Families of fast elliptic curves from $\mathbb{Q}$-curves

Benjamin Smith

Team GRACE, INRIA Saclay–Île-de-France
and Laboratoire d'Informatique de l'École polytechnique (LIX)
Bâtiment Alan Turing, 1 rue Honoré d'Estienne d'Orves
Campus de l'École polytechnique, 91120 Palaiseau, France

Abstract. We construct new families of elliptic curves over $\mathbb{F}_{p^2}$ with efficiently computable endomorphisms, which can be used to accelerate elliptic curve-based cryptosystems in the same way as Gallant–Lambert–Vanstone (GLV) and Galbraith–Lin–Scott (GLS) endomorphisms. Our construction is based on reducing $\mathbb{Q}$-curves—curves over quadratic number fields without complex multiplication, but with isogenies to their Galois conjugates—modulo inert primes. As a first application of the general theory we construct, for every $p > 3$, two one-parameter families of elliptic curves over $\mathbb{F}_{p^2}$ equipped with endomorphisms that are faster than doubling. Like GLS (which appears as a degenerate case of our construction), we offer the advantage over GLV of selecting from a much wider range of curves, and thus finding secure group orders when p is fixed. Unlike GLS, we also offer the possibility of constructing twist-secure curves. Among our examples are prime-order curves equipped with fast endomorphisms, with almost-prime-order twists, over $\mathbb{F}_{p^2}$ for $p = 2^{127} - 1$ and $p = 2^{255} - 19$.

Keywords: Elliptic curve cryptography, endomorphisms, GLV, GLS, exponentiation, scalar multiplication, $\mathbb{Q}$-curves.

1 Introduction

Let $\mathcal{E}$ be an elliptic curve over a finite field $\mathbb{F}_q$, and let $\mathcal{G} \subset \mathcal{E}(\mathbb{F}_q)$ be a cyclic subgroup of prime order N. When implementing cryptographic protocols using $\mathcal{G}$, the fundamental operation is *scalar multiplication* (or *exponentiation*):

$$\text{Given } P \text{ in } \mathcal{G} \text{ and } m \text{ in } \mathbb{Z}, \text{ compute } [m]P := \underbrace{P \oplus \cdots \oplus P}_{m \text{ times}}.$$

The literature on general scalar multiplication algorithms is vast, and we will not explore it in detail here (see [11, §2.8,§11.2] and [5, Chapter 9] for introductions to exponentiation and multiexponentiation algorithms). For our purposes, it suffices to note that the dominant factor in scalar multiplication time using conventional algorithms is the bitlength of m. As a basic example, if $\mathcal{G}$ is a generic cyclic abelian group, then we may compute $[m]P$ using a variant of the binary method, which requires at most $\lceil \log_2 m \rceil$ doublings and (in the worst case) about as many addings in $\mathcal{G}$.

But elliptic curves are not generic groups: they have a rich and concrete geometric structure, which should be exploited for fun and profit. For example, endomorphisms of elliptic curves may be used to accelerate generic scalar multiplication algorithms, and thus to accelerate basic operations in curve-based cryptosystems.

Suppose $\mathcal{E}$ is equipped with an efficient endomorphism ψ, defined over $\mathbb{F}_q$. By *efficient*, we mean that we can compute the image $\psi(P)$ of any point P in $\mathcal{E}(\mathbb{F}_q)$ for the cost of $O(1)$ operations in $\mathbb{F}_q$. In practice, we want this to cost no more than a few doublings in $\mathcal{E}(\mathbb{F}_q)$.

Assume $\psi(\mathcal{G}) \subseteq \mathcal{G}$, or equivalently, that ψ restricts to an endomorphism of $\mathcal{G}$.[1] Now $\mathcal{G}$ is a finite cyclic group, isomorphic to $\mathbb{Z}/N\mathbb{Z}$; and every endomorphism of $\mathbb{Z}/N\mathbb{Z}$ is just an integer multiplication modulo N. Hence, ψ acts on $\mathcal{G}$ as multiplication by some integer eigenvalue λ_ψ: that is,

$$\psi|_{\mathcal{G}} = [\lambda_\psi]_{\mathcal{G}}.$$

The eigenvalue λ_ψ must be a root in $\mathbb{Z}/N\mathbb{Z}$ of the characteristic polynomial of ψ.

Returning to the problem of scalar multiplication: we want to compute $[m]P$. Rewriting m as

$$m = a + b\lambda_\psi \pmod{N}$$

for some a and b, we can compute $[m]P$ using the relation

$$[m]P = [a]P + [b\lambda_\psi]P = [a]P + [b]\psi(P)$$

and a two-dimensional multiexponentation such as Straus's algorithm [26], which requires has a loop length of $\log_2 \|(a,b)\|_\infty$ (ie, $\log_2 \|(a,b)\|_\infty$ doubles and as many adds; recall that $\|(a,b)\|_\infty = \max(|a|,|b|)$). If λ_ψ is not too small, then we can easily find (a,b) such that $\log_2 \|(a,b)\|_\infty$ is roughly half of $\log_2 N$. (We remove the "If" and the "roughly" for our ψ in §4.) The endomorphism lets us replace conventional $\log_2 N$-bit scalar multiplications with $\frac{1}{2}\log_2 N$-bit multiexponentiations. In terms of basic binary methods, we are halving the loop length, cutting the number of doublings in half.

Of course, in practice we are not halving the execution time. The precise speedup ratio depends on a variety of factors, including the choice of exponentiation and multiexponentiation algorithms, the cost of computing ψ, the shortness of a and b on the average, and the cost of doublings and addings in terms of bit operations—to say nothing of the cryptographic protocol, which may prohibit some other conventional speedups. For example: in [12], Galbraith, Lin, and Scott report experiments where cryptographic operations on GLS curves required between 70% and 83% of the time required for the previous best practice curves—with the variation depending on the architecture, the underyling point arithmetic, and the protocol.

[1] This assumption is satisfied almost by default in the context of old-school discrete log-based cryptosystems. If $\psi(\mathcal{G}) \not\subseteq \mathcal{G}$, then $\mathcal{E}[N](\mathbb{F}_q) = \mathcal{G} + \psi(\mathcal{G}) \cong (\mathbb{Z}/N\mathbb{Z})^2$, so $N^2 \mid \#\mathcal{E}(\mathbb{F}_q)$ and $N \mid q-1$; such $\mathcal{E}$ are cryptographically inefficient, and discrete logs in $\mathcal{G}$ are vulnerable to the Menezes–Okamoto–Vanstone reduction [21]. However, these $\mathcal{G}$ do arise naturally in pairing-based cryptography; in that context the assumption should be verified carefully.

To put this technique into practice, we need a source of cryptographic elliptic curves equipped with efficient endomorphisms. To date, in the large characteristic case[2], there have been essentially only two constructions:

1. The classic *Gallant–Lambert–Vanstone* (GLV) construction [13]. Elliptic curves over number fields with explicit complex multiplication by CM-orders with small discriminants are reduced modulo suitable primes p; an explicit endomorphism on the CM curve reduces to an efficient endomorphism over the finite field.
2. The more recent *Galbraith–Lin–Scott* (GLS) construction [12]. Here, curves over $\mathbb{F}_p$ are viewed over $\mathbb{F}_{p^2}$; the p-power sub-Frobenius induces an extremely efficient endomorphism on the quadratic twist (which can have prime order).

These two constructions have since been combined to give 3- and 4-dimensional variants [18, 30], and extended to hyperelliptic curves in a variety of ways [3, 17, 24, 27]. However, basic GLV and GLS remain the archetypal constructions.

Our contribution: new families of endomorphisms. In this work, we propose a new source of elliptic curves over $\mathbb{F}_{p^2}$ with efficient endomorphisms: quadratic $\mathbb{Q}$-curves.

Definition 1. *A* quadratic $\mathbb{Q}$-curve of degree d *is an elliptic curve* $\mathcal{E}$ without *complex multiplication, defined over a quadratic number field K, such that there exists an isogeny of degree d from $\mathcal{E}$ to its Galois conjugate ${}^\sigma\mathcal{E}$, where* $\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q})$. *(The Galois conjugate ${}^\sigma\mathcal{E}$ is the curve formed by applying σ to all of the coefficients of $\mathcal{E}$.)*

$\mathbb{Q}$-curves are well-established objects of interest in number theory, where they have formed a natural setting for generalizations of the Shimura–Taniyama conjecture. Ellenberg's survey [9] gives an excellent introduction to this beautiful theory.

Our application of quadratic $\mathbb{Q}$-curves is rather more prosaic: given a d-isogeny $\widetilde{\mathcal{E}} \to {}^\sigma\widetilde{\mathcal{E}}$ over a quadratic field, we reduce modulo an inert prime p to obtain an isogeny $\mathcal{E} \to {}^\sigma\mathcal{E}$ over $\mathbb{F}_{p^2}$. We then exploit the fact that the p-power Frobenius isogeny maps ${}^\sigma\mathcal{E}$ back onto $\mathcal{E}$; composing with the reduced d-isogeny, we obtain an endomorphism of $\mathcal{E}$ of degree dp. For efficiency reasons, d must be small; it turns out that for small values of d, we can write down one-parameter families of $\mathbb{Q}$-curves (our approach below was inspired by the explicit techniques of Hasegawa [15]). We thus obtain one-parameter families of elliptic curves over $\mathbb{F}_{p^2}$ equipped with efficient non-integer endomorphisms. For these endomorphisms we can give convenient explicit formulæ for short scalar decompositions (see §4).

For concrete examples, we concentrate on the cases $d = 2$ and 3 (in §5 and §6, respectively), where the endomorphism is more efficient than a single doubling (we briefly discuss higher degrees in §10). For maximum generality and flexibility, we define our curves in short Weierstrass form; but we include transformations to Montgomery, twisted Edwards, and Doche–Icart–Kohel models where appropriate in §8.

Comparison with GLV. Like GLV, our method involves reducing curves defined over number fields to obtain curves over finite fields with explicit complex multiplication. However, we emphasise a profound difference: in our method, the curves over the number fields generally *do not have complex multiplication themselves.*

[2] We are primarily interested in the large characteristic case, where $q = p$ or p^2; so we will not discuss τ-adic/Frobenius expansion-style techniques here.

GLV curves are necessarily isolated examples—and the really useful examples are extremely limited in number (see [18, App. A] for a list of curves). The scarcity of GLV curves[3] is their Achilles' heel: as noted in [12], if p is fixed then there is no guarantee that there will exist a GLV curve with prime (or almost-prime) order over $\mathbb{F}_p$. Consider the situation discussed in [12, §1]: the most efficient GLV curves have CM discriminants -3 and -4. If we are working at a 128-bit security level, then the choice $p = 2^{255} - 19$ allows particularly fast arithmetic in $\mathbb{F}_p$. But the largest prime factor of the order of a curve over $\mathbb{F}_p$ with CM discriminant -4 (resp. -3) has 239 (resp. 230) bits: using these curves wastes 9 (resp. 13) potential bits of security. In fact, we are lucky with $D = -3$ and -4: for all of the other discriminants offering endomorphisms of degree at most 3, we can do no better than a 95-bit prime factor, which represents a catastrophic 80-bit loss of relative security.

In contrast, our construction yields true families of curves, covering $\sim p$ isomorphism classes over $\mathbb{F}_{p^2}$. This gives us a vastly higher probability of finding prime (or almost-prime)-order curves over practically important fields.

Comparison with GLS. Like GLS, we construct curves over $\mathbb{F}_{p^2}$ equipped with an inseparable endomorphism. While these curves are not defined over the prime field, the fact that the extension degree is only 2 means that Weil descent attacks offer no advantage when solving DLP instances (see [12, §9]). And like GLS, our families offer around p distinct isomorphism classes of curves, making it easy to find secure group orders when p is fixed.

But unlike GLS, our curves have j-invariants in $\mathbb{F}_{p^2}$: they are not isomorphic to or twists of subfield curves. This allows us to find twist-secure curves, which are resistant to the Fouque–Lercier–Réal–Valette fault attack [10]. As we will see in §9, our construction reduces to GLS in the degenerate case $d = 1$ (that is, where $\widetilde{\phi}$ is an isomorphism). Our construction is therefore a sort of generalized GLS—though it is not the higher-degree generalization anticipated by Galbraith, Lin, and Scott themselves, which composes the sub-Frobenius with a non-rational separable homomorphism and its dual homomorphism (cf. [12, Theorem 1]).

In §4, we prove that we can immediately obtain decompositions of the same bitlength as GLS for curves over the same fields: the decompositions produced by our Proposition 2 are identical to the GLS decompositions of [12, Lemma 2] when $d = 1$, up to sign. For this reason, we do not provide extensive implementation details in this paper: while our endomorphisms cost a few more $\mathbb{F}_q$-operations to evaluate than the GLS endomorphism, this evaluation is typically carried out only once

[3] The scarcity of useful GLV curves is easily explained: efficient *separable* endomorphisms have extremely small degree (so that the dense defining polynomials can be evaluated quickly). But the degree of the endomorphism is the norm of the corresponding element of the CM-order; and to have non-integers of very small norm, the CM-order must have a tiny discriminant. Up to twists, the number of elliptic curves with CM discriminant D is the Kronecker class number $h(D)$, which is in $O(\sqrt{D})$. Of course, for the tiny values of D in question, the asymptotics of $h(D)$ are irrelevant; for the six D corresponding to endomorphisms of degree at most 3, we have $h(D) = 1$, so there is only one j-invariant. For $D = -4$ (corresponding to $j = 1728$) there are two or four twists over $\mathbb{F}_p$; for $D = -3$ (corresponding to $j = 0$) we have two or six, and otherwise we have only two. In particular, there are at most 18 distinct curves over $\mathbb{F}_p$ with a non-integer endomorphism of degree at most 3.

per scalar multiplication. This evaluation is the only difference between a GLS scalar multiplication and one of ours: the subsequent multiexponentiations have exactly the same length as in GLS, and the underlying curve and field arithmetic is the same, too.

2 Notation and conventions

Throughout, we work over fields of characteristic not 2 or 3. Let

$$\mathcal{E} : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

be an elliptic curve over such a field K.

Galois conjugates. For every automorphism σ of K, we define the conjugate curve

$${}^{\sigma}\mathcal{E} : y^2 = x^3 + {}^{\sigma}a_2x^2 + {}^{\sigma}a_4x + {}^{\sigma}a_6.$$

If $\phi : \mathcal{E} \to \mathcal{E}_1$ is an isogeny, then we obtain a conjugate isogeny ${}^{\sigma}\phi : {}^{\sigma}\mathcal{E} \to {}^{\sigma}\mathcal{E}_1$ by applying σ to the defining equations of ϕ, $\mathcal{E}$, and $\mathcal{E}_1$.

Quadratic twists. For every $\lambda \neq 0$ in $\overline{K}^{\times}$, we define a twisting isomorphism

$$\delta(\lambda) : \mathcal{E} \longrightarrow \mathcal{E}^{\lambda} : y^2 = x^3 + \lambda^2 a_2x^2 + \lambda^4 a_4x + \lambda^6 a_6$$

by

$$\delta(\lambda) : (x, y) \longmapsto (\lambda^2 x, \lambda^3 y).$$

The twist $\mathcal{E}^{\lambda}$ is defined over $K(\lambda^2)$, and $\delta(\lambda)$ is defined over $K(\lambda)$. For every K-endomorphism ψ of $\mathcal{E}$, there is a $K(\lambda^2)$-endomorphism $\psi^{\lambda} = \delta(\lambda)\psi\delta(\lambda^{-1})$ of $\mathcal{E}^{\lambda}$. Observe that $\delta(\lambda_1)\delta(\lambda_2) = \delta(\lambda_1\lambda_2)$ for any λ_1, λ_2 in K, and $\delta(-1) = [-1]$. Also, ${}^{\sigma}(\mathcal{E}^{\lambda}) = {}^{\sigma}\mathcal{E}^{{}^{\sigma}\lambda}$ for all automorphisms σ of $\overline{K}$.

If μ is a nonsquare in K, then $\mathcal{E}^{\sqrt{\mu}}$ is called a *quadratic twist*. If $K = \mathbb{F}_q$, then $\mathcal{E}^{\sqrt{\mu_1}}$ and $\mathcal{E}^{\sqrt{\mu_2}}$ are $\mathbb{F}_q$-isomorphic for all nonsquares μ_1, μ_2 in $\mathbb{F}_q$ (the isomorphism $\delta(\sqrt{\mu_1/\mu_2})$ is defined over $\mathbb{F}_q$ because μ_1/μ_2 must be a square). When the choice of nonsquare is not important, we denote the quadratic twist by $\mathcal{E}'$. Similarly, if ψ is an $\mathbb{F}_q$-endomorphism of $\mathcal{E}$, then ψ' is the corresponding $\mathbb{F}_q$-endomorphism of $\mathcal{E}'$. (*Conjugates are marked by left-superscripts, twists by right-superscripts.*)

The trace. If $K = \mathbb{F}_q$, then $\pi_{\mathcal{E}}$ denotes the q-power Frobenius endomorphism of $\mathcal{E}$. Recall that the characteristic polynomial of $\pi_{\mathcal{E}}$ has the form

$$\chi_{\mathcal{E}}(T) = T^2 - \operatorname{tr}(\mathcal{E})T + q, \qquad \text{with} \qquad |\operatorname{tr}(\mathcal{E})| \leq 2\sqrt{q}.$$

The integer $\operatorname{tr}(\mathcal{E})$ is the *trace* of $\mathcal{E}$; we have $\#\mathcal{E}(\mathbb{F}_q) = q + 1 - \operatorname{tr}(\mathcal{E})$ and $\operatorname{tr}(\mathcal{E}') = -\operatorname{tr}(\mathcal{E})$.

p-th powering. We write (p) for the p-th powering automorphism of $\overline{\mathbb{F}}_p$. Note that (p) is almost trivial to compute on $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{\Delta})$, because ${}^{(p)}(a + b\sqrt{\Delta}) = a - b\sqrt{\Delta}$ for all a and b in $\mathbb{F}_p$.

3 Quadratic $\mathbb{Q}$-curves and their reductions

Suppose $\widetilde{\mathscr{E}}/\mathbb{Q}(\sqrt{\Delta})$ is a quadratic $\mathbb{Q}$-curve of prime degree d (cf. Definition 1), where Δ is a discriminant prime to d, and let $\widetilde{\phi}:\widetilde{\mathscr{E}}\to{}^{\sigma}\widetilde{\mathscr{E}}$ be the corresponding d-isogeny. In general, $\widetilde{\phi}$ is only defined over a quadratic extension $\mathbb{Q}(\sqrt{\Delta},\gamma)$ of $\mathbb{Q}(\sqrt{\Delta})$. We can compute γ from Δ and $\ker\widetilde{\phi}$ using [14, Proposition 3.1], but after a suitable twist we can always reduce to the case where $\gamma=\sqrt{\pm d}$ (see [14, remark after Lemma 3.2]). The families of explicit $\mathbb{Q}$-curves of degree d that we treat below have their isogenies defined over $\mathbb{Q}(\sqrt{\Delta},\sqrt{-d})$; so to simplify matters, from now on we will

Assume $\widetilde{\phi}$ is defined over $\mathbb{Q}(\sqrt{\Delta},\sqrt{-d})$.

Let p be a prime of good reduction for $\widetilde{\mathscr{E}}$ that is inert in $\mathbb{Q}(\sqrt{\Delta})$ and prime to d. If $\mathscr{O}_{\Delta}$ is the ring of integers of $\mathbb{Q}(\sqrt{\Delta})$, then

$$\mathbb{F}_{p^2}=\mathscr{O}_{\Delta}/(p)=\mathbb{F}_p(\sqrt{\Delta}).$$

Looking at the Galois groups of our fields, we have a series of injections

$$\langle (p)\rangle=\mathrm{Gal}(\mathbb{F}_p(\sqrt{\Delta})/\mathbb{F}_p)\hookrightarrow\mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q})\hookrightarrow\mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta},\sqrt{-d})/\mathbb{Q}).$$

The image of (p) in $\mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q})$ is σ, because p is inert in $\mathbb{Q}(\sqrt{\Delta})$. When extending σ to an automorphism of $\mathbb{Q}(\sqrt{\Delta},\sqrt{-d})$, we extend it to be the image of (p): that is,

$${}^{\sigma}\!\left(\alpha+\beta\sqrt{\Delta}+\gamma\sqrt{-d}+\delta\sqrt{-d\Delta}\right)=\alpha-\beta\sqrt{\Delta}+\left(-d/p\right)\left(\gamma\sqrt{-d}-\delta\sqrt{-d\Delta}\right) \tag{3.1}$$

for all α,β,γ, and $\delta\in\mathbb{Q}$. (Recall that the Legendre symbol $\left(n/p\right)$ is 1 if n is a square mod p, -1 if n is not a square mod p, and 0 if p divides n.)

Now let $\mathscr{E}$ be the reduction modulo p of $\widetilde{\mathscr{E}}$. The curve ${}^{\sigma}\widetilde{\mathscr{E}}$ reduces to ${}^{(p)}\mathscr{E}$, while the d-isogeny $\widetilde{\phi}:\widetilde{\mathscr{E}}\to{}^{\sigma}\widetilde{\mathscr{E}}$ reduces to a d-isogeny $\phi:\mathscr{E}\to{}^{(p)}\mathscr{E}$ defined over $\mathbb{F}_{p^2}$.

Applying σ to $\widetilde{\phi}$, we obtain a second d-isogeny ${}^{\sigma}\widetilde{\phi}:{}^{\sigma}\widetilde{\mathscr{E}}\to\widetilde{\mathscr{E}}$ travelling in the opposite direction, which reduces mod p to a conjugate isogeny ${}^{(p)}\phi:{}^{(p)}\mathscr{E}\to\mathscr{E}$ over $\mathbb{F}_{p^2}$. Composing ${}^{\sigma}\widetilde{\phi}$ with $\widetilde{\phi}$ yields endomorphisms ${}^{\sigma}\widetilde{\phi}\circ\widetilde{\phi}$ of $\widetilde{\mathscr{E}}$ and $\widetilde{\phi}\circ{}^{\sigma}\widetilde{\phi}$ of ${}^{\sigma}\widetilde{\mathscr{E}}$, each of degree d^2. But (by definition) $\widetilde{\mathscr{E}}$ and ${}^{\sigma}\widetilde{\mathscr{E}}$ do not have complex multiplication, so all of their endomorphisms are integer multiplications; and since the only integer multiplications of degree d^2 are $[d]$ and $[-d]$, we can conclude that

$${}^{\sigma}\widetilde{\phi}\circ\widetilde{\phi}=[\epsilon_p d]_{\widetilde{\mathscr{E}}}\quad\text{and}\quad\widetilde{\phi}\circ{}^{\sigma}\widetilde{\phi}=[\epsilon_p d]_{{}^{\sigma}\widetilde{\mathscr{E}}},\quad\text{where }\epsilon_p\in\{\pm1\}.$$

Technically, ${}^{\sigma}\widetilde{\phi}$ and ${}^{(p)}\phi$ are—*up to sign*—the dual isogenies of $\widetilde{\phi}$ and ϕ, respectively. The sign ϵ_p depends on p (as well as on $\widetilde{\phi}$): if τ is the extension of σ to $\mathbb{Q}(\sqrt{\Delta},\sqrt{-d})$ that is *not* the image of (p), then ${}^{\tau}\widetilde{\phi}\circ\widetilde{\phi}=[-\epsilon_p d]_{\widetilde{\mathscr{E}}}$. Reducing mod p, we see that

$${}^{(p)}\phi\circ\phi=[\epsilon_p d]_{\mathscr{E}}\quad\text{and}\quad\phi\circ{}^{(p)}\phi=[\epsilon_p d]_{{}^{(p)}\mathscr{E}}. \tag{3.2}$$

The map $(x,y)\mapsto(x^p,y^p)$ defines p-isogenies

$$\pi_0:{}^{(p)}\mathscr{E}\longrightarrow\mathscr{E}\quad\text{and}\quad{}^{(p)}\pi_0:\mathscr{E}\longrightarrow{}^{(p)}\mathscr{E}.$$

Clearly, ${}^{(p)}\pi_0 \circ \pi_0$ (resp. $\pi_0 \circ {}^{(p)}\pi_0$) is the p^2-power Frobenius endomorphism of $\mathscr{E}$ (resp. ${}^{(p)}\mathscr{E}$). Composing π_0 with ϕ yields a degree-pd endomorphism

$$\psi := \pi_0 \circ \phi \in \mathrm{End}(\mathscr{E}).$$

If d is very small—say, less than 10—then ψ is efficient because ϕ is defined by polynomials of degree about d, and π_0 acts as a simple conjugation on coordinates in $\mathbb{F}_{p^2}$, as in Eq. (3.1). (The efficiency of ψ depends primarily on its separable degree, d, and not on the inseparable part p.)

We also obtain an endomorphism ψ' on the quadratic twist $\mathscr{E}'$ of $\mathscr{E}$. Indeed, if $\mathscr{E}' = \mathscr{E}^{\sqrt{\mu}}$, then $\psi' = \psi^{\sqrt{\mu}}$, and ψ' is defined over $\mathbb{F}_{p^2}$.

Proposition 1. *With the notation above:*

$$\psi^2 = [\epsilon_p d]\pi_{\mathscr{E}} \qquad \textit{and} \qquad (\psi')^2 = [-\epsilon_p d]\pi_{\mathscr{E}'}.$$

There exists an integer r satisfying $dr^2 = 2p + \epsilon_p \mathrm{tr}(\mathscr{E})$ such that

$$\psi = \frac{1}{r}\left(\pi_{\mathscr{E}} + \epsilon_p p\right) \qquad \textit{and} \qquad \psi' = \frac{-1}{r}\left(\pi_{\mathscr{E}'} - \epsilon_p p\right).$$

The characteristic polynomial of both ψ and ψ' is

$$P_\psi(T) = P_{\psi'}(T) = T^2 - \epsilon_p r d T + dp.$$

Proof. Clearly, $\pi_0 \circ \phi = {}^{(p)}\phi \circ {}^{(p)}\pi_0$. Hence

$$\psi^2 = \pi_0 \circ \phi \circ \pi_0 \circ \phi = \pi_0 \circ \phi \circ {}^{(p)}\phi \circ {}^{(p)}\pi_0 = \pi_0 [\epsilon_p d]\, {}^{(p)}\pi_0 = [\epsilon_p d]\pi_0\, {}^{(p)}\pi_0 = [\epsilon_p d]\pi_{\mathscr{E}}.$$

Choosing a nonsquare μ in $\mathbb{F}_{p^2}$, so $\mathscr{E}' = \mathscr{E}^{\sqrt{\mu}}$ and $\psi' = \psi^{\sqrt{\mu}}$, we find

$$\begin{aligned}(\psi')^2 = \delta(\mu^{1/2}) \circ \psi^2 \circ \delta(\mu^{-1/2}) &= \delta(\mu^{1/2}) \circ [\epsilon_p d]\pi_{\mathscr{E}} \circ \delta(\mu^{-1/2}) \\ &= \delta(\mu^{(1-p^2)/2})[\epsilon_p d]\pi_{\mathscr{E}'} = \delta(-1)[\epsilon_p d]\pi_{\mathscr{E}'} = [-\epsilon_p d]\pi_{\mathscr{E}'}\end{aligned}$$

Using the relations $\pi_{\mathscr{E}}^2 - \mathrm{tr}(\mathscr{E})\pi_{\mathscr{E}} + p^2 = 0$ and $\pi_{\mathscr{E}'}^2 + \mathrm{tr}(\mathscr{E})\pi_{\mathscr{E}'} + p^2 = 0$, we verify that the expressions for ψ and ψ' give the two square roots of $\epsilon_p d\pi_{\mathscr{E}}$ in $\mathbb{Q}(\pi_{\mathscr{E}})$, and $-\epsilon_p d\pi_{\mathscr{E}'}$ in $\mathbb{Q}(\pi'_{\mathscr{E}})$, and that the claimed characteristic polynomial is satisfied. □

Now we just need a source of quadratic $\mathbb{Q}$-curves of small degree. Elkies [8] shows that all $\mathbb{Q}$-curves correspond to rational points on certain modular curves: Let $X^*(d)$ be the quotient of the modular curve $X_0(d)$ by all of its Atkin–Lehner involutions, let K be a quadratic field, and let σ be the involution of K over $\mathbb{Q}$. If e is a point in $X^*(d)(\mathbb{Q})$ and E is a preimage of e in $X_0(d)(K) \setminus X_0(d)(\mathbb{Q})$, then E parametrizes (up to $\overline{\mathbb{Q}}$-isomorphism) a d-isogeny $\widetilde{\phi} : \widetilde{\mathscr{E}} \to {}^{\sigma}\widetilde{\mathscr{E}}$ over K.

Luckily enough, for very small d, the curves $X_0(d)$ and $X^*(d)$ have genus zero—so not only do we get plenty of rational points on $X^*(d)$, we get a whole one-parameter family of $\mathbb{Q}$-curves of degree d. Hasegawa gives explicit universal curves for $d = 2$, 3, and 7 in [15, Theorem 2.2]: for each squarefree integer $\Delta \neq 1$, every $\mathbb{Q}$-curve of degree $d = 2, 3, 7$ over $\mathbb{Q}(\sqrt{\Delta})$ is $\overline{\mathbb{Q}}$-isomorphic to a rational specialization of one of these families. Hasegawa's curves for $d = 2$ and 3 ($\widetilde{\mathscr{E}}_{2,\Delta,s}$ in §5 and $\widetilde{\mathscr{E}}_{3,\Delta,s}$ in §6) suffice not only to illustrate our ideas, but also to give useful practical examples.

4 Short scalar decompositions

Before moving on to concrete constructions, we will show that the endomorphisms developed in §3 yield short scalar decompositions. Proposition 2 below gives explicit formulæ for producing decompositions of at most $\lceil log_2 p \rceil$ bits.

Suppose $\mathcal{G}$ is a cyclic subgroup of $\mathcal{E}(\mathbb{F}_{p^2})$ such that $\psi(\mathcal{G}) = \mathcal{G}$, and let $N = \#\mathcal{G}$. Proposition 1 shows that ψ acts as a square root of $\epsilon_p d$ on $\mathcal{G}$: its eigenvalue is

$$\lambda_\psi \equiv (1 + \epsilon_p p)/r \pmod{N}. \tag{4.1}$$

We want to compute a decomposition

$$m = a + b\lambda_\psi \pmod{N}$$

so as to efficiently compute

$$[m]P = [a]P + [b\lambda_\psi]P = [a]P + [b]\psi(P).$$

The decomposition of m is not unique: far from it. The set of all decompositions (a, b) of m is the coset $(m, 0) + \mathcal{L}$, where

$$\mathcal{L} := \langle (N, 0), (-\lambda_\psi, 1) \rangle \subset \mathbb{Z}^2$$

is the lattice of decompositions of 0 (that is, of (a, b) such that $a + b\lambda_\psi \equiv 0 \pmod{N}$).

We want to find a decomposition where a and b have minimal bitlength: that is, where $\lceil \log_2 \|(a, b)\|_\infty \rceil$ is as small as possible. The standard technique is to (pre)-compute a short basis of $\mathcal{L}$, then use Babai rounding [1] to transform each scalar m into a short decomposition (a, b). The following lemma outlines this process; for further detail and analysis, see [13, §4] and [11, §18.2].

Lemma 1. *Let $\mathbf{e}_1, \mathbf{e}_2$ be linearly independent vectors in $\mathcal{L}$. Let m be an integer, and set*

$$(a, b) := (m, 0) - \lfloor \alpha \rceil \mathbf{e}_1 - \lfloor \beta \rceil \mathbf{e}_2,$$

where (α, β) is the (unique) solution in $\mathbb{Q}^2$ to the linear system $(m, 0) = \alpha\mathbf{e}_1 + \beta\mathbf{e}_2$. Then

$$m \equiv a + \lambda_\psi b \pmod{N} \qquad \textit{and} \qquad \|(a, b)\|_\infty \le \max(\|\mathbf{e}_1\|_\infty, \|\mathbf{e}_2\|_\infty).$$

Proof. This is just [13, Lemma 2] (under the infinity norm). □

We see that better decompositions of m correspond to shorter bases for $\mathcal{L}$. If $|\lambda_\psi|$ is not unusually small, then we can compute a basis for $\mathcal{L}$ of size $O(\sqrt{N})$ using the Gauss reduction or Euclidean algorithms (cf. [13, §4] and [11, §17.1.1]).[4] The basis depends only on N and λ_ψ, so it can be precomputed.

In our case, lattice reduction is unnecessary: we can immediately write down two linearly independent vectors in $\mathcal{L}$ that are "short enough", and thus give explicit formulae for (a, b) in terms of m. These decompositions have length $\lceil \log_2 p \rceil$, which is near-optimal in cryptographic contexts: if $N \sim \#\mathcal{E}(\mathbb{F}_{p^2}) \sim p^2$, then $\log_2 p \sim \frac{1}{2} \log_2 N$.

[4] Bounds on the constant hidden by the $O(\sqrt{N})$ are derived in [24], but they are suboptimal for our endomorphisms. In cryptographic contexts, Proposition 2 gives better results.

Proposition 2. *With the notation above: given an integer m, let*

$$a = m - \lfloor m(1+\epsilon_p p)/\#\mathscr{E}(\mathbb{F}_{p^2}) \rceil (1+\epsilon_p p) + \lfloor mr/\#\mathscr{E}(\mathbb{F}_{p^2}) \rceil \epsilon_p dr \qquad \textit{and}$$
$$b = \lfloor m(1+\epsilon_p p)/\#\mathscr{E}(\mathbb{F}_{p^2}) \rceil r - \lfloor mr/\#\mathscr{E}(\mathbb{F}_{p^2}) \rceil (1+\epsilon_p p).$$

Then, assuming $d \ll p$ and $m \not\equiv 0 \pmod{N}$, we have

$$m \equiv a + b\lambda_\psi \pmod{N} \qquad \textit{and} \qquad \lceil \log_2 \|(a,b)\|_\infty \rceil \le \lceil \log_2 p \rceil.$$

Proof. Eq. (4.1) yields $r\lambda_\psi \equiv 1+\epsilon_p p \pmod{N}$ and $r\epsilon_p d \equiv (1+\epsilon_p p)\lambda_\psi \pmod{N}$, so the vectors $\mathbf{e}_1 = (1+\epsilon_p p, -r)$ and $\mathbf{e}_2 = (-\epsilon_p dr, 1+\epsilon_p p)$ are in $\mathscr{L}$ (they generate a sublattice of determinant $\#\mathscr{E}(\mathbb{F}_{p^2})$). Applying Lemma 1 with $\alpha = m(1+\epsilon_p p)/\#\mathscr{E}(\mathbb{F}_{p^2})$ and $\beta = mr/\#\mathscr{E}(\mathbb{F}_{p^2})$, we see that $m \equiv a + b\lambda_\psi \pmod{N}$ and $\|(a,b)\|_\infty \le \|\mathbf{e}_2\|_\infty$. But $d|r| \le 2\sqrt{dp}$ (since $|\mathrm{tr}(\mathscr{E})| \le 2p$) and $d \ll p$, so $\|\mathbf{e}_2\|_\infty = p + \epsilon_p$. The result follows on taking logs, and noting that $\lceil \log_2(p \pm 1) \rceil = \lceil \log_2 p \rceil$ (since $p > 3$). □

5 Endomorphisms from quadratic $\mathbb{Q}$-curves of degree 2

Let Δ be a squarefree integer. Hasegawa defines a one-parameter family of elliptic curves over $\mathbb{Q}(\sqrt{\Delta})$ by

$$\widetilde{\mathscr{E}}_{2,\Delta,s} : y^2 = x^3 - 6(5 - 3s\sqrt{\Delta})x + 8(7 - 9s\sqrt{\Delta}), \tag{5.1}$$

where s is a free parameter taking values in $\mathbb{Q}$ [15, Theorem 2.2]. The discriminant of $\widetilde{\mathscr{E}}_{2,\Delta,s}$ is $2^9 \cdot 3^6 (1 - s^2\Delta)(1 + s\sqrt{\Delta})$, so the curve $\widetilde{\mathscr{E}}_{2,\Delta,s}$ has good reduction at every $p > 3$ with $(\Delta/p) = -1$, for every s in $\mathbb{Q}$.

The curve $\widetilde{\mathscr{E}}_{2,\Delta,s}$ has a rational 2-torsion point $(4,0)$, which generates the kernel of a 2-isogeny $\widetilde{\phi}_{2,\Delta,s} : \widetilde{\mathscr{E}}_{2,\Delta,s} \to {}^\sigma\widetilde{\mathscr{E}}_{2,\Delta,s}$ defined over $\mathbb{Q}(\sqrt{\Delta}, \sqrt{-2})$. We construct $\widetilde{\phi}_{2,\Delta,s}$ explicitly: Vélu's formulae [28] define the (normalized) quotient $\widetilde{\mathscr{E}}_{2,\Delta,s} \to \widetilde{\mathscr{E}}_{2,\Delta,s}/\langle(4,0)\rangle$, and then the isomorphism $\widetilde{\mathscr{E}}_{2,\Delta,s}/\langle(4,0)\rangle \to {}^\sigma\widetilde{\mathscr{E}}_{2,\Delta,s}$ is the quadratic twist $\delta(1/\sqrt{-2})$. Composing, we obtain an expression for the isogeny as a rational map:

$$\widetilde{\phi}_{2,\Delta,t} : (x,y) \longmapsto \left(\frac{-x}{2} - \frac{9(1+s\sqrt{\Delta})}{x-4}, \frac{y}{\sqrt{-2}} \left(\frac{-1}{2} + \frac{9(1+s\sqrt{\Delta})}{(x-4)^2} \right) \right).$$

Conjugating and composing, we recognise that ${}^\sigma\widetilde{\phi}_{2,\Delta,t} \circ \widetilde{\phi}_{2,\Delta,t} = [2]$ if $\sigma(\sqrt{-2}) = -\sqrt{-2}$, and $[-2]$ if $\sigma(\sqrt{-2}) = \sqrt{-2}$: that is, the sign function for $\widetilde{\phi}_{2,\Delta,t}$ is

$$\epsilon_p = -\left(-2/p\right) = \begin{cases} 1 & \text{if } p \equiv 5,7 \pmod{8}, \\ -1 & \text{if } p \equiv 1,3 \pmod{8}. \end{cases} \tag{5.2}$$

Theorem 1. *Let $p > 3$ be a prime, and define ϵ_p as in Eq. (5.2). Let Δ be a nonsquare*[5] *in $\mathbb{F}_p$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{\Delta})$. Let $C_{2,\Delta} : \mathbb{F}_p \to \mathbb{F}_{p^2}$ be the mapping defined by*

$$C_{2,\Delta}(s) := 9(1 + s\sqrt{\Delta}).$$

[5] The choice of Δ is (theoretically) irrelevant, since all quadratic extensions of $\mathbb{F}_p$ are isomorphic. If Δ and Δ' are two nonsquares in $\mathbb{F}_p$, then $\Delta/\Delta' = a^2$ for some a in $\mathbb{F}_p$, so $\mathscr{E}_{2,\Delta,t}$ and $\mathscr{E}_{2,\Delta',at}$ are identical. We are therefore free to choose any practically convenient value for Δ, such as one permitting faster arithmetic in $\mathbb{F}_p(\sqrt{\Delta})$.

For each s in $\mathbb{F}_p$, let $\mathscr{E}_{2,\Delta,s}$ be the elliptic curve over $\mathbb{F}_{p^2}$ defined by

$$\mathscr{E}_{2,\Delta,s} : y^2 = x^3 + 2(C_{2,\Delta}(s) - 24)x - 8(C_{2,\Delta}(s) - 16).$$

Then $\mathscr{E}_{2,\Delta,s}$ has an efficient $\mathbb{F}_{p^2}$-endomorphism

$$\psi_{2,\Delta,s} : (x, y) \longmapsto \left(\frac{-x^p}{2} - \frac{C_{2,\Delta}(s)^p}{x^p - 4}, \frac{y^p}{\sqrt{-2}} \left(\frac{-1}{2} + \frac{C_{2,\Delta}(s)^p}{(x^p - 4)^2} \right) \right),$$

of degree $2p$, such that

$$\psi_{2,\Delta,s} = \frac{1}{r}\left(\pi_{\mathscr{E}_{2,\Delta,s}} + \epsilon_p p\right) \qquad \text{and} \qquad \psi_{2,\Delta,s}^2 = [\epsilon_p 2]\pi_{\mathscr{E}_{2,\Delta,s}}$$

for some integer r satisfying $2r^2 = 2p + \epsilon_p \mathrm{tr}(\mathscr{E}_{2,\Delta,s})$. The characteristic polynomial of $\psi_{2,\Delta,s}$ is $P_{2,\Delta,s}(T) = T^2 - \epsilon_p r T + 2p$. The twisted endomorphism $\psi'_{2,\Delta,s}$ on $\mathscr{E}'_{2,\Delta,s}$ satisfies $\psi'_{2,\Delta,s} = (-\pi_{\mathscr{E}'_{2,\Delta,s}} + \epsilon_p p)/r$, and $(\psi'_{2,\Delta,s})^2 = [-\epsilon_p 2]\pi_{\mathscr{E}'_{2,\Delta,s}}$, and $P_{2,\Delta,s}(\psi'_{2,\Delta,s}) = 0$.

Proof. Reduce $\widetilde{\mathscr{E}}_{2,\Delta,s}$ and $\widetilde{\phi}_{2,\Delta,s}$ mod p and compose with π_0 as in §3, then apply Proposition 1 using Eq. (5.2). □

If $\mathscr{G} \subset \mathscr{E}_{2,\Delta,s}(\mathbb{F}_{p^2})$ is a cyclic subgroup of order N such that $\psi_{2,\Delta,s}(\mathscr{G}) = \mathscr{G}$, then the eigenvalue of $\psi_{2,\Delta,s}$ on $\mathscr{G}$ is

$$\lambda_{2,\Delta,s} = \frac{1}{r}\left(1 + \epsilon_p p\right) \equiv \pm\sqrt{\epsilon_p 2} \pmod{N}.$$

Applying Proposition 2, we can decompose scalar multiplications in $\mathscr{G}$ as $[m]P = [a]P + [b]\psi_{2,\Delta,s}(P)$ where a and b have at most $\lceil \log_2 p \rceil$ bits.

Proposition 3. *Theorem 1 yields at least $p - 3$ non-isomorphic curves (and at least $2p - 6$ non-$\mathbb{F}_{p^2}$-isomorphic curves, if we count the quadratic twists) equipped with efficient endomorphisms.*

Proof. It suffices to show that the j-invariant $j\left(\mathscr{E}_{2,\Delta,s}\right) = \frac{2^6(5-3s\sqrt{\Delta})^3}{(1-s^2\Delta)(1+s\sqrt{\Delta})}$ takes at least $p-3$ distinct values in $\mathbb{F}_{p^2}$ as s ranges over $\mathbb{F}_p$. If $j(\mathscr{E}_{2,\Delta,s}) = j(\mathscr{E}_{2,\Delta,s_1})$ with $s_1 \neq s_2$, then s_1 and s_2 satisfy $F_0(s_1, s_2) - 2\sqrt{\Delta}F_1(s_1, s_2) = 0$, where $F_1(s_1, s_2) = (s_1 + s_2)(63\Delta s_1 s_2 - 65)$ and $F_0(s_1, s_2) = (\Delta s_1 s_2 + 1)(81\Delta s_1 s_2 - 175) + 49\Delta(s_1 + s_2)^2$ are polynomials over $\mathbb{F}_p$. If s_1 and s_2 are in $\mathbb{F}_p$, then we must have $F_0(s_1, s_2) = F_1(s_1, s_2) = 0$. Solving the simultaneous equations, discarding the solutions that can never be in $\mathbb{F}_p$, and dividing by two (since (s_1, s_2) and (s_2, s_1) represent the same collision) yields at most 3 collisions $j(\mathscr{E}_{2,\Delta,s_1}) = j(\mathscr{E}_{2,\Delta,s_2})$ with $s_1 \neq s_2$ in $\mathbb{F}_p$. □

We observe that ${}^{\sigma}\widetilde{\mathscr{E}}_{2,\Delta,s} = \widetilde{\mathscr{E}}_{2,\Delta,-s}$, so we do not gain any more isomorphism classes in Proposition 3 by including the codomain curves.

6 Endomorphisms from quadratic $\mathbb{Q}$-curves of degree 3

Let Δ be a squarefree discriminant; Hasegawa defines a one-parameter family of elliptic curves over $\mathbb{Q}(\sqrt{\Delta})$ by

$$\widetilde{\mathscr{E}}_{3,\Delta,s} : y^2 = x^3 - 3\big(5 + 4s\sqrt{\Delta}\big)x + 2\big(2s^2\Delta + 14s\sqrt{\Delta} + 11\big), \tag{6.1}$$

where s is a free parameter taking values in $\mathbb{Q}$. As for the curves in §5, the curve $\widetilde{\mathscr{E}}_{3,\Delta,s}$ has good reduction at every $p > 3$ with $\big(\Delta/p\big) = -1$, for every s in $\mathbb{Q}$.

The curve $\widetilde{\mathscr{E}}_{3,\Delta,s}$ has a subgroup of order 3 defined by the polynomial $x - 3$, consisting of 0 and $(3, \pm 2(1 - s\sqrt{\Delta}))$. Exactly as in §5, taking the Vélu quotient and twisting by $1/\sqrt{-3}$ yields an explicit 3-isogeny $\widetilde{\phi}_{3,\Delta,s} : \widetilde{\mathscr{E}}_{3,\Delta,s} \to {}^{\sigma}\widetilde{\mathscr{E}}_{3,\Delta,s}$; its sign function is

$$\epsilon_p = -\big(-3/p\big) = \begin{cases} 1 & \text{if } p \equiv 2 \pmod 3, \\ -1 & \text{if } p \equiv 1 \pmod 3. \end{cases} \tag{6.2}$$

Theorem 2. *Let $p > 3$ be a prime, and define ϵ_p as in Eq.* (6.2)*. Let Δ be a nonsquare*[6] *in $\mathbb{F}_p$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{\Delta})$. Let $C_{3,\Delta} : \mathbb{F}_p \to \mathbb{F}_{p^2}$ be the mapping defined by*

$$C_{3,\Delta}(s) := 2(1 + s\sqrt{\Delta}).$$

For each s in $\mathbb{F}_p$, we let $\mathscr{E}_{3,\Delta,s}$ be the elliptic curve over $\mathbb{F}_{p^2}$ defined by

$$\mathscr{E}_{3,\Delta,s} : y^2 = x^3 - 3\big(2C_{3,\Delta}(s) + 1\big)x + \big(C_{3,\Delta}(s)^2 + 10C_{3,\Delta}(s) - 2\big).$$

Then $\mathscr{E}_{3,\Delta,s}$ has an efficient $\mathbb{F}_{p^2}$-endomorphism

$$\psi_{3,\Delta,s} : (x,y) \longmapsto \left(-\frac{x^p}{3} - \frac{4C_{3,\Delta}(s)^p}{x^p - 3} - \frac{4C_{3,\Delta}(s)^{2p}}{3(x^p-3)^2}, \frac{y^p}{\sqrt{-3}}\left(\frac{-1}{3} + \frac{4C_{3,\Delta}(s)^p}{(x^p-3)^2} + \frac{8C_{3,\Delta}(s)^{2p}}{3(x^p-3)^3}\right)\right)$$

of degree $3p$, such that

$$\psi_{3,\Delta,s}^2 = [\epsilon_p 3]\pi_{\mathscr{E}_{3,\Delta,s}} \qquad \textit{and} \qquad \psi_{3,\Delta,s} = \frac{1}{r}\left(\pi + \epsilon_p p\right)$$

for some integer r satisfying $3r^2 = 2p + \epsilon_p \mathrm{tr}(\mathscr{E}_{3,\Delta,s})$. The characteristic polynomial of $\psi_{3,\Delta,s}$ is $P_{3,\Delta,s}(T) = T^2 - \epsilon_p r T + 3p$. The twisted endomorphism $\psi'_{3,\Delta,s}$ on $\mathscr{E}'_{3,\Delta,s}$ satisfies $(\psi'_{3,\Delta,s})^2 = [-\epsilon_p 3]\pi_{\mathscr{E}'_{3,\Delta,s}}$, and $\psi'_{3,\Delta,s} = (-\pi_{\mathscr{E}'_{3,\Delta,s}} + \epsilon_p p)/r$, and $P_{3,\Delta,s}(\psi'_{3,\Delta,s}) = 0$.

Proof. Reduce $\widetilde{\mathscr{E}}_{3,\Delta,s}$ and $\widetilde{\phi}_{3,\Delta,s}$ mod p, compose with π_0 as in §3, and apply Proposition 1 using Eq. (6.2). ◻

Proposition 4. *Theorem 2 yields at least $p - 8$ non-isomorphic curves (and counting quadratic twists, at least $2p - 16$ non-$\mathbb{F}_{p^2}$-isomorphic curves) equipped with efficient endomorphisms.*

Proof. The proof is exactly as for Proposition 3. ◻

[6] As in Theorem 1, the particular value of Δ is theoretically irrelevant.

7 Cryptographic-sized curves

We will now exhibit some curves with our families with cryptographic parameter sizes, and secure and twist-secure group orders. We computed the curve orders below using Magma's implementation of the Schoof–Elkies–Atkin algorithm [23, 19, 4].

First, consider the degree-2 curves of §5. By definition, $\mathcal{E}_{2,\Delta,s}$ and its quadratic twist $\mathcal{E}'_{2,\Delta,s}$ have points of order 2 over $\mathbb{F}_{p^2}$: they generate the kernels of our endomorphisms. If $p \equiv 2 \pmod 3$, then $2r^2 = 2p + \epsilon_p \mathrm{tr}(\mathcal{E})$ implies $\mathrm{tr}(\mathcal{E}) \not\equiv 0 \pmod 3$, so when $p \equiv 2 \pmod 3$ either $p^2 - \mathrm{tr}(\mathcal{E}) + 1 = \#\mathcal{E}_{2,\Delta,s}(\mathbb{F}_{p^2})$ or $p^2 + \mathrm{tr}(\mathcal{E}) + 1 = \#\mathcal{E}'_{2,\Delta,s}(\mathbb{F}_{p^2})$ is divisible by 3. However, when $p \equiv 1 \pmod 3$ we can hope to find curves of order twice a prime whose twist also has order twice a prime.

Example 1. Let $p = 2^{80} - 93$ and $\Delta = 2$. For $s = 4556$, we find a twist-secure curve: $\#\mathcal{E}_{2,2,4556}(\mathbb{F}_{p^2}) = 2N$ and $\#\mathcal{E}'_{2,2,4556}(\mathbb{F}_{p^2}) = 2N'$ where

$$N = 730750818665451459101729015265709251634505119843 \quad \text{and}$$
$$N' = 730750818665451459101730957248125446994932083047$$

are 159-bit primes. Proposition 2 lets us replace 160-bit scalar multiplications in $\mathcal{E}_{2,2,4556}(\mathbb{F}_{p^2})$ and $\mathcal{E}'_{2,2,4556}(\mathbb{F}_{p^2})$ with 80-bit multiexponentiations.

Now, consider the degree-3 curves of §6. The order of $\mathcal{E}_{3,\Delta,s}(\mathbb{F}_{p^2})$ is always divisible by 3: the kernel of $\psi_{3,\Delta,s}$ is generated by the rational point $(3, C_{3,\Delta}(s))$. However, on the quadratic twist, the nontrivial points in the kernel of $\psi'_{3,\Delta,s}$ are *not* defined over $\mathbb{F}_{p^2}$ (they are conjugates over $\mathbb{F}_{p^2}$), so $\mathcal{E}'_{3,\Delta,s}(\mathbb{F}_{p^2})$ can have prime order.

Example 2. Let $p = 2^{127} - 1$; then $\Delta = -1$ is a nonsquare in $\mathbb{F}_p$. The parameter value $s = 122912611041315220011572494331480107107$ yields

$$\#\mathcal{E}_{3,-1,s}(\mathbb{F}_{p^2}) = 3 \cdot N \qquad \text{and} \qquad \#\mathcal{E}'_{3,-1,s}(\mathbb{F}_{p^2}) = N',$$

where N is a 253-bit prime and N' is a 254-bit prime. Using Proposition 2, any scalar multiplication in $\mathcal{E}_{3,-1,s}(\mathbb{F}_{p^2})$ or $\mathcal{E}'_{3,-1,s}(\mathbb{F}_{p^2})$ can be computed via a 127-bit multiexponentiation.

Example 3. Let $p = 2^{255} - 19$; then $\Delta = -2$ is a nonsquare in $\mathbb{F}_p$. The parameter $s =$ `0x7516D419C4937E5E8F0761FDB9BB0382FE20E9D0B7AB6924BA1DA02561C5145E` yields $\#\mathcal{E}_{3,-2,s}(\mathbb{F}_{p^2}) = 3 \cdot N$ and $\#\mathcal{E}_{3,-2,s}(\mathbb{F}_{p^2}) = N'$, where N and N' are 509- and 510-bit primes, respectively. Proposition 2 transforms any 510-bit scalar multiplication in $\mathcal{E}_{3,-2,s}(\mathbb{F}_{p^2})$ or $\mathcal{E}'_{2,-2,s}(\mathbb{F}_{p^2})$ into a 255-bit multiexponentiation.

8 Montgomery, Twisted Edwards, and Doche–Icart–Kohel models

Montgomery models. The curve $\mathcal{E}_{2,\Delta,s}$ has a Montgomery model over $\mathbb{F}_{p^2}$ if and only if $2C_{2,\Delta}(s)$ is a square in $\mathbb{F}_{p^2}$ (by [22, Proposition 1]): in that case, setting

$$B_{2,\Delta}(s) := \sqrt{2C_{2,\Delta}(s)} \qquad \text{and} \qquad A_{2,\Delta}(s) = 12/B_{2,\Delta}(s),$$

the birational mapping $(x, y) \mapsto (X/Z, Y/Z) = \left((x-4)/B_{2,\Delta}(s), y/B_{2,\Delta}(s)^2\right)$ takes us from $\mathscr{E}_{2,\Delta,s}$ to the projective Montgomery model

$$\mathscr{E}^{\mathrm{M}}_{2,\Delta,s} : B_{2,\Delta}(s)Y^2 Z = X\left(X^2 + A_{2,\Delta}(s)XZ + Z^2\right). \tag{8.1}$$

(If $2C_{2,\Delta}(s)$ is not a square, then $\mathscr{E}^{\mathrm{M}}_{2,\Delta,s}$ is $\mathbb{F}_{p^2}$-isomorphic to the quadratic twist $\mathscr{E}'_{2,\Delta,s}$.) These models offer a particularly efficient arithmetic, where we use only the X and Z coordinates [20]. The endomorphism is defined (on the X and Z coordinates) by

$$\psi_{2,\Delta,s} : (X : Z) \longmapsto (X^{2p} + A_{2,\Delta}(s)^p X^p Z^p + Z^{2p} : -2B_{2,\Delta}(s)^{1-p} X^p Z^p).$$

Twisted Edwards models. Every Montgomery model corresponds to a twisted Edwards model (and vice versa) [2, 16]. With $u = X/Z$ and $v = Y/Z$, the birational maps

$$(u, v) \longmapsto (x_1, x_2) = \left(\frac{u}{v}, \frac{u-1}{u+1}\right) \qquad \text{and} \qquad (x_1, x_2) \longmapsto (u, v) = \left(\frac{1+x_2}{1-x_2}, \frac{1+x_2}{x_1(1-x_2)}\right)$$

take us between the Montgomery model of Eq. (8.1) and the twisted Edwards model

$$\mathscr{E}^{\mathrm{TE}}_{2,\Delta,s} : a_2(s)x_1^2 + x_2^2 = 1 + d_2(s)x_1^2 x_2^2, \quad \text{where} \quad \begin{cases} a_2(s) & = (A_{2,\Delta}(s)+2)/B_{2,\Delta}(s) \\ d_2(s) & = (A_{2,\Delta}(s)-2)/B_{2,\Delta}(s). \end{cases}$$

Doche–Icart–Kohel models. Doubling-oriented Doche–Icart–Kohel models of elliptic curves are defined by equations of the form

$$y^2 = x(x^2 + Dx + 16D).$$

These curves have a rational 2-isogeny ϕ, with kernel $\langle (0,0) \rangle$; in this form, we can double more quickly by using the decomposition $[2] = \phi^\dagger \phi$ (see [7, §3.1] for details).

Our curves $\mathscr{E}_{2,\Delta,s}$ come equipped with a rational 2-isogeny, so it is natural to try putting them in Doche–Icart–Kohel form. The isomorphism

$$\alpha : (x, y) \longmapsto (u, v) = \left(\mu^2(x+4), \mu^3 y\right) \quad \text{with} \quad \mu = 4\sqrt{6/C_{2,\Delta}(s)}$$

takes us from $\mathscr{E}_{2,\Delta,s}$ into a doubling-oriented Doche–Icart–Kohel model

$$\mathscr{E}^{\mathrm{DIK}}_{2,\Delta,s} : v^2 = u\left(u^2 + D_{2,\Delta}(s)u + 16D_{2,\Delta}(s)\right), \quad \text{where} \quad D_{2,\Delta}(s) = 2^7/(1 + s\sqrt{\Delta}).$$

While $\mathscr{E}^{\mathrm{DIK}}_{2,\Delta,s}$ is defined over $\mathbb{F}_{p^2}$, the isomorphism is only defined over $\mathbb{F}_{p^2}(\sqrt{1+s\sqrt{\Delta}})$; so if $1 + s\sqrt{\Delta}$ is not a square in $\mathbb{F}_{p^2}$ then $\mathscr{E}^{\mathrm{DIK}}_{2,\Delta,s}$ is $\mathbb{F}_{p^2}$-isomorphic to $\mathscr{E}'_{2,\Delta,s}$.

The endomorphism $\psi^{\mathrm{DIK}}_{2,\Delta,s} := \alpha\psi_{2,\Delta,s}\alpha^{-1}$ is $\overline{\mathbb{F}}_p$-isomorphic to the Doche–Icart–Kohel isogeny, since they have the same kernel. The eigenvalue of $\psi_{2,\Delta,s}$ on cryptographic subgroups is $\pm\sqrt{\pm 2}$, so computing $[m]P$ as $[a]P + [b]\psi^{\mathrm{DIK}}_{2,\Delta,s}$ with Doche–Icart–Kohel doubling for $[a]$ and $[b]$ is like using a $\sqrt{\pm 2}$-adic expansion of m.

Similarly, we can exploit the rational 3-isogeny on $\mathscr{E}_{3,\Delta,s}$ for Doche–Icart–Kohel tripling (see [7, §3.2]). The isomorphism $(x, y) \mapsto (u, v) = \left(a_{3,\Delta}(s)(x/3 - 1), b_{3,\Delta}(s)^3 y\right)$, with $a_{3,\Delta}(s) = 9/C_{3,\Delta}(s)$ and $b_{3,\Delta}(s) = a_{3,\Delta}(s)^{-1/2}$, takes us from $\mathscr{E}_{3,\Delta,s}$ to the tripling-oriented Doche–Icart-Kohel model

$$\mathscr{E}^{\mathrm{DIK}}_{3,\Delta,s} : v^2 = u^3 + 3a_{3,\Delta}(s)(u+1)^2.$$

9 Degree one: GLS as a degenerate case

Returning to the framework of §3, suppose $\widetilde{\mathscr{E}}$ is a curve defined over $\mathbb{Q}$, and base-extended to $\mathbb{Q}(\sqrt{D})$: then $\widetilde{\mathscr{E}} = {}^{\sigma}\widetilde{\mathscr{E}}$, and we can apply the construction of §3 taking $\widetilde{\phi} : \widetilde{\mathscr{E}} \to {}^{\sigma}\widetilde{\mathscr{E}}$ to be the identity map. Reducing modulo an inert prime p, the endomorphism ψ is nothing but π_0 (which is an endomorphism, since $\mathscr{E}$ is a subfield curve). We have $\psi^2 = \pi_0^2 = \pi_{\mathscr{E}}$, so the eigenvalue of ψ is ± 1 on cryptographic subgroups of $\mathscr{E}(\mathbb{F}_{p^2})$. Clearly, this endomorphism is of no use to us for scalar decompositions.

However, looking at the quadratic twist $\mathscr{E}'$, the twisted endomorphism ψ' satisfies $(\psi')^2 = -\pi_{\mathscr{E}'}$; the eigenvalue of ψ' on cryptographic subgroups is a square root of -1. We have recovered the Galbraith–Lin–Scott endomorphism (cf. [12, Theorem 2]).

More generally, suppose $\widetilde{\phi} : \widetilde{\mathscr{E}} \to {}^{\sigma}\widetilde{\mathscr{E}}$ is a $\overline{\mathbb{Q}}$-isomorphism: that is, an isogeny of degree 1. If $\widetilde{\mathscr{E}}$ does not have CM, then ${}^{\sigma}\widetilde{\phi} = \epsilon_p \widetilde{\phi}^{-1}$, so $\psi^2 = [\epsilon_p]\pi_{\mathscr{E}}$ with $\epsilon_p = \pm 1$. This situation is isomorphic to GLS. In fact, $\widetilde{\mathscr{E}} \cong {}^{\sigma}\widetilde{\mathscr{E}}$ implies $j(\widetilde{\mathscr{E}}) = j({}^{\sigma}\widetilde{\mathscr{E}}) = {}^{\sigma}j(\widetilde{\mathscr{E}})$, so $j(\widetilde{\mathscr{E}})$ is in $\mathbb{Q}$, and $\widetilde{\mathscr{E}}$ is isomorphic to (or a quadratic twist of) a curve defined over $\mathbb{Q}$. We note that in the case $d = 1$, we have $r = \pm t_0$ in Proposition 1, and the basis constructed in the proof of Proposition 2 is (up to sign) the same as the basis of [12, Lemma 3].

While $\mathscr{E}'(\mathbb{F}_{p^2})$ may have prime order, $\mathscr{E}(\mathbb{F}_{p^2})$ cannot: the points fixed by π_0 form a subgroup of order $p + 1 - t_0$, where $t_0^2 - 2p = \mathrm{tr}(\mathscr{E})$ (the complementary subgroup, where π_0 has eigenvalue -1, has order $p+1+t_0$). We see that the largest prime divisor of $\#\mathscr{E}(\mathbb{F}_{p^2})$ can be no larger than $O(p)$. If we are in a position to apply the Fouque–Lercier–Réal–Valette fault attack [10]—for example, if Montgomery ladders are used for scalar multiplication and multiexponentiation—then we can solve DLP instances in $\mathscr{E}'(\mathbb{F}_{p^2})$ in $O(p^{1/2})$ group operations (in the worst case!). While $O(p^{1/2})$ is still exponentially difficult, it falls far short of the ideal $O(p)$ for general curves over $\mathbb{F}_{p^2}$. GLS curves should therefore be avoided where the fault attack can be put into practice.

10 Higher degrees

We conclude with some brief remarks on $\mathbb{Q}$-curves of other small degrees. Hasegawa provides a universal curve for $d = 7$ (and any Δ) in [15, Theorem 2.2], and our results for $d = 2$ and $d = 3$ carry over to $d = 7$ in an identical fashion, though the endomorphism is slightly less efficient in this case (its defining polynomials are sextic).

For $d = 5$, Hasegawa notes that it is impossible to give a universal $\mathbb{Q}$-curve for every discriminant Δ: there exists a quadratic $\mathbb{Q}$-curve of degree 5 over $\mathbb{Q}(\sqrt{\Delta})$ if and only if $\left(5/p_i\right) = 1$ for every prime $p_i \neq 5$ dividing Δ [15, Proposition 2.3]. But this is no problem when reducing modulo p, if we are prepared to give up the freedom of choosing Δ: we could take $\Delta = -11$ for $p \equiv 1 \pmod 4$ and $\Delta = -1$ for $p \equiv 3 \pmod 4$, and then use the curves defined in [15, Table 6].

Composite degree $\mathbb{Q}$-curves (such as $d = 6$ and 10) promise more interesting results, as do exceptional CM specializations of the universal curves; we will return to these cases in future work. Degrees greater than 10 yield less efficient endomorphisms, and so are less interesting from a practical point of view.

Acknowledgements The author thanks François Morain and David Gruenewald for their comments.

References

1. L. Babai, *On Lovasz' lattice reduction and the nearest lattice point problem.* Combinatorica **6** (1986) 1–13
2. D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, *Twisted Edwards curves.* In S. Vaudenay (ed.), *AFRICACRYPT 2008.* Lecture Notes in Comput. Sci. **5023** (2008) 389–405
3. J. W. Bos, C. Costello, H. Hisil, and K. Lauter, *Fast cryptography in genus 2.* In T. Johansson and P. Q. Nguyen (eds), *Advances in cryptology – EUROCRYPT 2013*, Lecture Notes in Comput. Sci. **7881** (2013) 194–210
4. W. Bosma, J. J. Cannon, C. Fieker, and A. Steel (eds), *Handbook of Magma functions.* Edition 2.19 (2013)
5. H. Cohen and G. Frey (eds), *Handbook of elliptic and hyperelliptic curve cryptography.* Chapman & Hall / CRC (2006)
6. J. Cremona, J. C. Lario, J. Quer, and K. Ribet (eds), *Modular Curves and Abelian Varieties.* Birkhäuser, Basel (2004)
7. C. Doche, T. Icart, and D. R. Kohel, *Efficient scalar multiplication by isogeny decompositions.* In M. Yung, Y. Dodis, A. Kiayias, and T. Malkin (eds), *Public Key Cryptography 2006*, Lecture Notes in Comput. Sci **3958** (2006) 191–206
8. N. D. Elkies, *On elliptic k-curves.* In [6], pp. 81–92
9. J. S. Ellenberg, *$\mathbb{Q}$-curves and Galois representations.* In [6], pp. 93–103
10. P.-A. Fouque, R. Lercier, D. Réal, and F. Valette, *Fault attack on elliptic curve with Montgomery ladder.* FDTC '08, IEEE-CS (2008) 92–98
11. S. D. Galbraith, *Mathematics of public key cryptography.* Cambridge University Press (2012)
12. S. D. Galbraith, X. Lin, and M. Scott, *Endomorphisms for faster elliptic curve cryptography on a large class of curves.* J. Crypt. **24** #3 (2011) 446–469
13. R. P. Gallant, R. J. Lambert, and S. A. Vanstone, *Faster point multiplication on elliptic curves with efficient endomorphisms.* In J. Kilian (ed.), Advances in Cryptology: CRYPTO 2001, Lecture Notes in Comput. Sci. **2139** (2001) 190–200
14. J. Gonzalez, *Isogenies of polyquadratic $\mathbb{Q}$-curves to their Galois conjugates.* Arch. Math. **77** (2001) 383–90
15. Y. Hasegawa, *$\mathbb{Q}$-curves over quadratic fields.* Manuscripta Math. **94** #1 (1997) 347–64
16. H. Hisil, K. Wong, G. Carter, and E. Dawson, *Twisted Edwards curves revisited.* In J. Pieprzyk (ed.), *Advances in Cryptology — ASIACRYPT 2008*, Lecture Notes in Comput. Sci **5350** (2008) 326–343
17. D. R. Kohel and B. Smith, *Efficiently computable endomorphisms for hyperelliptic curves.* In F. Hess, S. Pauli, and M. Pohst (eds), *Algorithmic number theory: ANTS-VII*, Lecture Notes in Comput. Sci. **4076** (2006) 495–509
18. P. Longa and F. Sica, *Four-dimensional Gallant–Lambert–Vanstone scalar multiplication.* In X. Wang and K. Sako (eds), *Advances in Cryptology – ASIACRYPT 2012.* Lecture Notes in Comput. Sci. **7658** (2012) 718–739 . Full version: http://eprint.iacr.org/2011/608
19. The Magma computational algebra system. http://magma.maths.usyd.edu.au/
20. P. L. Montgomery, *Speeding the Pollard and Elliptic Curve Methods of factorization.* Math. Comp. **48** #177 (1987) 243–264
21. A. Menezes, T. Okamoto, and S. A. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field.* IEEE Trans. Inform. Theory **39** #5 (1993) 1639–46

22. K. Okeya, H. Kurumatani, and K. Sakurai, *Elliptic curves with the Montgomery-form and their cryptographic applications.* In H. Imai and Y. Zheng (eds), *Public Key Cryptography: PKC 2000*, Lecture Notes in Comput. Sci. **1751** (2000) 238–57
23. R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*. Math. Comp. **44** (1985) 745–63
24. F. Sica, M. Ciet, and J.-J. Quisquater, *Analysis of the Gallant-Lambert-Vanstone method based on efficient endomorphisms: Elliptic and hyperelliptic curves.* In K. Nyberg and H. M. Heys (eds), *Selected Areas in Cryptography: SAC 2002*, Lecture Notes in Comput. Sci. **2595** (2003) 21–36
25. J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. **106** (2e), Springer (2009)
26. E. G. Straus, *Addition chains of vectors.* Amer. Math. Monthly **71** #7 (1964) 806–8
27. K. Takashima, *A new type of fast endomorphisms on Jacobians of hyperelliptic curves and their cryptographic application.* IEICE Trans. Fundamentals **E89-A** #1 (2006) 124–133
28. J. Vélu, *Isogénies entre courbes elliptiques.* C. R. Math. Acad. Sci. Paris **273** (1971) 238–41
29. E. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems.* J. Crypt. **17** (2004) 277–96
30. Z. Zhou, Z. Hu, M. Xu, and W. Song, *Efficient 3-dimensional GLV method for faster point multiplication on some GLS elliptic curves.* Inf. Proc. Lett. **110** #22 (2010) 1003–1006