\overline{\mathbb{F}}_p$ correspond to the $\overline{\mathbb{F}}_p$-isomorphism classes of pairs (E, C) of an elliptic curve E and a subgroup C of E of order 2, and let w_2 be the Atkin–Lehner involution on $X_0(2)$, which maps the class of (E, C) to that of $(E/C, E[2]/C)$. There is a map from the set of isomorphism classes of $(2, \varepsilon)$-structures over $\mathbb{F}_{p^2}$ to $X_0(2)(\mathbb{F}_{p^2})$ mapping (E, ψ) to the class of $(E, \ker\psi)$. Since ψ induces an isomorphism $E/\ker\psi \to E^{(p)}$ mapping $E[2]/\ker\psi$ to $\ker\widehat{\psi} = (\ker\psi)^{(p)}$, the image of this map is contained in

$$X_0^{\mathrm{tw}}(2)(\mathbb{F}_p) \coloneqq \{x \in X_0(2)(\mathbb{F}_{p^2}) \mid x^{(p)} = w_2(x)\},$$

the set of $\mathbb{F}_p$-rational points of the quadratic twist of $X_0(2)$ by w_2[2]. In fact, the image is the whole $X_0^{\mathrm{tw}}(2)(\mathbb{F}_p)$, and for $j(E) \neq 1728$ the inverse image of the point corresponding to (E, ψ) is $\{(E, \psi), (E, -\psi)\}$; see Theorem 10 and its proof. The curve $X_0(2)$ has genus 0, and so does its twist $X_0^{\mathrm{tw}}(2)$; the parametrization of $\mathbb{Q}$-curves of degree 2 by Hasegawa [25, Theorem 2.2] is precisely a rational parametrization of the number field analogue of $X_0^{\mathrm{tw}}(2)$. Therefore, this correspondence suggests a representation of $(2, \varepsilon)$-structures by a point in $\mathbb{P}^1(\mathbb{F}_p)$ and a sign. However, we need to consider the following three points to obtain a one-to-one correspondence.

1. The point corresponding to the j-invariant 1728, whose automorphism group is larger than $\{\pm 1\}$.
2. The uniqueness of the representation, that is, we need to ensure that (E, ψ) and $(E, -\psi)$ are not isomorphic.
3. A point of $X_0(2)$ only determines the isomorphism class of $(E, \ker\psi)$ over $\overline{\mathbb{F}}_p$, but we need the isomorphism class over $\mathbb{F}_{p^2}$. In particular, $X_0^{\mathrm{tw}}(2)(\mathbb{F}_p)$ does not have any information about the sign ε: the quadratic twist of a $(2, \varepsilon)$-structure is a $(2, -\varepsilon)$-structure [20, §2] with the same image.

To address these points, we discuss the explicit representation of $(2, \varepsilon)$-structures in the following subsections rather than using the modular curve $X_0(2)$. This approach has a further advantage. The proof provides explicit equations of the curves and the isogenies for each representative, which are exactly what we need in Section 4 to derive the radical isogeny formulas.

§3.2 gives a representation of $(2, \varepsilon)$-structures by the parametrization by Hasegawa [25]. §3.3 gives a representation of $(2, \varepsilon)$-structures by Montgomery curves; since the Montgomery coefficient A is a coordinate on $X_0(4)$ and A^2 is one on $X_0(2)$, this representation comes from the natural projection $X_0(4) \to X_0(2)$.

[2] Chenu and Smith used the quotient $X_0^+(2) \coloneqq X_0(2)/\langle w_2\rangle$ and stated that the map from the isomorphism classes of $(2, \varepsilon)$-structures to $X_0^+(2)(\mathbb{F}_p)$ is four-to-one and surjective. However, this map is not surjective since $X_0^+(2)(\mathbb{F}_p)$ also contains the classes of pairs (E, C) with E defined over $\mathbb{F}_p$ and C stable under the p-th power Frobenius map, and such a point does not come from any $(2, \varepsilon)$-structure unless it is fixed by w_2. This is why we use the twist $X_0^{\mathrm{tw}}(2)$ instead of $X_0^+(2)$.

3.2 Hasegawa parameter

The approach suggested by Chenu and Smith [20] to represent $(2,\varepsilon)$-structures is to use the parametrization of $\mathbb{Q}$-curves of degree 2 by Hasegawa [25]. The reductions of these $\mathbb{Q}$-curves of degree 2 to $\mathbb{F}_{p^2}$ were considered by Smith [38, §5].

For $u \in \mathbb{F}_p$, we define an elliptic curve E_u by

$$E_u : y^2 = x^3 - 6(5 - 3u\sqrt{\Delta})x + 8(7 - 9u\sqrt{\Delta}).$$

Then there exists an isogeny of degree 2 from E_u with kernel $\langle (4,0) \rangle$ to ${E_u}^{(p)} = E_{-u}$ defined by

$$\psi_u : (x,y) \mapsto \left(-\frac{x}{2} - \frac{9(1+u\sqrt{\Delta})}{x-4}, \frac{y}{\sqrt{-2}} \left(-\frac{1}{2} + \frac{9(1+u\sqrt{\Delta})}{(x-4)^2} \right) \right). \tag{1}$$

Then (E_u, ψ_u) and $(E_u, -\psi_u)$ are $(2,\varepsilon)$-structures, where $\varepsilon = -\left(\frac{-2}{p}\right)$ [38, Theorem 2]. We denote this ε by ε_{H}; note that it depends only on p.

We have $j(E_u) = 2^6 \frac{(3u\sqrt{\Delta}-5)^3}{(u\sqrt{\Delta}-1)(u\sqrt{\Delta}+1)^2}$ [25, Theorem 2.2]. As pointed out in [38, §9], curves of the form E_u lack the j-invariant 1728 and it is obtained as the limit as $u \to \infty$. Based on this observation, we also define an elliptic curve E_∞ by

$$E_\infty : y^2 = x^3 + \sqrt{\Delta}x.$$

Then $j(E_\infty) = 1728$. We define ψ_∞ by

$$\psi_\infty : (x,y) \mapsto \left(-\frac{x^2+\sqrt{\Delta}}{2x}, -\frac{y(\sqrt{\Delta}-x^2)}{2\sqrt{-2}x^2} \right). \tag{2}$$

Then ψ_∞ is an isogeny of degree 2 from E_∞ to ${E_\infty}^{(p)}$ with kernel $\langle (0,0) \rangle$. By computing the dual isogeny of ψ_∞, we can show that (E_∞, ψ_∞) is a $(2,\varepsilon_{\mathrm{H}})$-structure.

For $u \in \mathbb{P}^1(\mathbb{F}_p)$, we call E_u the *Hasegawa curve* [3] with parameter u and u the *Hasegawa parameter* of E_u. In the parts of this paper where Hasegawa curves appear together with Montgomery curves (Sections 4.3, 4.4, and 5), we write E_u^{H} and ψ_u^{H} for E_u and ψ_u, and similarly for the other symbols introduced in this subsection and in Section 4.1, to distinguish them from the Montgomery ones, which are then written with the superscript M.

Thanks to the assumption that $p > 7$, if $u \in \mathbb{F}_p$, then the automorphism group of E_u is $\{\pm 1\}$, i.e., $j(E_u) \neq 0, 1728$. This can be shown as follows. An easy calculation shows that $j(E_u) \in \mathbb{F}_p$ if and only if $u = 0$ or $u^2\Delta = -7\left(\frac{5}{3^2}\right)^2$. In the former case, we have $j(E_0) = 8000$, which corresponds to the elliptic curve with CM by $\mathbb{Q}(\sqrt{-2})$. In the latter case (if a solution u exists in $\mathbb{F}_p$), we have $j(E_u) = -3375$, which corresponds

[3] Since Hasegawa [25] gave the parametrization of $\mathbb{Q}$-curves of other degrees, we should call u the *Hasegawa parameter of degree* 2. However, we do not use the parametrization of other degrees in this paper. Therefore, we call u the *Hasegawa parameter* to ease the notation.

to the elliptic curve with CM by $\mathbb{Q}(\sqrt{-7})$. Since we assume $p > 7$, these j-invariants are not equal to 0 or 1728.

Therefore, if $u \in \mathbb{F}_p$, then E_u has exactly two isogenies of degree 2 to its Galois conjugate E_{-u}, one of which is ψ_u and the other is $-\psi_u$. These give $(2, \varepsilon_{\mathrm{H}})$-structures. On the other hand, if $u = \infty$, then E_∞ has exactly four isogenies of degree 2 to its Galois conjugate ${E_\infty}^{(p)}$, $\pm\psi_\infty$ and $\pm\theta\circ\psi_\infty$. The isogenies $\pm\psi_\infty$ give $(2, \varepsilon_{\mathrm{H}})$-structures, and the isogenies $\pm\theta \circ \psi_\infty$ give $(2, \varepsilon)$-structures for some $\varepsilon \in \{\pm 1\}$. Here, ε is not necessarily ε_{H}. Indeed, we have the following lemma.

Lemma 9 *$(E_\infty, \theta \circ \psi_\infty)$ and $(E_\infty, -\theta \circ \psi_\infty)$ are $(2, -\varepsilon_{\mathrm{H}})$-structures if $p \equiv 1 \pmod 4$ and $(2, \varepsilon_{\mathrm{H}})$-structures if $p \equiv 3 \pmod 4$.*

Proof The lemma follows by a direct computation using $\widehat{\psi_\infty}$. □

For $\mathbf{u} = (u, s) \in \mathbb{P}^1(\mathbb{F}_p) \times \{\pm 1\}$, we define $\psi_{\mathbf{u}}$ by

$$\psi_{\mathbf{u}} = \begin{cases} s\psi_u & \text{if } u \in \mathbb{F}_p \text{ or } p \equiv 1 \pmod 4, \\ \psi_\infty & \text{if } s = 1,\ u = \infty, \text{ and } p \equiv 3 \pmod 4, \\ \theta \circ \psi_\infty & \text{if } s = -1,\ u = \infty, \text{ and } p \equiv 3 \pmod 4. \end{cases}$$

Based on this definition, we can represent all the $(2, \varepsilon_{\mathrm{H}})$-structures over $\mathbb{F}_{p^2}$ by the Hasegawa parameter u and a sign $s \in \{\pm 1\}$.

Theorem 10 *Let (E, ψ) be a $(2, \varepsilon_{\mathrm{H}})$-structure over $\mathbb{F}_{p^2}$. If $j(E) \neq 1728$ or $p \equiv 3 \pmod 4$, then there exists a unique $\mathbf{u} = (u, s) \in \mathbb{P}^1(\mathbb{F}_p) \times \{\pm 1\}$ such that $(E, \psi) \simeq (E_u, \psi_{\mathbf{u}})$. If $j(E) = 1728$ and $p \equiv 1 \pmod 4$, then there exists a unique $s \in \{\pm 1\}$ such that $(E, \psi) \simeq (E_\infty, \psi_{(\infty,s)})$ or $(E, \psi)^{\mathrm{tw}} \simeq (E_\infty, \theta \circ \psi_{(\infty,s)})$.*

Proof We first note that if $u \in \mathbb{F}_p$, by shifting the x-coordinate by -4, E_u is isomorphic to the elliptic curve defined by

$$y^2 = x^3 + 12x^2 + 18(1 + u\sqrt{\Delta})x.$$

We denote this elliptic curve by $\widetilde{E}_u$. Furthermore, we let $\widetilde{E}_\infty$ be E_∞ since the kernel of ψ_∞ is generated by $(0, 0)$ so that we do not need to shift the x-coordinate.

We may assume that E is defined by

$$y^2 = x^3 + ax^2 + bx, \quad (a, b \in \mathbb{F}_{p^2})$$

and the generator of $\ker\psi$ is $(0, 0)$ by shifting the x-coordinate of the generator of $\ker\psi$ to 0.

Assume $j(E) \neq 1728$, then we have $a \neq 0$. Let ν be a square root of $12/a$ in $\mathbb{F}_{p^4}$. Then E is isomorphic to the elliptic curve E' defined by

$$y^2 = x^3 + 12x^2 + \frac{12^2 b}{a^2}x$$

via the isomorphism $\tau_\nu : E \to E'$. To ease the notation, we denote $\frac{12^2 b}{a^2}$ by b' and $(E', \tau_\nu^{(p)} \circ \psi \circ \tau_\nu^{-1})$ by (E', ψ'). If $\nu \in \mathbb{F}_{p^2}$, then (E', ψ') is a $(2, \varepsilon_{\mathrm{H}})$-structure isomorphic to (E, ψ). Otherwise, (E', ψ') is a $(2, -\varepsilon_{\mathrm{H}})$-structure isomorphic to $(E, \psi)^{\mathrm{tw}}$. Since τ_ν sends $(0,0)$ to $(0,0)$, the kernel of ψ' is $\langle (0,0) \rangle$. In addition, the kernel of $\widehat{\psi'}$ is generated by $(0,0)$ on ${E'}^{(p)}$ since $\widehat{\psi'} = \pm {\psi'}^{(p)}$.

By composing the isogeny in Example III.4.5 in [28] with the isomorphism $\tau_{1/\sqrt{-2}}$, we obtain the isogeny φ from E' to the elliptic curve E'' defined by

$$y^2 = x^3 + 12x^2 + (36 - b')x$$

with kernel $\langle (0,0) \rangle$. By construction, the kernel of $\widehat{\varphi}$ is generated by $(0,0)$ on E''. Therefore, there exists an isomorphism $\eta : {E'}^{(p)} \to E''$ such that $\eta((0,0)) = (0,0)$. This means that η is τ_1 or τ_{-1}. In particular, $b'^p = 36 - b'$. Therefore, we have $b' = 18(1 + u\sqrt{\Delta})$ for some $u \in \mathbb{F}_p$. This means that E' is isomorphic to E_u by shifting the x-coordinate by 4. Let η be the isomorphism from E' to E_u and $\psi'' = \eta^{(p)} \circ \psi' \circ \eta^{-1}$. Then the kernel of ψ'' is $\langle (4,0) \rangle$ on E_u. Therefore, there exists an automorphism κ of E_{-u} such that $\psi'' = \kappa \circ \psi_u$. Since $j(E)$ is neither 0 nor 1728, κ is either $[1]$ or $[-1]$. Therefore, we have $(E', \psi') \simeq (E_u, s\psi_u)$ for some $s \in \{\pm 1\}$. This means (E', ψ') is a $(2, \varepsilon_{\mathrm{H}})$-structure, thus is isomorphic to (E, ψ).

Assume $j(E) = 1728$. Then we have $a = 0$ and $b \neq 0$. In addition, the kernel of ψ is $\langle (0,0) \rangle$ because the codomain of the isogenies of degree 2 from E with other kernel has j-invariant 66^3, which is not equal to 1728 since $p > 7$. From Example III.4.5 in [28], we have an isogeny

$$\psi' : E \to E' : y^2 = x^3 - 4bx; \quad (x, y) \mapsto \left(\frac{x^2 + b}{x}, \frac{y(b - x^2)}{x^2} \right)$$

with kernel $\langle (0,0) \rangle$. Since ψ' and ψ are isogenies defined over $\mathbb{F}_{p^2}$ with the same kernel, there exists an isomorphism $\eta : E' \to E^{(p)}$ defined over $\mathbb{F}_{p^2}$ such that $\psi = \eta \circ \psi'$. In other words, there exists $v \in \mathbb{F}_{p^2}^\times$ such that $v^4 = -\frac{b^{p-1}}{4}$ and

$$\psi = \tau_v \circ \psi' : (x, y) \mapsto \left(v^2 \frac{x^2 + b}{x}, v^3 \frac{y(b - x^2)}{x^2} \right).$$

The dual isogeny $\widehat{\psi}$ is given by

$$\widehat{\psi} : (x, y) \mapsto \left(-\frac{v^2}{b^{p-1}} \frac{x^2 + b^p}{x}, \frac{1}{8v^3} \frac{y(b^p - x^2)}{x^2} \right).$$

Since $\widehat{\psi} = \varepsilon_{\mathrm{H}} \psi^{(p)}$, we have

$$v^{2(p-1)} b^{p-1} = -1 \text{ and } 8v^{3(p+1)} = \varepsilon_{\mathrm{H}}. \tag{3}$$

Let $\varepsilon \in \{\pm 1\}$ be the sign such that $v^2 = \varepsilon \frac{b^{(p-1)/2}}{2\sqrt{-1}}$. Then the equations in (3) are equivalent to

$$b^{\frac{p^2-1}{2}} = -(-1)^{\frac{p-1}{2}} \text{ and } b^{\frac{p^2-1}{4}} = -\varepsilon^{\frac{p+1}{2}} (-\sqrt{-1})^{\frac{p+1}{2}}. \tag{4}$$

Especially, the latter implies the former.

Assume that $p \equiv 3 \pmod 4$. Then we have $\sqrt{\Delta}^{(p^2-1)/4} = (-1)^{(p+1)/4}$. This and (4) implies that b and $\sqrt{\Delta}$ are in the same class in $\mathbb{F}_{p^2}^\times / (\mathbb{F}_{p^2}^\times)^4$. Therefore, E is isomorphic to E_∞ over $\mathbb{F}_{p^2}$. Let η be an isomorphism from E to E_∞ defined over $\mathbb{F}_{p^2}$. Then $(E, \psi) \cong (E_\infty, \eta^{(p)} \circ \psi \circ \eta^{-1})$. Since $\eta^{(p)} \circ \psi \circ \eta^{-1}$ is an isogeny of degree 2 with kernel $\langle (0,0) \rangle$ from E_∞ to ${E_\infty}^{(p)}$, this isogeny is $\pm\psi_\infty$ or $\pm\theta \circ \psi_\infty$. It is easy to show that the automorphism θ of E_∞ induces $(E_\infty, \psi_\infty) \cong (E_\infty, -\psi_\infty)$ and $(E_\infty, \theta \circ \psi_\infty) \cong (E_\infty, -\theta \circ \psi_\infty)$. Therefore, we have $(E, \psi) \cong (E_\infty, \psi_{(\infty, s)})$ for some $s \in \{\pm 1\}$.

Assume that $p \equiv 1 \pmod 4$. Then we have $\sqrt{\Delta}^{(p^2-1)/2} = (-1)^{(p+1)/2}$. This and (4) implies that b and $\sqrt{\Delta}$ are in the same class in $\mathbb{F}_{p^2}^\times/(\mathbb{F}_{p^2}^\times)^2$. Therefore, E or E^{tw} is isomorphic to E_∞ over $\mathbb{F}_{p^2}$. The same discussion in the previous paragraph shows that (E,ψ) or $(E,\psi)^{\mathrm{tw}}$ is isomorphic to $(E_\infty, \psi_{(\infty,s)})$ or $(E_\infty, \theta\circ\psi_{(\infty,s)})$ for some $s \in \{\pm 1\}$. From Lemma 9 and the fact that $(E,\psi)^{\mathrm{tw}}$ is a $(2,-\varepsilon_{\mathrm{H}})$-structure, we have $(E,\psi) \cong (E_\infty, \psi_{(\infty,s)})$ or $(E,\psi)^{\mathrm{tw}} \cong (E_\infty, \theta\circ\psi_{(\infty,s)})$.

Next, we show the uniqueness of $\mathbf{u}$. Let $\mathbf{u} = (u,s)$ and $\mathbf{u}' = (u',s')$ be elements of $\mathbb{P}^1(\mathbb{F}_p)\times\{\pm 1\}$ such that $(E_u, s\psi_u) \simeq (E_{u'}, s'\psi_{u'})$, and η be an isomorphism between these two $(2,\varepsilon_{\mathrm{H}})$-structures. Then η induces an isomorphism from $\widetilde{E}_u$ to $\widetilde{E}_{u'}$. We denote this isomorphism by η_0. Since η_0 sends $(0,0)$ to $(0,0)$, we have $\eta_0 = \tau_v$ for some square (resp. fourth) root of unity in $\mathbb{F}_{p^2}$ if $u \in \mathbb{F}_p$ (resp. $u = \infty$). If $u \in \mathbb{F}_p$, then η_0 is $[\pm 1]$ and thus $u = u'$ and $s = s'$. If $u = \infty$, then η_0 is $[\pm 1]$ or $\pm\theta$. In the former case, we have $s = s'$. Since $\theta\circ\psi_\infty = \psi_\infty\circ\theta$ and $\theta^{(p)} = (-1)^{\frac{p-1}{2}}\theta$, we have $(\pm\theta)^{(p)}\circ\psi_{(\infty,s)}\circ(\pm\theta)^{-1} = (-1)^{\frac{p-1}{2}}\psi_{(\infty,s)}$. On the other hand, $\psi_{(\infty,-s)}$ is $-\psi_{(\infty,s)}$ if $p \equiv 1 \pmod 4$ and $\theta^{\pm 1}\circ\psi_{(\infty,s)}$ if $p \equiv 3 \pmod 4$. Hence $s = s'$. □

We define a set

$$\mathcal{D}_p^{\mathrm{H}} \coloneqq \{(u,s) \in \mathbb{P}^1(\mathbb{F}_p)\times\{\pm 1\} \mid E_u \text{ is supersingular}\}.$$

Since $\mathbb{Z}[\sqrt{-2p}]$ is the maximal order of $\mathbb{Q}(\sqrt{-2p})$, we have $\mathcal{D}_{d,\varepsilon}(p) = \mathcal{D}_{d,\varepsilon}^{\max}(p)$. Therefore, we have the following corollary.

Corollary 11 *The map*

$$\mathcal{D}_p^{\mathrm{H}} \to \mathcal{D}_{2,\varepsilon_{\mathrm{H}}}^{\max}(p);\ \mathbf{u} = (u,s) \mapsto (E_u, \psi_{\mathbf{u}})$$

is bijective.

Proof This follows from Theorem 10 and the fact that E_∞ is supersingular if and only if $p \equiv 3 \pmod 4$. □

Under the bijection in Corollary 11, we define an action of $\mathrm{cl}(\mathbb{Z}[\sqrt{-2p}])$ on $\mathcal{D}_p^{\mathrm{H}}$ as follows: For $\mathbf{u} = (u,s) \in \mathcal{D}_p^{\mathrm{H}}$ and an invertible ideal $\mathfrak{a}$ of $\mathbb{Z}[\sqrt{-2p}]$, we define $[\mathfrak{a}] * \mathbf{u}$ as the element $\mathbf{u}' = (u',s') \in \mathcal{D}_p^{\mathrm{H}}$ such that $(E_{u'}, \psi_{\mathbf{u}'}) \cong [\mathfrak{a}] * (E_u, \psi_{\mathbf{u}})$.

3.3 Montgomery coefficient

Let E_A be a Montgomery curve over $\mathbb{F}_{p^2}$ such that $A^2 - 4 \in (\mathbb{F}_{p^2}^\times)^4$. Then, for a fourth root v of A^2-4, the isogeny φ_v in Lemma 4 is defined over $\mathbb{F}_{p^2}$. The following proposition shows that E_A admits a $(2,\varepsilon)$-structure whose isogeny has kernel $\langle(0,0)\rangle$ if and only if the norm of A^2-4 is 16.

Proposition 12 *Let A be an element in $\mathbb{F}_{p^2}^\times$ such that $A^2 - 4 \in (\mathbb{F}_{p^2}^\times)^4$. Then there exist an isogeny ψ with kernel $\langle(0,0)\rangle$ and $\varepsilon \in \{\pm 1\}$ such that (E_A,ψ) is a $(2,\varepsilon)$-structure if and only if $\mathrm{N}_{p^2}(A^2-4) = 16$.*

Proof Assume (E_A, ψ) is a $(2,\varepsilon)$-structure such that ψ is an isogeny with kernel $\langle(0,0)\rangle$. Let v be a fourth root of A^2-4. Then the kernels of ψ and φ_v are the same. Therefore, there exists an isomorphism $\eta : E_{A^p} \to E_{-2Av^{-2}}$ such that $\eta\circ\psi = \varphi_v$. Since $\widehat{\psi} = \varepsilon\psi^{(p)}$, the kernel of $\widehat{\psi}$ is generated by $(0,0)$ on E_{A^p}. The kernel of φ_v is generated by $(0,0)$ on $E_{-2Av^{-2}}$. This implies that η sends $(0,0)$ on E_{A^p} to $(0,0)$ on $E_{-2Av^{-2}}$. From Proposition 1 in [34], we have $A^{2p} = (-2Av^{-2})^2$. Thus, we have $\mathrm{N}_{p^2}(A^2-4) = 16$.

Conversely, assume $\mathrm{N}_{p^2}(A^2-4) = 16$. Then we have $A^{2p} = 4A^2/(A^2-4)$. Therefore, there exists a fourth root v of A^2-4 such that $A^p = -2Av^{-2}$. From Lemma 4, (E_A,φ_v) is a $(2,\varepsilon)$-structure if and only if $v^{2p+2} = 4$ and $v^{3p+3} = 8\varepsilon$. We have

$$v^{2p+2} = (-2)^{p+1}A^{p+1}/A^{p(p+1)} = (-2)^{p-1+2}/A^{p^2-1} = 4,$$
$$v^{3p+3} = (-8)^{(p+1)/2}/A^{3(p-1)(p+1)/2} = -8(-8)^{(p-1)/2}/A^{3(p^2-1)/2}.$$

Let $\varepsilon = -(-8)^{(p-1)/2}/A^{3(p^2-1)/2}$. Then $\varepsilon \in \{\pm 1\}$. Therefore, (E_A,φ_v) is a $(2,\varepsilon)$-structure. □

Proposition 13 *Let E_0 be the Montgomery curve with coefficient 0 over $\mathbb{F}_{p^2}$. Then there exist an isogeny ψ with kernel $\langle(0,0)\rangle$ and $\varepsilon \in \{\pm 1\}$ such that (E_0,ψ) is a $(2,\varepsilon)$-structure if and only if $p \equiv 3 \pmod 4$.*

Proof By taking $A = 0$ in Lemma 4, we see that the codomain of any isogeny of degree 2 with kernel $\langle(0,0)\rangle$ from E_0 is isomorphic to E_0 itself. Let $v = 1+\sqrt{-1}$. Then we have $v^4 = -4$. Then any isogeny ψ of degree 2 with kernel $\langle(0,0)\rangle$ from E_0 to itself is of the form $\psi = \theta^k\circ\varphi_v$ for $k \in \{0,1,2,3\}$. From the explicit formula of φ_v and $\widehat{\varphi_v}$ in Lemma 4, it is easy to see that (E_0,ψ) is a $(2,\varepsilon)$-structure if and only if $p \equiv 3 \pmod 4$. □

Unlike the case of Hasegawa curves, there exists a $(2,\varepsilon)$-structures over $\mathbb{F}_{p^2}$ whose curve is not isomorphic over $\overline{\mathbb{F}}_p$ to any Montgomery curves over $\mathbb{F}_{p^2}$. For example, if $p = 11$ then there is no Montgomery curve over $\mathbb{F}_{11^2}$ with j-invariant $3+2\sqrt{-1}$. This can be confirmed by listing all the Montgomery curves over $\mathbb{F}_{11^2}$. On the other hand, E_7^{H} has the j-invariant $3+2\sqrt{-1}$ and $(E_7^{\mathrm{H}},\psi_7^{\mathrm{H}})$ is a $(2,\varepsilon_{\mathrm{H}})$-structure.

However, in the case of supersingular curves, a similar result as Corollary 11 holds. To describe this result, we define notations for the Montgomery curves.

For $\mathbf{A} = (A,s) \in \mathbb{F}_{p^2}\times\{\pm 1\}$ such that $\mathrm{N}_{p^2}(A^2-4) = 16$, we define $v_{\mathbf{A}}$ as

$$v_{\mathbf{A}} = \begin{cases} s\sqrt{-2}A^{-\frac{p-1}{2}} & \text{if } A \neq 0, \\ s+\sqrt{-1} & \text{if } A = 0. \end{cases} \tag{5}$$

Then we have $v_{\mathbf{A}}^4 = A^2-4$, and we define an isogeny $\psi_{\mathbf{A}}$ of degree 2 from E_A over $\mathbb{F}_{p^2}$ by $\psi_{\mathbf{A}} \coloneqq \varphi_{v_{\mathbf{A}}}$.

From the explicit formula in Lemma 4, we have $\varphi_{-v} = -\varphi_v$ and $\theta\circ\varphi_v = \varphi_{\sqrt{-1}v}$. Hence $\psi_{(A,-s)} = -\psi_{\mathbf{A}}$ if $A \neq 0$, and $\psi_{(0,-1)} = \theta\circ\psi_{(0,1)}$. As explained in the proofs of Propositions 12 and 13, we have $(E_A,\psi_{\mathbf{A}})$ is a $(2,\varepsilon)$-structure for some $\varepsilon \in \{\pm 1\}$. From Lemma 3 and Proposition 5 (2), we have $\varepsilon = -(-1)^{(p-1)/2}$. We denote this ε by ε_{M}; note that it depends only on p.

We define a set

$$\mathcal{D}_p^{\mathrm{M}} := \{(A, s) \in \mathbb{F}_{p^2} \times \{\pm 1\} \mid E_A \text{ is supersingular and } \mathrm{N}_{p^2}(A^2 - 4) = 16\}.$$

Then we have the following theorem.

Theorem 14 *The map*

$$\mathcal{D}_p^{\mathrm{M}} \to \mathcal{D}_{2,\varepsilon_{\mathrm{M}}}^{\max}(p);\ \mathbf{A} = (A, s) \mapsto (E_A, \psi_{\mathbf{A}})$$

is surjective. In addition, (A, s) and (A', s') have the same image if and only if $A = \pm A'$ and $s = s'$.

Proof Let (E, ψ) be a supersingular $(2, \varepsilon_{\mathrm{M}})$-structure over $\mathbb{F}_{p^2}$, and T be the generator of $\ker \psi$. From Proposition 5 (2), we have $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p + \varepsilon_{\mathrm{M}})\mathbb{Z})^2$, thus, $E[4] \subset E(\mathbb{F}_{p^2})$. From this and Lemma 2, there exist $A \in \mathbb{F}_{p^2}$ and an isomorphism $\eta : E \to E_A$ defined over $\mathbb{F}_{p^2}$ such that $\eta(T) = (0, 0)$. This induces a $(2, \varepsilon_{\mathrm{M}})$-structure $(E_A, \eta^{(p)} \circ \psi \circ \eta^{-1})$. Since $\ker \eta^{(p)} \circ \psi \circ \eta^{-1} = \langle (0, 0) \rangle$, we have $\mathrm{N}_{p^2}(A^2 - 4) = 16$ by Proposition 12. In addition, we have $\eta^{(p)} \circ \psi \circ \eta^{-1} = \kappa \circ \psi_{(A,1)}$ for some automorphism κ of E_{A^p}.

If $j(E) \neq 1728$, then $A \neq 0$ and κ is either $[1]$ or $[-1]$. Therefore, (E, ψ) is isomorphic to $(E_A, \psi_{(A,s)})$ for some $s \in \{\pm 1\}$.

If $j(E) = 1728$, then there are three Montgomery coefficients A such that $j(E_A) = 1728$. It is easy to see that $A = 0$ is the only one such that $\mathrm{N}_{p^2}(A^2 - 4) = 16$. As we mentioned in the proof of Theorem 10, the automorphism θ of E_0 induces $(E_0, \psi_{(0,1)}) \cong (E_0, -\psi_{(0,1)})$ and $(E_0, \psi_{(0,-1)}) \cong (E_0, -\psi_{(0,-1)})$. Therefore, (E, ψ) is isomorphic to $(E_0, \psi_{(0,1)})$ or $(E_0, \psi_{(0,-1)})$. This shows the surjectivity of the map.

Assume that (A, s) and (A', s') have the same image. Then there exists an isomorphism $\eta : E_A \to E_{A'}$ such that $\eta((0, 0)) = (0, 0)$. This implies that $A = \pm A'$. Therefore, we have the following cases.

- $\eta = [1]$ or $[-1]$ and $A = A'$,
- $\eta = \theta$ or θ^{-1} and $A = -A'$.

In both cases, it is easy to see that $s = s'$.

It is also easy to see that $\theta : E_A \to E_{-A}$ induces $(E_A, \psi_{(A,s)}) \cong (E_{-A}, \psi_{(-A,s)})$ for $A \neq 0$. This completes the proof. □

4 Radical 3-isogenies on $(2, \varepsilon)$-structures

In this section, we propose new 3-radical isogenies which correspond to the ideal class group action on the set of isomorphism classes of supersingular $(2, \varepsilon)$-structures. Since $\mathcal{D}_{2,\varepsilon}^{\mathrm{sub}} = \emptyset$, we consider the action on $\mathcal{D}_{2,\varepsilon}^{\max}(p)$, which is represented by Hasegawa curves in Section 4.1 and Montgomery curves in Section 4.2. To ease the notation, we denote $\mathcal{D}_{2,\varepsilon}^{\max}(p)$ by $\mathcal{D}_{2,\varepsilon}(p)$. We assume $p \equiv 1 \bmod 3$ so that 3 splits into two distinct prime ideals in $\mathbb{Q}(\sqrt{-2p})$.

We denote the ideal generated by 3 and $1 + \sqrt{-2p}$ in $\mathbb{Z}[\sqrt{-2p}]$ by $\mathfrak{l}$. Then $\mathfrak{l}$ and its conjugate $\bar{\mathfrak{l}}$ are distinct prime ideals in $\mathbb{Z}[\sqrt{-2p}]$ above 3. Throughout this section,

T denotes a point of order 3 generating the kernel of a 3-isogeny, and t denotes its x-coordinate. For a $(2,\varepsilon)$-structure (E,ψ), the x-coordinate t differs from the x-coordinate of the generator of $\ker\psi$. This means that $t \neq 4$ if $E = E_u^{\mathrm{H}}$ with $u \in \mathbb{F}_p$, and $t \neq 0$ if $E = E_\infty^{\mathrm{H}}$ or is a Montgomery curve. We use these facts without further mention when dividing by $t-4$, t^p-4, or t.

4.1 Hasegawa parameter

Here, we present 3-radical isogenies on supersingular $(2,\varepsilon_{\mathrm{H}})$-structures represented by the Hasegawa parameter. From Corollary 11, we can regard $\mathcal{D}_{2,\varepsilon_{\mathrm{H}}}(p)$ as $\mathcal{D}_p^{\mathrm{H}}$. For $\mathbf{u} = (u,s) \in \mathcal{D}_p^{\mathrm{H}}$, we denote its associated endomorphism by $\mu_{\mathbf{u}}$ and its natural orientation by $\iota_{\mathbf{u}}$, and we write $E_{\mathbf{u}}[\mathfrak{a}]$ for $E_u[\iota_{\mathbf{u}}(\mathfrak{a})]$ (see Section 2.2). Note that $\mu_{(u,-s)} = -\mu_{\mathbf{u}}$, hence $\iota_{(u,-s)}(\beta) = \iota_{\mathbf{u}}(\bar{\beta})$ for $\beta \in \mathbb{Z}[\sqrt{-2p}]$ and $E_{(u,-s)}[\mathfrak{l}] = E_{\mathbf{u}}[\bar{\mathfrak{l}}]$. Thus the subgroup $E_{\mathbf{u}}[\mathfrak{a}]$ depends on the sign s, not only on the curve E_u. To simplify the discussion, we mainly focus on the case $u \in \mathbb{F}_p$ in this subsection. The case $u = \infty$ is discussed in Appendix A.

First, we give a condition on the x-coordinate t of a generator of $E_{\mathbf{u}}[\mathfrak{l}]$ or $E_{\mathbf{u}}[\bar{\mathfrak{l}}]$.

Lemma 15 *Let $\mathbf{u} = (u,s) \in \mathcal{D}_p^{\mathrm{H}}$ with $u \in \mathbb{F}_p$, let $T \in E_u[3]$, and let t be the x-coordinate of T. Then, $T \in E_{\mathbf{u}}[\mathfrak{l}]$ or $E_{\mathbf{u}}[\bar{\mathfrak{l}}]$ if and only if*

$$-18(1-u\sqrt{\Delta}) = (t^p-4)(t^p+2t) \tag{6}$$

Proof Let $\mu_{\mathbf{u}}$ be the associated endomorphism of $(E_u, s\psi_u)$. Then we have

- $T \in E_{\mathbf{u}}[\mathfrak{l}]$ if and only if $T = -\mu_{\mathbf{u}}(T)$,
- $T \in E_{\mathbf{u}}[\bar{\mathfrak{l}}]$ if and only if $T = \mu_{\mathbf{u}}(T)$.

Therefore, $T \in E_{\mathbf{u}}[\mathfrak{l}]$ or $E_{\mathbf{u}}[\bar{\mathfrak{l}}]$ if and only if t is equal to the x-coordinate of $\mu_{\mathbf{u}}(T)$. From the definition (1) of ψ_u, the x-coordinate of $\pm\mu_{\mathbf{u}}(T)$ is given by

$$-\frac{t^p}{2} - \frac{9(1-u\sqrt{\Delta})}{t^p-4}.$$

The condition in the lemma is equivalent to this x-coordinate being equal to t. □

Note that t in Lemma 15 is in $\mathbb{F}_{p^2}$ since the p^2-th power Frobenius endomorphism on E_u acts as $[1]$ or $[-1]$ on $E_u[3]$. The next lemma gives a condition on such t.

Lemma 16 *Let t be an element in $\mathbb{F}_{p^2}$ satisfying Equation (6). Then the following equation holds:*

$$\mathrm{N}_{p^2}\left(\frac{t^p+t-2}{t-4}\right) = -2.$$

Proof By taking the trace on $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$ of Equation (6), we have

$$t^{2p} + t^2 + 4t^{1+p} - 12t^p - 12t + 36 = 0.$$

This leads to

$$(t + t^p - 2)^2 + 2(t-4)(t^p - 4) = 0.$$

The equation in the lemma follows from this equation. □

From the above lemma and $\sqrt{-2}^{p-1} \in \{\pm 1\}$, we have

$$\frac{t^p + t - 2}{\sqrt{-2}^p (t-4)^{\frac{p+1}{2}}} \in \{\pm 1\}. \tag{7}$$

We denote this element by $\chi(t)$. By using this, we can determine $T \in E_{\mathbf{u}}[\mathfrak{l}]$ or $E_{\mathbf{u}}[\bar{\mathfrak{l}}]$.

Lemma 17 *Let $\mathbf{u} = (u, s) \in \mathcal{D}_p^{\mathrm{H}}$ with $u \in \mathbb{F}_p$, let $T \in E_{\mathbf{u}}[\mathfrak{l}]$ or $E_{\mathbf{u}}[\bar{\mathfrak{l}}]$, and let t be the x-coordinate of T. Then, we have*

- *$T \in E_{\mathbf{u}}[\mathfrak{l}]$ if and only if $\chi(t) = s$,*
- *$T \in E_{\mathbf{u}}[\bar{\mathfrak{l}}]$ if and only if $\chi(t) = -s$.*

Proof Let y_t be the y-coordinate of T. From the definition (1) of ψ_u, the y-coordinate of $\mu_{\mathbf{u}}(T)$ is given by

$$s \left(\frac{y_t}{\sqrt{-2}}\right)^p \left(-\frac{1}{2} + \frac{9(1 - u\sqrt{\Delta})}{(t^p - 4)^2}\right).$$

$T \in E_{\mathbf{u}}[\mathfrak{l}]$ if and only if y_t is the negative of the y-coordinate of $\mu_{\mathbf{u}}(T)$. Therefore, $T \in E_{\mathbf{u}}[\mathfrak{l}]$ if and only if

$$s \frac{y_t^{p-1}}{\sqrt{-2}^p} \left(-\frac{1}{2} + \frac{9(1 - u\sqrt{\Delta})}{(t^p - 4)^2}\right) = -1. \tag{8}$$

If $T \in E_{\mathbf{u}}[\bar{\mathfrak{l}}]$, then the right-hand side of (8) is 1. Therefore, it suffices to show that the left-hand side of (8) is equal to $-s \cdot \chi(t)$.

From the defining equation of E_u,

$$\begin{aligned} y_t^2 &= t^3 - 6(5 - 3u\sqrt{\Delta})t + 8(7 - 9u\sqrt{\Delta}) \\ &= t^3 - 18(1 - u\sqrt{\Delta})t + 4 \cdot 18(1 - u\sqrt{\Delta}) - 12t - 16. \end{aligned}$$

By substituting Equation (6) into the above equation, we have

$$\begin{aligned} y_t^2 &= t^3 + t(t^p - 4)(t^p + 2t) - 4(t^p - 4)(t^p + 2t) - 12t - 16 \\ &= (t-4)(t^p + t - 2)^2. \end{aligned} \tag{9}$$

Therefore, we have $y_t^{p-1} = (t-4)^{\frac{p-1}{2}}(t^p + t - 2)^{p-1} = (t-4)^{\frac{p-1}{2}}$. On the other hand, we have

$$\begin{aligned} -\frac{1}{2} + \frac{9(1 - u\sqrt{\Delta})}{(t^p - 4)^2} &= \frac{-(t^p - 4)^2 + 18(1 - u\sqrt{\Delta})}{2(t^p - 4)^2} \\ &= \frac{-(t^p - 4)^2 - (t^p - 4)(t^p + 2t)}{2(t^p - 4)^2} \\ &= -\frac{t^p + t - 2}{(t-4)^p} \end{aligned}$$

Therefore, the left-hand side of (8) is

$$s\frac{(t-4)^{\frac{p-1}{2}}}{\sqrt{-2^p}}\left(-\frac{t^p+t-2}{(t-4)^p}\right) = -s\cdot\chi(t).$$

This completes the proof. □

Before presenting the radical isogenies for the case where $u \in \mathbb{F}_p$, we give the formula for the case where $u = \infty$. Note that E_∞ is supersingular if and only if $p \equiv 3 \pmod 4$. Therefore, we can suppose $p \equiv 7 \bmod 12$ in the following theorem.

Theorem 18 *Suppose that $p \equiv 7 \bmod 12$ and let $\sqrt{3}$ be a square root of 3 in $\mathbb{F}_{p^2}$ such that $\sqrt{3}/\sqrt{\Delta}$ is in $(\mathbb{F}_p^\times)^2$. Then, if $p \equiv 3 \pmod 8$,*

$$[\mathfrak{l}]*(\infty,s) = \left(-s\frac{7\sqrt{3}}{12\sqrt{\Delta}}, -s_p\right) \text{ and } [\bar{\mathfrak{l}}]*(\infty,s) = \left(-s\frac{7\sqrt{3}}{12\sqrt{\Delta}}, s_p\right),$$

and if $p \equiv 7 \pmod 8$,

$$[\mathfrak{l}]*(\infty,s) = \left(s\frac{7\sqrt{3}}{12\sqrt{\Delta}}, -s\cdot s_p\right) \text{ and } [\bar{\mathfrak{l}}]*(\infty,s) = \left(s\frac{7\sqrt{3}}{12\sqrt{\Delta}}, s\cdot s_p\right),$$

where s_p is defined in (A1) in Appendix A. In addition, let $\mathbf{u}' = (u, s')$ be $[\mathfrak{l}]*(\infty,s)$ and ε be the sign such that $u = \varepsilon\frac{7\sqrt{3}}{12\sqrt{\Delta}}$. Then the x-coordinate of a generator of $E_{\mathbf{u}'}[\mathfrak{l}]$ is given by

$$\alpha = \left(2\varepsilon - \sqrt{3}\right)^{\frac{p+2}{3}} \text{ and } (3+3\sqrt{3}\varepsilon)\alpha^2 + 2\sqrt{3}\alpha - \frac{1-\sqrt{3}\varepsilon}{2}.$$

The same holds for the action of $\bar{\mathfrak{l}}$.

The proof of this theorem is given in Appendix A.

From Theorem 18, we can see that the neighbors of (∞, s) in terms of the actions by $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ are $\left(\pm\frac{7\sqrt{3}}{12\sqrt{\Delta}}, \pm 1\right)$. The next lemma shows that the denominator of the radical isogenies which we will present later vanishes only at these points.

Lemma 19 *Let $\mathbf{u} = (u, s) \in \mathcal{D}_p^{\mathrm{H}}$ and $\mathfrak{a}$ be $\mathfrak{l}$ or $\bar{\mathfrak{l}}$. Let t be the x-coordinate of a generator of $E_{\mathbf{u}}[\mathfrak{a}]$. Then, $t^p + t - 3 = 0$ if and only if $[\mathfrak{a}]*\mathbf{u} = (\infty, s')$ for some $s' \in \{\pm 1\}$. In this case, $u = \varepsilon\frac{7\sqrt{3}}{12\sqrt{\Delta}}$, where $\varepsilon = -s'$ if $p \equiv 3 \pmod 8$ and $\varepsilon = s'$ if $p \equiv 7 \pmod 8$.*

The proof of this lemma is also given in Appendix A.

To derive 3-radical isogenies for the case where $u \in \mathbb{F}_p$, we need to compute the Tate pairing $\langle T, -T\rangle_3$ for $T \in E_{\mathbf{u}}[\mathfrak{l}]$ or $E_{\mathbf{u}}[\bar{\mathfrak{l}}]$. Let t be the x-coordinate of T, and y_T be the y-coordinate of T. From Lemma 1 and Equation (9), we have

$$\langle T, -T\rangle_3 \equiv 2y_T \equiv 2y_T^{-2} \equiv \frac{2(t^p+t-2)}{t-4} \pmod{(\mathbb{F}_{p^2}^\times)^3}.$$

Using this, we can derive the radical isogenies as follows.

Theorem 20 *Let $\mathbf{u} = (u, s) \in \mathcal{D}_p^{\mathrm{H}}$ with $u \neq \infty$, and $\mathfrak{a}$ be $\mathfrak{l}$ or $\bar{\mathfrak{l}}$. Let t be the x-coordinate of a generator of $E_{\mathbf{u}}[\mathfrak{a}]$ and $\mathbf{u}' = (u', s') = [\mathfrak{a}] * \mathbf{u}$. Assume that $t^p + t - 3 \neq 0$. Then, the x-coordinate t' of a generator of $E_{\mathbf{u}'}[\mathfrak{a}]$ is given by*

$$t' = \frac{-3(t-4)\alpha^2 - 2(t^p + 2t - 6)\alpha - t}{t + t^p - 3}, \tag{10}$$

where

$$\alpha = -\frac{1}{2}\left(\frac{2(t + t^p - 2)}{t - 4}\right)^{\frac{p+2}{3}}.$$

Proof We use SageMath to aid the computation. Here, we use the file named `supporting_proofs/proof_theorem_Hasegawa_radical.sage` in our GitHub repository.

From Vélu's formulas (of the form in [29, Theorem 12.16]), we obtain an isogeny $\varphi : E_u \to E'$ for some elliptic curve E' with kernel $\langle T \rangle$. This isogeny sends $(4, 0)$ to $(-4(t + t^p - 3), 0)$. By evaluating a point in $E_u[3] \setminus \ker \varphi$, we can see that the x-coordinate of a generator of the kernel of the dual isogeny $\hat{\varphi}$ is $-3t$. Since $t + t^p - 3 \in \mathbb{F}_p^\times$, this element belongs to $(\mathbb{F}_{p^2}^\times)^2$. Let v be a square root of $-1/(t + t^p - 3)$ in $\mathbb{F}_{p^2}$. Then, the composition $\tau_v \circ \varphi$ gives an isogeny from E_u to another Hasegawa curve $E_{u'}$ with kernel $\langle T \rangle$.

Let $\Psi_3(x)$ be the 3-division polynomial of $E_{u'}$, and $t_d = -3t/(t + t^p - 3)$. Then, t_d is the x-coordinate of a generator of $\ker \widehat{\tau_v \circ \varphi}$. Therefore, $\Psi_3(x)$ is divisible by $x - t_d$. An explicit computation shows that $\Psi_3(x)/(3(x - t_d))$ is equal to

$$\begin{aligned} F(x) \coloneqq & x^3 + \frac{3t}{t + t^p - 3}x^2 + \frac{3(12(t-4)t^p - 11t^3 - 24t + 288)}{(t + t^p - 3)^2}x \\ & - \frac{12(t-4)(19t - 72)t^p + (13t - 48)(t^2 + 72t - 288)}{(t + t^p - 3)^3}. \end{aligned}$$

From Lemma 16, α is a cube root of $\langle T, -T \rangle_3$, where T is a point on E_u with x-coordinate t. Therefore, the theory of radical isogenies (see Section 3 in [24]) shows that $F(x)$ has a root represented by a rational function in t and α. Indeed, we can verify that $F(t') = 0$ for t' defined in Equation (10) (we found such an expression by using `supporting_proofs/guess_Hasegawa_radical.sage` in our GitHub repository).

From Lemma 16, we have $\mathrm{N}_{p^2}(\alpha) = -2$. Since a primitive cube root of unity is in $\mathbb{F}_p$, another cube root of $\langle T, -T \rangle_3$ has norm -2ω for a primitive cube root of unity ω. By using this, we can verify that t' in Equation (10) derived from α satisfies the same condition as in Lemma 16, and that the x-coordinate defined from the other cube root of $\langle T, -T \rangle_3$ does not satisfy the condition. This means that t' is the x-coordinate of a generator of $E_{\mathbf{u}'}[\mathfrak{a}]$. □

4.2 Montgomery coefficients

Here, we present 3-radical isogenies on supersingular $(2, \varepsilon_{\mathrm{M}})$-structures represented by Montgomery coefficients. From Theorem 14, we can regard $\mathcal{D}_{2,\varepsilon_{\mathrm{M}}}(p)$ as $\mathcal{D}_p^{\mathrm{M}}$ up to sign of the first component. For $\mathbf{A} = (A, s) \in \mathcal{D}_p^{\mathrm{M}}$, we denote its associated endomorphism by $\mu_{\mathbf{A}}$ and its natural orientation by $\iota_{\mathbf{A}}$, and we write $E_{\mathbf{A}}[\mathfrak{a}]$ for $E_A[\iota_{\mathbf{A}}(\mathfrak{a})]$ as in Section 4.1. We let $v_{\mathbf{A}}$ be as defined in Equation (5), so that $\psi_{\mathbf{A}} = \varphi_{v_{\mathbf{A}}}$.

The 3-division polynomial of E_A is given by

$$\Psi_3(x) = 3x^4 + 4Ax^3 + 6x^2 - 1.$$

Let t be the x-coordinate of a point of order 3 in E_A. Then, t satisfies $\Psi_3(t) = 0$, which is equivalent to

$$t^2 + At + 1 = \frac{t^2}{4}\left(1 - \frac{1}{t^2}\right)^2. \tag{11}$$

First, we give a condition on the x-coordinate t of a generator of $E_{\mathbf{A}}[\mathfrak{l}]$ or $E_{\mathbf{A}}[\bar{\mathfrak{l}}]$.

Lemma 21 *Let $\mathbf{A} = (A, s) \in \mathcal{D}_p^{\mathrm{M}}$, let T be a point of order 3 in E_A, and let t be the x-coordinate of T. Then, T generates $E_{\mathbf{A}}[\mathfrak{l}]$ or $E_{\mathbf{A}}[\bar{\mathfrak{l}}]$ if and only if*

$$v_{\mathbf{A}}^2 = \frac{1}{4t^{p-1}}\left(1 - \frac{1}{t^2}\right)^2.$$

Proof As in the proof of Lemma 15, T generates $E_{\mathbf{A}}[\mathfrak{l}]$ or $E_{\mathbf{A}}[\bar{\mathfrak{l}}]$ if and only if $T = \pm\mu_{\mathbf{A}}(T)$. This is equivalent to

$$t = \left(\frac{t^2 + At + 1}{v_{\mathbf{A}}^2 t}\right)^p.$$

From Equation (11), this equation is equivalent to the equation in the lemma. □

Let t be the same as in Lemma 21. We define

$$\chi(t) \coloneqq \frac{1}{2v_{\mathbf{A}} t^{\frac{p-1}{2}}}\left(1 - \frac{1}{t^2}\right). \tag{12}$$

From Lemma 21, we have $\chi(t) \in \{\pm 1\}$. We first show that t satisfies a condition on its norm, which will be used in the proof of the next lemma and to compute a cube root in the 3-radical isogenies.

Lemma 22 *Let $\mathbf{A} = (A, s) \in \mathcal{D}_p^{\mathrm{M}}$, let T be a point generating $E_{\mathbf{A}}[\mathfrak{l}]$ or $E_{\mathbf{A}}[\bar{\mathfrak{l}}]$, and let t be the x-coordinate of T. Then, we have*

$$\mathrm{N}_{p^2}\left(1 - \frac{1}{t^2}\right) = -8.$$

Proof By taking the norm of (12), we have

$$\mathrm{N}_{p^2}\left(1 - \frac{1}{t^2}\right) = 4\,\mathrm{N}_{p^2}(v_{\mathbf{A}}) t^{\frac{p^2-1}{2}}.$$

Since $(E_A, \psi_{\mathbf{A}})$ is a $(2, \varepsilon_{\mathrm{M}})$-structure, we have $\widehat{\psi_{\mathbf{A}}} = \varepsilon_{\mathrm{M}}\psi_{\mathbf{A}}^{(p)}$. By comparing the explicit forms of $\varphi_{v_{\mathbf{A}}}$ and $\widehat{\varphi_{v_{\mathbf{A}}}}$ in Lemma 4, we have $\mathrm{N}_{p^2}(v_{\mathbf{A}})^2 = 4$ and $\mathrm{N}_{p^2}(v_{\mathbf{A}})^3 = 8\varepsilon_{\mathrm{M}}$. Therefore, we have $\mathrm{N}_{p^2}(v_{\mathbf{A}}) = 2\varepsilon_{\mathrm{M}}$. To show the lemma, we need to show that $\varepsilon_{\mathrm{M}} t^{\frac{p^2-1}{2}} = -1$. In other words, we need to show that $t \in (\mathbb{F}_{p^2}^{\times})^2$ if and only if $E_A(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p-1)\mathbb{Z})^2$.

Assume that $E_A \cong (\mathbb{Z}/(p-1)\mathbb{Z})^2$. Then, $T \in E_A(\mathbb{F}_{p^2})$. In particular, $T \in 2E_A(\mathbb{F}_{p^2})$ since $T = [2](-T)$. From Theorem 4.1 in [39, Chapter 1], we have $t \in (\mathbb{F}_{p^2}^{\times})^2$.

Assume that $E_A \cong (\mathbb{Z}/(p+1)\mathbb{Z})^2$. Let δ be a non-square element in $\mathbb{F}_{p^2}$, and take a square root $\sqrt{\delta}$ of δ in $\mathbb{F}_{p^4}$. Let E be a quadratic twist of E_A obtained by $\tau_{\sqrt{\delta}} : E_A \to E$. Then, $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p-1)\mathbb{Z})^2$. Therefore, the same discussion in the previous paragraph implies δt, which is the x-coordinate of $\tau_{\sqrt{\delta}}(T)$, is in $(\mathbb{F}_{p^2}^{\times})^2$. This means that t is not in $(\mathbb{F}_{p^2}^{\times})^2$. □

Next, we show that $\chi(t)$ determines whether T generates $E_{\mathbf{A}}[\mathfrak{l}]$ or $E_{\mathbf{A}}[\bar{\mathfrak{l}}]$.

Lemma 23 *Let $\mathbf{A} = (A, s) \in \mathcal{D}_p^{\mathrm{M}}$, let T be a generator of $E_{\mathbf{A}}[\mathfrak{l}]$ or $E_{\mathbf{A}}[\bar{\mathfrak{l}}]$, and let t be the x-coordinate of T. Then, we have*

- *T generates $E_{\mathbf{A}}[\mathfrak{l}]$ if and only if $\chi(t) = -t^{\frac{p^2-1}{2}}$,*
- *T generates $E_{\mathbf{A}}[\bar{\mathfrak{l}}]$ if and only if $\chi(t) = t^{\frac{p^2-1}{2}}$.*

Proof Let y_T be the y-coordinate of T, and y_μ be the y-coordinate of $\mu_{\mathbf{A}}(T)$. Note that $T \in E_{\mathbf{A}}[\mathfrak{l}]$ if and only if $y_\mu/y_T = -1$, and $T \in E_{\mathbf{A}}[\bar{\mathfrak{l}}]$ if and only if $y_\mu/y_T = 1$.

By the definition of $\psi_{\mathbf{A}}$, we have

$$y_\mu/y_T = y_T^{p-1}\left(\frac{1-t^2}{v_{\mathbf{A}}^3 t^2}\right)^p.$$

From Lemma 21 and Equation (12), we have

$$v_{\mathbf{A}}^{-3p} = 8\chi(t)t^{\frac{3(p^2-p)}{2}}\left(1-\frac{1}{t^2}\right)^{-3p}.$$

From Equation (11), we have

$$y_T^{p-1} = t^{\frac{3(p-1)}{2}}\left(1-\frac{1}{t^2}\right)^{p-1}.$$

Therefore, we have

$$\frac{y_\mu}{y_T} = -8\chi(t)t^{\frac{p^2-1}{2}}\,\mathrm{N}_{p^2}\left(1-\frac{1}{t^2}\right)^{-1}.$$

From Lemma 22, we have $y_\mu/y_T = \chi(t)t^{\frac{p^2-1}{2}}$. This completes the proof. □

To derive 3-radical isogenies, we need to compute the Tate pairing $\langle T, -T\rangle_3$ for $T \in E_{\mathbf{A}}[\mathfrak{l}]$ or $E_{\mathbf{A}}[\bar{\mathfrak{l}}]$. Let t be the x-coordinate of T. From Lemma 1 and Equation (11), we have

$$\langle T, -T\rangle_3 \equiv 2y_T \equiv 2y_T^{-2} \equiv \left(1-\frac{1}{t^2}\right) \pmod{(\mathbb{F}_{p^2}^{\times})^3}.$$

Using this, we can derive the radical isogenies as follows.

Theorem 24 *Let $\mathbf{A} = (A, s) \in \mathcal{D}_p^{\mathrm{M}}$, and $\mathfrak{a}$ be $\mathfrak{l}$ or $\bar{\mathfrak{l}}$. Let t be the x-coordinate of a generator of $E_{\mathbf{A}}[\mathfrak{a}]$. Then, the x-coordinate t' of a generator of $E_{\mathbf{A}'}[\mathfrak{a}]$, where $\mathbf{A}' = (A', s') = [\mathfrak{a}] * \mathbf{A}$, is given by*

$$t' = 3t^3\alpha^2 + (3t^2-1)t\alpha + 3t^3 - 2t, \tag{13}$$

where

$$\alpha = -\frac{1}{2}\left(1-\frac{1}{t^2}\right)^{\frac{p+2}{3}}.$$

Proof We note that the proof is similar to that of Theorem 20.

We use SageMath to aid the computation. Here, we use the file named `supporting_proofs/proof_theorem_Montgomery_radical.sage` in our GitHub repository.

From the isogeny formula between Montgomery curves in [40, Theorem 1], we obtain an isogeny $\varphi : E_A \to E_{A'}$ for some elliptic curve $E_{A'}$ with kernel $\langle T \rangle$. By evaluating a point in $E_A[3] \setminus \ker \varphi$, we can see that the x-coordinate of a generator of the kernel of the dual isogeny $\hat{\varphi}$ is $-1/(3t)$.

Let $\Psi_3(x)$ be the 3-division polynomial of $E_{A'}$. By dividing $\Psi_3(x)$ by $3(x + 1/(3t))$, we obtain the following polynomial:

$$F(x) \coloneqq x^3 + (-9t^3 + 6t)x^2 + 3t^2x - t.$$

From Lemma 22, α is a cube root of $\langle T, -T \rangle_3$, where T is a point on E_A with x-coordinate t. Therefore, the theory of radical isogenies shows that $F(x)$ has a root represented by a rational function in t and α. Indeed, we can verify that $F(t') = 0$ for t' defined in Equation (13) (we found such an expression by using `supporting_proofs/guess_Montgomery_radical.sage` in our GitHub repository).

From Lemma 22, we have $\mathrm{N}_{p^2}(\alpha) = -2$. Another cube root of $\langle T, -T \rangle_3$ has norm -2ω for a primitive cube root of unity ω. By using this, we can verify that t' in Equation (13) derived from α satisfies the same condition as in Lemma 22, and that the x-coordinate defined from the other cube root of $\langle T, -T \rangle_3$ does not satisfy the condition. This means that t' is the x-coordinate of a generator of $E_{\mathbf{A}'}[\mathfrak{a}]$. □

4.3 Computing a chain of 3-isogenies

We summarize the procedure to compute a chain of 3-isogenies on supersingular $(2, \varepsilon)$-structures using the radical isogenies in previous subsections.

Given a starting $(2, \varepsilon_{\mathrm{H}})$-structure $\mathbf{u} = (u, s) \in \mathcal{D}_p^{\mathrm{H}}$, an ideal $\mathfrak{a}$ in $\{\mathfrak{l}, \bar{\mathfrak{l}}\}$, and a positive integer n, the $(2, \varepsilon_{\mathrm{H}})$-structure $[\mathfrak{a}^n] * \mathbf{u}$ can be computed as follows:

1. If $u = \infty$, go to Step 4. Otherwise, generate the x-coordinate t of a point T of order 3 in E_u^{H}. Note that T is not $\mathbb{F}_{p^2}$-rational in general, but its x-coordinate t is in $\mathbb{F}_{p^2}$. Therefore, we do not need to extend the field to generate t.
2. Check t satisfies Equation (6) in Lemma 15. If not, go back to Step 1 and generate another t.
3. Compute $\chi(t)$ defined in Equation (7) and check whether T generates $E_{\mathbf{u}}^{\mathrm{H}}[\mathfrak{a}]$ using Lemma 17. If not, go back to Step 1 and generate another t.
4. Repeat the following n times:
   - If $u = \infty$, compute $\mathbf{u} \leftarrow [\mathfrak{a}] * \mathbf{u}$ and the x-coordinate t of a generator of $E_{\mathbf{u}}^{\mathrm{H}}[\mathfrak{a}]$ by Theorem 18.
   - If $u \neq \infty$ and $t^p + t - 3 = 0$, compute u from t by Equation (6) and set $\mathbf{u} \leftarrow (\infty, s')$, where s' is given in Lemma 19.
   - Otherwise, compute the new x-coordinate t' using the radical isogenies in Theorem 20 and set $t \leftarrow t'$.

   In the last case, we update only t, and $\mathbf{u}$ is not updated.
5. Finally, if $\mathbf{u}$ was updated in the last iteration of Step 4, then $[\mathfrak{a}^n] * \mathbf{u}$ is the current $\mathbf{u}$. Otherwise, compute $\mathbf{u}' = (u', s') = [\mathfrak{a}^n] * \mathbf{u}$ from t using Lemma 15 and Lemma 17.

The first two cases in Step 4 occur only if $p \equiv 7 \pmod{12}$, since E_∞^{H} is supersingular if and only if $p \equiv 3 \pmod{4}$. A similar procedure can be applied to compute $[\mathfrak{a}^n] * \mathbf{A}$ for a starting $(2, \varepsilon_{\mathrm{M}})$-structure $\mathbf{A} = (A, s) \in \mathcal{D}_p^{\mathrm{M}}$, using the theorem and the lemmas in Subsection 4.2.

4.4 Examples

We present examples of the actions of $\mathfrak{l}$ on $\mathcal{D}_{2,\varepsilon}^{\max}(p)$ for $p = 31$ and 79 by using the method described in the previous subsection. In these cases, the class number of $\mathbb{Q}(\sqrt{-2p})$ is 8, and the order of the ideal class $[\mathfrak{l}]$ is also 8. Thus, we can obtain a cycle of length 8 by applying the action of $\mathfrak{l}$ repeatedly, and the cycle contains all the elements in $\mathcal{D}_{2,\varepsilon}^{\max}(p)$.

The results for $(2, \varepsilon_{\mathrm{H}})$-structures represented by Hasegawa parameters are shown in Figure 1, and the results for $(2, \varepsilon_{\mathrm{M}})$-structures represented by Montgomery coefficients are shown in Figure 2. In these figures, we write i for $\sqrt{-1}$ and represent elements of $\mathbb{F}_{p^2} = \mathbb{F}_p[i]$ as $a + bi$ with $a, b \in \mathbb{F}_p$. The figures are computed with $\Delta = -1$, $\sqrt{\Delta} = i$, and $\sqrt{-2} = -8i$ for $p = 31$ and $\sqrt{-2} = -9i$ for $p = 79$; the values of u and the signs s depend on these choices.

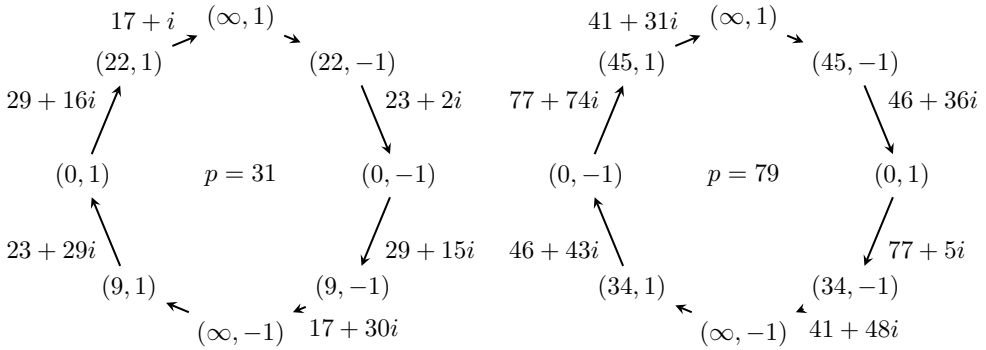

Fig. 1 The actions of $\mathfrak{l}$ on $\mathcal{D}_p^{\mathrm{H}}$ for $p = 31$ and 79. Each node represents $\mathbf{u} = (u, s) \in \mathcal{D}_p^{\mathrm{H}}$, and each arrow corresponds to the action of $\mathfrak{l}$ and is labeled by t, the x-coordinate of a generator of $E_{\mathbf{u}}^{\mathrm{H}}[\mathfrak{l}]$.

The computation for these examples is done by using SageMath, and the code is available at `experiment/examples_for_actions.sage` in our GitHub repository.

5 Application to the generalized Delfs–Galbraith algorithm

Delfs and Galbraith [21] proposed an algorithm to compute an isogeny between two given supersingular elliptic curves over $\mathbb{F}_p$. Later, Chenu and Smith [20] extended the Delfs–Galbraith algorithm to use (d, ε)-structures, which they called the generalized Delfs–Galbraith algorithm. This section gives an application of our results to the generalized Delfs–Galbraith algorithm.

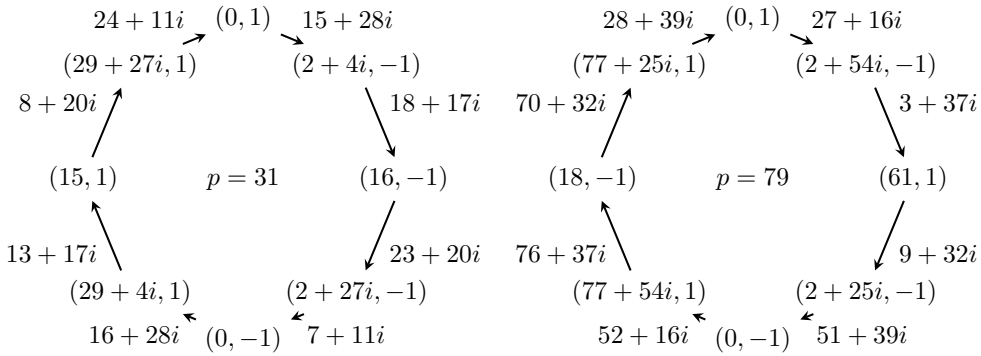

Fig. 2 The actions of $\mathfrak{l}$ on $\mathcal{D}_p^{\mathrm{M}}$ for $p = 31$ and 79. Each node represents $\mathbf{A} = (A, s) \in \mathcal{D}_p^{\mathrm{M}}$, and each arrow corresponds to the action of $\mathfrak{l}$ and is labeled by t, the x-coordinate of a generator of $E_{\mathbf{A}}^{\mathrm{M}}[\mathfrak{l}]$.

5.1 Delfs–Galbraith algorithm

First, we briefly recall the Delfs–Galbraith algorithm and the generalized Delfs–Galbraith algorithm. Given two supersingular elliptic curves E_1 and E_2 over $\mathbb{F}_{p^2}$, the Delfs–Galbraith algorithm computes an isogeny from E_1 to E_2 by the following steps:

1. Compute a chain of ℓ-isogenies from E_1 to a supersingular elliptic curve E_1' defined over $\mathbb{F}_p$ by a random walk on the ℓ-isogeny graph for some small prime ℓ. Let φ_1 be the isogeny composed of the ℓ-isogenies in the chain.
2. Similarly, compute a chain of ℓ-isogenies from E_2 to a supersingular elliptic curve E_2' defined over $\mathbb{F}_p$. Let φ_2 be the isogeny composed of the ℓ-isogenies in the chain.
3. Find an ideal class $[\mathfrak{a}]$ in $\mathrm{cl}(\mathbb{Q}(\sqrt{-p}))$ such that $[\mathfrak{a}] * E_1' = E_2'$. Let $\varphi_{\mathfrak{a}}$ be an isogeny corresponding to the action of $[\mathfrak{a}]$.
4. Output the isogeny $\hat{\varphi}_2 \circ \varphi_{\mathfrak{a}} \circ \varphi_1$ from E_1 to E_2.

Note that we may assume that the $\mathbb{F}_p$-endomorphism rings of E_1' and E_2' are isomorphic to the ring of integers of $\mathbb{Q}(\sqrt{-p})$ since there is a 2-isogeny from any supersingular elliptic curve over $\mathbb{F}_p$ to a supersingular elliptic curve with $\mathbb{F}_p$-endomorphism ring isomorphic to the ring of integers of $\mathbb{Q}(\sqrt{-p})$.

The dominating cost of the above algorithm is Steps 1 and 2, which require $O(\sqrt{p})$ ℓ-isogeny computations. This is because there are approximately $p/12$ supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ while there are approximately $\sqrt{p}$ supersingular elliptic curves defined over $\mathbb{F}_p$. Step 3 can be performed in $\tilde{O}(p^{1/4})$ bit operations using the meet-in-the-middle method on the class group $\mathrm{cl}(\mathbb{Q}(\sqrt{-p}))$ [13, §7.1].

The generalized Delfs–Galbraith algorithm extends this framework by allowing the intermediate curves E_1' and E_2' to carry (d, ε)-structures for small values of d. The two curves may carry different such structures. Suppose that E_1' carries a (d_1, ε_1)-structure, E_2' carries a (d_2, ε_2)-structure, and there exists a supersingular elliptic curve E_0 carrying both a (d_1, ε_1)-structure and a (d_2, ε_2)-structure. Then, by finding an ideal class $[\mathfrak{a}]$ such that $[\mathfrak{a}] * E_1' = E_0$ and an ideal class $[\mathfrak{b}]$ such that $[\mathfrak{b}] * E_2' = E_0$, we can compute an isogeny from E_1' to E_2'. For such a curve E_0, we can use an elliptic curve with CM by an order with small discriminant. For example, if $p \equiv 3 \bmod 4$, then a

supersingular elliptic curve with j-invariant 1728 has (d, ε)-structures for $d = 1, 2$ and primes $d \equiv 1 \bmod 4$.

This extension increases the number of supersingular elliptic curves that can serve as E_1' and E_2'. Since the number of supersingular elliptic curves admitting a (d, ε)-structure is also approximately $\sqrt{p}$, the generalized Delfs–Galbraith algorithm has the same asymptotic complexity as the original Delfs–Galbraith algorithm. However, Chenu and Smith observed that for small d the ratio $\#\mathcal{D}_{d,\varepsilon}(p)/\#\mathcal{D}_{1,\varepsilon}(p)$ can be substantially larger than $\sqrt{d}$, so that Steps 1 and 2 can be faster by a constant factor by allowing more choices for E_1' and E_2' [20, §6.4]. This gain is counterbalanced by the cost of Step 3, which involves walks in the graph of (d, ε)-structures; our radical isogenies reduce this cost for $d = 2$.

We note that there is another direction to improve Steps 1 and 2 by using a fast root detection method on the modular polynomials [41]. This method could be combined with the generalized Delfs–Galbraith algorithm to reduce the cost of Steps 1 and 2.

5.2 Application of our results

Let E_1 and E_2 be supersingular elliptic curves over $\mathbb{F}_{p^2}$ admitting $(2, \varepsilon)$-structures. We explain how our radical isogenies can be used to find an ideal class connecting such structures. This applies to Step 3 of the generalized Delfs–Galbraith algorithm whenever at least one of E_1' and E_2' carries a $(2, \varepsilon)$-structure. Although this step is not the dominant cost of the overall algorithm, improving it is still worthwhile because its cost is exponential in $\log p$.

As in Section 4, we assume that $p \equiv 1 \bmod 3$ and let $\mathfrak{l}$ be the prime ideal generated by 3 and $1 + \sqrt{-2p}$ in $\mathbb{Q}(\sqrt{-2p})$. Let N be the class number of $\mathbb{Q}(\sqrt{-2p})$, let $\mathfrak{t}$ be the prime ideal above 2, let $q > 3$ be the smallest prime that splits in $\mathbb{Q}(\sqrt{-2p})$, and let $\mathfrak{q}$ be a prime ideal above q. We may assume that the structure of the class group $\mathrm{cl}(\mathbb{Q}(\sqrt{-2p}))$ has already been computed, since it can be obtained in subexponential time in $\log p$ using McCurley's algorithm [42, Chap. 5.5].

Let ψ_1 and ψ_2 be 2-isogenies giving $(2, \varepsilon)$-structures (E_1, ψ_1) and (E_2, ψ_2), respectively. Our goal is to find integers a, b, c with $0 \le a, b \le \lceil \sqrt{N} \rceil$ and $c \in \{0, 1\}$ such that either

$$[\mathfrak{l}^a \mathfrak{q}^b \mathfrak{t}^c] * (E_1, \psi_1) = (E_2, \psi_2) \quad \text{or} \quad [\mathfrak{l}^a \mathfrak{q}^{-b} \mathfrak{t}^c] * (E_1, \psi_1) = (E_2, \psi_2).$$

Heuristically, such integers exist as discussed in [13, §7.1]. Although the ideal $\mathfrak{l}^a \mathfrak{q}^b \mathfrak{t}^c$ does not have a compact representation in general, it can be replaced by a compactly represented ideal using the method of CSI-FiSh [43]. The ambiguity in the sign of b is harmless: once (a, b, c) has been found, we can evaluate both candidate classes by replacing with compact representations, and test which codomain is E_2. This can be done in polynomial time in $\log p$.

To explain our approach to find such integers a, b, c, we use the following lemmas.

Lemma 25 *Let (E, ψ) and (E', ψ') be supersingular $(2, \varepsilon)$-structures, and $\mathfrak{a}$ be an ideal in $\mathbb{Q}(\sqrt{-2p})$. Then, $[\mathfrak{a}] * (E, \psi) = (E', \psi')$ if and only if $[\mathfrak{a}^{-1}] * (E, -\psi) = (E', -\psi')$.*

Proof This follows from the fact that an isogeny corresponding to the ideal $\mathfrak{a}$ on (E, ψ) has the same kernel as an isogeny corresponding to the ideal $\bar{\mathfrak{a}}$ on $(E, -\psi)$, where $\bar{\mathfrak{a}}$ is the complex conjugate of $\mathfrak{a}$. □

Lemma 26 *Let (E, ψ) be a supersingular $(2, \varepsilon)$-structure. If E has a $(2, \varepsilon)$-structure other than (E, ψ) and $(E, -\psi)$, then E has CM by $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-7})$ or $\mathbb{Q}(\sqrt{-15})$. In particular, the number of j-invariants of such supersingular elliptic curves is at most 4.*

Proof As we already showed in Section 3, if E has CM by $\mathbb{Q}(\sqrt{-1})$, then E has $(2, \varepsilon)$-structures other than (E, ψ) and $(E, -\psi)$. Since a curve with j-invariant 0 does not have a $(2, \varepsilon)$-structure, we may assume that the automorphism group of E is $\{\pm 1\}$. Let φ be a 2-isogeny from E such that (E, φ) is a $(2, \varepsilon)$-structure different from (E, ψ) and $(E, -\psi)$. Then, the kernel of φ is different from the kernels of ψ, thus, the composition $\hat{\varphi} \circ \psi$ is a non-integer endomorphism of E of degree 4. This means that E has CM by an order having a non-integer element of norm 4. Such an order is one of $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[2\sqrt{-1}]$, $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$, and $\mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$. Since in the second and the third cases, E does not have a $(2, \varepsilon)$-structure, we obtain the first statement of the lemma. The second statement follows from the class numbers of $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-15})$. □

To find the desired integers a, b, c, we use a meet-in-the-middle search based on the following two observations.

1. Suppose that the j-invariants of $[\mathfrak{l}^a] * (E_1, \psi_1)$ and $[\mathfrak{q}^b] * (E_2, \psi_2)$ are equal. By Lemma 26, we may assume that there exists a $(2, \varepsilon)$-structure (E_m, ψ_m) such that

$$[\mathfrak{l}^a] * (E_1, \psi_1) = (E_m, \psi_m) \text{ and } [\mathfrak{q}^b] * (E_2, \psi_2) = (E_m, \psi_m) \text{ or } (E_m, -\psi_m).$$

   This means

$$[\mathfrak{l}^a \mathfrak{q}^{-b}] * (E_1, \psi_1) = (E_2, \psi_2), \text{ or } [\mathfrak{l}^a \mathfrak{q}^b] * (E_1, \psi_1) = (E_2, -\psi_2)$$

   by Lemma 25.
2. Suppose instead that the j-invariant of $[\mathfrak{l}^a] * (E_1, \psi_1)$ is the Frobenius conjugate of the j-invariant of $[\mathfrak{q}^b] * (E_2, \psi_2)$. Then the same argument shows that either

$$[\mathfrak{l}^a \mathfrak{q}^{-b} \mathfrak{t}] * (E_1, \psi_1) = (E_2, \psi_2) \text{ or } [\mathfrak{l}^a \mathfrak{q}^b \mathfrak{t}] * (E_1, \psi_1) = (E_2, -\psi_2).$$

For the computation of $[\mathfrak{l}^a] * (E_1, \psi_1)$, we use our radical 3-isogenies in Theorem 20 or Theorem 24. For the computation of $[\mathfrak{q}^b] * (E_2, \psi_2)$, we use the approach using modular polynomials in [20, §4.4]. We briefly recall the approach using modular polynomials. For a prime ℓ, we denote by $\Phi_\ell(X, Y)$ the modular polynomial of level ℓ. Let (E, ψ) and (E', ψ') be supersingular $(2, \varepsilon)$-structures such that there is a q-isogeny between these two structures. Then, we have $\Phi_q(j(E), j(E')) = 0$ and $\Phi_2(j(E'), j(E')^p) = 0$. Therefore, $j(E')$ is a root of $g(X) := \gcd(\Phi_q(X, j(E)), \Phi_2(X, X^p))$. Since there are two q-isogenies from the $(2, \varepsilon)$-structure (E, ψ) up to isomorphism, the degree of $g(X)$

Algorithm 1: Meet-in-the-middle using Hasegawa parameters

Input: Two supersingular elliptic curves E_1 and E_2 over $\mathbb{F}_{p^2}$ admitting $(2,\varepsilon)$-structures, and a 2-isogeny ψ_1 defining a $(2,\varepsilon)$-structure (E_1,ψ_1)

Output: A tuple (a,b,c) of integers such that $[\mathfrak{l}^a\mathfrak{q}^b\mathfrak{t}^c]*(E_1,\psi_1)$ or $[\mathfrak{l}^a\mathfrak{q}^{-b}\mathfrak{t}^c]*(E_1,\psi_1)$ is a $(2,\varepsilon)$-structure on E_2, or `Failure` if there is no such tuple.

$\mathbf{u}=(u,s) \leftarrow$ the Hasegawa representation of (E_1,ψ_1);
$\mathcal{H} \leftarrow \{j(E_u^{\mathrm{H}}) : 0\}$; `// hash table with key j-invariant`
if $u \neq \infty$ **then** $t \leftarrow$ the x-coordinate of a generator of $E_{\mathbf{u}}^{\mathrm{H}}[\mathfrak{l}]$;
for $a \leftarrow 1$ **to** $\lceil\sqrt{N}\rceil$ **do**
  `// radical 3-isogeny`
  if $u=\infty$ **then**
    $\mathbf{u} \leftarrow [\mathfrak{l}]*\mathbf{u}$ and $t \leftarrow$ the x-coordinate of a generator of $E_{\mathbf{u}}^{\mathrm{H}}[\mathfrak{l}]$ given in Theorem 18;
  else if $t^p+t-3=0$ **then**
    $\mathbf{u} \leftarrow (\infty,s')$ with s' given in Lemma 19 ; `//` $[\mathfrak{l}]*\mathbf{u}=(\infty,s')$
  else
    $t \leftarrow t'$ in Theorem 20 for t;
    $\mathbf{u} \leftarrow (u,s)$ with u in Equation (6) and $s=\chi(t)$ in Lemma 17 for t;
  $\mathcal{H} \leftarrow \mathcal{H} \cup \{j(E_u^{\mathrm{H}}) : a\}$;
$j_0 \leftarrow j(E_2)$;
if $j_0 \in \mathcal{H}$ **then**
  $a \leftarrow \mathcal{H}(j_0)$;
  return $(a,0,0)$;
if $j_0^p \in \mathcal{H}$ **then**
  $a \leftarrow \mathcal{H}(j_0^p)$;
  return $(a,0,1)$;
$j_1 \leftarrow$ a root of $\gcd(\Phi_q(X,j_0),\Phi_2(X,X^p))$;
for $b \leftarrow 1$ **to** $\lceil\sqrt{N}\rceil$ **do**
  if $j_1 \in \mathcal{H}$ **then**
    $a \leftarrow \mathcal{H}(j_1)$;
    return $(a,b,0)$;
  if $j_1^p \in \mathcal{H}$ **then**
    $a \leftarrow \mathcal{H}(j_1^p)$;
    return $(a,b,1)$;
  $j_0, j_1 \leftarrow j_1$, the root of $\gcd(\Phi_q(X,j_1),\Phi_2(X,X^p))/(X-j_0)$;
return `Failure` ; `// there is no` (a,b,c) `satisfying the condition`

is at least 2. Moreover, the degree of $g(X)$ is 2 in most cases since the probability that a random supersingular elliptic curve has $(2,\varepsilon)$-structures is approximately $1/\sqrt{p}$.

The above discussion leads to the algorithm described in Algorithm 1. We describe the case for Hasegawa parameters, but the case for Montgomery coefficients can be described similarly. The first two branches in the for loop handle the special vertex $u = \infty$, at which the Hasegawa curve E^{H}_{∞} has j-invariant 1728: by Lemma 19, the denominator of the radical isogeny formula in Theorem 20 vanishes exactly when the next structure is (∞, s'), and the step from (∞, s') is given by Theorem 18. In the Montgomery case, no such special treatment is needed since Theorem 24 covers the coefficient $A = 0$. Our proof-of-concept implementation of Algorithm 1 is available at `experiment/exec_mitm.sage` in our GitHub repository, which includes both the Hasegawa parameter case and the Montgomery coefficient case.

Remark 1 If the polynomial $g(X)$ defined above has degree greater than 2, then the problem may in fact become easier. Let ψ be a q-isogeny from E such that the codomain has a $(2, \varepsilon)$-structure, and ψ is not an isogeny corresponding to the action of $\mathfrak{q}$. Then, the orientation of the codomain of ψ induces an orientation on E different from that given by the $(2, \varepsilon)$-structure. This means that we obtain a rank-4 subgroup of $\mathrm{End}(E)$, which could help recover the full endomorphism ring of E. Then, we can compute an isogeny from E to a curve E_0 with CM by an order with small discriminant by using the computational Deuring correspondence (see, e.g., [44, §4.3]).

Remark 2 We can compute the action of $\mathfrak{l}$ by using the approach using modular polynomials as well. However, our radical 3-isogenies are more efficient than the approach using modular polynomials. The reason is as follows. The approach using modular polynomials requires computing the p-th power of the variable X in $\mathbb{F}_{p^2}[X]/(\Phi_3(X, j(E)))$ while our radical 3-isogenies require computing an exponentiation with an exponent of size approximately p in $\mathbb{F}_{p^2}$. The computation in $\mathbb{F}_{p^2}$ is more efficient than the computation in $\mathbb{F}_{p^2}[X]/(\Phi_3(X, j(E)))$, thus our radical 3-isogenies are more efficient than the approach using modular polynomials.

Remark 3 It is known that the modular polynomials for the Montgomery coefficients exist if the level is odd [45, §5.1]. By using the modular polynomial for the Montgomery coefficients, we can use Montgomery coefficients instead of j-invariants in Algorithm 1 for the Montgomery coefficient case.

Let $\Phi_q^{\mathsf{Mont}}(X, Y)$ be the modular polynomial for the Montgomery coefficients of level q. Then we can replace $\gcd(\Phi_q(X, j(E)), \Phi_2(X, X^p))$ in Algorithm 1 with $\gcd(\Phi_q^{\mathsf{Mont}}(X, A(E)), X^{2p+2} - 4(X^{2p} + X^2))$, where $A(E)$ is the Montgomery coefficient of E. The second polynomial $X^{2p+2} - 4(X^{2p} + X^2)$ is derived from Proposition 12, which states that a root of this polynomial corresponds to a supersingular $(2, \varepsilon)$-structure. In this case, the key of the hash table $\mathcal{H}$ is the square of the Montgomery coefficient instead of the j-invariant since $(A, s) \cong (-A, s)$ for any $(A, s) \in \mathcal{D}_p^{\mathrm{M}}$ by Theorem 14. Our proof-of-concept implementation for the Montgomery coefficient case uses this approach.

6 Conclusion and future work

In this work, we provided explicit representations of supersingular $(2, \varepsilon)$-structures through Hasegawa parameters and Montgomery coefficients, and we derived radical 3-isogenies that correspond to the action of the classes of the prime ideals above 3

in $\mathbb{Q}(\sqrt{-2p})$. We also presented an algorithm to compute a chain of 3-isogenies on supersingular $(2,\varepsilon)$-structures. Finally, we showed an application of our results to the generalized Delfs–Galbraith algorithm.

We see two natural directions for future work. First, it would be valuable to generalize our approach to ℓ-radical isogenies on supersingular (d,ε)-structures for other pairs of d and ℓ. In particular, if we can derive ℓ-radical isogenies for $(2,\varepsilon)$-structures for some $\ell \neq 3$, then the efficiency of our meet-in-the-middle algorithm in the generalized Delfs–Galbraith algorithm could be further improved since we can use ℓ-isogenies instead of the method using modular polynomials. Second, a conceptual explanation of the norm-based cube-root selection criterion established in Theorems 20 and 24 would be valuable. Clarifying why this condition singles out the correct root would potentially point to further algebraic structure behind radical isogenies on (d,ε)-structures.

Acknowledgements. This work is based on a part of the master's thesis of the first author supervised by the third author at the University of Tokyo.

Declarations

- **Funding.** This work was supported by the Japan Science and Technology Agency (JST) K Program, Grant Number JPMJKP24U2, and by the Japan Society for the Promotion of Science (JSPS) KAKENHI, Grant Number 24K20770.
- **Competing interests.** The authors have no relevant financial or non-financial interests to disclose.
- **Ethics approval and consent.** Not applicable.
- **Data availability.** No datasets were generated or analysed during the current study.
- **Code availability.** The SageMath code supporting the proofs and the experiments in this paper is available at https://github.com/hiroshi-onuki/2epsilon_structure_sagemath. The coefficients of the modular polynomials for Montgomery coefficients used in Section 5 are taken from the repository accompanying [45].
- **Author contributions.** All authors contributed to the research and to the writing of the manuscript, and read and approved the final manuscript.
- **Use of AI tools.** We used Claude Fable 5.1 and Opus 5.5, a large language model developed by Anthropic, during the revision of this paper to check the consistency of notation and sign conventions, to recompute the examples in Section 4.4 independently of our implementation, and to draft the wording of parts of the text. The authors verified all mathematical content and take full responsibility for the final version.

References

[1] Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic hash functions from expander graphs. Journal of Cryptology **22**(1), 93–113 (2009) https://doi.org/10.1007/s00145-007-9002-x

[2] Castryck, W., Decru, T., Smith, B.: Hash functions from superspecial genus-2 curves using Richelot isogenies. Journal of Mathematical Cryptology **14**(1), 268–292 (2020) https://doi.org/10.1515/jmc-2019-0021

[3] De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: SQISign: Compact post-quantum signatures from quaternions and isogenies. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020, Part I. Lecture Notes in Computer Science, vol. 12491, pp. 64–93. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64837-4_3

[4] Aardal, M.A., Adj, G., Aranha, D.F., Basso, A., Borin, G., Canales Martínez, I.A., Chávez-Saab, J., Corte-Real Santos, M., Dartois, P., De Feo, L., Duparc, M., Espitau, T., Eriksen, J.K., Fouotsa, T.B., Gazzoni Filho, D.L., Hess, B., Invernizzi, R., Kohel, D., Leroux, A., Longa, P., Maino, L., Meyer, M., Mula, M., Nakagawa, K., Onuki, H., Panny, L., Patranabis, S., Petit, C., Pope, G., Reijnders, K., Robert, D., Rodríguez-Henríquez, F., Schaeffler, S., Vercauteren, F., Wallet, A., Wesolowski, B., van Woerden, W.: SQIsign. Technical report, National Institute of Standards and Technology (2026). https://sqisign.org

[5] Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 423–447. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-30589-4_15

[6] Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 448–471. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-30589-4_16

[7] Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023, Part V. Lecture Notes in Computer Science, vol. 14008, pp. 472–503. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-30589-4_17

[8] Basso, A., Maino, L., Pope, G.: FESTA: Fast encryption from supersingular torsion attacks. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology – ASIACRYPT 2023, Part VII. Lecture Notes in Computer Science, vol. 14444, pp. 98–126. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-8739-9_4

[9] Nakagawa, K., Onuki, H.: QFESTA: Efficient algorithms and parameters for FESTA using quaternion algebras. In: Reyzin, L., Stebila, D. (eds.) Advances in Cryptology – CRYPTO 2024, Part V. Lecture Notes in Computer Science, vol. 14924, pp. 75–106. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-68388-6_4

[10] Basso, A., Maino, L.: POKÉ: A compact and efficient PKE from higher-dimensional isogenies. In: Fehr, S., Fouque, P.-A. (eds.) Advances in Cryptology – EUROCRYPT 2025, Part II. Lecture Notes in Computer Science, vol. 15602, pp. 94–123. Springer, Cham (2025). https://doi.org/10.1007/978-3-031-91124-8_4

[11] Couveignes, J.-M.: Hard Homogeneous Spaces. Cryptology ePrint Archive, Report 2006/291 (2006). https://eprint.iacr.org/2006/291

[12] Rostovtsev, A., Stolbunov, A.: Public-Key Cryptosystem Based On Isogenies. Cryptology ePrint Archive, Report 2006/145 (2006). https://eprint.iacr.org/2006/145

[13] Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology – ASIACRYPT 2018, Part III. Lecture Notes in Computer Science, vol. 11274, pp. 395–427. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03332-3_15

[14] Castryck, W., Decru, T.: CSIDH on the surface. In: Ding, J., Tillich, J.-P. (eds.) Post-Quantum Cryptography – 11th International Conference, PQCrypto 2020, pp. 111–129. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-44223-1_7

[15] Colò, L., Kohel, D.: Orienting supersingular isogeny graphs. Journal of Mathematical Cryptology **14**(1), 414–437 (2020) https://doi.org/10.1515/jmc-2019-0034

[16] De Feo, L., Fouotsa, T.B., Kutas, P., Leroux, A., Merz, S.-P., Panny, L., Wesolowski, B.: SCALLOP: Scaling the CSI-FiSh. In: Boldyreva, A., Kolesnikov, V. (eds.) PKC 2023: 26th International Conference on Theory and Practice of Public Key Cryptography, Part I. Lecture Notes in Computer Science, vol. 13940, pp. 345–375. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-31368-4_13

[17] De Feo, L., Galbraith, S.D.: SeaSign: Compact isogeny signatures from class group actions. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2019, Part III. Lecture Notes in Computer Science, vol. 11478, pp. 759–789. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-17659-4_26

[18] De Feo, L., Meyer, M.: Threshold schemes from isogeny assumptions. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020: 23rd International Conference on Theory and Practice of Public Key Cryptography, Part II. Lecture Notes in Computer Science, vol. 12111, pp. 187–212. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-45388-6_7

[19] Abdalla, M., Eisenhofer, T., Kiltz, E., Kunzweiler, S., Riepel, D.: Password-authenticated key exchange from group actions. In: Dodis, Y., Shrimpton, T.

(eds.) Advances in Cryptology – CRYPTO 2022, Part II. Lecture Notes in Computer Science, vol. 13508, pp. 699–728. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-15979-4_24

[20] Chenu, M., Smith, B.: Higher-degree supersingular group actions. Mathematical Cryptology **1**(2), 85–101 (2022)

[21] Delfs, C., Galbraith, S.D.: Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. Designs, Codes and Cryptography **78**(2), 425–440 (2016) https://doi.org/10.1007/s10623-014-0010-1

[22] Wesolowski, B.: The supersingular isogeny problem in time and memory $p^{1/3+o(1)}$. Cryptology ePrint Archive, Report 2026/1486 (2026). https://eprint.iacr.org/2026/1486

[23] Mamah, M.: Complexity Analysis and Security Implications of the New Isogeny-Path Algorithm. Cryptology ePrint Archive, Report 2026/1821 (2026). https://eprint.iacr.org/2026/1821

[24] Castryck, W., Decru, T., Vercauteren, F.: Radical isogenies. In: Moriai, S., Wang, H. (eds.) Advances in Cryptology – ASIACRYPT 2020, Part II. Lecture Notes in Computer Science, vol. 12492, pp. 493–519. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-64834-3_17

[25] Hasegawa, Y.: Q-curves over quadratic fields. Manuscripta Mathematica **94**, 347–364 (1997) https://doi.org/10.1007/bf02677859

[26] Kunzweiler, S., Maino, L., Moriya, T., Petit, C., Pope, G., Robert, D., Stopar, M., Ti, Y.B.: Radical 2-isogenies and cryptographic hash functions in dimensions 1, 2 and 3. In: Jager, T., Pan, J. (eds.) PKC 2025: 28th International Conference on Theory and Practice of Public Key Cryptography, Part III. Lecture Notes in Computer Science, vol. 15676, pp. 265–299. Springer, Cham (2025). https://doi.org/10.1007/978-3-031-91826-1_9

[27] The Sage Developers: SageMath, the Sage Mathematics Software System (Version 10.7). (2025). `https://www.sagemath.org`

[28] Silverman, J.H.: The Arithmetic of Elliptic Curves, 2nd edn. Graduate Texts in Mathematics, vol. 106. Springer, New York (2009). https://doi.org/10.1007/978-0-387-09494-6

[29] Washington, L.C.: Elliptic Curves: Number Theory and Cryptography, 2nd edn. Chapman & Hall/CRC, Boca Raton, FL (2008). https://doi.org/10.1201/9781420071474

[30] Corte-Real Santos, M., Eriksen, J.K., Meyer, M., Reijnders, K.: AprèsSQI: Extra fast verification for SQIsign using extension-field signing. In: Joye, M., Leander,

G. (eds.) Advances in Cryptology – EUROCRYPT 2024, Part I. Lecture Notes in Computer Science, vol. 14651, pp. 63–93. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-58716-0_3

[31] Auer, R., Top, J.: Legendre elliptic curves over finite fields. Journal of Number Theory **95**(2), 303–312 (2002) https://doi.org/10.1006/jnth.2001.2760

[32] Onuki, H.: On oriented supersingular elliptic curves. Finite Fields and Their Applications **69**, 101777 (2021) https://doi.org/10.1016/j.ffa.2020.101777

[33] Streng, M.: Generators of the group of modular units for $\Gamma^1(N)$ over the rationals. arXiv:1503.08127v2. https://arxiv.org/abs/1503.08127v2 (2019)

[34] Onuki, H., Moriya, T.: Radical isogenies on Montgomery curves. In: Hanaoka, G., Shikata, J., Watanabe, Y. (eds.) PKC 2022: 25th International Conference on Theory and Practice of Public Key Cryptography, Part I. Lecture Notes in Computer Science, vol. 13177, pp. 473–497. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-97121-2_17

[35] Bernstein, D.J., De Feo, L., Leroux, A., Smith, B.: Faster computation of isogenies of large prime degree. In: Galbraith, S.D. (ed.) Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS XIV). The Open Book Series, vol. 4, pp. 39–55. Mathematical Sciences Publishers, Berkeley, CA (2020). https://doi.org/10.2140/obs.2020.4.39

[36] Castryck, W., Decru, T., Houben, M., Vercauteren, F.: Horizontal racewalking using radical isogenies. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology – ASIACRYPT 2022, Part II. Lecture Notes in Computer Science, vol. 13792, pp. 67–96. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-22966-4_3

[37] Decru, T.: Radical $\sqrt[N]{\text{élu}}$ isogeny formulae. In: Reyzin, L., Stebila, D. (eds.) Advances in Cryptology – CRYPTO 2024, Part V. Lecture Notes in Computer Science, vol. 14924, pp. 107–128. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-68388-6_5

[38] Smith, B.: The $\mathbb{Q}$-curve construction for endomorphism-accelerated elliptic curves. Journal of Cryptology **29**(4), 806–832 (2016) https://doi.org/10.1007/s00145-015-9210-8

[39] Husemöller, D.: Elliptic Curves, 2nd edn. Graduate Texts in Mathematics, vol. 111. Springer, New York (2004). https://doi.org/10.1007/b97292

[40] Costello, C., Hisil, H.: A simple and compact algorithm for SIDH with arbitrary degree isogenies. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017, Part II. Lecture Notes in Computer Science, vol. 10625, pp. 303–329. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70697-9_11

[41] Corte-Real Santos, M., Costello, C., Shi, J.: Accelerating the Delfs-Galbraith algorithm with fast subfield root detection. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology – CRYPTO 2022, Part III. Lecture Notes in Computer Science, vol. 13509, pp. 285–314. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-15982-4_10

[42] Cohen, H.: A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics, vol. 138. Springer, Berlin, Heidelberg (1993). https://doi.org/10.1007/978-3-662-02945-9

[43] Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: Efficient isogeny based signatures through class group computations. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019, Part I. Lecture Notes in Computer Science, vol. 11921, pp. 227–247. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34578-5_9

[44] Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017, Part I. Lecture Notes in Computer Science, vol. 10624, pp. 3–33. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70694-8_1

[45] Onuki, H., Uchida, Y., Yoshizumi, R.: Geometric construction of modular polynomials with level structures (2026). https://arxiv.org/abs/2601.17338

Appendix A 3-radical isogenies for $(2, \varepsilon_{\mathrm{H}})$-structures on E_{∞}^{H}

The purpose of this section is to prove Theorem 18 and Lemma 19.

Throughout this section, we assume that $p \equiv 7 \bmod 12$ so that E_{∞} is supersingular and 3 splits in $\mathbb{Q}(\sqrt{-2p})$. Then, 3 is not a square in $\mathbb{F}_p$, and we can choose its square root $\sqrt{3}$ in $\mathbb{F}_{p^2}$ such that $\sqrt{3}/\sqrt{\Delta}$ is in $(\mathbb{F}_p^{\times})^2$. This implies that $\sqrt{3}/\sqrt{\Delta}$ is in $(\mathbb{F}_{p^2}^{\times})^4$.

To simplify the calculation, we first assume that $\sqrt{\Delta} = \sqrt{3}$. We denote a Hasegawa curve of parameter u with respect to $\sqrt{\Delta} = \sqrt{3}$ by $E_{u,3}$.

Lemma 27 *Let $s \in \{\pm 1\}$ and $t \in \mathbb{F}_{p^2}$. Then t is the x-coordinate of a generator of $E_{\infty,3}[\iota_{(\infty,s)}(\mathfrak{l})]$ or $E_{\infty,3}[\iota_{(\infty,s)}(\overline{\mathfrak{l}})]$ if and only if $t^2 = 2s \cdot \varepsilon_{\mathrm{H}} - \sqrt{3}$.*

Proof Let T be a point of order 3 in $E_{\infty,3}$ and t be the x-coordinate of T. The 3-division polynomial of $E_{\infty,3}$ is given by $3x^4 + 6\sqrt{3}x^2 - 3$. The roots of this polynomial are

$$\pm\frac{1+\sqrt{3}}{\sqrt{-2}}, \quad \pm\frac{\sqrt{-1}(1-\sqrt{3})}{\sqrt{-2}}.$$

In particular, we have $t^{p+1} = -\varepsilon_{\mathrm{H}}$.

From the definition of $\iota_{(\infty,s)}$ and ψ_∞ in Equation (2), it holds that $T \in E_{\infty,3}[\iota_{(\infty,s)}(\mathfrak{l})]$ or $E_{\infty,3}[\iota_{(\infty,s)}(\bar{\mathfrak{l}})]$ if and only if

$$2t^{p+1} + s(t^{2p} - \sqrt{3}) = 0.$$

This is equivalent to $t^2 = 2s \cdot \varepsilon_{\mathrm{H}} - \sqrt{3}$. □

Since $\left(\frac{1+\sqrt{3}}{\sqrt{-2}}\right)^{p+1} = -\varepsilon_{\mathrm{H}}$, we have $\left(\frac{1+\sqrt{3}}{\sqrt{-2}}\right)^{(p+1)/2}$ is ± 1 if $p \equiv 3 \pmod 8$ and $\pm\sqrt{-1}$ if $p \equiv 7 \pmod 8$. We denote the sign by s_p, i.e.,

$$\left(\frac{1+\sqrt{3}}{\sqrt{-2}}\right)^{\frac{p+1}{2}} = \begin{cases} s_p & \text{if } p \equiv 3 \pmod 8, \\ s_p \cdot \sqrt{-1} & \text{if } p \equiv 7 \pmod 8. \end{cases} \tag{A1}$$

To compute the action of the classes of $\mathfrak{l}$ and $\bar{\mathfrak{l}}$, we need to determine the sign of t, whose square is given by Lemma 27. The following lemma gives the sign of t.

Lemma 28 *Let T be a point on $E_{\infty,3}$ with x-coordinate t. Then, the following holds:*

- *If $p \equiv 3 \pmod 8$,*
  - *$T \in E_{\infty,3}[\iota_{(\infty,1)}(\mathfrak{l})]$ if and only if $t = s_p \dfrac{1+\sqrt{3}}{\sqrt{-2}}$,*
  - *$T \in E_{\infty,3}[\iota_{(\infty,-1)}(\mathfrak{l})]$ if and only if $t = -s_p \cdot \sqrt{-1}\dfrac{1-\sqrt{3}}{\sqrt{-2}}$,*
- *If $p \equiv 7 \pmod 8$,*
  - *$T \in E_{\infty,3}[\iota_{(\infty,1)}(\mathfrak{l})]$ if and only if $t = s_p \cdot \sqrt{-1}\dfrac{1-\sqrt{3}}{\sqrt{-2}}$,*
  - *$T \in E_{\infty,3}[\iota_{(\infty,-1)}(\mathfrak{l})]$ if and only if $t = s_p \dfrac{1+\sqrt{3}}{\sqrt{-2}}$.*

Proof Let y_T be the y-coordinate of T. By the definition of $\iota_{(\infty,s)}$ and ψ_∞ in Equation (2), we have $T \in E_{\infty,3}[\iota_{(\infty,1)}(\mathfrak{l})]$ if and only if

$$-\frac{y_T^p(-\sqrt{3} - t^{2p})}{2\sqrt{-2}^p t^{2p}} = -y_T. \tag{A2}$$

From Lemma 27, we have $t^{2p} = 2\varepsilon_{\mathrm{H}} + \sqrt{3}$. From this and $\sqrt{-2}^p = -\varepsilon_{\mathrm{H}}\sqrt{-2}$ imply that (A2) is equivalent to

$$y_T^{p-1}(\varepsilon_{\mathrm{H}} + \sqrt{3}) = \sqrt{-2}(2 + \varepsilon_{\mathrm{H}}\sqrt{3}).$$

By multiplying both sides by $(2 - \varepsilon_{\mathrm{H}}\sqrt{3})/\sqrt{-2}$, we obtain

$$y_T^{p-1}\frac{-\varepsilon_{\mathrm{H}} + \sqrt{3}}{\sqrt{-2}} = 1.$$

A similar calculation shows that $T \in E_{\infty,3}[\iota_{(\infty,-1)}(\mathfrak{l})]$ if and only if

$$iy_T^{p-1}\frac{\varepsilon_{\mathrm{H}} + \sqrt{3}}{\sqrt{-2}} = 1.$$

Since $y_T^2 = t(t^2+\sqrt{3})$, we have $y_T^2 = 2s\cdot\varepsilon_{\mathrm{H}}\cdot t$ if T is a generator of $E_{\infty,3}[\iota_{(\infty,s)}(\mathfrak{l})]$.

Consider the case $p \equiv 3 \pmod 8$ and $s=1$. Then, we have $t = \varepsilon\frac{1+\sqrt{3}}{\sqrt{-2}}$ for some $\varepsilon \in \{\pm 1\}$. Therefore, T is a generator of $E_{\infty,3}[\iota_{(\infty,1)}(\mathfrak{l})]$ if and only if

$$\varepsilon(-2)^{\frac{p-1}{2}}\left(\frac{1+\sqrt{3}}{\sqrt{-2}}\right)^{\frac{p+1}{2}} = 1.$$

This is equivalent to $\varepsilon = s_p$.

The other cases can be shown in the same way. □

The above lemmas determine the isogenies from $E_{\infty,3}$ corresponding to the action of the classes of $\mathfrak{l}$ and $\bar{\mathfrak{l}}$. The codomains of these isogenies are given by the following lemma.

Lemma 29 *Let $\varepsilon \in \{\pm 1\}$ and t be a square root of $2\varepsilon - \sqrt{3}$. Let $u = (7/12)\varepsilon$ and T be a point on $E_{\infty,3}$ with x-coordinate t. Then, there exists a 3-isogeny $\varphi : E_{\infty,3} \to E_{u,3}$ over $\mathbb{F}_{p^2}$ with kernel generated by T such that $\varphi((0,0)) = (4,0)$. In addition, the x-coordinate of a generator of $\ker\hat{\varphi}$ is $(3-3\sqrt{3}\varepsilon)/2$.*

Proof We verified this lemma by SageMath [27]. Here, we used the file named `supporting_proofs/proof_lemma_3isogeny_from_j1728.sage` in our GitHub repository. Here, we give a sketch of the proof for the case where $\varepsilon = 1$ and $t = \sqrt{-1}\frac{1-\sqrt{3}}{\sqrt{-2}}$. The other cases can be shown in the same way.

From Vélu's formula (of the form in [29, Theorem 12.16]), we obtain an isogeny $\psi : E_{\infty,3} \to E$ of degree 3 whose kernel is generated by T, where E is defined by

$$y^2 = x^3 - (60-21\sqrt{3})x - 4\sqrt{-1}\sqrt{-2}(28-21\sqrt{3}).$$

Then, we have $\psi((0,0)) = (-4\sqrt{-1}\sqrt{-2}, 0)$. Let v be a square root of $-\sqrt{-1}\sqrt{-2}$. Note that $v \in \mathbb{F}_{p^2}$ since $p \equiv 3 \pmod 4$. Then we can take φ as $\tau_{v^{-1}} \circ \psi$, which sends $(0,0)$ to $(4,0)$. The last statement can be shown by computing the image of a point with x-coordinate $-t$ under φ. □

For determining the signs of the $(2,\varepsilon_{\mathrm{H}})$-structure on $E_{u,3}$ for $u = \frac{7}{2}\varepsilon$, we use Lemma 17. To do this, we need to compute $\chi(t)$ defined in Equation (7). The following lemma gives the value of $\chi(t)$.

Lemma 30 *Let $\varepsilon \in \{\pm 1\}$ and $t = (3-3\sqrt{3}\varepsilon)/2$. Then, we have*

$$\chi(t) = \begin{cases} s_p & \text{if } p \equiv 3 \pmod 8, \\ \varepsilon\cdot s_p & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Proof Since $t^p + t - 2 = 1$, we have $\chi(t) = \sqrt{-2}^p(t-4)^{(p+1)/2}$. An easy calculation shows that $(1+\sqrt{3}\varepsilon)^3 = 2(5+3\sqrt{3}\varepsilon)$. Therefore, we have

$$\chi(t) = \sqrt{-2}^p\left(\frac{-5-3\sqrt{3}\varepsilon}{2}\right)^{\frac{p+1}{2}} = \sqrt{-2}^p\left(\frac{-(1+\sqrt{3}\varepsilon)^3}{2}\right)^{\frac{p+1}{4}}$$

Table A1 The actions of $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ on $E_{\infty,3}$. Here, t is the x-coordinate of a generator of the kernel of the isogeny, and s_p is defined in (A1).

p mod 8	domain	action of $\mathfrak{l}$		action of $\bar{\mathfrak{l}}$	
		t	codomain	t	codomain
3	$(\infty, 1)$	$s_p \frac{1+\sqrt{3}}{\sqrt{-2}}$	$\left(-\frac{7}{12}, -s_p\right)$	$-s_p \frac{1+\sqrt{3}}{\sqrt{-2}}$	$\left(-\frac{7}{12}, s_p\right)$
3	$(\infty, -1)$	$-s_p \cdot \sqrt{-1}\frac{1-\sqrt{3}}{\sqrt{-2}}$	$\left(\frac{7}{12}, -s_p\right)$	$s_p \cdot \sqrt{-1}\frac{1-\sqrt{3}}{\sqrt{-2}}$	$\left(\frac{7}{12}, s_p\right)$
7	$(\infty, 1)$	$s_p \cdot \sqrt{-1}\frac{1-\sqrt{3}}{\sqrt{-2}}$	$\left(\frac{7}{12}, -s_p\right)$	$-s_p \cdot \sqrt{-1}\frac{1-\sqrt{3}}{\sqrt{-2}}$	$\left(\frac{7}{12}, s_p\right)$
7	$(\infty, -1)$	$s_p \frac{1+\sqrt{3}}{\sqrt{-2}}$	$\left(-\frac{7}{12}, s_p\right)$	$s_p \frac{1+\sqrt{3}}{\sqrt{-2}}$	$\left(-\frac{7}{12}, -s_p\right)$

$$= \sqrt{-2}^{\frac{p-1}{2}} \left(\frac{1+\sqrt{3}\varepsilon}{\sqrt{-2}}\right)^{3\frac{p+1}{2}}.$$

If $p \equiv 3 \pmod 8$, this is equal to s_p since $\sqrt{-2}$ is a square in $\mathbb{F}_p$. If $p \equiv 7 \pmod 8$, then $\sqrt{-2} = 2^{(p+1)/4}/\sqrt{-1}$ and

$$\left(\frac{1+\sqrt{3}\varepsilon}{\sqrt{-2}}\right)^{3\frac{p+1}{2}} = \varepsilon \cdot s_p \cdot \sqrt{-1}^3.$$

The lemma directly follows from these. □

Using the above lemmas, we can determine the actions of $\mathfrak{l}$ and $\bar{\mathfrak{l}}$ on $(E_{\infty,3}, \pm 1)$. The results are summarized in Table A1.

To derive 3-radical isogenies on $E_{\infty,3}$, we need to compute the Tate pairing $\langle T, -T\rangle_3$ for a point T on $E_{\infty,3}$ generating the kernel of the isogeny. Let t be the x-coordinate of T and y_T be the y-coordinate of T. From Lemma 1, we have

$$\langle T, -T\rangle_3 \equiv 2y_T \equiv 2y_T^{-2} \equiv 2(t^3 + \sqrt{3}t)^{-1} \equiv 2t^2(t^2+\sqrt{3})^{-1} \bmod (\mathbb{F}_{p^4}^\times)^3.$$

From Lemma 27, we have $t^2 = 2\varepsilon - \sqrt{3}$ for some $\varepsilon \in \{\pm 1\}$. Therefore, we have $\langle T, -T\rangle_3 \equiv 2\varepsilon - \sqrt{3} \bmod (\mathbb{F}_{p^4}^\times)^3$. Note that Lemma 29 shows that the Hasegawa parameter of the codomain of the isogeny is given by $u = (7/12)\varepsilon$. These observations give 3-radical isogenies on $E_{\infty,3}$ as follows.

Theorem 31 *Let $\varepsilon \in \{\pm 1\}$ and $u = \frac{7}{12}\varepsilon \in \mathbb{F}_{p^2}$. We define*

$$\alpha = \left(2\varepsilon - \sqrt{3}\right)^{\frac{p+2}{3}} \text{ and } t = (3+3\sqrt{3}\varepsilon)\alpha^2 + 2\sqrt{3}\alpha - \frac{1-\sqrt{3}\varepsilon}{2}.$$

Then, a point on $E_{u,3}$ with x-coordinate t has order 3 and t satisfies the equation (6) with $\sqrt{\Delta} = \sqrt{3}$.

Proof The following computation can be verified by SageMath [27]. Here, we use the file named `supporting_proofs/proof_theorem_radical_from_j1728.sage` in our GitHub repository.

We first note that α is the unique cube root of $2\varepsilon - \sqrt{3}$ such that $\mathrm{N}_{p^2}(\alpha) = 1$.

Let L be a number field containing $\sqrt{3}$, a primitive cube ω root of unity, and a cube root $\bar{\alpha}$ of $2\varepsilon - \sqrt{3}$. Let E be a Hasegawa curve defined over L with parameter $\frac{7}{12}\varepsilon$. Then the theory of radical isogenies shows that the 3-division polynomial of E has all roots in L. In particular, the roots are given by

$$(3 - 3\sqrt{3}\varepsilon)/2 \text{ and } (3 + 3\sqrt{3}\varepsilon)(\omega^i\bar{\alpha})^2 + 2\sqrt{3}(\omega^i\bar{\alpha}) - \frac{1 - \sqrt{3}\varepsilon}{2}$$

for $i = 0, 1, 2$. This shows the first statement.

To show the second statement, we use Lemma 15. Let $\bar{t}$ be the second root of the above with $i = 0$, and $\bar{t}_p$ be an element obtained by replacing $\bar{\alpha}$ with $\bar{\alpha}^{-1}$ and $\sqrt{3}$ with $-\sqrt{3}$ in the expression of $\bar{t}$. Then, a direct calculation shows that

$$-18\left(1 - \frac{7}{12}\varepsilon\sqrt{3}\right) = (\bar{t}_p - 4)(\bar{t}_p + 2\bar{t}).$$

Since the reductions of $\bar{t}$ and $\bar{t}_p$ modulo a prime ideal above p in L are equal to t and t^p respectively, we obtain the desired equation. □

Finally, we remove the assumption $\sqrt{\Delta} = \sqrt{3}$ to prove Theorem 18 and Lemma 19.

Proof of Theorem 18 Let $v \in \mathbb{F}_{p^2}$ be a fourth root of $\sqrt{3}/\sqrt{\Delta}$. Then, it is easy to see that the isomorphism $\tau_v : E_\infty \to E_{\infty,3}$ induces an isomorphism $(E_\infty, \psi_{(\infty,s)}) \to (E_{\infty,3}, \psi_{(\infty,s),3})$ for $s \in \{\pm 1\}$, where $\psi_{(\infty,s),3}$ is defined as in Equation (2) by replacing $\sqrt{\Delta}$ with $\sqrt{3}$. We can also see that $(E_{u\sqrt{3}/\sqrt{\Delta}}, \psi_{(u\sqrt{3}/\sqrt{\Delta},s)}) = (E_{u,3}, \psi_{(u,s),3})$.

By combining these observations, the theorem directly follows from Theorem 31 and Table A1. □

Proof of Lemma 19 Assume that $[\mathfrak{a}] * \mathbf{u} = (\infty, s')$ for some $s' \in \{\pm 1\}$. Then, Lemma 29 shows that $t = (3 - 3\sqrt{3}\varepsilon)/2$ for some $\varepsilon \in \{\pm 1\}$. This means that $t^p + t - 3 = 0$.

Conversely, assume that $t^p + t - 3 = 0$. From this assumption and Lemma 15, we have

$$t^2 + 4t - 15 + 18u\sqrt{\Delta} = 0.$$

By regarding t as a variable and taking the resultant of the left-hand side of the above equation and the 3-division polynomial of $E_{u\sqrt{3}/\sqrt{\Delta}}$, we have

$$u^2\Delta = \frac{49}{48} \text{ or } \frac{425}{432}.$$

For each $u\Delta$ satisfying the above, we can obtain t by taking the gcd of the two polynomials.

In the former case, we have $u = \varepsilon\frac{7}{12}$ and $t = (3 - 3\sqrt{3}\varepsilon)/2$ for some $\varepsilon \in \{\pm 1\}$. Then, Lemma 29 shows that $[\mathfrak{a}] * \mathbf{u} = (\infty, s')$ for some $s' \in \{\pm 1\}$.

The computation of the resultants and gcds can be verified by the SageMath code named `supporting_proofs/proof_lemma_Hasegawa_denominator.sage` in our GitHub repository.

In the latter case, we have $u = \varepsilon\frac{5\sqrt{17}}{12\sqrt{3}}$ and $t = (1 - \varepsilon\sqrt{3}\sqrt{17})/2$ for some $\varepsilon \in \{\pm 1\}$, where $\sqrt{17}$ is a square root of 17 in $\mathbb{F}_p$. Note that $u\sqrt{\Delta} \notin \mathbb{F}_p$, hence $\sqrt{17}$ must be in $\mathbb{F}_p$ in this case. However, $t + t^p - 3 = -2$ in this case, which is a contradiction. Therefore, the former case only occurs.

The latter statement follows from the fact that $E_{u\sqrt{3}/\sqrt{\Delta}} = E_{u,3}$ and Table A1. □