© de Gruyter 2009
J. Math. Crypt. **3** (2009), 1–18 DOI 10.1515 / JMC.2009.001

Distortion maps for supersingular genus two curves

Steven D. Galbraith, Jordi Pujolàs, Christophe Ritzenthaler and Benjamin Smith

Communicated by Hugh Williams

Abstract. Distortion maps are a useful tool for pairing based cryptography. Compared with elliptic curves, the case of hyperelliptic curves of genus $g > 1$ is more complicated, since the full torsion subgroup has rank $2g$. In this paper, we prove that distortion maps always exist for supersingular curves of genus $g > 1$. We also give several examples of curves of genus 2 with explicit distortion maps for embedding degrees 4, 5, 6, and 12.

Keywords. Hyperelliptic curve cryptography, pairings, supersingular curves, distortion maps.

AMS classification. 11G20 (Primary), 11G15, 11T71, 14G50, 14K02 (Secondary).

1 Introduction

Let C be a nonsingular, geometrically irreducible, projective curve over $\mathbb{F}_q$, where q is a power of a prime p. The Jacobian variety of C is denoted by $\mathrm{Jac}(C)$, and the q-power Frobenius map is denoted by π; we identify $\mathrm{Jac}(C)(\mathbb{F}_{q^n})$ with the degree zero divisor class group of C over $\mathbb{F}_{q^n}$ for each $n > 0$. Let r be a prime dividing $\#\mathrm{Jac}(C)(\mathbb{F}_q)$ and coprime to p. We define the *embedding degree* to be the smallest positive integer k such that r divides $q^k - 1$; note that $\mathbb{F}_{q^k}$ is the field generated over $\mathbb{F}_q$ by adjoining the group μ_r of r^{th} roots of unity in $\overline{\mathbb{F}}_q$. Throughout,

$$e_r : \mathrm{Jac}(C)[r] \times \mathrm{Jac}(C)[r] \to \mu_r \subset \mathbb{F}_{q^k}^*$$

denotes a non-degenerate, bilinear, and Galois-invariant pairing on $\mathrm{Jac}(C)[r]$, such as the Weil pairing or the reduced Tate pairing; we refer the reader to [1, 2, 8, 7, 16, 17] for details on pairings and pairing-based cryptography.

An elliptic curve E over $\mathbb{F}_q$ is *supersingular* if $\#E(\mathbb{F}_q)$ is congruent to 1 modulo p. If E is a supersingular elliptic curve, then $\mathrm{End}(E)$ is an order in a quaternion algebra.[1] More generally, an abelian variety A of dimension g over $\mathbb{F}_q$ is supersingular if it is isogenous over $\overline{\mathbb{F}}_q$ to a product E^g, where E is a supersingular elliptic curve; in this case, $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a $\mathbb{Q}$-algebra of dimension $(2g)^2$ as a $\mathbb{Q}$-vector space. Finally, a curve C is supersingular if $\mathrm{Jac}(C)$ is a supersingular abelian variety. When $\mathrm{Jac}(C)$ is supersingular, the embedding degree k is bounded above by a constant $k(g)$ depending only on the genus g of C (see [8, 19]).

[1] If A is an abelian variety, then $\mathrm{End}_K(A)$ denotes the ring of endomorphisms of A defined over a field K, and $\mathrm{End}(A)$ the ring of endomorphisms of A defined over an algebraic closure of K. Unless otherwise noted, all morphisms are defined over the algebraic closure of the base field.

Bilinearity is an important property of pairings in cryptography: for all integers a and b and elements D_1 and D_2 of $\mathrm{Jac}(C)[r]$, we have $e_r(aD_1, bD_2) = e_r(D_1, D_2)^{ab}$. For bilinearity to be useful, however, it is necessary to have $e_r(D_1, D_2) \neq 1$. The Weil and Tate pairings are non-degenerate: for each non-zero divisor class D_1 of order r, there is a divisor class D_2 such that $e_r(D_1, D_2) \neq 1$. A problem arises when one wants to pair two specific divisors D_1 and D_2 where $e_r(D_1, D_2) = 1$; this can happen, for example, when for efficiency reasons both divisors are defined over $\mathbb{F}_q$ and $k > 1$. In these situations we need distortion maps.

Definition 1.1. A *distortion map* for a non-degenerate pairing e_r and non-zero divisor classes D_1, D_2 of prime order r on C is an endomorphism ψ of $\mathrm{Jac}(C)$ such that $e_r(D_1, \psi(D_2)) \neq 1$.

Distortion maps were introduced by Verheul [29] for elliptic curves in the case where the divisors D_1 and D_2 are defined over the ground field. We stress that our definition depends on the choice of divisor classes, and also on the pairing. In general, there is no single choice of ψ that is a distortion map for all pairs of divisor classes on C.

The goal of this paper is to provide, for certain supersingular curves, a collection of efficiently computable endomorphisms such that there is a suitable distortion map in the collection for any pair of non-zero divisor classes on the curves. Note that the Frobenius or trace maps may be used as distortion maps for some pairs of divisor classes, even on ordinary curves. However, to be able to handle all possible pairs of non-zero divisor classes one needs extra endomorphisms, and it seems to be necessary to restrict to supersingular curves to present general results.

The problem of finding distortion maps for elliptic curves is relatively easy to handle: if D_1 and D_2 are nonzero divisor classes on an elliptic curve and $e_r(D_1, D_2) = 1$, then any divisor D_3 of order r that is independent of D_2 (that is, $\langle D_2 \rangle \cap \langle D_3 \rangle = \{0\}$) satisfies $e_r(D_1, D_3) \neq 1$. This follows from the non-degeneracy of the pairing, and the fact that the r-torsion of an elliptic curve has rank 2. An algorithm to find distortion maps for any supersingular elliptic curve has been given by Galbraith and Rotger [10].[2]

In this paper we discuss the situation for $g > 1$, with particular emphasis on curves of genus 2. For curves C of genus $g > 1$, the r-torsion of the Jacobian has rank $2g$, so independent divisors may have a trivial pairing. Indeed, elementary linear algebra implies that for every non-trivial divisor D of order r, there exists a basis for $\mathrm{Jac}(C)[r]$ such that D pairs trivially with all but one of the basis elements.

In Section 2, we prove that distortion maps always exist for supersingular abelian varieties. However, existence of distortion maps is not sufficient for cryptographic applications: we also need explicit descriptions of distortion maps, so that they can be computed in practice. Elements of $\mathrm{End}(\mathrm{Jac}(C))$ are more complicated to handle than endomorphisms of an elliptic curve, as they generally do not correspond to maps from C to itself. Ideally, we would like an algorithm to construct distortion maps for any given supersingular abelian variety, but this seems to be completely out of reach. The best we can currently achieve is to work on a case-by-case basis. The main

[2] Note that there is a missing condition in Lemma 5.1 of [10], which should require that $\psi(P) \neq 0$. Since the degree of ψ in [10] is d, which is much smaller than r, this condition is always satisfied in the applications.

contribution of this paper, therefore, is to give sets of distortion maps for genus 2 curves which are potentially useful in practice.

In Section 3, we provide a list of examples of supersingular curves with suitable embedding degrees. We explore each example in depth in the subsequent sections, providing non-trivial, efficient, explicit distortion maps. Section 4 presents distortion maps for curves with $k = 4$ obtained by reduction of CM curves over $\mathbb{Q}$. Section 5 deals with the cases $k = 5$, which only arises when $p = 5$, and $k = 6$ which occurs for all $p \equiv 2 \mod 3$. Section 5.3 gives a construction for curves with $k = 6$ when $p \equiv 2 \pmod 3$ (and $p \neq 2$). This is one of our main results: while the existence of supersingular abelian varieties with $k = 6$ was proven by Rubin and Silverberg [19], an explicit construction for these abelian varieties as Jacobians of curves has not previously appeared in the literature. Finally, Section 6 treats the case $k = 12$ in characteristic $p = 2$.

Our results for $k = 4$ and $k = 12$ are conditional: they depend on the assumption (verified in practice) that some denominators can be canceled, which is the case if they are prime to r. Subsequently, Takashima [23] has obtained unconditional results for some of these curves. In these cases, there seems to be no straightforward explicit decomposition of $\mathrm{Jac}(C)$: even when we know that the Jacobian is isogenous to a product $E \times E$, the degrees of the induced morphisms from C to E are unknown. For $k = 5$ and $k = 6$, our results are unconditional. In these cases, our curves are twists of $y^2 = x^6 + 1$, which has two degree-2 maps to an elliptic curve E. We use this structure to avoid the assumption on the denominators.

2 The existence of distortion maps

We begin by showing that distortion maps always exist for supersingular abelian varieties. This generalizes the work of Schoof and Verheul [30] on supersingular elliptic curves.

First, we recall an important theorem of Tate [24]. Suppose A is an abelian variety over a finite field K of characteristic p, and let $G = \mathrm{Gal}(\overline{K}/K)$. Choose a prime $l \neq p$, and let $T_l(A) := \varprojlim A[l^n]$ be the l-Tate module of A. Let $\mathrm{End}_G(T_l(A))$ be the ring of endomorphisms of $T_l(A)$ commuting with the action of G. Tate's theorem states that the canonical injection

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_l \longrightarrow \mathrm{End}_G(T_l(A))$$

is an isomorphism.

Theorem 2.1. *Let A be a g-dimensional supersingular abelian variety over $\mathbb{F}_q$, and let r be a prime not dividing q. For every two non-trivial elements D_1 and D_2 of $A[r]$, there exists an endomorphism ϕ of A such that $e_r(D_1, \phi(D_2)) \neq 1$.*

Proof. Let d be an integer such that the q^d-power Frobenius map acts as an integer multiplication on A. Let $K = \mathbb{F}_{q^d}$ and $G = \mathrm{Gal}(\overline{K}/K)$. By definition, $\mathrm{End}_K(A)$ is contained in $\mathrm{End}(A)$, so we may view $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_r$ as a submodule of $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_r$. By Tate's theorem, $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_r$ is isomorphic to the $\mathbb{Z}_r$-module $\mathrm{End}_G(T_r(A))$ of

endomorphisms commuting with the q^d-power Frobenius — but the q^d-power Frobenius is an integer, so it commutes with every endomorphism of A (and $T_r(A)$). Thus $\mathrm{End}_G(T_r(A)) = \mathrm{End}(T_r(A))$. Since $T_r(A) \cong \mathbb{Z}_r^{2g}$ as a $\mathbb{Z}_r$-module, we have

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_r \cong \mathrm{End}_G(T_r(A)) \cong M_{2g}(\mathbb{Z}_r).$$

Hence $\mathrm{End}_K(A) \cong \mathrm{End}(A)$ also has rank $(2g)^2$. By reduction,

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}/r\mathbb{Z} \cong M_{2g}(\mathbb{Z}/r\mathbb{Z}).$$

Let D_3 be an element of $A[r]$ such that $e_r(D_1, D_3) \neq 1$. There exists some matrix Φ in $M_{2g}(\mathbb{Z}/r\mathbb{Z})$ corresponding to a mapping of the subspace $\langle D_2 \rangle$ into $\langle D_3 \rangle$. Let ϕ be a preimage in $\mathrm{End}(A)$ of Φ: by construction, $e_r(D_1, \phi(D_2)) \neq 1$. □

Remark 2.2. It is important to note that the proof of Theorem 2.1 is not constructive: in practice it is not feasible to construct an element of $\mathrm{End}(A)$ given a corresponding matrix in $M_{2g}(\mathbb{Z}/r\mathbb{Z})$.

3 Embedding degrees of supersingular genus 2 curves

In this section we list some supersingular genus 2 curves which are of potential interest for applications. First, we recall the results of Rubin and Silverberg [19] classifying the possible embedding degrees for simple supersingular abelian varieties of dimension 2. We focus on the case where q is an odd power of p: this gives the largest values for k, and so is usually the most interesting case in practice.

Theorem 3.1 (Rubin–Silverberg [19]). *Let q be an odd power of a prime p. The precise set of possible embedding degrees for simple supersingular abelian surfaces over $\mathbb{F}_q$ is given in the following table.*

p	*Possible embedding degrees k*
2	$\{1, 3, 6, 12\}$
3	$\{1, 3, 4\}$
5	$\{1, 3, 4, 5, 6\}$
≥ 7	$\{1, 3, 4, 6\}$

We note that other embedding degrees, such as $k = 2$, may be realised using non-simple abelian surfaces. Since large embeddings degrees are of the most interest, we focus on the cases $k = 4$, 5, 6, and 12. Our examples are briefly described below.

$k = 4$: The curve $y^2 = x^5 + A$ over $\mathbb{F}_p$ where $p > 2$ and $p \equiv 2, 3 \pmod 5$ is supersingular, and has embedding degree 4. More generally, reductions modulo certain primes of each of the CM curves listed by van Wamelen [27] have embedding degree 4. We discuss these curves in Section 4.

$k = 5$: The curves $y^2 = x^5 - x \pm 1$ where $p = 5$, described by Duursma and Sakurai [6], are supersingular and have embedding degree 5. We discuss these curves in Section 5.2.

$k = 6$: An abelian variety over $\mathbb{F}_q$ has embedding degree 6 if the characteristic polynomial of its Frobenius endomorphism is $T^4 - qT^2 + q^2$. A result of Howe, Maisner, Nart, and Ritzenthaler [12, Theorem 1] implies that these abelian varieties have a principal polarisation if and only if $p \not\equiv 1 \pmod 3$. Hence, Jacobians of curves of genus 2 can have embedding degree 6 only when $p \not\equiv 1 \pmod 3$. In Section 5.3, we give an algorithm to construct supersingular curves with embedding degree 6 when $p \equiv 2 \pmod 3$ and $p \geq 5$, by taking suitable twists of the curve $y^2 = x^6 + 1$.

$k = 12$: The curves $y^2 + y = x^5 + x^3 + b$ over $\mathbb{F}_{2^m}$ where $b = 0, 1$ are supersingular, with embedding degree 12. We discuss these curves in Section 6.

4 Curves with embedding degree 4

Let p be a prime, and let $C/\mathbb{F}_p$ be a curve of genus $g \geq 1$ such that $\mathrm{End}(\mathrm{Jac}(C))$ contains an automorphism α which generates a CM-field $F = \mathbb{Q}(\alpha)$ of degree $2g$ over $\mathbb{Q}$. We denote by π the p-power Frobenius map of $\mathrm{Jac}(C)$ and let σ denote the topological generator of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ defined by $\sigma(x) = x^p$. One has for all integer j, $\pi^j \alpha = \alpha^{\sigma^j} \pi^j$.

Given endomorphisms $\alpha_1, \ldots, \alpha_n$ of $\mathrm{Jac}(C)$, we let $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ denote the subring of $\mathrm{End}(\mathrm{Jac}(C))$ generated by the α_i. Similarly, we let $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ denote the $\mathbb{Q}$-algebra $\mathbb{Z}[\alpha_1, \ldots, \alpha_n] \otimes_{\mathbb{Z}} \mathbb{Q}$. Since $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ is a finitely generated $\mathbb{Z}$-module, $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ is a finite dimensional $\mathbb{Q}$-vector space. In general, neither $\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$ nor $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ is commutative.

Proposition 4.1. *Let C and F be as above. Let assume that there exists a generator α of $F/\mathbb{Q}$ whose minimal field of definition is $\mathbb{F}_{p^{2g}}$ and such that α commutes with α^σ. Then* $\mathrm{Jac}(C)$ *is supersingular, and*

$$\mathrm{End}^0(\mathrm{Jac}(C)) = \mathbb{Q}[\pi, \alpha] = \left\{ \sum_{0 \leq i,j \leq 2g-1} \lambda_{i,j} \pi^i \alpha^j : \lambda_{i,j} \in \mathbb{Q} \right\}.$$

Proof. We will first show that for all j, $\alpha^{\sigma^j} \in F$. By assumption α^σ commutes with α and so with any element of F. By [14, Theorem 3.1], since the degree of F is $2g$, it is its own commutant in $\mathrm{End}^0(\mathrm{Jac}(C))$ so $\alpha^\sigma \in F$. By induction we can assume that α^{σ^j} is in F. Clearly α^{σ^j} is a generator of F and $\alpha^{\sigma^{j+1}}$ commutes with α^{σ^j}. Hence $\alpha^{\sigma^{j+1}}$ belongs to F.

We will now show that as a $\mathbb{Q}$-vector space, $\mathbb{Q}[\pi, \alpha]$ has a direct sum decomposition

$$\mathbb{Q}[\pi, \alpha] = \mathbb{Q}(\alpha) \oplus \pi\mathbb{Q}(\alpha) \oplus \pi^2\mathbb{Q}(\alpha) \oplus \ldots \oplus \pi^{2g-1}Q(\alpha).$$

We will prove by induction that the sum $\bigoplus_{i=0}^{t} \pi^i \mathbb{Q}(\alpha)$ is direct for each $0 \leq t \leq 2g-1$. The case $t = 0$ is trivial. For the inductive step, assume $U_n = \bigoplus_{i=0}^{n} \pi^i \mathbb{Q}(\alpha)$ is direct for $0 \leq n \leq 2g-2$; we will show that $U_n \cap \pi^{n+1}\mathbb{Q}(\alpha) = \{0\}$. Suppose the contrary: then there exists a non-zero z in $\mathbb{Q}(\alpha)$ such that $\pi^{n+1} z$ is in U_n. Dividing by z, we

write $\pi^{n+1} = z_0 + \pi z_1 + \cdots + \pi^n z_n$, with coefficients z_i in $\mathbb{Q}(\alpha)$ for $0 \leq i \leq n$, and with at least one of the z_i not zero. Let us write

$$\begin{aligned} 0 &= \pi^{n+1}\alpha - \alpha^{\sigma^{n+1}}\pi^{n+1} \\ &= (z_0 + \pi z_1 + \cdots + \pi^n z_n)\,\alpha - \alpha^{\sigma^{n+1}}(z_0 + \pi z_1 + \cdots + \pi^n z_n) \\ &= z_0\alpha + \pi z_1\alpha + \cdots + \pi^n z_n\alpha - z_0\alpha^{\sigma^{n+1}} - \pi z_1\alpha^{\sigma^n} - \cdots - \pi^n z_n\alpha^{\sigma} \\ &= z_0(\alpha - \alpha^{\sigma^{n+1}}) + \pi z_1(\alpha - \alpha^{\sigma^n}) + \cdots + \pi^n z_n(\alpha - \alpha^{\sigma}). \end{aligned}$$

Since α is only defined on $\mathbb{F}_{p^{2g}}$, $\alpha^{\sigma^j} \neq \alpha$ for $1 \leq j \leq 2g-1$; Now U_n is a direct sum, therefore all of the coefficients z_j must be zero, which is a contradiction.

We see that $\mathbb{Q}[\pi, \alpha]$ is a direct sum of $2g$ $\mathbb{Q}$-vector spaces, each of dimension $2g$; it is therefore a $\mathbb{Q}$-vector space of dimension $(2g)^2$. A classical result of Tate [24, Theorem 2] then implies that

$$\mathrm{End}^0(\mathrm{Jac}(C)) = \mathbb{Q}[\pi, \alpha],$$

and that $\mathrm{Jac}(C)$ is supersingular. □

Suppose C is as in Proposition 4.1. Since $\mathrm{Jac}(C)$ is supersingular, for every pair (D_1, D_2) of non-trivial points of order r there exists a distortion map ϕ by Theorem 2.1: that is, an endomorphism ϕ such that $e_r(D_1, \phi(D_2)) \neq 1$. By Proposition 4.1, there exist rational numbers $\lambda_{i,j}$ such that $\phi = \sum_{i,j} \lambda_{i,j}\pi^i\alpha^j$ in $\mathbb{Q}[\pi, \alpha]$. Let m be the least common multiple of the denominators of the $\lambda_{i,j}$; the endomorphism $m\phi$ is an element of $\mathbb{Z}[\alpha, \pi]$.

Assumption 4.2. We assume that for every pair (D_1, D_2) of non-trivial points of order r on $\mathrm{Jac}(C)$, a distortion map ϕ may be chosen such that m and r are coprime, where m is as above.

Remark 4.3. It is instructive to consider the case where $\mathrm{Jac}(C)$ is a supersingular elliptic curve E. In this case, $\mathrm{End}(E)$ is a maximal order $\mathcal{O}$ in a quaternion algebra $\mathbb{Q}[\pi, \psi]$ where π is the q-power Frobenius and ψ is some other endomorphism. In most cryptographical applications E is constructed by the CM method, so $\psi^2 = -d$ for some relatively small positive integer d (see [10] for more details). Hence $\mathbb{Z}[\pi, \psi]$ is contained in $\mathcal{O}$, and Assumption 4.2 holds in this case when $r > d$.

Corollary 4.4. *Let p be a prime, and let $C/\mathbb{F}_p$ be a curve of genus $g \geq 1$. Assume that* $\mathrm{End}^0(\mathrm{Jac}(C))$ *contains a CM-field F of degree $2g$ generated by an element α whose minimal field of definition is $\mathbb{F}_{p^{2g}}$ and such that α and α^σ commute. If Assumption 4.2 holds, then for all pairs (D_1, D_2) of non-zero points of order r on* $\mathrm{Jac}(C)$ *and all non-degenerate pairings e_r there exists a distortion map of the form $\pi^i\alpha^j$ with $0 \leq i, j \leq 2g-1$.*

Proof. Theorem 2.1 shows that there exists an endomorphism ϕ that is a suitable distortion map for (D_1, D_2); Proposition 4.1 shows that ϕ is in $\mathbb{Q}[\alpha, \pi]$. Under Assumption 4.2, we may take an integer m prime to r such that $m\phi$ is in $\mathbb{Z}[\alpha, \pi]$ and

$$e_r(D_1, m\phi(D_2)) = e_r(D_1, \phi(D_2))^m \neq 1;$$

so $m\phi$ is also a distortion map for (D_1, D_2). Since $m\phi$ is an integer combination of the endomorphisms $\pi^i\alpha^j$, we must have $e_r(D_1, \pi^i\alpha^j(D_2)) \neq 1$ for some $0 \leq i, j \leq 2g-1$: otherwise, if all $e_r(D_1, \pi^i\alpha^j(D_2)) = 1$, then we would have $e_r(D_1, m\phi(D_2)) = 1$ by the linearity of the pairing. □

Now, we would like to have control over the embedding degree.

Proposition 4.5. *Let $\tilde{C}/\mathbb{Q}$ be a curve of genus $g \geq 1$ such that $\mathrm{End}^0(\mathrm{Jac}(\tilde{C}))$ contains a CM-field F of degree $2g$; let Φ be the type of F and let F' be the associated reflex field. If p is a prime which is inert in F', then $\mathrm{Jac}(\tilde{C})$ has good reduction at p and the characteristic polynomial of the p-power Frobenius endomorphism is*

$$P(T) = T^{2g} + p^g.$$

In particular, the embedding degree k of $\tilde{C}$ is $2g/t$, where t is an odd divisor of g.

Proof. Since p is not ramified, $\mathrm{Jac}(\tilde{C})$ indeed has good reduction at p ([14, §6 Theorem 6.1]). The rest of the proposition is the simplest case of [14, §6 Theorem 6.2]: with Lang's notation

$$T^{2g} \cdot P(1/T) = \det(I - R_l(\pi)T) = \prod_{\tau \in \mathcal{T}} \prod_{\mathfrak{p}|p} (1 - \alpha(\mathfrak{p})^\tau T^{f(\mathfrak{p})}),$$

where R_l is the representation on the l-adic Tate module of the reduction of $\mathrm{Jac}(\tilde{C})$ at p for some prime l not equal to p, $\mathcal{T}$ is a certain set of embeddings of F, α is a CM-character associated to $\mathrm{Jac}(\tilde{C})$ and F', and $\mathfrak{p}$ ranges over the primes over p in F'. Since the residue degree $f(\mathfrak{p})$ of $\mathfrak{p}$ is $2g$, we have $\mathfrak{p} = p$. Further, since $\deg(P) = 2g$ we have $\#\mathcal{T} = 1$, so

$$\det(I - R_l(\pi)T) = 1 - \alpha(p)^\tau T^{2g}.$$

The only possibility is $\det(I - R_l(\pi)T) = 1 + p^g T^{2g}$. It remains to determine the embedding degree for a prime r dividing $\#\mathrm{Jac}(C)(\mathbb{F}_p)$. Since r divides $P(1) = 1 + p^g$, it must divide $p^{2g} - 1$; so the embedding degree k is $2g/t$ where t is an odd divisor of g. □

Corollary 4.6. *Let $\tilde{C}/\mathbb{Q}$ be a curve of genus $g \geq 1$ such that $\mathrm{Jac}(\tilde{C})$ is absolutely simple, and such that $\mathrm{End}^0(\mathrm{Jac}(\tilde{C}))$ contains a Galois CM-field F of degree $2g$. If p is a prime which is inert in F, then $\mathrm{Jac}(\tilde{C})$ has good reduction at p and the characteristic polynomial of the Frobenius endomorphism π is*

$$P(T) = T^{2g} + p^g.$$

In particular, the embedding degree k of $\tilde{C}$ is $2g/t$, where t is an odd divisor of g.

Proof. We only need to prove that if F' is a reflex field associated to F then $F' = F$. Since $\mathrm{Jac}(\tilde{C})$ is absolutely simple and F is Galois, any type (F, Φ) is simple (also called primitive) by [14, §3 Theorem 3.5], and so $F' = F$ (see [21, Example II.8.4]). □

Remark 4.7. Note that while Proposition 4.5 and Corollary 4.6 are 'local', one needs to start from a CM curve over a number field to get a curve over a finite field with the stated properties. Consider for instance the elliptic curves $E : y^2 + y = x^3$ and $E' : y^2 + y = x^3 + x$ over $\mathbb{F}_2$. Both E and E' have j-invariant 0, so these curves are twists, and $\mathrm{End}^0(E) = \mathrm{End}^0(E')$. Both $\mathrm{End}^0(E)$ and $\mathrm{End}^0(E')$ contain the CM-field $\mathbb{Q}(\zeta_3)$, where ζ_3 is a primitive third root of unity. The prime 2 is inert in $\mathbb{Q}(\zeta_3)$, but the 2-power Frobenius has characteristic polynomial $T^2 + 2$ on E and $T^2 + 2T + 2$ on E'. This is because E is the reduction of a CM curve defined over $\mathbb{Q}$, while E' is not.

We now give an explicit example. The following proposition generalizes the example of the curve $y^2 = x^5 + 1$ over $\mathbb{F}_p$ where $p \equiv 2, 3 \pmod 5$; the results of this section in that case were first presented in [9].

Proposition 4.8. *Let g be a positive integer such that $2g + 1$ is prime, let p be an odd prime such that p is primitive modulo $2g + 1$, and let A be a nonzero element of $\mathbb{F}_p$. The curve $C : y^2 = x^{2g+1} + A$ is supersingular, and the characteristic polynomial of Frobenius on $\mathrm{Jac}(C)$ is $P(T) = T^{2g} + p^g$. Moreover, its embedding degree k is $2g$. In the case $g = 2$, we obtain $k = 4$. If Assumption 4.2 holds, then there exists a distortion map of the form $\pi^i\alpha^j$ with $0 \leq i, j \leq 2g - 1$, where α is the automorphism defined by $(x, y) \mapsto (\zeta_{2g+1}x, y)$, where ζ_{2g+1} is a primitive $(2g + 1)^{\text{th}}$ root of unity.*

Proof. The automorphism of $\mathrm{Jac}(C)$ induced by α generates the cyclotomic field F of degree $(2g+1)-1 = 2g$ contained in $\mathrm{End}^0(\mathrm{Jac}(C))$. Since p is a primitive root modulo $2g + 1$, both ζ_{2g+1} and α are defined over the minimal extension $\mathbb{F}_{p^{2g}}$. Moreover α and α^σ commute. Applying Corollary 4.4 under Assumption 4.2, we see that $\mathrm{Jac}(C)$ is supersingular, and that there exist distortion maps in the stated form. We now prove that $P(T) = T^{2g} + p^g$. Clearly C can be lifted to a curve $\tilde{C} : y^2 = x^{2g+1} + \tilde{A}$ over $\mathbb{Q}$ with CM by the same cyclotomic field F. The prime p is inert in F, since p is primitive modulo $2g + 1$. Therefore, to apply Corollary 4.6 we need only prove that $\mathrm{Jac}(\tilde{C})$ is absolutely simple. By [14, §3 Theorem 3.5], $\mathrm{Jac}(\tilde{C})$ is absolutely simple if F has a simple type; but this is shown in the last example of [14, p. 34]. We already know that the embedding degree divides $2g$. Since p is primitive modulo $2g + 1$, we have $p^g \equiv -1 \pmod{2g+1}$. Hence $2g + 1$ divides $\#\mathrm{Jac}(C)(\mathbb{F}_p)$, and the smallest integer k such that $p^k \equiv 1 \pmod{2g + 1}$ is $2g$. □

In the case $g = 2$, Proposition 4.8 considers the curve $C : y^2 = x^5 + A$ over $\mathbb{F}_p$. When $p > 2$ is a prime such that $p \equiv 2, 3 \pmod 5$, the curve C has embedding degree 4. Takashima shows in [23] that Assumption 4.2 holds in this case. Let D_1 be a nonzero element of $\mathrm{Jac}(C)$ of order r, defined over $\mathbb{F}_p$ (and hence fixed by π). It is easy to show that $e_r(D_1, \alpha^j(D_1)) \neq 1$ for some $1 \leq j \leq 3$; this supports the suggestion in [4] of using α as a distortion map. When implementing pairings, it is desirable to use denominator elimination techniques to improve efficiency (see [1]); to this end, the map α^j might be composed with a trace map (see Scott [20] for an example of this in the elliptic curve case).

In [27] and [28], van Wamelen describes the nineteen $\mathbb{C}$-isomorphism classes of curves of genus 2 over $\mathbb{Q}$ whose Jacobians have CM by the ring of integers of a CM-field. Each isomorphism class of curves is presented with a representative curve and

an explicit endomorphism $\tilde{\alpha}$ generating the CM-field (see [18] and [27]). Reducing modulo suitable inert primes we obtain curves over $\mathbb{F}_p$ with endomorphisms α defined over $\mathbb{F}_{p^4}$; using the result of [14, p. 119], the results of this section apply to these curves.

5 Curves with embedding degree 5 and 6

We now consider genus 2 curves over $\mathbb{F}_p$ with embedding degree 5 and 6. We show in §5.2 and §5.3 that one can obtain such curves as twists of the curve $C : y^2 = x^6 + 1$. To prove the existence of efficiently computable distortion maps it suffices to give a $\mathbb{Z}$-module basis for a sub-module of $\mathrm{End}(\mathrm{Jac}(C))$ of bounded index; we do this in §5.1.

5.1 The endomorphism ring of the Jacobian of the curve $y^2 = x^6 + 1$

Let p be a prime such that $p \equiv 2 \pmod 3$. Let E denote the elliptic curve $y^2 = x^3 + 1$ over $\mathbb{F}_p$, and let π_E denote its p-power Frobenius map. Let ζ_3 be a primitive cube root of unity in $\mathbb{F}_{p^2}$, and let ρ_3 be the automorphism $(x, y) \mapsto (\zeta_3 x, y)$ of E over $\mathbb{F}_{p^2}$.

Lemma 5.1. *With E, ρ_3, and π_E defined as above,*

(1) E is supersingular,

(2) the characteristic polynomial of π_E is $T^2 + p$, and

(3) $\mathbb{Z}[\pi_E, \rho_3]$ is an order of index 3 in $\mathrm{End}(E)$.

Proof. Observe that $\pi_E \circ \rho_3 \neq \rho_3 \circ \pi_E$ when $p \equiv 2 \pmod 3$, so $\mathrm{End}(E)$ is non-commutative; it follows that E is supersingular. The characteristic polynomial of π_E has the form $T^2 - tT + p$, where $-2\sqrt{p} \leq t \leq 2\sqrt{p}$; but p divides t because E is supersingular [22, Theorem V.3.1]. The only such t is 0, so the characteristic polynomial of Frobenius is $T^2 + p$. Since E is supersingular, $\mathrm{End}(E)$ is isomorphic to a maximal order of the quaternion algebra ramified at p and ∞; its discriminant is therefore p [31, Cor. 5.3]. Explicit calculation shows that $\mathbb{Z}[\pi_E, \rho_3]$ is an order of discriminant $3p$, and thus an order of index 3 in $\mathrm{End}(E)$. □

Let C be the curve $y^2 = x^6 + 1$ over $\mathbb{F}_p$; we let π_C denote the p-power Frobenius map on C, and also the induced endomorphism of $\mathrm{Jac}(C)$. Let $f : C \to E$ be the morphism defined by $f(x, y) = (x^2, y)$, and let $f' : C \to E$ be the morphism defined by $f'(x, y) = (1/x^2, y/x^3)$. We define homomorphisms

$$\begin{aligned} \mu : E \times E &\longrightarrow \mathrm{Jac}(C) \\ (P, Q) &\longmapsto f^*(P) + f'^*(Q) - 2D_\infty \end{aligned}$$

and

$$\begin{aligned} \tilde{\mu} : \mathrm{Jac}(C) &\longrightarrow E \times E \\ P + Q - D_\infty &\longmapsto (f_*(P) + f_*(Q), f'_*(P) + f'_*(Q)), \end{aligned}$$

where $D_\infty = (\infty^+) + (\infty^-)$ is the divisor at infinity on the desingularisation of C.

Observe that $\tilde{\mu} \circ \mu = [2]_{E\times E}$ and $\mu \circ \tilde{\mu} = [2]_{\mathrm{Jac}(C)}$, so μ and $\tilde{\mu}$ are $(2,2)$-isogenies. We can therefore define an injective (group) homomorphism

$$\begin{aligned} T : \mathrm{End}(\mathrm{Jac}(C)) &\longrightarrow \mathrm{End}(E \times E) \\ \psi &\longmapsto \tilde{\mu} \circ \psi \circ \mu. \end{aligned}$$

While T is not a ring homomorphism, one easily checks that

$$T(\psi)T(\psi') = 2T(\psi\psi')$$

for all endomorphisms ψ and ψ' in $\mathrm{End}(\mathrm{Jac}(C))$.

Since $\mathrm{Jac}(C)$ and $E \times E$ are isogenous, it follows from Lemma 5.1 that C is supersingular, and that the characteristic polynomial of π_C is $(T^2 + p)^2$ (and in particular, we have $\pi_C^2 = [-p]$). Let χ and ρ_6 denote the automorphisms of C (and the induced endomorphisms of $\mathrm{Jac}(C)$) defined by

$$\chi(x, y) = (1/x, y/x^3) \quad \text{and} \quad \rho_6(x, y) = (\zeta_6 x, y). \tag{5.1}$$

Let $A = \mathbb{Z}[\pi_C, \chi, \rho_6]$ denote the subring of $\mathrm{End}(\mathrm{Jac}(C))$ generated by π_C, χ, and ρ_6. We will compute an upper bound for the index of $T(A)$ in $\mathrm{End}(E\times E) = M_2(\mathrm{End}(E))$.

Lemma 5.2. *The images of π_C, χ, and ρ_6 in* $\mathrm{End}(E \times E)$ *are given by*

$$T(\pi_C) = 2\begin{pmatrix} \pi_E & 0 \\ 0 & \pi_E \end{pmatrix},\ T(\chi) = 2\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \textit{and} \quad T(\rho_6) = 2\begin{pmatrix} \rho_3 & 0 \\ 0 & -\rho_3^2 \end{pmatrix}.$$

Proof. We prove the result for ρ_6; the computations for π_C and χ are similar. Consider a point (x^2, y) on E. We have $f^*(x^2, y) = (x, y) + (-x, y) - D_\infty$ in $\mathrm{Jac}(C)$, and D_∞ is fixed by π_C, χ, and ρ_6, so

$$\rho_6 \circ f^*(x^2, y) = (\zeta_6 x, y) + (-\zeta_6 x, y) - D_\infty.$$

We have

$$\begin{aligned} (f_* \circ \rho_6 \circ f^*)(x^2, y) &= ((\zeta_6 x)^2, y) + ((-\zeta_6 x)^2, y) \\ &= 2(\zeta_3 x^2, y) \\ &= ([2] \circ \rho_3)(x^2, y), \end{aligned}$$

while

$$\begin{aligned} (f'_* \circ \rho_6 \circ f^*)(x^2, y) &= \left(1/(\zeta_6 x)^2, y/(\zeta_6 x)^3\right) + \left(1/(-\zeta_6 x)^2, y/(-\zeta_6 x)^3\right) \\ &= \left(1/(\zeta_3 x^2), -y/x^3\right) + \left(1/(\zeta_3 x^2), y/x^3\right) \\ &= 0. \end{aligned}$$

In the same way $f'^* \left(1/x^2, y/x^3\right) = (x, y) + (-x, -y)$, so

$$\begin{aligned} (f'_* \circ \rho_6 \circ f'^*) \left(1/x^2, y/x^3\right) &= \left(1/(\zeta_6 x)^2, y/(\zeta^6 x)^3\right) + \left(1/(-\zeta_6 x)^2, -y/(-\zeta^6 x)^3\right) \\ &= \left(1/(\zeta_3 x^2), -y/x^3\right) + \left(1/(\zeta_3 x^2), -y/x^3\right) \\ &= ([-2] \circ \rho_3^2) \left(1/x^2, y/x^3\right), \end{aligned}$$

while $(f_* \circ \rho_6 \circ f'^*) \left(1/x^2, y/x^3\right) = 0$. □

Theorem 5.3. *If C, π_C, χ, and ρ_6 are defined as above, then the index of $\mathbb{Z}[\pi_C, \chi, \rho_6]$ in* End(Jac(C)) *divides* $2^8 3^4$.

Proof. Using Lemma 5.2, we see that the images of $1+\rho_6^3$, $1-\rho_6^3$, $\chi+\chi\rho_6^3$ and $\chi-\chi\rho_6^3$ in End$(E \times E)$ are the "projectors"

$$4\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, 4\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, 4\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \text{ and } 4\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Composing with the images of π_C and ρ_6, we get

$$M_2(4\mathbb{Z}[\pi_E, \rho_3]) \subset T(A) \subset (M_2(\text{End}(E)).$$

Since $\mathbb{Z}[\pi_E, \rho_3]$ has index 3 in End(E), the index of $T(A)$ in $M_2(\text{End}(E))$ must divide $2^8 \cdot 3^4$. Suppose r is a prime different from p, 2 and 3. Following the proof of Theorem 2.1, by tensoring with $\mathbb{Z}/r\mathbb{Z}$ we get an isomorphism

$$T_r : \text{End}(\text{Jac}(C)) \otimes \mathbb{Z}/r\mathbb{Z} \xrightarrow{\sim} M_2(\text{End}(E)) \otimes \mathbb{Z}/r\mathbb{Z} \simeq M_4(\mathbb{Z}/r\mathbb{Z}),$$

and $T_r(A)$ is of index dividing $2^8 \cdot 3^4$ in $M_4(\mathbb{Z}/r\mathbb{Z})$. □

If D_1 and D_2 are non-zero points of Jac(C) of order r, then by Theorem 5.3 we can find a map Φ in $M_4(\mathbb{Z}/r\mathbb{Z})$ such that $e_r(D_1, \Phi(D_2)) \neq 1$. Hence there exists a ψ in A such that $2^8 3^4 \Phi = T_r(\psi)$, and

$$e_r(D_1, \psi(D_2)) = e_r(D_1, [2^8 3^4]\Phi(D_2)) = e_r(D_1, \Phi(D_2))^{2^8 3^4} \neq 1.$$

Remark 5.4. Applying the construction of [11, p. 12] with the group-scheme isomorphism $\eta : E[2] \to E[2]$ mapping $(-1, 0)$ to itself and $(\zeta_6, 0)$ to $(1/\zeta_6, 0)$, we see that Jac$(C) \cong (E \times E)/\text{Graph}(\eta)$. Moreover, if λ is the canonical polarization on Jac(C) and $\lambda_{E\times E}$ is the split polarization on $E \times E$, then $\lambda_{E\times E} = \hat{\mu}(2\lambda)\mu$. Therefore, if D_1 and D_2 are elements of Jac$(C)[r]$, then

$$\begin{aligned} e_r^{\lambda}(D_1, D_2)^8 &= e_r^{2\lambda}(2D_1, 2D_2) \\ &= e_r^{2\lambda}(\mu\tilde{\mu}D_1, \mu\tilde{\mu}D_2) \\ &= e_r^{\lambda_{E\times E}}(\tilde{\mu}D_1, \tilde{\mu}D_2) \\ &= e_r^{\lambda_E}(f_*(D_1), f_*(D_2)) \cdot e_r^{\lambda_E}(f'_*(D_1), f'_*(D_2)), \end{aligned}$$

where the pairings e_r^{λ}, $e_r^{2\lambda}$, $e_r^{\lambda_{E\times E}}$, and $e_r^{\lambda_E}$ are defined as in [15, §16]. In particular, if C' is any twist of C then we can pull back points of Jac(C') first to Jac(C) and then to $E \times E$, thus reducing computation of the pairing on Jac(C') to computing two pairings on E.

5.2 Curves with embedding degree 5

The construction in this subsection applies only in characteristic 5. We will construct an isomorphism defined over $\mathbb{F}_{5^{20}}$ from the curve $C : y^2 = x^6 + 1$ over $\mathbb{F}_5$ to the curve $C' : y^2 = x^5 - x + b$ where $b = \pm 1$. Let $q = 5^m$ where $\gcd(m, 10) = 1$. The characteristic polynomial of the (q-power) Frobenius for C' is

$$P_m^{\pm}(T) = T^4 \pm 5^{(m+1)/2}T^3 + 3 \cdot 5^m T^2 \pm 5^{(3m+1)/2}T + 5^{2m}.$$

Observe that

$$P_m^+(T)P_m^-(T) = T^8 + qT^6 + q^2T^4 + q^3T^2 + q^4,$$

so $(T^2 - q)P_m^+(T)P_m^-(T) = T^{10} - q^5$. Let $N := \#\mathrm{Jac}(C')(\mathbb{F}_q)$. Since N is equal to either $P_m^+(1)$ or $P_m^-(1)$, it follows that N divides $q^5 - 1$. Let $r \mid N$ be a large prime. The embedding degree of elements of $\mathrm{Jac}(C)$ of order r is therefore $k = 5$. The characteristic polynomial of the q^5-power Frobenius is $(T^2 - 5^{5m})^2$, so the full r-torsion is defined over $\mathbb{F}_{q^{10}}$, but not over $\mathbb{F}_{q^5}$.

The curve C' is a special case of the family of curves $y^2 = x^p - x + b$ over $\mathbb{F}_p$ of genus $(p-1)/2$ considered by Duursma and Sakurai [6]. Efficient pairing computation on these curves over extension fields $\mathbb{F}_{p^m}$ was studied by Duursma and Lee [5].

We define an isomorphism ϕ_1 from $C : y^2 = x^6 + 1$ to $C_1 : y^2 = x^5 + x$ over $\mathbb{F}_5$ by

$$\phi_1(x, y) = \left(\frac{1 - 2x}{x - 2}, \frac{y}{(x - 2)^3} \right).$$

Let u be an element of $\mathbb{F}_{5^4}$ satisfying $u^8 = -1$, and let ϕ_2 be the isomorphism from C_1 to the curve $C_2 : y^2 = x^5 - x$ defined by $\phi_2(x, y) = (u^2x, 2uy)$. Finally, let w be an element of $\mathbb{F}_{5^5}$ satisfying $w^5 - w + b = 0$, and let $\phi_3 : C_2 \to C'$ be the isomorphism defined by $\phi_3(x, y) = (x + w, y)$.

Theorem 5.5. *Let $C : y^2 = x^6 + 1$ and $C' : y^2 = x^5 - x + b$ with $b = \pm 1$ be the curves over $\mathbb{F}_5$ defined above. Let $\phi = \phi_1^{-1}\phi_2^{-1}\phi_3^{-1} : C' \to C$ be the composition of the isomorphisms defined above, and let π_C, χ, ρ_6 be the endomorphisms of $\mathrm{Jac}(C)$ as defined in Section 5.1. Let $r > 3$ be prime divisor of $\#\mathrm{Jac}(C')(\mathbb{F}_{5^m})$ where $\gcd(m, 10) = 1$. Suppose D and D' are points in $\mathrm{Jac}(C')[r]$. Then there exists a distortion map for (D, D') of the form*

$$\phi^{-1}\pi_C^i\chi^j\rho_6^l\phi \tag{5.2}$$

where $0 \le i < 4$ and $0 \le j, l < 2$.

Proof. We know there exists a distortion map ψ for the pair (D, D') in $\mathrm{End}(\mathrm{Jac}(C'))$. The index of $\mathbb{Z}[\phi^{-1}\pi_C\phi, \phi^{-1}\chi\phi, \phi^{-1}\rho_6\phi]$ in $\mathrm{End}(\mathrm{Jac}(C'))$ must divide $2^8 3^4$ by Theorem 5.3. If $r > 3$, then $2^8 3^4 \psi$ is also a suitable distortion map for the pair (D, D'). Hence, there exists a distortion map of the form

$$\sum_{i,j,l} a_{i,j,l}\phi^{-1}\pi_C^i\chi^j\rho_6^l\phi,$$

where the sum is over $0 \le i < 4$, $0 \le j < 2$, and $0 \le l < 2$, with the $a_{i,j,l}$ in $\mathbb{Z}$. The result follows by the argument at the end of the proof of Corollary 4.4. □

In practice, one might prefer to use simpler maps than those of Equation (5.2). For example, in many applications it is convenient to use the distortion map on C' proposed by Duursma and Lee [5], given by

$$\psi : (x, y) \longmapsto (\rho - x, 2y)$$

where ρ is an element of $\mathbb{F}_{5^5}$ satisfying $\rho^5 - \rho + 2b = 0$.

5.3 Curves with embedding degree 6

Let p be an odd prime such that $p \equiv 2 \pmod 3$. The main contribution of this section is Theorem 5.6, which gives a construction of supersingular genus 2 curves over $\mathbb{F}_p$ with embedding degree 6. Equation (5.1) gives a set of distortion maps for these curves, and Theorem 5.3 shows that they are sufficient for cryptographic applications (that is, when the orders of the divisors are different from 2, 3, and p).

Let ζ_6 be a primitive sixth root of unity in $\mathbb{F}_{p^2}$, and set $\zeta_3 := \zeta_6^2$. We wish to construct a curve $C'/\mathbb{F}_p$ with embedding degree 6; the characteristic polynomial of Frobenius on $\mathrm{Jac}(C')$ must therefore be $T^4 - pT^2 + p^2$. Following [13, p. 32], we obtain C' by twisting the curve $C : y^2 = x^6 + 1$ with respect to a suitable automorphism. The following theorem gives an algorithm to find C'.

Theorem 5.6. *Let $p \equiv 2 \pmod 3$ be an odd prime. Let $\gamma \in \overline{\mathbb{F}}_p$ satisfy $\gamma^{p^2-1} = \zeta_3$, and let $a = \gamma^p$, $b = \zeta_3^2\gamma^p$, $c = \gamma$, and $d = \zeta_3\gamma$. The genus 2 curve*

$$C' : Y^2 = (aX + b)^6 + (cX + d)^6$$

is defined over $\mathbb{F}_p$, and is supersingular with embedding degree $k = 6$.

Proof. Observe that $\gamma^{p^2} = \zeta_3\gamma$; hence $\gamma^{p^6} = \gamma$, so γ is an element of $\mathbb{F}_{p^6}$. Also note that $\gamma^{p+1} = \zeta_3$ and that $ad - bc = -\zeta_3 - 2 \neq 0$. Taking the p-power of the coefficients of the polynomial $(aX + b)^6 + (cX + d)^6$, and using $a = c^p$ and $b = d^p$, we find

$$\begin{aligned}(a^pX + b^p)^6 + (c^pX + d^p)^6 &= (c^{p^2}X + d^{p^2})^6 + (c^pX + d^p)^6 \\ &= (\zeta_3(cX + d))^6 + (aX + b)^6 \\ &= (aX + b)^6 + (cX + d)^6,\end{aligned}$$

so C' is defined over $\mathbb{F}_p$. Let $\phi : C' \to C$ be the isomorphism defined over $\overline{\mathbb{F}}_p$ by

$$\phi : (X, Y) \longmapsto (x, y) = \left(\frac{aX + b}{cX + d}, \frac{Y}{(cX + d)^3}\right).$$

Write π' for the p-power Frobenius map on C' (and the induced endomorphism of

Jac(C')). Since $a^p = \zeta_3 c$, $b^p = \zeta_3 d$, $c^p = a$, and $d^p = b$, we have

$$\begin{aligned}
\phi\pi'(X,Y) &= \left(\tfrac{aX^p+b}{cX^p+d}, \tfrac{Y^p}{(cX^p+d)^3}\right) \\
&= \left(\tfrac{\zeta_3(c^pX^p+d^p)}{a^pX^p+b^p}, \tfrac{Y^p}{(a^pX^p+b^p)^3}\right) \\
&= \rho_3\left(\tfrac{c^pX^p+d^p}{a^pX^p+b^p}, \tfrac{Y^p}{(a^pX^p+b^p)^3}\right) \\
&= \rho_3\chi\left(\tfrac{a^pX^p+b^p}{c^pX^p+d^p}, \tfrac{Y^p}{(c^pX^p+d^p)^3}\right) \\
&= \rho_3\chi\pi\left(\tfrac{aX+b}{cX+d}, \tfrac{Y}{(cX+d)^3}\right) \\
&= \rho_3\chi\pi\phi(X,Y),
\end{aligned}$$

and therefore

$$\pi' = \phi^{-1}\rho_3\chi\pi\phi.$$

Using $\chi\pi = \pi\chi$, $\chi\rho_3 = \rho_3^{-1}\pi$, $\pi\rho_3 = \rho_3^{-1}\pi$, and $\pi^2 = [-p]$, we find

$$(\pi')^2 = \phi^{-1}[-p]\rho_3^2\phi \quad \text{and} \quad (\pi')^4 = \phi^{-1}[p^2]\rho_3\phi,$$

and in particular

$$(\pi')^4 - [p](\pi')^2 + [p^2] = \phi^{-1}[p^2](\rho_3^2 + \rho_3 + [1])\phi.$$

But $\rho_3^2 + \rho_3 + [1] = 0$, so π' satisfies the characteristic polynomial $T^4 - pT^2 + p^2 = 0$, and the embedding degree of C' is therefore 6. □

Remark 5.7. Explicit equations for C' which do not depend on the element γ are given in [3, Table 9].

Finally, we exhibit distortion maps for Jac(C'). We know $\phi^{-1}\mathbb{Z}[\pi_C, \chi, \rho_6]\phi$ has small index in End(Jac(C')) by Theorem 5.3. As in Theorem 5.5, it follows that for any pair of points on Jac(C') one can choose a distortion map of the form

$$\phi^{-1}\pi_C^i\chi^j\rho_6^l\phi$$

where $0 \leq i < 4$ and $0 \leq j, l < 2$.

6 Curves with embedding degree 12

Let m be an integer such that $m \equiv \pm 1 \pmod 6$. The curves $C : y^2 + y = x^5 + x^3 + b$ over $\mathbb{F}_{2^m}$ with $b = 0, 1$ were studied by van der Geer and van der Vlugt in [26] and [25] for their applications in coding theory.

Let π denote the 2^m-power Frobenius endomorphism of Jac(C). Its characteristic polynomial is

$$P_m^{\pm}(T) = T^4 \pm 2^{(m+1)/2}T^3 + 2^mT^2 \pm 2^{(3m+1)/2}T + 2^{2m},$$

so Jac(C) is supersingular and simple over $\mathbb{F}_{2^m}$. We have

$$P_m^+(T)P_m^-(T) = T^8 - 2^{2m}T^4 + 2^{4m}$$

and

$$(T^8 - 2^{4m})(T^8 + 2^{2m}T^4 + 2^{4m})P_m^+(T)P_m^-(T) = T^{24} - 2^{12m},$$

so the embedding degree is $k = 12$.

The automorphisms of C have the form

$$\sigma_\omega : (x, y) \longmapsto (x + \omega, y + s_2x^2 + s_1x + s_0)$$

where ω is any root of the polynomial

$$\begin{aligned} &T^{16} + T^8 + T^2 + T \\ &= (T^6 + T^5 + T^3 + T^2 + 1)(T^3 + T^2 + 1)(T^3 + T + 1)(T^2 + T + 1)(T + 1)T, \end{aligned}$$

and where $s_2 = \omega^8+\omega^4+\omega$, $s_1 = \omega^4+\omega^2$, and s_0 is a root of $y^2+y = \omega^5+\omega^3$ (the other root is $s_0 + 1$). For each choice of ω, we arbitrarily fix one of the corresponding values of s_0, and denote the resulting automorphism by σ_ω; we will view these automorphisms as elements of $\mathrm{End}(\mathrm{Jac}(C))$. These automorphisms satisfy the relations

$$\sigma_\omega\sigma_{\omega'} = \pm\sigma_{\omega'}\sigma_\omega = \pm\sigma_{\omega+\omega'}.$$

Fix a root τ in $\mathbb{F}_{2^6}$ of $T^6+T^5+T^3+T^2+1$, and set $\xi = \tau^4+\tau^2$ and $\theta = \tau^4+\tau^2+\tau$. Note that ξ and θ are roots of the polynomial $T^{16} + T^8 + T^2 + T$, and that $\theta^2 = \theta + 1$, $\tau^8 = \tau + 1$, and $\theta + \tau = \xi$.

Proposition 6.1. *If C, π, σ_τ, σ_θ, and σ_ξ are defined as above, then* $\mathrm{End}^0(\mathrm{Jac}(C)) = \mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta]$*, and we have a direct sum decomposition (of $\mathbb{Q}$-vector spaces)*

$$\mathrm{End}^0(\mathrm{Jac}(C)) = \mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta] = \mathbb{Q}(\pi) \oplus \sigma_\tau\mathbb{Q}(\pi) \oplus \sigma_\theta\mathbb{Q}(\pi) \oplus \sigma_\xi\mathbb{Q}(\pi).$$

Proof. We easily verify the relations

$$\begin{aligned} \pi\sigma_\omega &= \pm\sigma_{\omega^{2^m}}\pi, \\ \sigma_\tau^2 &= [-1], \\ \sigma_\theta\sigma_\tau &= \pm\sigma_\xi, \\ \pi^3\sigma_\tau\pi^{-3} &= \pm\sigma_{\tau^{2^3}} = \pm\sigma_{\tau+1} = \pm\sigma_\tau\sigma_1, \\ \pi\sigma_\theta\pi^{-1} &= \pm\sigma_{\theta^2} = \pm\sigma_{\theta+1} = \pm\sigma_1\sigma_\theta. \end{aligned}$$

Let F denote $\mathbb{Q}(\pi)$; since F is a degree-4 CM field, it is a 4-dimensional $\mathbb{Q}$-vector space. Since σ_1 commutes with Frobenius, σ_1 is an element of F by [21, II, Proposition 1].

The sum $F \oplus \sigma_\tau F$ is direct, because σ_τ is not in F, so $F \oplus \sigma_\tau F$ is an 8-dimensional $\mathbb{Q}$-vector space (though it is not a $\mathbb{Q}$-algebra). Suppose $(F \oplus \sigma_\tau F) \oplus \sigma_\xi F$ is not a direct sum: then there exists some non-zero z in F such that $\sigma_\xi z$ lies in $F \oplus \sigma_\tau F$. Dividing by z, there exist some z_1 and z_2 in F such that

$$\sigma_\xi = z_1 + \sigma_\tau z_2.$$

Since ξ is in $\mathbb{F}_{2^3}$, we have $\sigma_\xi = \pi^3 \sigma_\xi \pi^{-3}$. The relations above imply

$$\begin{aligned} z_1 + \sigma_\tau z_2 &= \pi^3 \sigma_\xi \pi^{-3} \\ &= \pi^3 (z_1 + \sigma_\tau z_2) \pi^{-3} \\ &= z_1 \pm \sigma_{\tau^{2^3}} z_2 \\ &= z_1 \pm \sigma_\tau \sigma_1 z_2. \end{aligned}$$

Since $F \oplus \sigma_\tau F$ is a direct sum and $\sigma_1 \neq \pm 1$, we have $z_2 = 0$: that is, σ_ξ must lie in F. This is a contradiction, because σ_ξ does not commute with π: hence $F \oplus \sigma_\tau F \oplus \sigma_\xi F$ is a direct sum. Finally, suppose $(F \oplus \sigma_\tau F \oplus \sigma_\xi F) \oplus \sigma_\theta F$ is not a direct sum: then

$$\sigma_\theta = z_1 + \sigma_\tau z_2 + \sigma_\xi z_3$$

for some z_1, z_2 and z_3 in F. Again using the relations above, we have

$$\begin{aligned} 0 &= \sigma_1 \sigma_\theta \pi^3 \pm \pi^3 \sigma_\theta \\ &= \sigma_1 (z_1 + \sigma_\tau z_2 + \sigma_\xi z_3) \pi^3 \pm \pi^3 (z_1 + \sigma_\tau z_2 + \sigma_\xi z_3) \\ &= \sigma_1 (z_1 + \sigma_\tau z_2 + \sigma_\xi z_3) \pi^3 \pm (z_1 \pm \sigma_{\tau^{2^3}} z_2 \pm \sigma_{\xi^{2^3}} z_3) \pi^3 \\ &= (\sigma_1 \pm 1) z_1 \pi^3 \pm (\sigma_1 \pm \sigma_1) \sigma_\tau z_2 \pi^3 \pm (\sigma_1 \pm 1) \sigma_\xi z_3 \pi^3 \\ &= z_1 (\sigma_1 \pm 1) \pi^3 \pm \sigma_\tau z_2 (\sigma_1 \pm \sigma_1) \pi^3 \pm \sigma_\xi z_3 (\sigma_1 \pm 1) \pi^3. \end{aligned}$$

This last equality holds because σ_1 is in F and commutes (up to sign) with σ_τ and σ_ξ. Since $F \oplus \sigma_\tau F \oplus \sigma_\xi F$ is direct and $\sigma_1 \neq \pm 1$, we must have $z_1 = z_3 = 0$. Therefore $\sigma_\theta = \sigma_\tau z$ for some z in F; but this is a contradiction, since σ_θ is defined over $\mathbb{F}_{2^2}$, while σ_τ is defined over $\mathbb{F}_{2^6}$. We conclude that $(F \oplus \sigma_\tau F \oplus \sigma_\xi F) \oplus \sigma_\theta F$ is direct.

We therefore have $\mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta] = F \oplus \sigma_\tau F \oplus \sigma_\xi F \oplus \sigma_\theta F$, so $\mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta]$ is a 16-dimensional $\mathbb{Q}$-vector space. But $\mathrm{End}^0(\mathrm{Jac}(C))$ is a 16-dimensional $\mathbb{Q}$-vector space containing $\mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta]$; hence $\mathrm{End}^0(\mathrm{Jac}(C)) = \mathbb{Q}[\pi, \sigma_\tau, \sigma_\theta]$. □

Let r be a large prime. One can show that for any non-trivial pair (D, D') of divisors in $\mathrm{Jac}(C)[r]$ there exists a distortion map of the form

$$\pi^i \sigma_\tau^j \sigma_\theta^l$$

where $0 \leq i < 4$ and $0 \leq j, l < 2$, subject to an assumption analogous to Assumption 4.2. We will not give the details here, as Takashima [23] has proved this result unconditionally.

Acknowledgments. The authors would like to thank Ryuichi Harasawa, David Kohel, Enric Nart, and the anonymous referees for their helpful suggestions. The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the authors' views, is provided as is, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. This research was also supported by the EU SOCRATES/ERASMUS programme and by the EPSRC.

References

[1] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, *Efficient algorithms for pairing-based cryptosystems*. CRYPTO 2002, Lecture Notes in Computer Science 2442, pp. 354–368. Springer-Verlag, 2002.

[2] I. Blake, G. Seroussi, and N. Smart (eds.), *Advanced topics in elliptic curve cryptography*. Cambridge, 2005.

[3] G. Cardona and E. Nart, *Zeta functions and cryptographic exponent of supersingular curves of genus* 2. Pairing-Based Cryptography, Tokyo 2007 (T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, eds.), Lecture Notes in Computer Science 4575, pp. 132–151. Springer-Verlag, 2007.

[4] Y.-J. Choie and E. Lee, *Implementation of Tate pairing on hyperelliptic curves of genus 2*. ICISC 2003 (J. I. Lim and D. H. Lee, eds.), Lecture Notes in Computer Science 2971, pp. 97–111. Springer-Verlag, 2004.

[5] I. M. Duursma and H. S. Lee, *Tate pairing implementation for hyperelliptic curves* $y^2 = x^p - x + d$. ASIACRYPT 2003 (C.-S. Laih, ed.), Lecture Notes in Computer Science 2894, pp. 111–123. Springer-Verlag, 2003.

[6] I. M. Duursma and K. Sakurai, *Efficient algorithms for the Jacobian variety of hyperelliptic curves* $y^2 = x^p - x + 1$ *over a finite field of odd characteristic* p. Coding theory, cryptography and related areas, Guanajuato, 1998, pp. 73–89, 2000.

[7] M. Gagné, *Identity-based encryption: a survey*, RSA Laboratories - CryptoBytes 6 (2003), pp. 10–19.

[8] S. D. Galbraith, *Supersingular curves in cryptography*. ASIACRYPT 2001 (C. Boyd, ed.), Lecture Notes in Computer Science 2248, pp. 495–513. Springer-Verlag, 2001.

[9] S. D. Galbraith and J. Pujolàs, *Distortion maps for genus two curves*. CRM Barcelona (R. Cramer and T. Okamoto, eds.), Proceedings of a workshop on Mathematical Problems and Techniques in Cryptology, pp. 46–58, 2005.

[10] S. D. Galbraith and V. Rotger, *Easy decision Diffie-Hellman groups*, LMS J. Comput. Math. 7 (2004), pp. 201–218.

[11] E. W. Howe, F. Leprévost, and B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. 12 (2000), pp. 315–364.

[12] E. W. Howe, D. Maisner, E. Nart, and C. Ritzenthaler, *Principally polarizable isogeny classes of abelian surfaces over finite fields*, Math. Res. Lett. 15 (2008), pp. 121–127.

[13] E. W. Howe, E. Nart, and C. Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields (Jacobiennes dans les classes d'isogénie des surfaces abéliennes sur les corps finis)*, Ann. Inst. Fourier 59 (2009), pp. 239–289.

[14] S. Lang, *Complex Multiplication*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen 255. Springer-Verlag, Berlin-Heidelberg, 1983.

[15] J. S. Milne, *Abelian Varieties*. Arithmetic Geometry (G. Cornell and J. Silverman, eds.). Springer-Verlag, 1986.

[16] K. G. Paterson, *Cryptography from pairings: a snapshot of current research*, Information Security Technical Report, Report, 2002. , pp. 41–54.

[17] ———, *Pairing based cryptography*, [2], ch. 10, Cambridge, 2005.

[18] J. Pujolàs, *On the decisional Diffie-Hellman problem in genus* 2, Ph.D. thesis, Universitat Politècnica de Catalunya, 2006.

[19] K. Rubin and A. Silverberg, *Supersingular abelian varieties in cryptology*. Advances in Cryptology – CRYPTO 2002 (T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, eds.), Lecture Notes in Computer Science 2442, pp. 336–353. Springer-Verlag, 2002.

[20] M. Scott, *Faster identity based encryption*, Elec. Letters 40 (2004), p. 861.

[21] G. Shimura, *Abelian varieties with complex multiplication and modular functions*. Princeton university press, Princeton, 1996.

[22] J. Silverman, *The arithmetic of elliptic curves*. Springer-Verlag, 1986.

[23] K. Takashima, *Efficiently computable distortion maps for supersingular curves*. ANTS-VIII (A. van der Poorten and A. Stein, eds.), Lecture Notes in Computer Science 5011, pp. 88–101. Springer-Verlag, 2008.

[24] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inv. Math. 2 (1966), pp. 134–144.

[25] G. van der Geer and M. van der Vlugt, *Reed-Muller codes and supersingular curves I*, Compositio Math. 84 (1992), pp. 333–367.

[26] ———, *Supersingular curves of genus* 2 *over finite fields of characteristic* 2, Math. Nachr. 159 (1992), pp. 73–81.

[27] P. van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Comp. 68 (1999), pp. 307–320.

[28] ———, *Proving that a genus* 2 *curve has complex multiplication*, Math. Comp. 68 (1999), pp. 1663–1677.

[29] E. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*. EUROCRYPT 2001 (B. Pfitzmann, ed.), Lecture Notes in Computer Science 2045, pp. 195–210. Springer-Verlag, 2001.

[30] ———, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Crypt. 17 (2004), pp. 277–296.

[31] M.-F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics 800. Springer-Verlag, Berlin, 1980.

Received 30 November, 2006; revised 8 January, 2009

Author information

Steven D. Galbraith, Mathematics Department, Royal Holloway University of London, Egham, Surrey TW20 0EX, United Kingdom.
Email: Steven.Galbraith@rhul.ac.uk

Jordi Pujolàs, Departament de Matemàtica, Universitat de Lleida, Jaume II 69, 25001 Lleida, Spain.
Email: jpujolas@matematica.udl.es

Christophe Ritzenthaler, Institut de Mathématiques de Luminy, UMR 6206 du CNRS, Luminy, Case 907, 13288 Marseille, France.
Email: ritzenth@iml.univ-mrs.fr

Benjamin Smith, INRIA Saclay–Île-de-France, Laboratoire d'Informatique (LIX), École polytechnique, 91128 Palaiseau, France.
Email: smith@lix.polytechnique.fr