DISTORTION MAPS FOR GENUS TWO CURVES

STEVEN D. GALBRAITH AND JORDI PUJOLÀS

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 $g > 1$ and we give several examples.
Keywords: hyperelliptic curve cryptography, pairings, supersingular curves, distortion maps.

1. Introduction

Let q be a power of some prime p. Let C be a (non-singular, geometrically irreducible, projective) curve defined over the finite field $\mathbb{F}_q$. Let l be a prime number satisfying $l \mid \#\mathrm{Jac(C)}(\mathbb{F}_q)$. We define the *embedding degree* to be the smallest integer k such that $l \mid q^k - 1$. In other words, $\mathbb{F}_{q^k}$ is the field generated over $\mathbb{F}_q$ by adjoining the l-th roots of unity. Throughout this paper, we identify $\mathrm{Jac(C)}(\mathbb{F}_{q^k})$ with the degree zero divisor class group of C over $\mathbb{F}_{q^k}$.

An elliptic curve E over $\mathbb{F}_q$ is called supersingular if the number of points on E over $\mathbb{F}_q$ is congruent to 1 modulo p. In this case $\mathrm{End}(E)$ is an order in a quaternion algebra (by $\mathrm{End}(A)$ we mean the ring of all homomorphisms of the abelian variety A to itself which are defined over an algebraic closure of the ground field). An abelian variety A of dimension g over $\mathbb{F}_q$ is called supersingular if A is isogenous over $\overline{\mathbb{F}}_q$ to a product E^g of a supersingular elliptic curve. In this case it follows that $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a $\mathbb{Q}$-algebra of dimension $(2g)^2$ as a $\mathbb{Q}$-vector space. A curve C is called supersingular if Jac(C) is a supersingular abelian variety.

Let $l > 2$ be a prime such that $l \nmid q$. The Tate pairing (see Frey and Rück [4]) is a pairing of the l-torsion in the divisor class group of C over $\mathbb{F}_{q^k}$ with a certain quotient group of the divisor class group over $\mathbb{F}_{q^k}$. When C is supersingular and $l \| \#\mathrm{Jac(C)}(\mathbb{F}_q)$ then we have $\mathrm{Jac(C)}[l] \subseteq \mathrm{Jac(C)}(\mathbb{F}_{q^k})$ (see [12]). We therefore obtain from the Tate pairing a bilinear pairing $e_l(\cdot,\cdot)$ from $\mathrm{Jac(C)}[l]$ to the group μ_l of l-th roots of unity in $\mathbb{F}_{q^k}^*$ (see [6]). If the embedding degree is small then this pairing may be useful for implementing pairing-based cryptosystems (see [5, 8, 9] for a survey).

When Jac(C) is supersingular the embedding degree k is known to be bounded by a constant $k(g)$ which depends only on g [6] (also see [10]). For cryptography one tends to be interested in cases where the embedding degree is larger than 1 but not too large.

An important property of pairings for cryptography is the bilinearity property $e_l(aD_1, bD_2) = e_l(D_1, D_2)^{ab}$. However, to be useful it is necessary that $e_l(D_1, D_2) \neq 1$. It is known that the Tate pairing is non-degenerate, i.e., for each non-zero divisor class D_1 of order l there is a divisor class D_2 such that

$e_l(D_1, D_2) \neq 1$. A problem arises when one wants to pair two specific divisors D_1 and D_2 (for example, when for efficiency reasons they are both defined over $\mathbb{F}_q$ and $k > 1$) such that $e_l(D_1, D_2) = 1$. In this case we need distortion maps.

Definition. A *distortion map* for the pairing e_l and non-zero divisor classes D_1 , D_2 on C is an endomorphism ϕ of Jac(C) such that $e_l(D_1, \phi(D_2)) \neq 1$.

This concept was introduced by Verheul [16] in the elliptic curve case. Note that the Frobenius (or trace) map can be used as a distortion map in many situations, including ordinary curves, but distortion maps for every case can only be obtained for supersingular curves.

The elliptic curve case is rather simple: If $D_1, D_2 \neq 0$ and $e_l(D_1, D_2) = 1$ then any divisor D_3 which is independent of D_2 (i.e., $\langle D_2 \rangle \cap \langle D_3 \rangle = \{0\}$) satisfies $e_l(D_1, D_3) \neq 1$. This is true because the l-torsion has rank 2. For this reason (and others) the problem of finding distortion maps in the elliptic curve case is relatively easy to handle. An algorithm to find distortion maps for any supersingular elliptic curve has been given by Galbraith and Rotger [7].

When working in genus $g > 1$ the l-torsion has rank $2g$ and so independence of points is not sufficient to imply non-triviality of their pairing. Indeed, elementary linear algebra implies that for every non-trivial divisor D of order l there is a generating set $\{D_1, \ldots, D_{2g}\}$ for $\mathrm{Jac(C)}[l]$ such that $e_l(D, D_1) \neq 1$ but $e_l(D, D_i) = 1$ for $2 \leq i \leq 2g$. Furthermore, elements of End(Jac(C)) may be difficult to handle as they do not necessarily correspond to maps from C to itself. In this paper we give a discussion of this situation. We first prove that distortion maps always exist for supersingular curves of genus $g > 1$. We then study some specific examples in depth and explain some methods to overcome the obstacles mentioned above.

2. The existence of distortion maps

It was proved by Schoof and Verheul [17] that distortion maps always exist for supersingular elliptic curves over $\mathbb{F}_q$. We now generalise their result.

We first recall an important theorem of Tate [13]. Let A be an abelian variety over a finite field K of characteristic p and let $G = \mathrm{Gal}(\overline{K}/K)$. Let l be a prime such that $l \neq p$ and let $T_l(A)$ be the Tate module of A. Define $\mathrm{End}_K(A)$ to be the ring of homomorphisms from A to itself which are defined over K and define $\mathrm{End}_G(T_l(A))$ to be the ring of homomorphisms from $T_l(A)$ to itself which commute with the action of G. Then Tate's theorem is that the canonical map

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

is a bijection.

Theorem 2.1. *Let* C *be a supersingular curve of genus* g *over* $\mathbb{F}_q$*. Let* $l \mid \#\mathrm{Jac(C)}(\mathbb{F}_q)$ *be prime and let the embedding degree be* k*. Let* D_1, D_2 *be non-trivial divisor classes of order* l*. Then there is an element* $\phi \in \mathrm{End(Jac(C))}$ *such that* $e_l(D_1, \phi(D_2)) \neq 1$*.*

Proof. Let $K = \mathbb{F}_{q^k}$ and $G = \mathrm{Gal}(\overline{K}/K)$. Since Jac(C) is supersingular then $\mathrm{End(Jac(C))} \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is a $\mathbb{Z}_l$-module of rank $(2g)^2$. Obviously, we have the fact that $\mathrm{End}_K(\mathrm{Jac(C)}) \subseteq \mathrm{End(Jac(C))}$. By Tate's theorem $\mathrm{End}_K(\mathrm{Jac(C)}) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is isomorphic to the $\mathbb{Z}_l$-module $\mathrm{End}_G(T_l(\mathrm{Jac(C)}))$ of homomorphisms which commute with the q^k-power Frobenius.

Since Jac(C) is supersingular, the Frobenius over K is an integer (namely, $-q^{k/2}$) and so it commutes with everything. Since $T_l(\mathrm{Jac}(\mathrm{C})) \cong \mathbb{Z}_l^{2g}$ as a $\mathbb{Z}_l$-module, it follows that

$$\mathrm{End}_G(T_l(\mathrm{Jac}(\mathrm{C}))) \cong M_{2g}(\mathbb{Z}_l).$$

Hence $\mathrm{End}_K(\mathrm{Jac}(\mathrm{C})) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong M_{2g}(\mathbb{Z}_l)$ and so $\mathrm{End}_K(\mathrm{Jac}(\mathrm{C})) \cong \mathrm{End}(\mathrm{Jac}(\mathrm{C}))$ also has rank $(2g)^2$. By restriction, we have

$$\mathrm{End}_K(\mathrm{Jac}(\mathrm{C})) \otimes_{\mathbb{Z}} \mathbb{Z}/l\mathbb{Z} \cong M_{2g}(\mathbb{Z}/l\mathbb{Z}).$$

Let $D_3 \in \mathrm{Jac}(\mathrm{C})[l]$ be such that $e_l(D_1, D_3) \neq 1$. There exists some matrix $\Phi \in M_{2g}(\mathbb{Z}/l\mathbb{Z})$ which corresponds to a mapping of a subspace $\langle D_2 \rangle$ to $\langle D_3 \rangle$. Let ϕ be a preimage in $\mathrm{End}(\mathrm{Jac}(\mathrm{C}))$ of Φ. Then $e_l(D_1, \phi(D_2)) \neq 1$. □

Remark. The above result is presented for Jacobians, since that is the interesting case, but the proof clearly also works when Jac(C) is replaced by a general supersingular abelian variety A and when D_i are replaced by points in $A[l]$.

Remark. It follows from the proof above that a full rank $(2g)^2$ module of endomorphisms is needed to distort any pair of divisors. In other words, if Jac(C) has endomorphism ring which has rank strictly less than $(2g)^2$ then there will exist divisors D_1 and D_2 in $\mathrm{Jac}(\mathrm{C})[l]$ such that $e_l(D_1, \varphi(D_2)) = 1$ for all $\varphi \in \mathrm{End}(\mathrm{Jac}(\mathrm{C}))$.

3. A family of supersingular curves

In this section we work with $q = p$ such that $p \equiv 2, 3 \pmod 5$. Let

$$\tilde{\mathrm{C}}\colon y^2 = x^5 + A$$

over $\mathbb{Q}$ where $A \neq 0$. Reducing $\tilde{\mathrm{C}}$ modulo p one obtains a curve C defined over $\mathbb{F}_p$.

Let ξ_5 be a fifth root of unity. The curve $\tilde{\mathrm{C}}$ has the automorphism $(x, y) \longmapsto (\xi_5 x, y)$ which we call ξ_5. This automorphism extends to give an element of the ring $\mathrm{End}(\mathrm{Jac}(\tilde{\mathrm{C}}))$ which we again call ξ_5. Moreover, since $p \neq 1 \pmod 5$ then ξ_5 reduces to a non-trivial endomorphism of Jac(C) which we call ξ_5 yet again. The map ξ_5 was used by Choie and Lee [3] as a distortion map.

Clearly, $\mathrm{End}^0(\mathrm{Jac}(\mathrm{C}))$ contains the algebra generated by the p-power Frobenius map π and the automorphism ξ_5. But this is not enough to guarantee that combinations of these maps can always be used as distortion maps. The goal of this section is to show that these maps generate the full algebra of endomorphisms and to justify that combinations of powers of π and the map ξ_5 are sufficient for distortion maps in all cases.

Lemma 3.1. *If $p \equiv 2, 3 \pmod 5$ then* Jac(C) *is simple, supersingular and has embedding degree* 4.

Proof. Since 5 is coprime to $p-1$ it follows that, for every $y \in \mathbb{F}_p$, there is a unique value $x = (y^2 - A)^{1/5}$. Hence, since C has a single point at infinity, $\#\mathrm{C}(\mathbb{F}_p) = p+1$. Since 5 is also coprime to $p^2 - 1$ we obtain $\#\mathrm{C}(\mathbb{F}_{p^2}) = p^2 + 1$.

Hence, the characteristic polynomial of the p-power Frobenius endomorphism $\pi \in \mathrm{End}(\mathrm{Jac}(\mathrm{C}))$ is $P(T) = T^4 + p^2$. It is easy to show that this polynomial is irreducible over $\mathbb{Z}$ and hence Jac(C) is simple. It also follows from the shape of $P(T)$ (see [12, 6]) that C is supersingular.

If $l \mid \mathrm{Jac}(\mathrm{C})(\mathbb{F}_p) = p^2 + 1$ is a prime larger than 2 then it follows that $l \mid p^4 - 1$ and $l \nmid (p^i - 1)$ for $1 \leq i \leq 3$, and so the embedding degree is $k = 4$. □

Remark. Note that, while Jac(C) is simple over $\mathbb{F}_p$, it is not simple over $\mathbb{F}_{p^4}$. Also, note that if $p \equiv 4 \pmod 5$ then C is supersingular, but the embedding degree is only 2 and so we are less interested in this case. If $p \equiv 1 \pmod 5$ then C is ordinary.

Hence, as we saw in section 2, distortion maps do exist for C. Our goal is to explicitly determine distortion maps for every pair $D_1, D_2 \in \mathrm{Jac(C)}$. As before, let $l \mid \#\mathrm{Jac(C)}(\mathbb{F}_p)$.

Lemma 3.2. *Let $p \equiv 2, 3 \pmod 5$ and let $l > 2$ be a prime such that $l \mid p^2 + 1$. The eigenvalues of the p-power Frobenius on the l-torsion of* Jac(C) *are $1, -1, p$ and $-p$ and there is a corresponding eigenbasis D_1, D_2, D_3 and D_4.*

Proof. Since $l \mid p^2 + 1$ it follows that

$$T^4 + p^2 \equiv T^4 - 1 = (T^2 + 1)(T^2 - 1) \pmod l.$$

Further, the factor $T^2 + 1 \equiv T^2 - p^2 \equiv (T + p)(T - p) \pmod l$. Hence, the eigenvalues of π on $\mathrm{Jac(C)}[l]$ are $1, -1, p$ and $-p$.

Since the eigenvalues are distinct one can diagonalise to obtain a corresponding π-eigenbasis D_1, D_2, D_3 and D_4. □

Remark. To construct such an eigenbasis in practice one can choose a random $D \in \mathrm{Jac(C)}(\mathbb{F}_{p^4})[l]$ and define

$$D_1 = \tfrac{p^2D + p^2\pi(D) - \pi^2(D) - \pi^3(D)}{2(p^2-1)}, \quad D_2 = \tfrac{p^2D - p^2\pi(D) - \pi^2(D) + \pi^3(D)}{2(p^2-1)},$$
$$D_3 = \tfrac{-p^2D - p^2\pi(D) + \pi^2(D) + \pi^3(D)}{2(p^2-1)}, \quad D_4 = \tfrac{-p^2D + p^2\pi(D) + \pi^2(D) - \pi^3(D)}{2(p^2-1)}.$$

One can check that if D is sufficiently generic then these divisors are all non-zero and that they do yield an eigenbasis as above.

Lemma 3.3. *Let $p \equiv 2, 3 \pmod 5$ and let $l > 2$ be a prime such that $l \mid p^2 + 1$. Let (D_1, D_2, D_3, D_4) be the ordered π-eigenbasis as above. Then if $1 \leq i, j \leq 4$, we have $e_l(D_i, D_j) = 1$ unless $(i, j) = (1, 3), (3, 1), (2, 4)$ or $(4, 2)$.*

Proof. We use Galois invariance of e_l. For example, for D_1 one has

$$\pi(e_l(D_1, D_1)) = e_l(\pi(D_1), \pi(D_1)) = e_l(D_1, D_1).$$

This implies $e_l(D_1, D_1) \in \mathbb{F}_p \cap \mu_l$ (recall that μ_l is the group of l-th roots of unity) and hence $e_l(D_1, D_1) = 1$.

Similarly,

$$e_l(D_1, D_2)^p = \pi(e_l(D_1, D_2)) = e_l(\pi(D_1), \pi(D_2)) = e_l(D_1, -D_2) = e_l(D_1, D_2)^{-1}.$$

Since, $l \nmid (p + 1)$ this implies $e_l(D_1, D_2) = 1$.

Similarly,

$$e_l(D_1, D_4)^p = \pi(e_l(D_1, D_4)) = e_l(\pi(D_1), \pi(D_4)) = e_l(D_1, -pD_4) = e_l(D_1, D_4)^{-p}.$$

Since $l \nmid 2p$ it follows that $e_l(D_1, D_4) = 1$.

By non-degeneracy of e_l, one must have $e_l(D_1, D_3) \neq 1$.

The other cases are similar. □

We see that π can be used as a distortion map. For example, suppose $D = D_1 + D_2$ and $D' = D_3 + mD_4$, with respect to the basis above, where $m \in \mathbb{Z}$ is such that $e_l(D, D') = e_l(D_1, D_3)e_l(D_2, D_4)^m = 1$. Then we have

$$e_l(D, \pi(D')) = e_l(D_1, pD_3)e_l(D_2, -pmD_4) = e_l(D_1, D_3)^p e_l(D_2, D_4)^{-pm}$$

and this is not equal to 1 if $m \not\equiv 0 \pmod{l}$. Note that, for efficient implementation, there are often reasons to prefer the trace map $\mathrm{Tr}(D) = \sum_{i=0}^{3} \pi^i(D)$ to π, though in the above example we have $\mathrm{Tr}(D') = 0$ so in this particular case the trace map is not useful.

Lemma 3.4. *For $p \not\equiv 1 \pmod 5$ and $j \in \{0,1,2,3\}$ the following relations hold: $\xi_5 \pi^j = \pi^j \xi_5^{[p^j]^{-1}}$, where square brackets denote the class modulo 5.*

Proof. In the ring $\mathrm{End}(\mathrm{Jac}(\mathrm{C})) \otimes_{\mathbb{Z}} \mathbb{Q}$, for $j \in \{0,1,2,3\}$, $(\pi^j)^{-1}\xi_5\pi^j$ is a fifth root of unity. Indeed, by considering the explicit equations we determine that

$$(\pi^j)^{-1}\xi_5\pi^j \colon (x,y) \longmapsto ((\xi_5 x^{p^j})^{1/p^j}, (y^{p^j})^{1/p^j}) = (\xi_5^{1/p^j} x, y).$$

and so the precise root is $(\xi_5)^{1/p^j}$. □

Remark. The preceding lemma implies that if $p \equiv 2,3 \pmod 5$ then conjugation by π is a generator of the cyclic group $\mathrm{Gal}(\mathbb{Q}(\xi_5)/\mathbb{Q})$ and, because this group is cyclic, it also implies that all conjugated elements by j-powers of π for $j < n$ are different.

We write $\mathbb{Z}[\xi_5, \pi]$ for the non-commutative ring generated over $\mathbb{Z}$ by ξ_5 and π. Clearly, $\mathbb{Z}[\xi_5, \pi] \subseteq \mathrm{End}(\mathrm{Jac}(\mathrm{C}))$. We write $\mathbb{Q}[\xi_5, \pi]$ for the non-commutative algebra $\mathbb{Z}[\xi_5, \pi] \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proposition 3.5. *Let $p \equiv 2,3 \pmod 5$. Then $\mathbb{Q}[\xi_5, \pi] = \mathbb{Q}(\xi_5) \oplus \pi\mathbb{Q}(\xi_5) \oplus \pi^2\mathbb{Q}(\xi_5) \oplus \pi^3\mathbb{Q}(\xi_5)$ as $\mathbb{Q}$-vector spaces.*

Proof. We will prove that for every $0 \le r \le 3$ one has the following direct sum $\bigoplus_{i=0}^{r} \pi^i\mathbb{Q}(\xi_5)$. For $r = 0$ there is nothing to prove. For $r \ge 1$, we assume we have a direct sum $U_t = \bigoplus_{i=0}^{t} \pi^i\mathbb{Q}(\xi_5)$ for $0 \le t < r$ and we make the following claim: for every $j > t$ then $U_t \cap \pi^j\mathbb{Q}(\xi_5) = \emptyset$. If we can prove this claim then clearly the proposition follows.

Suppose the contrary: $U_t \cap \pi^j\mathbb{Q}(\xi_5) \neq \emptyset$. Then $\pi^j\mathbb{Q}(\xi_5)$ contains a nonzero element $\pi^j z \in U_t$, for some nonzero $z \in \mathbb{Q}(\xi_5)$. This means $\pi^j \in U_t$ and hence we can write $\pi^j = z_0 + \pi z_1 + ... + \pi^t z_t$ with $z_k \in \mathbb{Q}(\xi_5)$ for $0 \le k \le t$ and some $z_k \neq 0$.

But then, by Lemma 3.4 we have

$$\begin{gathered} 0 = \xi_5\pi^j - \pi^j\xi_5^{[p^j]^{-1}} = \\ = \xi_5 z_0 + \xi_5\pi z_1 + ... + \xi_5\pi^t z_t - z_0\xi_5^{[p^j]^{-1}} - \pi z_1\xi_5^{[p^j]^{-1}} - ... - \pi^t z_t\xi_5^{[p^j]^{-1}} = \\ = z_0\xi_5 + \pi z_1\xi_5^{[p]^{-1}} + ... + \pi^t z_t\xi_5^{[p^t]^{-1}} - z_0\xi_5^{[p^j]^{-1}} - \pi z_1\xi_5^{[p^j]^{-1}} - ... - \pi^t z_t\xi_5^{[p^j]^{-1}} = \\ = z_0(\xi_5 - \xi_5^{[p^j]^{-1}}) + \pi z_1(\xi_5^{[p]^{-1}} - \xi_5^{[p^j]^{-1}}) + ... + \pi^t z_t(\xi_5^{[p^t]^{-1}} - \xi_5^{[p^j]^{-1}}). \end{gathered}$$

Since $\xi_5^{[p^k]^{-1}} \neq \xi_5^{[p^j]^{-1}}$ for $1 \le k \le t < j$ and since U_t is a direct sum, this implies that $z_0 = z_1 = \cdots = z_t = 0$ which is a contradiction. □

Remark. Actually the proposition above is a particular case of a theorem on the structure of central simple algebras one can find for example in [1]. Algebras like $\mathbb{Q}[\xi_5, \pi]$ are called cyclic because there is a maximal subfield with cyclic Galois group (that of $\mathbb{Q}(\xi_5)$). In these cases there always exists another element (in our case π), with the powers of which one can describe the whole algebra (as in Proposition 3.5). The set of powers of this element is known as a factor base, and it is related to the class of the algebra in the Brauer group of $\mathbb{Q}$.

Write $\mathrm{End}^0(\mathrm{Jac}(\mathrm{C})) = \mathrm{End}(\mathrm{Jac}(\mathrm{C})) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Corollary 3.6. *Let $p \equiv 2, 3 \pmod 5$. Then $\mathrm{End}^0(\mathrm{Jac}(\mathrm{C})) = \mathbb{Q}[\xi_5, \pi]$ and*

$$\mathbb{Q}[\xi_5, \pi] \cong \left\{ \sum_{0 \leq i,j \leq 3} \lambda_{i,j} \pi^i \xi_5^j : \lambda_{i,j} \in \mathbb{Q} \right\}.$$

Proof. From the theory of abelian varieties, we know that $\mathrm{End}^0(\mathrm{Jac}(\mathrm{C}))$ is a 16-dimensional $\mathbb{Q}$-algebra. As $\dim_{\mathbb{Q}} \mathbb{Q}(\xi_5) = 4$, Proposition 3.5 implies that $\mathbb{Q}[\xi_5, \pi]$ is also 16-dimensional. As $\mathbb{Q}[\xi_5, \pi]$ is contained in $\mathrm{End}^0(\mathrm{Jac}(\mathrm{C}))$ the result follows.

The claim about the structure of $\mathbb{Q}[\xi_5, \pi]$ also follows from Proposition 3.5 since $\{1, \xi_5, \xi_5^2, \xi_5^3\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\xi_5)$. □

We have established in Theorem 2.1 that, for every pair D_1, D_2 of non-trivial divisors of order l on Jac(C) there is some $\phi \in \mathrm{End}(\mathrm{Jac}(\mathrm{C}))$ such that $e_l(D_1, \phi(D_2)) \neq 1$. We also know that $\mathrm{End}(\mathrm{Jac}(\mathrm{C}))$ is an order $\mathcal{O}$ in $\mathbb{Q}[\xi_5, \pi]$ which contains $\mathbb{Z}[\xi_5, \pi]$. Corollary 3.6 implies that $\phi = \sum_{i,j} \lambda_{i,j} \pi^i \xi_5^j$ where the $\lambda_{i,j} \in \mathbb{Q}$. Let m be the least common multiple of the denominators of the $\lambda_{i,j}$. Then $m\phi \in \mathbb{Z}[\xi_5, \pi]$. We now must make an assumption.

Assumption: We assume that ϕ may be chosen such that $\gcd(m, l) = 1$.

If one considers the case of elliptic curves, the assumption is simply that the index of the order $\mathbb{Z}[\pi, \xi_5]$ in the maximal order is not divisible by l. This cannot happen if l is sufficiently large. In the case of dimension 2 it is currently unclear to us whether it can ever happen or not. But in any case we do not expect it to occur for most examples.

Under the above assumption, we have that

$$e_l(D_1, m\phi(D_2)) = e_l(D_1, \phi(D_2))^m \neq 1.$$

Since $m\phi$ is an integer combination of the $\pi^i \xi_5^j$ it follows that for some pair (i, j) we have $e_l(D_1, \pi^i \xi_5^j(D_2)) \neq 1$ (otherwise, if all $e_l(D_1, \pi^i \xi_5^j(D_2)) = 1$ then $e_l(D_1, m\phi(D_2)) = 1$).

Hence, we have established that a combination of a power of ξ_5 and a power of π are sufficient for a distortion map if the above assumption is satisfied.

Example: Consider the divisor $D_1 \in \mathrm{Jac}(C)[l]$ which is defined over $\mathbb{F}_p$. We have $\pi(D_1) = D_1$. It is easy to show that, as long as the assumption holds, $e_l(D_1, \xi_5^j(D_1)) \neq 1$ for some $1 \leq j \leq 3$. This supports the suggestion in [3] of using ξ_5 as a distortion map. Note that when implementing pairings it is desirable to utilise denominator elimination, and so the map ξ_5^j would be combined with a trace operation to increase efficiency (see Scott [11] for an example of this in the elliptic case).

4. The van Wamelen cases

There are exactly 18 more isomorphism classes of curves $\tilde{\mathrm{C}}$ of genus two over $\mathbb{Q}$ with complex multiplication by an order in a CM field of degree 4. Explicit equations for these curves have been given by van Wamelen [14], [15]. Van Wamelen also provides an explicit description of the x-coordinate of the endomorphism α on Jac(C) which satisfies a degree four characteristic polynomial corresponding to the

CM field (it is possible to obtain a full description of the endomorphism from the x-coordinate). It turns out that all these CM fields have cyclic Galois group. Reducing such curves modulo supersingular primes of good reduction, one obtains curves over $\mathbb{F}_p$ whose endomorphism ring has a structure very similar to that of the curve in section 3.

For this section we assume that C is the reduction modulo p of one of van Wamelen's curves such that C is supersingular with characteristic polynomial of Frobenius equal to T^4+p^2 so that the embedding degree is $k=4$. For each of them we obtain results analogous to those in section 3, in particular Lemmas 3.2 and 3.3 apply in this case too.

Let $\tilde{\mathrm{C}}$ be a CM curve of genus two over $\mathbb{Q}$ and let α be a root of the corresponding CM polynomial. We write $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{\sigma_0 = id, \sigma_1, \sigma_2, \sigma_3\}$. Note that, in all examples considered, this is a cyclic group.

Let p be as above and let $j \in \{0,1,2,3\}$. Clearly, $\alpha\pi^j = \pi^j \alpha^{\sigma_{j(p)}}$, where $\sigma_{j(p)} \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. We make the further assumption that $\sigma_{j(p)}$ is a generator of the cyclic group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. This was the case for the example in section 3.

One can then prove the following result using exactly the same method as used to prove Proposition 3.5.

Proposition 4.1. *Let $\mathbb{Q}[\alpha,\pi]$ be the non-commutative $\mathbb{Q}$-algebra generated by α and π. Then $\mathbb{Q}[\alpha,\pi] = \mathbb{Q}(\alpha) \oplus \pi\mathbb{Q}(\alpha) \oplus \pi^2\mathbb{Q}(\alpha) \oplus \pi^3\mathbb{Q}(\alpha)$ as $\mathbb{Q}$-vector spaces.*

As a result, we have that $\mathbb{Q}[\alpha,\pi]$ is 16-dimensional as a $\mathbb{Q}$-vector space and, as before, under an assumption about the denominators m such that $m\phi \in \mathbb{Z}[\alpha,\pi]$ it follows that one can also choose a distortion map of the form $\pi^i\alpha^j$ with $0 \le i,j \le 3$. In other words, subject to the above assumptions on the choice of prime p, the van Wamelen curves are suitable for cryptography in the sense that, for every pair of divisors, one can easily find a distortion map which makes their pairing non-trivial.

In practice, the maps α are rather complicated and so, for efficiency reasons, the case $y^2 = x^5 + A$ seems to be the most appealing.

5. An example of a non-simple Jacobian

In the previous sections we have shown examples of supersingular abelian varieties all of whose endomorphisms can be relatively easily expressed (in the case $y^2 = x^5 + A$ they are even expressed in terms of maps on the curve).

We now discuss an example for which it seems to be impossible to express the full ring of endomorphisms in terms of nice maps on C or even on the Mumford representation of Jac(C). In this example, there is a subring of endomorphisms which can be easily described in terms of C, but this subring is too small for it to provide distortion maps for all pairs of divisors. This emphasises the obvious fact that one cannot always expect distortion maps on Jac(C) to be easily expressed in terms of the curve.

We illustrate with an example an approach which might be useful for constructing distortion maps in this situation. It is not clear whether this approach is practical for real applications. Note that, since we have seen more convenient examples such as $y^2 = x^5 + A$, it seems that curves like the one in this section are less interesting in practice.

Let $\tilde{\mathrm{C}}\colon y^2 = f(x) = x^6 + 1$ over $\mathbb{Q}$. Note that the non-singular projective curve associated with this model has two points ∞^+, ∞^- at infinity. To compute with

this curve we usually work modulo a prime p such that x^6+1 has a root modulo p and so there is an isomorphic model with a single point at infinity.

On $\tilde{\mathrm{C}}$ there is the automorphism

$$\xi_6 \colon (x,y) \mapsto (-\xi_3 x, y)$$

defined over $\mathbb{Q}(\sqrt{-3})$ where ξ_3 and ξ_6 are 3rd and 6-th roots of unity respectively.

This curve admits two morphisms to the elliptic curve $\tilde{E}\colon y^2 = x^3+1$, namely

$$\psi_1 \colon (x,y) \longmapsto (x^2, y)$$

and

$$\psi_2 \colon (x,y) \longmapsto \left(\frac{1}{x^2}, \frac{y}{x^3}\right).$$

It follows that $\mathrm{Jac}(\tilde{\mathrm{C}})$ is isogenous to the product $\tilde{E}\times\tilde{E}$ and so $\mathrm{Jac}(\tilde{\mathrm{C}})$ is not simple over $\mathbb{Q}$.

Since $\tilde{E}$ has j-invariant equal to zero, reducing $\tilde{E}$ modulo a prime $p \equiv 2 \pmod 3$ gives a supersingular elliptic curve E. Write C for $\tilde{C}$ reduced modulo $p \equiv 2 \pmod 3$. It follows that C is supersingular and that the characteristic polynomial of the Frobenius element $\pi \in \mathrm{End}(\mathrm{Jac}(\mathrm{C}))$ is $P(T) = (T^2+p)^2$. If $l \mid \mathrm{Jac}(\mathrm{C})(\mathbb{F}_p) = (p+1)^2$ then $l \mid p^2-1$, and so the embedding degree for C is $k=2$. For applications in cryptography, this may be less convenient than $k=4$.

Since $\mathrm{Jac}(C)$ is supersingular it follows that $\mathrm{End}^0(\mathrm{Jac}(\mathrm{C}))$ is a $\mathbb{Q}$-algebra which has dimension 16 as a vector space over $\mathbb{Q}$. However, the maps π and ξ_6 only generate a sub-algebra $\mathbb{Q}[\pi,\xi_6] \subseteq \mathrm{End}^0(\mathrm{Jac}(\mathrm{C}))$.

Lemma 5.1. *With notation as above, we have* $\dim_{\mathbb{Q}} \mathbb{Q}[\pi,\xi_6] = 4$.

Proof. Considering the explicit equations and using the fact that $p \equiv 2 \pmod 3$ implies that $\pi\xi_6 = -\xi_6\pi = \xi_6^5\pi$. Since π and ξ_6 satisfy quadratic polynomials it therefore follows that $\dim_{\mathbb{Q}} \mathbb{Q}[\pi,\xi_6] \leq 4$.

Also, the fact that π and ξ_6 do not commute implies that $\pi \notin \mathbb{Q}(\xi_6)$ and $\xi_6 \notin \mathbb{Q}(\pi)$. Hence $\dim_{\mathbb{Q}} \mathbb{Q}[\pi,\xi_6] > 2$. Finally, $\mathbb{Q}[\pi,\xi_6]$ is a $\mathbb{Q}(\xi_6)$ algebra so its dimension over $\mathbb{Q}$ is even. □

Since the dimension is only 4, we do not expect to always be able to choose distortion maps which are combinations of π and ξ_6. Indeed, one can easily generate explicit examples of divisors D_1, D_2 in $\mathrm{Jac}(\mathrm{C})$ such that $e_l(D_1, \phi(D_2)) = 1$ for all $\phi \in \mathrm{End}(\mathrm{Jac}(\mathrm{C})) \cap \mathbb{Q}[\pi,\xi_6]$.

The main observation is that $\mathrm{End}^0(E\times E) \cong M_2(\mathrm{End}^0(E))$ (see, for example, [13]). In our case, $\mathrm{End}^0(E) \cong \mathbb{Q}[\pi,\xi_3]$ is 4-dimensional as a $\mathbb{Q}$-vector space and so $M_2(\mathrm{End}^0(E))$ is 16-dimensional. One can clearly represent the action of an element

$$\Phi = \begin{pmatrix} \phi_1 & \phi_2 \\ \phi_3 & \phi_4 \end{pmatrix} \in M_2(\mathrm{End}(E))$$

on $E\times E$ as

$$\Phi(P,Q) = (\phi_1(P)+\phi_2(Q), \phi_3(P)+\phi_4(Q)).$$

While these endomorphisms are easily visualised on $E\times E$, it seems to be much less easy to view them directly on $\mathrm{Jac}(\mathrm{C})$.

Hence the natural way to proceed is to transform divisors in $\mathrm{Jac}(\mathrm{C})$ to pairs of points in $E\times E$ and compute the distortion maps there, and then to transform back to $\mathrm{Jac}(\mathrm{C})$.

We use the maps $\psi_i : \mathrm{C} \to E$. By the universal property of Jacobians, each of the maps ψ_i induces a map $\mathrm{Jac(C)} \to E$ which is a homomorphism composed with a translation. Fix ∞^+ as the base-point on C and the usual point at infinity ∞_E as the base-point on E. Since $\psi_1(\infty^+) = \infty_E$ it follows that ψ_1 induces a homomorphism from Jac(C) to E. The map on divisor classes is induced by linearity, in other words we simply map $\sum_P n_P(P) \in \mathrm{Jac(C)}$ to $\sum_P n_P \psi_1(P) \in E$. Since $\psi_2(\infty^+) = (0,1)$ on E we must define $\psi_2'(x,y) = \psi_2(x,y) + (0,-1)$. Then ψ_2' induces a homomorphism from Jac(C) to E.

Define

$$\Psi : \mathrm{Jac(C)} \to E \times E$$

as the map induced by linearity from $\Psi(P) = (\psi_1(P), \psi_2'(P))$. This is clearly a homomorphism of abelian varieties and one can check that in this case the kernel is trivial.

One can see that evaluating Ψ and computing the action of elements in $\mathrm{End}(E \times E)$ are straightforward, but there is a problem in that we are required to pull divisors back along Ψ to Jac(C). This can be solved using Gröbner basis ideas. Further investigation is required to assess the practicality of this approach. In any case, we have in principle solved the problem of computing distortion maps on Jac(C).

References

[1] A. A. Albert, *Structure of algebras*, AMS Colloq. Publ., 24, (1939).

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

[3] Y.-J. Choie and E. Lee, Implementation of tate pairing on hyperelliptic curves of genus 2, in J. I. Lim and D. H. Lee (eds.), ICISC 2003, Springer LNCS 2971 (2004) 97–111.

[4] G. Frey and H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves, *Math. Comp.*, **52** (1994) 865–874.

[5] M. Gagné, Identity-based encryption: a survey, CryptoBytes 6(1), RSA Laboratories (2003) 10–19.

[6] S. D. Galbraith, Supersingular curves in cryptography, in C. Boyd (ed.) ASIACRYPT 2001, Springer LNCS 2248 (2001) 495–513.

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

[8] K. G. Paterson, Cryptography from pairings: a snapshot of current research, Information Security Technical Report 7(3) (2002) 41–54.

[9] K. Paterson, Pairing based cryptography, Chapter 10 of [2].

[10] K. Rubin and A. Silverberg, Supersingular abelian varieties in cryptology, in M. Yung (ed.), CRYPTO 2002, Springer LNCS 2442 (2002) 336–353.

[11] M. Scott, Faster identity based encryption, *Elec. Letters*, Vol. 40, No. 14 (2004) 861.

[12] H. Stichtenoth and C. Xing, On the structure of the divisor class group of a class of curves over finite fields, *Arch. Math.*, **65** (1995) 141–150.

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

[14] P. van Wamelen, Examples of genus two CM curves defined over the rationals, *Math. Comp.*, vol. 68, no. 225 (1999) 307–320.

[15] P. van Wamelen, Proving that a genus 2 curve has complex multiplication, *Math. Comp.*, vol. 68, no. 228 (1999) 1663–1677.

[16] E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, in B. Pfitzmann (ed.), EUROCRYPT 2001, Springer LNCS 2045 (2001) 195–210.

[17] E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, *J. Crypt.*, 17, No. 4 (2004) 277–296.

Mathematics Department. Royal Holloway University of London, Egham, Surrey TW20 0EX, UK., and, Departament de Matemàtica Aplicada 4, Universitat Politècnica de Catalunya, Jordi Girona 1-3, 08034 Barcelona, Spain.