

ZETA FUNCTION AND CRYPTOGRAPHIC EXPONENT OF SUPERSINGULAR CURVES OF GENUS 2

GABRIEL CARDONA AND ENRIC NART

ABSTRACT. We compute in a direct (not algorithmic) way the zeta function of all supersingular curves of genus 2 over a finite field k , with many geometric automorphisms. We display these computations in an appendix where we select a family of representatives of all these curves up to \bar{k} -isomorphism and we exhibit equations and the zeta function of all their \bar{k}/k -twists. As an application we obtain a direct computation of the cryptographic exponent of the Jacobians of these curves.

INTRODUCTION

One-round tripartite Diffie-Hellman, identity based encryption, and short digital signatures are some problems for which good solutions have recently been found, making critical use of pairings on supersingular abelian varieties over a finite field k . The cryptographic exponent c_A of a supersingular abelian variety A is a half-integer that measures the security against an attack on the DL problem based on the Weil or the Tate pairings. Also, it is relevant to determine when pairings can be efficiently computed. Rubin and Silverberg showed in [RS04] that this invariant is determined by the zeta function of A .

In this paper we give a direct, non-algorithmic procedure to compute the zeta function of a supersingular curve of genus 2, providing thus a direct computation of the cryptographic exponent of its Jacobian. This is achieved in Sect. 1. For even characteristic the results are based on [MN06] and are summarized in Table 2; for odd characteristic we use results of Xing and Zhu on the structure of the group of k -rational points of a supersingular abelian surface and we almost determine the zeta function in terms of the Galois structure of the set of Weierstrass points of the curve (Tables 3, 4). In the rest of the paper we obtain a complete answer in the case of curves with many automorphisms. In Sect. 2 we study the extra information provided by these automorphisms and we show how to obtain the relevant data to compute the zeta function of a twisted curve in terms of data of the original curve and the 1-cocycle defining the twist. In Sect. 3 we select a family of representatives of these curves up to \bar{k} -isomorphism and we apply the techniques of the previous section to deal with each curve and all its \bar{k}/k -twists. The results are displayed in an Appendix in the form of tables.

In what cryptographic applications of pairings concerns, curves with many automorphisms are interesting too because they are natural candidates to provide

The authors acknowledge support from the projects MTM2006-15038-C02-01 and MTM2006-11391 from the Spanish MEC.

distortion maps on the Jacobian. In this regard the computation of the zeta function is a necessary step to study the structure of the endomorphism ring of the Jacobian (cf. [GPRS06]).

1. ZETA FUNCTION AND CRYPTOGRAPHIC EXPONENT

Let p be a prime number and let $k = \mathbb{F}_q$ be a finite field of characteristic p . We denote by k_n the extension of degree n of k in a fixed algebraic closure \bar{k} , $G_k := \text{Gal}(\bar{k}/k)$ is the absolute Galois group of k , and $\sigma \in G_k$ the Frobenius automorphism.

Let C be a projective, smooth, geometrically irreducible, supersingular curve of genus 2 defined over k . The Jacobian J of C is a supersingular abelian surface over k (the p -torsion subgroup of $J(\bar{k})$ is trivial). Let us recall how supersingularity is reflected in a model of the curve C :

Theorem 1.1. *If p is odd, any curve of genus 2 defined over k admits an affine Weierstrass model $y^2 = f(x)$, with $f(x)$ a separable polynomial in $k[x]$ of degree 5 or 6. The curve is supersingular if and only if $M^{(p)}M = 0$, where $M, M^{(p)}$ are the matrices:*

$$M = \begin{pmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{pmatrix}, \quad M^{(p)} = \begin{pmatrix} c_{p-1}^p & c_{p-2}^p \\ c_{2p-1}^p & c_{2p-2}^p \end{pmatrix}, \quad f(x)^{(p-1)/2} = \sum_{j \geq 0} c_j x^j.$$

If $p = 2$ a curve of genus 2 defined over k is supersingular if and only if it admits an affine Artin-Schreier model $y^2 + y = f(x)$, with $f(x)$ an arbitrary polynomial in $k[x]$ of degree 5.

For the first statement see [Yui78] or [IKO86], for the second see [VV92].

For any simple supersingular abelian variety A defined over k , Rubin and Silverberg computed in [RS04] the *cryptographic exponent* c_A , defined as the half-integer such that q^{c_A} is the size of the smallest field F such that every cyclic subgroup of $A(k)$ can be embedded in F^* . This invariant refines the concept of *embedding degree*, formerly introduced as a measure of the security of the abelian variety against the attacks to the DLP by using the Weil pairing [MOV93] or the Tate pairing [FR94] (see for instance [Gal01]).

Let us recall the result of Rubin-Silverberg, adapted to the dimension two case. After classical results of Tate and Honda, the isogeny class of A is determined by the Weil polynomial of A , $f_A(x) = x^4 + rx^3 + sx^2 + qrx + q^2 \in \mathbb{Z}[x]$, which is the characteristic polynomial of the Frobenius endomorphism of the surface. For A supersingular the roots of $f_A(x)$ in $\bar{\mathbb{Q}}$ are of the form $\sqrt{q}\zeta$, where \sqrt{q} is the positive square root of q and ζ is a primitive m -th root of unity.

Theorem 1.2. *Suppose A is a simple supersingular abelian surface over \mathbb{F}_q and let $\ell > 5$ be any prime number dividing $|A(\mathbb{F}_q)|$. Then, the smallest half-integer c_A such that $q^{c_A} - 1$ is an integer divisible by ℓ is given by*

$$c_A = \begin{cases} m/2, & \text{if } q \text{ is a square,} \\ m/(2, m), & \text{if } q \text{ is not a square.} \end{cases}$$

In particular, the cryptographic exponent c_A is an invariant of the isogeny class of A . The complete list of simple supersingular isogeny classes of abelian surfaces can be found in [MN02, Thm. 2.9]. It is straightforward to find out the m -th root of unity in each case. We display the computation of c_A in Table 1.

TABLE 1. Cryptographic exponent c_A of the simple supersingular abelian surface A with Weil polynomial $f_A(x) = x^4 + rx^3 + sx^2 + qrx + q^2$

(r, s)	conditions on p and q	c_A
$(0, -2q)$	q nonsquare	1
$(0, 2q)$	q square, $p \equiv 1 \pmod{4}$	2
$(2\sqrt{q}, 3q)$	q square, $p \equiv 1 \pmod{3}$	3/2
$(-2\sqrt{q}, 3q)$	q square, $p \equiv 1 \pmod{3}$	3
$(0, 0)$	$(q$ nonsquare, $p \not\equiv 2$) or $(q$ square, $p \not\equiv 1 \pmod{8})$	4
$(0, q)$	q nonsquare	3
$(0, -q)$	$(q$ nonsquare, $p \not\equiv 3$) or $(q$ square, $p \not\equiv 1 \pmod{12})$	6
(\sqrt{q}, q)	q square, $p \not\equiv 1 \pmod{5}$	5/2
$(-\sqrt{q}, q)$	q square, $p \not\equiv 1 \pmod{5}$	5
$(\pm\sqrt{5q}, 3q)$	q nonsquare, $p = 5$	5
$(\pm\sqrt{2q}, q)$	q nonsquare, $p = 2$	12

Therefore, the computation of the cryptographic exponent of the Jacobian J of a supersingular curve C amounts to the computation of the Weil polynomial of J , which is related in a well-known way to the zeta function of C . We shall call $f_J(x)$ the *Weil polynomial of C* too.

The computation of $f_J(x)$ has deserved a lot of attention because for the cryptographic applications one needs to know the cardinality $|J(\mathbb{F}_q)| = f_J(1)$ of the group of rational points of the Jacobian. However, in the supersingular case the current “counting points” algorithms are not necessary because there are more direct ways to compute the polynomial $f_J(x)$.

The aim of this section is to present these explicit methods, which take a different form for p odd or even. For $p = 2$ the computation of $f_J(x)$ is an immediate consequence of the methods of [MN06], based on ideas of van der Geer-van der Vlugt; for $p > 2$ we derive our results from the group structure of $J(\mathbb{F}_q)$, determined in [Xin96], [Zhu00], and from the exact knowledge of what isogeny classes of abelian surfaces do contain Jacobians [HNR06]. In both cases we shall show that $f_J(x)$ is almost determined by the structure as a Galois set of a finite subset of \bar{k} , easy to compute from the defining equation of C .

1.1. Computation of the Zeta Function when $p = 2$. We denote simply by tr the absolute trace $\text{tr}_{k/\mathbb{F}_2}$. Recall that $\ker(\text{tr}) = \{x + x^2 \mid x \in k\}$ is an \mathbb{F}_2 -linear subspace of k of codimension 1.

Every projective smooth geometrically irreducible supersingular curve C of genus 2 defined over k admits an affine Artin-Schreier model of the type:

$$C: \quad y^2 + y = ax^5 + bx^3 + cx + d, \quad a \in k^*, b, c, d \in k,$$

which has only one point at infinity [VV92]. The change of variables $y = y + u$, $u \in k$, allows us to suppose that $d = 0$ or $d = d_0$, with $d_0 \in k \setminus \ker(\text{tr})$ fixed. Twisting C by the hyperelliptic twist consists in adding d_0 to the defining equation. If we denote by J' the Jacobian of the twisted curve we have $f_{J'}(x) = f_J(-x)$. Thus, for the computation of $f_J(x)$ we can assume that $d = 0$.

The structure as a G_k -set of the set of roots in \bar{k} of the polynomial $P(x) = a^2x^5 + b^2x + a \in k[x]$ almost determines the zeta function of C [MN06, Sect.3].

TABLE 2. Weil polynomial $x^4 + rx^3 + sx^2 + qrx + q^2$ of the curve $y^2 + y = ax^5 + bx^3 + cx$, for q nonsquare (left) and q square (right)

$P(x)$	N, M	(r, s)
(1)(4)	$N = 0$ $N = 1$	$(\pm\sqrt{2q}, 2q)$ $(0, 0)$
(2)(3)	$M = 0$ $M = 1$	$(\pm\sqrt{2q}, q)$ $(0, q)$
(1) ³ (2)	$N = 0$ $N = 1$ $N = 2$ $N = 3$	$(\pm 2\sqrt{2q}, 4q)$ $(0, 2q)$ $(0, 0)$ $(0, -2q)$

$P(x)$	N, M	(r, s)
(5)		$(\pm\sqrt{q}, q)$
(1) ² (3)	$N = 0$ $N = 1$ $N = 2$	$(0, -q)$ $(0, q)$ $(\pm 2\sqrt{q}, 3q)$
(1)(2) ²	$M = 0$ $M = 1$ $M = 2$	$(\pm 2\sqrt{q}, 2q)$ $(0, 0)$ $(0, 2q)$
(1) ⁵	$N = 1$ $N = 3$ $N = 5$	$(0, -2q)$ $(0, 2q)$ $(\pm 4\sqrt{q}, 6q)$

In Table 2 we write $P(x) = (n_1)^{r_1}(n_2)^{r_2} \cdots (n_m)^{r_m}$ to indicate that r_i of the irreducible factors of $P(x)$ have degree n_i . Also, we consider the linear operator $T(x) := \text{tr}((c + b^2a^{-1})x)$ and we define

$N :=$ number of roots $z \in k$ of $P(x)$ s.t. $T(z) = 0$,

$M :=$ number of irred. quadratic factors $x^2 + vx + w$ of $P(x)$ s.t. $T(v) = 0$.

The ambiguity of the sign of r can be solved by computing nD in the Jacobian, where n is one of the presumed values of $|J(\mathbb{F}_q)|$ and D is a random rational divisor of degree 0.

1.2. Computation of the Zeta Function when p is odd. Let A be a super-singular abelian surface over k and let $\text{rk}_2(A) := \dim_{\mathbb{F}_2}(A[2](k))$.

The structure of $A(k)$ as an abelian group was studied in [Xin96], [Zhu00], where it is proven that it is almost determined by the isogeny class of A . In fact, if $F_i(x)$ are the different irreducible factors of $f_A(x)$ in $\mathbb{Z}[x]$:

$$f_A(x) = \prod_{i=1}^s F_i(x)^{e_i}, \quad 1 \leq s \leq 2 \quad \implies \quad A(k) \simeq \oplus_{i=1}^s (\mathbb{Z}/F_i(1)\mathbb{Z})^{e_i},$$

except for the following cases:

- (a) $p \equiv 3 \pmod{4}$, q is not a square and $f_A(x) = (x^2 + q)^2$,
- (b) $p \equiv 1 \pmod{4}$, q is not a square and $f_A(x) = (x^2 - q)^2$.
- (c) q is a square and $f_A(x) = (x^2 - q)^2$.

The possible structure of $A(k)$ in cases (a) and (b) is:

$$A(k) \simeq (\mathbb{Z}/F(1)\mathbb{Z})^m \oplus (\mathbb{Z}/(F(1)/2)\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})^n,$$

where $F(x)$ denotes respectively $x^2 + q$, $x^2 - q$, and m, n are non-negative integers such that $m + n = 2$ [Zhu00, Thm. 1.1]. In case (c) we have either:

$$\begin{aligned} A(k) &\simeq (\mathbb{Z}/((q-1)/2)\mathbb{Z})^2 \oplus (\mathbb{Z}/2\mathbb{Z})^2, & \text{or} \\ A(k) &\simeq (\mathbb{Z}/((q-1)/2^m)\mathbb{Z}) \oplus (\mathbb{Z}/((q-1)/2^n)\mathbb{Z}) \oplus (\mathbb{Z}/2^{m+n}\mathbb{Z}), \end{aligned}$$

where $0 \leq m, n \leq v_2(q-1)$ [Xin96, Thm. 3]. In this last case we have $\text{rk}_2(A) > 1$; in fact, $v_2(1 - \sqrt{q}) + v_2(1 + \sqrt{q}) = v_2(1 - q) = (1/2)v_2(F(1))$ and we can apply [Xin96, Lem. 4] to conclude that $A(k)$ has a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

TABLE 3. Weil polynomial $x^4 + rx^3 + sx^2 + qrx + q^2$ of the curve C when q is nonsquare. The sign ϵ is the Legendre symbol $(-1/p)$

W	p	$\text{rk}_2(J)$	(r, s)
$(1)^6$ or $(1)^4(2)$		4, 3	$(0, -2\epsilon q)$
$(1)^2(2)^2$ or $(2)^3$		2	$(0, \pm 2q)$
$(1)^3(3)$		2	not possible
$(1)(2)(3)$	$p > 3$ $p = 3$	1	not possible $(\pm\sqrt{3}q, 2q)$
$(1)^2(4)$ or $(2)(4)$		1	$(0, 0)$
$(1)(5)$	$p \neq 5$ $p = 5$	0	not possible $(\pm\sqrt{5}q, 3q)$
$(3)^2$	$p \equiv 1 \pmod{3}$ $p \equiv -1 \pmod{3}$ $p = 3$	0	$(0, q)$ $(0, \epsilon q)$ not possible
(6)	$p \equiv -1 \pmod{3}$ $p \not\equiv -1 \pmod{3}$	0	$(0, \pm q)$ $(0, q)$

Consider now a supersingular curve C of genus 2 defined over k , given by a Weierstrass equation $y^2 = f(x)$, for some separable polynomial $f(x) \in k[x]$ of degree 5 or 6. Let J be its Jacobian variety, $W = \{P_0, P_1, P_2, P_3, P_4, P_5\} \subseteq C(\bar{k})$ the set of Weierstrass points of C , and $W(k) \subseteq W$ the subset of k -rational Weierstrass points. Our aim is to show that the structure of W as a G_k -set contains enough information on the 2-adic value of $|C(k)|$ and $|J(k)|$ to almost determine the polynomial $f_J(x) = x^4 + rx^3 + sx^2 + qrx + q^2$.

From the fundamental identities

$$|C(k)| = q + 1 + r, \quad |J(k)| = f_J(1) = (q^2 + 1) + (q + 1)r + s,$$

and the free action of the hyperelliptic involution on $C(k) \setminus W(k)$ we get

$$(1) \quad r \equiv |W(k)| \pmod{2}, \quad s \equiv |J(k)| \pmod{2}.$$

On the other hand, $J[2]$ is represented by the classes of the 15 divisors:

$$P_i - P_0, \quad 1 \leq i \leq 5, \quad \text{and} \quad P_i + P_j - 2P_0, \quad 1 \leq i < j \leq 5,$$

together with the trivial class.

Lemma 1.3. *Let $D = P_i - P_j$, with $i \neq j$, or $D = P_i + P_j - 2P_0$, with $0, i, j$ pairwise different. Then, the class of the divisor D is k -rational if and only if P_i, P_j are both k -rational or quadratic conjugate.*

Hence, the Galois structure of W determines $\text{rk}_2(J)$ and this limits the possible values of the zeta function of C . Our final results are given in Tables 3, 4, where we write $W = (n_1)^{r_1}(n_2)^{r_2} \cdots (n_m)^{r_m}$ to indicate that there are r_i G_k -orbits of length n_i of Weierstrass points. If $f(x)$ has degree 6 this Galois structure mimics the decomposition $f(x) = (n_1)^{r_1}(n_2)^{r_2} \cdots (n_m)^{r_m}$ (same notation as in Sect. 1.1) of $f(x)$ into a product of irreducible polynomials $k[x]$. If $f(x)$ has degree 5 then $W = (1)f(x)$, because in these models the point at infinity is a k -rational Weierstrass point.

The proof of the content of Tables 3 and 4 is elementary, but long. Instead of giving all details we only sketch the main ideas:

TABLE 4. Weil polynomial $x^4 + rx^3 + sx^2 + qrx + q^2$ of the curve C when q is a square

W	p	$\text{rk}_2(J)$	(r, s)
$(1)^6$		4	$(0, -2q)$ or $(\pm 4\sqrt{q}, 6q)$
$(1)^4(2)$		3	$(0, -2q)$
$(1)^2(2)^2$ or $(2)^3$		2	$(0, \pm 2q)$
$(1)^3(3)$	$p > 3$ $p = 3$	2	not possible $(\pm\sqrt{q}, 0)$
$(1)(2)(3)$		1	not possible
$(1)^2(4)$ or $(2)(4)$	$p \equiv 1 \pmod{8}$ $p \not\equiv 1 \pmod{8}$	1	not possible $(0, 0)$
$(1)(5)$	$p \equiv 1 \pmod{5}$ $p \not\equiv 1 \pmod{5}$	0	not possible $(\pm\sqrt{q}, q)$
$(3)^2$			$(0, q)$ or $(\pm 2\sqrt{q}, 3q)$
(6)	$p \equiv 5 \pmod{12}$ $p \not\equiv 5 \pmod{12}$	0	$(0, \pm q)$ $(0, q)$

(I) Waterhouse determined all possible isogeny classes of supersingular elliptic curves [Wat69]. Thus, it is possible to write down all isogeny classes of supersingular abelian surfaces by adding to the simple classes given in Table 1 the split isogeny classes. By [HNR06] we know exactly what isogeny classes of abelian surfaces do not contain Jacobians and they can be dropped from the list. By the results of Xing and Zhu we can distribute the remaining isogeny classes according to the possible values of rk_2 .

(II) Each structure of W as a G_k -set determines the value of rk_2 and, after (I), it has a reduced number of possibilities for the isogeny classes. By using (1) and looking for some incoherence in the behaviour under scalar extension to k_2 or k_3 of both, the Galois structure of W and the possible associated isogeny classes, we can still discard some of these possibilities.

In practice, among the few possibilities left in Tables 3 and 4 we can single out the isogeny class of the Jacobian of any given supersingular curve by computing iterates of random divisors of degree zero. However, if C has many automorphisms they provide enough extra information to completely determine the zeta function. This will be carried out in the rest of the paper. In the Appendix we display equations of the supersingular curves with many automorphisms and their Weil polynomial.

2. ZETA FUNCTION OF TWISTS

In this section we review some basic facts about twists and we show how to compute different properties of a twisted curve in terms of the defining 1-cocycle. From now on the ground field k will have odd characteristic.

Let C be a supersingular curve of genus 2 defined over k and let $W \subseteq C(\bar{k})$ be the set of Weierstrass points of C . We denote by $\text{Aut}(C)$ the k -automorphism group of C and by $\text{Aut}_{\bar{k}}(C)$ the full automorphism group of C .

Let $\phi: C \longrightarrow \mathbb{P}^1$ be a fixed k -morphism of degree 2 and consider the group of reduced geometric automorphisms of C :

$$\text{Aut}'_{\bar{k}}(C) := \{u' \in \text{Aut}_{\bar{k}}(\mathbb{P}^1) \mid u'(\phi(W)) = \phi(W)\} .$$

We denote by $\text{Aut}'(C)$ the subgroup of reduced automorphisms defined over k .

Any automorphism u of C fits into a commutative diagram:

$$\begin{array}{ccc} C & \xrightarrow{u} & C \\ \downarrow \phi & & \downarrow \phi \\ \mathbb{P}^1 & \xrightarrow{u'} & \mathbb{P}^1 \end{array}$$

for certain uniquely determined reduced automorphism u' . The map $u \mapsto u'$ is a group homomorphism (depending on ϕ) and we have a central exact sequence of groups compatible with Galois action:

$$1 \longrightarrow \{1, \iota\} \longrightarrow \text{Aut}_{\bar{k}}(C) \xrightarrow{\phi} \text{Aut}'_{\bar{k}}(C) \longrightarrow 1,$$

where ι is the hyperelliptic involution. This leads to a long exact sequence of Galois cohomology sets:

$$(2) \quad 1 \rightarrow \{1, \iota\} \rightarrow \text{Aut}(C) \xrightarrow{\phi} \text{Aut}'(C) \xrightarrow{\delta} H^1(G_k, \{1, \iota\}) \rightarrow H^1(G_k, \text{Aut}_{\bar{k}}(C)) \rightarrow \\ \rightarrow H^1(G_k, \text{Aut}'_{\bar{k}}(C)) \rightarrow H^2(G_k, \{1, \iota\}) \simeq \text{Br}_2(k) = 0 .$$

The \bar{k}/k -twists of C are parameterized by the pointed set $H^1(G_k, \text{Aut}_{\bar{k}}(C))$ and, since k is a finite field, a 1-cocycle is determined just by the choice of an automorphism $v \in \text{Aut}_{\bar{k}}(C)$. The twisted curve C_v associated to v is defined over k and is determined, up to k -isomorphism, by the existence of a \bar{k} -isomorphism $f: C \longrightarrow C_v$, such that $f^{-1}f^\sigma = v$.

For instance, the choice $v = \iota$ corresponds to the hyperelliptic twist C' ; if C is given by a Weierstrass equation $y^2 = f(x)$ then C' admits the model $y^2 = tf(x)$, for $t \in k^* \setminus (k^*)^2$. We say that C is *self-dual* if it is k -isomorphic to its hyperelliptic twist. If $f_J(x)$ is the Weil polynomial of C , the Weil polynomial of C' is $f_{J'}(x) = f_J(-x)$; in particular, for a self-dual curve one has $f_J(x) = x^4 + sx^2 + q^2$ for some integer s .

It is easy to deduce from (2) the following criterion for self-duality:

Lemma 2.1. *The curve C is self-dual if and only if $|\text{Aut}'(C)| = |\text{Aut}(C)|$.*

One can easily compute the data $\text{Aut}(C_v)$, $\text{Aut}'(C_v)$ of the twisted curve C_v , in terms of $\text{Aut}_{\bar{k}}(C)$, $\text{Aut}'_{\bar{k}}(C)$ and the 1-cocycle v .

Let $f: C \longrightarrow C_v$ be a geometric isomorphism such that $f^{-1}f^\sigma = v$. We have $\text{Aut}_{\bar{k}}(C_v) = f \text{Aut}_{\bar{k}}(C) f^{-1}$, and the k -automorphism group is

$$(3) \quad \text{Aut}(C_v) = \{fuf^{-1} \mid u \in \text{Aut}_{\bar{k}}(C), uv = vu^\sigma\} .$$

Once we fix any k -morphism of degree two, $\phi_v: C_v \longrightarrow \mathbb{P}^1$, it determines a unique geometric automorphism f' of \mathbb{P}^1 such that $\phi_v f = f' \phi$. The reduced group of k -automorphisms of C_v is

$$(4) \quad \text{Aut}'(C_v) = \{f'u'(f')^{-1} \mid u' \in \text{Aut}'_{\bar{k}}(C), u'v' = v'(u')^\sigma\} .$$

In order to compute the zeta function of C_v we consider the geometric isomorphism $f: J \longrightarrow J_v$ induced by f . We still have $f^{-1}f^\sigma = v_*$, where v_* is the

automorphism of J induced by v . Clearly, $\pi_v f = f^\sigma \pi$, where π, π_v are the respective q -power Frobenius endomorphisms of J, J_v . Hence,

$$f^{-1} \pi_v f = f^{-1} f^\sigma (f^\sigma)^{-1} \pi_v f = v_* \pi .$$

In particular, π_v has the same characteristic polynomial than $v_* \pi$. From this fact one can deduce two crucial results (cf. [HNR06, Props.13.1,13.4]).

Proposition 2.2. *Suppose q is a square. Let C be a supersingular genus 2 curve over k with Weil polynomial $(x + \sqrt{q})^4$ and let v be a geometric automorphism of C , $v \neq 1, \iota$. Then, the Weil polynomial $x^4 + rx^3 + sx^2 + rx + q^2$ of C_v is determined as follows in terms of v (in the column $v^6 = 1$ we suppose $v^2 \neq 1, v^3 \neq 1, \iota$):*

v	$v^2 = 1$	$v^2 = \iota$	$v^3 = 1$	$v^3 = \iota$	$v^4 = \iota$	$v^5 = 1$	$v^5 = \iota$	$v^6 = 1$	$v^6 = \iota$
(r, s)	$(0, -2q)$	$(0, 2q)$	$(-2\sqrt{q}, 3q)$	$(2\sqrt{q}, 3q)$	$(0, 0)$	$(-\sqrt{q}, q)$	(\sqrt{q}, q)	$(0, q)$	$(0, -q)$

Proposition 2.3. *Suppose q is nonsquare. Let C be a supersingular genus 2 curve over k with Weil polynomial $(x^2 + \epsilon q)^2$, $\epsilon \in \{1, -1\}$, and let v be a geometric automorphism of C . Then, the Weil polynomial $x^4 + rx^3 + sx^2 + rx + q^2$ of C_v is determined as follows in terms of the order n of the automorphism vv^σ :*

n	1	2	3	4	6
(r, s)	$(0, 2\epsilon q)$	$(0, -2\epsilon q)$	$(0, -\epsilon q)$	$(0, 0)$	$(0, \epsilon q)$

In applying these results the transitivity property of twists can be helpful.

Lemma 2.4. *Let u, v be automorphisms of C and let $f: C \rightarrow C_v$ be a geometric isomorphism with $f^{-1} f^\sigma = v$. Then the curve C_u is the twist of C_v associated to the automorphism $fuv^{-1}f^{-1}$ of C_v .*

For a curve with a large k -automorphism group the following remark, together with Tables 3 and 4, determines in some cases the zeta function:

Lemma 2.5. *Let $\mathcal{F} \subseteq C(k)$ be the subset of k -rational points of C that are fixed by some non-trivial k -automorphism of C . Then,*

$$|C(k)| \equiv |\mathcal{F}| \pmod{|\text{Aut}(C)|} .$$

Proof. The group $\text{Aut}(C)$ acts freely on $C(k) \setminus \mathcal{F}$. □

Note that \mathcal{F} contains the set $W(k)$ of k -rational Weierstrass points, all of them fixed by the hyperelliptic involution ι of C .

In order to apply this result to the twisted curve C_v we need to compute the G_k -set structure of W_v and $|\mathcal{F}_v|$ solely in terms of v .

Lemma 2.6. (1) *For any $P \in W$ the length of the G_k -orbit of $f(P) \in W_v$ is the minimum positive integer n such that $v v^\sigma \cdots v^{\sigma^{n-1}}(P^{\sigma^n}) = P$. In particular, $|W_v(k)| = |\{P \in W \mid v(P^\sigma) = P\}|$.*

(2) *The map f^{-1} establishes a bijection between \mathcal{F}_v and the set $\{P \in C(\bar{k}) \mid v(P^\sigma) = P = u(P) \text{ for some } 1 \neq u \in \text{Aut}_{\bar{k}}(C), \text{ s.t. } u v = v u^\sigma\}$.*

3. SUPERSINGULAR CURVES WITH MANY AUTOMORPHISMS

For several cryptographic applications of the Tate pairing the use of distortion maps is essential. A distortion map is an endomorphism ψ of the Jacobian J of C that provides an input for which the value of the pairing is non-trivial:

$e_\ell(D_1, \psi(D_2)) \neq 1$ for some fixed ℓ -torsion divisors D_1, D_2 . The existence of such a map is guaranteed, but in practice it is hard to find it in an efficient way. Usually, one can start with a nice curve C with many automorphisms, consider a concrete automorphism $u \neq 1, u \neq \iota$, and look for a distortion map ψ in the subring $\mathbb{Z}[\pi, u_*] \subseteq \text{End}(J)$, where π is the Frobenius endomorphism of J and u_* is the automorphism of the Jacobian induced by u . If $\mathbb{Z}[\pi, u_*] = \text{End}(J)$ it is highly probable that a distortion map is found. If $\mathbb{Z}[\pi, u_*] \neq \text{End}(J)$ it can be a hard problem to prove that some nice candidate is a distortion map, but at least one is able most of the time to find a “denominator” m such that $m\psi$ lies in the subring $\mathbb{Z}[\pi, u_*]$; in this case, if $\ell \nmid m$ one can use $m\psi$ as a distortion map on divisors of order ℓ . Several examples are discussed in [GPRS06].

The aim of this section is to exhibit all supersingular curves of genus 2 with many automorphisms, describe their automorphisms, and compute the characteristic polynomial of π , which is always a necessary ingredient in order to analyze the structure of the ring $\mathbb{Z}[\pi, u_*]$. Recall that a curve C is said to have *many automorphisms* if it has some geometric automorphism other than the identity and the hyperelliptic involution; in other words, if $|\text{Aut}_{\bar{k}}(C)| > 2$.

Igusa found equations for all geometric curves of genus 2 with many automorphisms, and he grouped these curves in six families according to the possible structure of the automorphism group [Igu60], [IKO86]. Cardona and Quer found a faithful and complete system of representatives of all these curves up to \bar{k} -isomorphism and they gave conditions to ensure the exact structure of the automorphism group of each concrete model [Car03], [CQ06]. The following theorem sums up these results.

Theorem 3.1. *Any curve of genus 2 with many automorphisms is geometrically isomorphic to one and only one of the curves in these six families:*

Equation of C		$\text{Aut}_{\bar{k}}'(C)$	$\text{Aut}_{\bar{k}}(C)$
$y^2 = x^6 + ax^4 + bx^2 + 1$	a, b satisfy (5)	C_2	$C_2 \times C_2$
$y^2 = x^5 + x^3 + ax$	$a \neq 0, 1/4, 9/100$	$C_2 \times C_2$	D_8
$y^2 = x^6 + x^3 + a$	$p \neq 3, a \neq 0, 1/4, -1/50$	S_3	D_{12}
$y^2 = ax^6 + x^4 + x^2 + 1$	$p = 3, a \neq 0$	S_3	D_{12}
$y^2 = x^6 - 1$	$p \neq 3, 5$	D_{12}	$2D_{12}$
$y^2 = x^5 - x$	$p \neq 5$	S_4	\tilde{S}_4
	$p = 5$	$\text{PGL}_2(\mathbb{F}_5)$	\tilde{S}_5
$y^2 = x^5 - 1$	$p \neq 5$	C_5	C_{10}

$$(5) \quad (4c^3 - d^2)(c^2 - 4d + 18c - 27)(c^2 - 4d - 110c + 1125) \neq 0, \quad c := ab, \quad d := a^3 + b^3.$$

Ibukiyama-Katsura-Oort determined, using Theorem 1.1, when the last three curves are supersingular [IKO86, Props. 1.11, 1.12, 1.13]:

$$\begin{aligned} y^2 = x^6 - 1 & \text{ is supersingular iff } p \equiv -1 \pmod{3} \\ y^2 = x^5 - x & \text{ is supersingular iff } p \equiv 5, 7 \pmod{8} \\ y^2 = x^5 - 1 & \text{ is supersingular iff } p \equiv 2, 3, 4 \pmod{5} \end{aligned}$$

It is immediate to check that $y^2 = ax^6 + x^4 + x^2 + 1$ is never supersingular if $p = 3$. One can apply Theorem 1.1 to the other curves in the first three families to distinguish the supersingular ones.

Theorem 3.2. *Suppose q is a square and let C be a supersingular curve belonging to one of the first five families of Theorem 3.1. Then there a twist of C with Weil polynomial $(x + \sqrt{q})^4$, and this twist is unique.*

Proof. Let E be a supersingular elliptic curve defined over \mathbb{F}_p . By [IKO86, Prop. 1.3] the Jacobian J of C is geometrically isomorphic to the product of two supersingular elliptic curves, which is in turn isomorphic to $E \times E$ by a well-known theorem of Deligne. The principally polarized surface (J, Θ) is thus geometrically isomorphic to $(E \times E, \lambda)$ for some principal polarization λ . Since E has all endomorphisms defined over \mathbb{F}_{p^2} , $(E \times E, \lambda)$ is defined over \mathbb{F}_{p^2} and by a classical result of Weil it is \mathbb{F}_{p^2} -isomorphic to the canonically polarized Jacobian of a curve C_0 defined over \mathbb{F}_{p^2} . By Torelli, C_0 is a twist of C . The Weil polynomial of C_0 is $(x \pm \sqrt{q})^4$ because the Frobenius polynomial of E is $x^2 + p$. The fact that C_0 and C'_0 are the unique twists of C_0 with Weil polynomial $(x \pm \sqrt{q})^4$ is consequence of Proposition 2.2. \square

Corollary 3.3. *Under the same assumptions:*

- (1) *The Weil polynomial of C is $(x \pm \sqrt{q})^4$ if and only if $W = (1)^6$.*
- (2) *If C belongs to one of the first three families of Theorem 3.1, then it admits no twist with Weil polynomial $x^4 \pm qx^2 + q^2$ or $x^4 + q^2$.*
- (3) *If any of the curves $y^2 = x^5 + x^3 + ax$, $y^2 = x^6 + x^3 + a$ is supersingular then $a \in \mathbb{F}_{p^2}$.*

Proof. (1) By Table 4, the set W_0 of Weierstrass points of C_0 has G_k -structure $W_0 = (1)^6$ and Lemma 2.6 shows that for all automorphisms $v \neq 1, \iota$ one has $W_v \neq (1)^6$; thus, only the twists C_0 and C'_0 have $W = (1)^6$.

(2) The geometric automorphisms v of C_0 satisfy neither $v^6 = 1$, $v^2 \neq 1$, $v^3 \neq 1, \iota$, nor $v^6 = \iota$, nor $v^4 = \iota$; thus, by Proposition 2.2 the Weil polynomial of a twist of C_0 is neither $x^4 \pm qx^2 + q^2$ nor $x^4 + q^2$.

(3) The Igusa invariants of C_0 take values in \mathbb{F}_{p^2} and a can be expressed in terms of these invariants [CQ05]. \square

In a series of papers Cardona and Quer studied the possible structures of the pointed sets $H^1(G_k, \text{Aut}_{\bar{k}}(C))$ and found representatives $v \in \text{Aut}_{\bar{k}}(C)$ (identified to 1-cocycles of $H^1(G_k, \text{Aut}_{\bar{k}}(C))$) of the twists of all curves with many automorphisms [Car03], [CQ05], [Car06], [CQ06]. In the next subsections we compute the zeta function and the number of k -automorphisms of these curves when they are supersingular. A general strategy that works in most of the cases is to apply the techniques of Sect. 2 to find a twist of C with Weil polynomial $(x \pm \sqrt{q})^4$ (for q square) or $(x^2 \pm q)^2$ (for q nonsquare) and apply then Propositions 2.2, 2.3 to obtain the zeta function of all other twists of C . The results are displayed in the Appendix in the form of Tables, where we exhibit moreover an equation of each curve.

3.1. Twists of the curve $C: y^2 = x^5 - 1$, for $p \not\equiv 0, 1 \pmod{5}$. We have $\phi(W) = \{\infty\} \cup \mu_5$ and $\text{Aut}_{\bar{k}}^L(C) \simeq \mu_5$. The zeta function of C can be computed from Tables 3,4 and Lemma 2.5 applied to $C \otimes k_2$. If $q \not\equiv 1 \pmod{5}$ the only twists are C, C' . If $q \equiv 1 \pmod{5}$ there are ten twists and their zeta function can be deduced from Proposition 2.2. Table 5 summarizes all computations.

3.2. Twists of the curve $C: y^2 = x^5 - x$, for $p \equiv 5, 7 \pmod{8}$. Now $\phi(W) = \{\infty, 0, \pm 1, \pm i\}$. If $p = 5$ we have $\text{Aut}'_k(C) = \text{Aut}(\mathbb{P}^1)$. If $p \neq 5$ the group $\text{Aut}'_k(C)$ is isomorphic to S_4 and it is generated by the transformations $T(x) = ix$, $S(x) = \frac{x-i}{x+i}$, with relations $S^3 = 1 = T^4$, $ST^3 = TS^2$. For q nonsquare the zeta function of C is determined by Table 3; since the curve is defined over \mathbb{F}_p we obtain the zeta function of C over k by scalar extension.

In all cases we can apply Propositions 2.2 and 2.3 to determine the zeta function of the twists of C . Tables 6, 7, 8 summarize all computations.

3.3. Twists of the curve $C: y^2 = x^6 - 1$, for $p \equiv -1 \pmod{3}$, $p \neq 5$. We have $\phi(W) = \mu_6$ and $\text{Aut}'_k(C) = \{\pm x, \pm \eta x, \pm \eta^2 x, \pm \frac{1}{x}, \pm \frac{\eta}{x}, \pm \frac{\eta^2}{x}\}$, where $\eta \in \mathbb{F}_{p^2}$ is a primitive third root of unity.

The zeta function of C can be computed from Tables 3,4 and Lemma 2.5 applied to C and $C \otimes k_2$. The zeta function of all twists can be determined by Propositions 2.2, 2.3. Tables 9, 10 summarize all computations.

3.4. Twists of the supersingular curve $C: y^2 = x^6 + x^3 + a$, for $p > 3$. Recall that a is a special value making the curve C supersingular and $a \neq 0, 1/4, -1/50$. We have now

$$\phi(W) = \{\theta, \eta\theta, \eta^2\theta, \frac{A}{\theta}, \eta\frac{A}{\theta}, \eta^2\frac{A}{\theta}\}, \quad \text{Aut}'_k(C) = \{x, \eta x, \eta^2 x, \frac{A}{x}, \eta\frac{A}{x}, \eta^2\frac{A}{x}\},$$

where $A, z, \theta \in \bar{k}$ satisfy $A^3 = a$, $z^2 + z + a = 0$, $\theta^3 = z$.

The Galois action on W and on $\text{Aut}'_k(C)$ depends on z and a/z being cubes or not in their minimum field of definition k^* or $(k_2)^*$. This is determined by the fact that a is a cube or not.

Lemma 3.4. *If a is a cube in k^* then $z, a/z$ are both cubes in k^* or in $(k_2)^*$, according to $1 - 4a \in (k^*)^2$ being a square or not.*

If a is not a cube in k^ then $z, a/z$ are both noncubes in k^* or in $(k_2)^*$, according to $1 - 4a \in (k^*)^2$ being a square or not.*

Proof. Let us check that all situations excluded by the statement lead to $W = (1)^3(3)$ or $W_v = (1)^3(3)$ for some twist, in contradiction with Tables 3, 4.

Suppose $q \equiv -1 \pmod{3}$. If $1 - 4a$ is a square then $a, z, a/z$ are all cubes in k^* . If $1 - 4a$ is not a square then a is a cube and if z, z^σ are not cubes in k_2 we have $\theta^\sigma = \omega(A/\theta)$, with $\omega^3 = 1$, $\omega \neq 1$, and the twist by $v = (\omega^{-1}(A/x), \sqrt{\omega}y/x^3)$ has $W_v = (1)^3(3)$ by Lemma 2.6.

Suppose $q \equiv 1 \pmod{3}$. If $1 - 4a$ is not a square we have $z^{(q^2-1)/3} = a^{(q-1)/3}$, so that a is a cube in k^* if and only if z, z^σ are cubes in k_2^* . Suppose now that $1 - 4a$ is a square. If exactly one of the two elements $z, a/z$ is a cube we have $W = (1)^3(3)$; thus $z, a/z$ are both cubes or noncubes in k^* . In particular, if a is not a cube then $z, a/z$ are necessarily both noncubes. Finally, if a is a cube and $z, a/z$ are noncubes in k^* , Lemma 2.6 shows that $W_v = (1)^3(3)$ for the twist corresponding to $v = (\eta x, y)$. \square \square

For the computation of the zeta functions of the twists it is useful to detect that some of the combinations a square/nonsquare and $1 - 4a$ square/nonsquare are not possible.

Lemma 3.5. *Suppose $q \equiv 1 \pmod{3}$.*

(1) *If $q \equiv -1 \pmod{4}$ then $1 - 4a$ is not a square.*

- (2) If q is nonsquare then a is not a square.
(3) If q is a square then a and $1 - 4a$ are both squares.

Proof. Let C_v be the twist of C corresponding to $v(x, y) = (\eta x, y)$.

(1) Suppose $1 - 4a$ is a square. If a is a cube we have $W = (1)^6$ and if a is not a cube we have $W_v = (1)^6$; by Table 3 we get $(r, s) = (0, -2 \left(\frac{-1}{p}\right) q)$ in both cases. On the other hand, Lemmas 2.5 and 2.6 applied to $C \otimes_k k_2$ show in both cases that $s \equiv 1 \pmod{3}$; thus, $p \equiv 1 \pmod{4}$.

(2) Suppose a is a square. If a is a cube (respectively a is not a cube) we have $W = (1)^6$ or $W = (2)^3$ (respectively $W_v = (1)^6$ or $W_v = (2)^3$), according to $1 - 4a$ being a square or not. In all cases we have $(r, s) = (0, \pm 2q)$ by Table 3, and a straightforward application of Lemma 2.5 and (2) of Lemma 2.6 leads to $r \equiv -1 \pmod{3}$, which is a contradiction.

(3) In all cases in which a or $1 - 4a$ are nonsquares we get $(r, s) = (0, q)$ either for the curve C or for the curve C_v . This contradicts Corollary 3.3. \square \square

After these results one can apply the general strategy. The results are displayed in Tables 11, 12, 13.

3.5. Twists of the supersingular curve $C: y^2 = x^5 + x^3 + ax$. Recall that a is a special value making C supersingular and $a \neq 0, 1/4, 9/100$. Given $z \in \bar{k}$ satisfying $z^2 + z + a = 0$ we have $\phi(W) = \{0, \infty, \pm\sqrt{z}, \pm\sqrt{a/z}\}$,

$$\text{Aut}_{\bar{k}}(C) = \{(\omega^2 x, \omega y) \mid \omega^4 = 1\} \cup \left\{ \left(\frac{w^2}{x}, \frac{w^3 y}{x^3} \right) \mid w^4 = a \right\}.$$

Lemma 3.6. *If $q \equiv 1 \pmod{4}$ then a and $1 - 4a$ are both squares or both nonsquares in k^* . If q is a square then necessarily a and $1 - 4a$ are both squares.*

Proof. If $a \notin (k^*)^2$, $1 - 4a \in (k^*)^2$, then $W = (1)^4(2)$ and $(r, s) = (0, -2q)$ by Tables 3,4; this contradicts Lemma 2.5 because $|\text{Aut}(C)| = |\mathcal{F}| = 4$ and $r \equiv 2 \pmod{4}$.

Suppose now $a \in (k^*)^2$, $1 - 4a \notin (k^*)^2$. If $a \in (k^*)^4$ then $W = (1)^2(2)^2$ and $(r, s) = (0, \pm 2q)$; this contradicts Lemma 2.5 because $|\text{Aut}(C)| = 8$, $|\mathcal{F}| = 6$ if $q \equiv 1 \pmod{8}$ and $|\mathcal{F}| = 2$ or 10 if $q \equiv 5 \pmod{8}$, so that $r \equiv 4 \pmod{8}$ in both cases. If $a \notin (k^*)^4$ we get a similar contradiction for the curve C_v for $v(x, y) = (-x, iy)$.

If $a, 1 - 4a$ are nonsquares, then $W = (1)^2(4)$ and the Weil polynomial of C is $x^4 + q^2$ by Tables 3,4. If q is a square this contradicts Corollary 3.3. \square \square

Lemma 3.7. *If q is a square then $a \in (k^*)^4$ if and only if $z \in (k^*)^2$.*

Proof. Suppose $a \in (k^*)^4$, $z \notin (k^*)^2$ and let us look for a contradiction. Consider the k -automorphisms $u(x, y) = (-x, iy)$, $v(x, y) = (\frac{w^2}{x}, \frac{w^3}{x^3}y)$ of C , where $w^4 = a$. By Lemma 2.6, $W_u = (1)^6$ and C_u has Weil polynomial $(x \pm \sqrt{q})^4$ by Corollary 3.3; since $u^2 = \iota$, the Weil polynomial of C is $(x^2 + q)^2$ by Proposition 2.2 and Lemma 2.4. The quotient $E := C/v$ is an elliptic curve defined over k and the Frobenius endomorphism π of E must satisfy $\pi^2 = -q$. Since q is a square, E has four automorphisms and its j invariant is necessarily $j_E = 1728$. Now, E has a Weierstrass equation: $Y^2 = (X + 2w)(X^2 + 1 - 2w^2)$, where $X = (x^2 + w^2)x^{-1}$, $Y = y(x + w)x^{-2}$ are invariant under the action of v . The condition $j_E = 1728$ is equivalent to $a = 0$ (which was excluded from the beginning) or $a = (9/14)^2$; in this latter case z is a square in \mathbb{F}_{p^2} and we get a contradiction.

Suppose now $a \notin (k^*)^4$, $z \in (k^*)^2$. We have $W = (1)^6$ and C has Weil polynomial $(x \pm \sqrt{q})^4$ by Corollary 3.3. By Proposition 2.2, the Weil polynomial of C_u is $(x^2 + q)^2$. For any choice of $w = \sqrt[4]{a}$, the morphism $f(x, y) = (\frac{x+w}{x-w}, \frac{8\sqrt{w^3}}{\sqrt{1+2w^2}} \frac{y}{(x-w)^3})$ sets a k_2 -isomorphism between C and the model:

$$C_u: y^2 = (x^2 - 1)(x^4 + bx^2 + 1), \quad b = (12\sqrt{a} - 2)/(2\sqrt{a} + 1),$$

of C_u . The quotient of this curve by the automorphism $(-x, y)$ is the elliptic curve $E: Y^2 = (X - 1)(X^2 + bX + 1)$. Arguing as above, E has j -invariant 1728, and this leads to $a = 0$ (excluded from the beginning) or $a = (9/14)^2$, which is a contradiction since a would be a fourth power in \mathbb{F}_{p^2} . \square \square

After these results one is able to determine the zeta function of all twists of C when q is a square; the results are displayed in Table 14. In the cases where the Weil polynomial is $(x - \epsilon\sqrt{q})^4$, $\epsilon = \pm 1$, the methods of section 2 are not sufficient to determine ϵ ; our computation of this sign follows from a study of the 4-torsion of an elliptic quotient of the corresponding curve.

In order to deal with the case q nonsquare we need to discard more cases.

Lemma 3.8. *Suppose q nonsquare. If $q \equiv -1 \pmod{4}$ then a and $1 - 4a$ cannot be both nonsquares.*

If $q \equiv 1 \pmod{4}$ and $a \in (k^)^2$ then $a \in (k^*)^4$ if and only if $z \notin (k^*)^2$.*

Proof. If $a, 1 - 4a$ are both nonsquares the polynomial $x^4 + x^2 + a$ is irreducible and the Weil polynomial of C is $x^4 + q^2$ by Table 3; hence, the Weil polynomial of $C \otimes_k k_2$ is $(x^2 + q^2)^2$. If $q \equiv -1 \pmod{4}$ we have $a \in k^* \subseteq (k_2^*)^4$ and this contradicts Table 14.

Suppose $q \equiv 1 \pmod{4}$ and $a \in (k^*)^2$; by Lemma 3.6, $1 - 4a$ is also a square and $z \in k^*$. If $a \in (k^*)^4$ and $z \in (k^*)^2$ we get $W = (1)^6$, and $(r, s) = (0, -2q)$ by Table 3; we get a contradiction because the Jacobian J of C is simple ([MN02, Thm. 2.9]) and C has elliptic quotients over k because the automorphisms $(w^2/x, (w^3y)/x^3)$ are defined over k . If $a \notin (k^*)^4$ and $z \notin (k^*)^2$ we get an analogous contradiction for the curve C_u twisted by $u(x, y) = (-x, iy)$. \square \square

The results for the case q nonsquare follow now by the usual arguments and they are displayed in Tables 15, 16.

3.6. Twists of the supersingular curve C : $y^2 = x^6 + ax^4 + bx^2 + 1$. Recall that $a, b \in k$ are special values satisfying (5) and making C supersingular; in particular $p > 3$. The curve C has four twists because $\text{Aut}_{\bar{k}}(C) = \text{Aut}(C) = \{(\pm x, \pm y)\}$ is commutative and has trivial Galois action. The Jacobian of C is k -isogenous to the product $E_1 \times E_2$ of the elliptic curves with Weierstrass equations $y^2 = x^3 + ax^2 + bx + 1$, $y^2 = x^3 + bx^2 + ax + 1$, obtained as the quotient of C by the respective automorphisms $v = (-x, y)$, $\iota v = (-x, -y)$. For q nonsquare, these elliptic curves have necessarily Weil polynomial $x^2 + q$ and the Weil polynomial of C is $(x^2 + q)^2$.

Lemma 3.9. *If q is a square C has Weil polynomial $(x \pm \sqrt{q})^4$.*

Proof. By Theorem 3.2 and Proposition 2.2 C has Weil polynomial $(x \pm \sqrt{q})^4$ or $(x^2 - q)^2$. In both cases the elliptic curves E_1, E_2 have Weil polynomial $(x \pm \sqrt{q})^2$ and we claim that they are isogenous. Since $E(k) \simeq (\mathbb{Z}/(1 \pm \sqrt{q})\mathbb{Z})^2$ as an abelian group, our elliptic curves have four rational 2-torsion points and the polynomial

TABLE 5. Twists of the curve $y^2 = x^5 - 1$ for $p \equiv 2, 3, 4 \pmod{5}$. The sign $\epsilon = \pm 1$ is determined by $\sqrt{q} \equiv \epsilon \pmod{5}$. The last row provides eight inequivalent twists corresponding to the four nontrivial values of $t \in k^* / (k^*)^5$

C_v	v		(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^5 - 1$	(x, y)	$q \equiv \pm 2 \pmod{5}$	$(0, 0)$	no	2
		$q \equiv -1 \pmod{5}$	$(0, 2q)$		2
		$q \equiv 1 \pmod{5}$	$(-4\epsilon\sqrt{q}, 6q)$		10
$y^2 = tx^5 - 1, \ t \notin (k^*)^5$	$(t^{\frac{1-q}{5}}x, y)$	$q \equiv 1 \pmod{5}$	$(\epsilon\sqrt{q}, q)$	no	10

TABLE 6. Twists of the curve $y^2 = x^5 - x$ when $q \equiv -1 \pmod{8}$

C_v	v	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^5 - x$	(x, y)	$(0, 2q)$	yes	8
$y^2 = x^5 + x$	$(ix, \frac{1+i}{\sqrt{2}}y)$	$(0, 2q)$	yes	4
$y^2 = (x^2 + 1)(x^2 - 2tx - 1)(x^2 + \frac{2}{t}x - 1)$ $t^2 + 1 \notin (k^*)^2$	$(-\frac{1}{x}, \frac{y}{x^3})$	$(0, -2q)$	yes	24
$y^2 = (x^2 + 1)(x^4 - 4tx^3 - 6x^2 + 4tx + 1)$, $t^2 + 1 \notin (k^*)^2$	$(\frac{i}{x}, \frac{i-1}{\sqrt{2}x^3}y)$	$(0, 0)$	yes	4
$y^2 = x^6 - (t+3)x^5 + 5(\frac{2+t-s}{2})x^4 + 5(s-1)x^3$ $+ 5(\frac{2-t-s}{2})x^2 + (t-3)x + 1$ irred., $s^2 + t^2 = -2$	$(\frac{x-i}{x+i}, \frac{2(1-i)y}{(x+i)^3})$	$(0, q)$	no	6

$x^3 + ax^2 + bx + 1$ has three roots $e_1, e_2, e_3 \in k$. Since $e_1e_2e_3 = 1$, either one or three of these roots are squares. If only one root is a square we have $W = (1)^2(2)^2$, $W_v = (1)^4(2)$ and C, C_v have both Weil polynomial $(x^2 \pm q)^2$, in contradiction with Theorem 3.2. Hence, the three roots are squares, $W = (1)^6$, and C has Weil polynomial $(x \pm \sqrt{q})^4$ by Corollary 3.3. \square \square

The zeta function of the twists of C is obtained from Propositions 2.2 and 2.3. The results are displayed in Table 17. For q square the sign of $(x \pm \sqrt{q})^4$ can be determined by analyzing the 4-torsion of the elliptic curve $y^2 = x^3 + ax^2 + bx + 1$.

Finally, there are special curves over k whose geometric model $y^2 = x^6 + ax^4 + bx^2 + 1$ is not defined over k (cf. [Car03, Sect.1]). It is straightforward to apply the techniques of this paper to determine their zeta function too.

4. APPENDIX

In this appendix we display in several tables the computation of the zeta function of the supersingular curves of genus 2 with many automorphisms. For each curve C_v , we exhibit the number of k -automorphisms and the pair of integers (r, s) determining the Weil polynomial $f_{J_v}(x) = x^4 + rx^3 + sx^2 + qrx + q^2$ of C_v . In the column labelled “s.d” we indicate if C is self-dual. For the non-self-dual curves we exhibit only one curve from the pair C_v, C'_v .

We denote by $\eta, i \in \bar{k}$ a primitive third, fourth root of unity. For n a positive integer and $x \in k^*$ we define

$$\nu_n(x) = 1 \text{ if } x \in (k^*)^n, \quad \nu_n(x) = -1 \text{ otherwise.}$$

In all tables the parameters s, t take values in k^* .

Conclusion. We show that the zeta function of a supersingular curve of genus two is almost determined by the Galois structure of a finite set easy to describe in terms of a defining equation. For curves with many automorphisms this result is refined to obtain a direct (non-algorithmic) computation of the zeta function in all cases. As

TABLE 7. Twists of the curve $y^2 = x^5 - x$ when $q \equiv 5 \pmod{8}$

C_v	v	p	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^5 - x$	(x, y)	$p > 5$ $p = 5$	$(0, -2q)$	yes	24 120
$y^2 = x^5 - 4x$	$(-x, iy)$		$(0, 2q)$	yes	8
$y^2 = x^5 - 2x$	$(ix, \frac{1+i}{\sqrt{2}}y)$		$(0, 0)$	yes	4
$y^2 = (x^2 + 2)(x^4 - 12x^2 + 4)$	$(\frac{i}{x}, \frac{i-1}{\sqrt{2}x^3}y)$	$p > 5$ $p = 5$	$(0, 2q)$	yes	4 12
$y^2 = f(t, x)f(\frac{18+(5i-3)t}{(5i+3)-2t}, x)$ $f(t, x) = x^3 - tx^2 + (t-3)x + 1$ irred.	$(\frac{x-i}{x+i}, \frac{2(1-i)y}{(x+i)^3})$	$p > 5$ $p = 5$	$(0, q)$	no yes	6
$y^2 = x^5 - x - t, \quad \text{tr}_{k/\mathbb{F}_5}(t) = 1$	$(x+1, y)$	$p = 5$	$(\sqrt{5}q, 3q)$	no	10
$y^2 = x^6 + tx^5 + (1-t)x + 2, \quad \text{irred.}$	$(\frac{3}{x-1}, \frac{\sqrt{2}y}{(x+1)^3})$	$p = 5$	$(0, -q)$	yes	6

 TABLE 8. Twists of the curve $y^2 = x^5 - x$ when $p \equiv 5, 7 \pmod{8}$ and q is a square. Here $\epsilon = (-1/\sqrt{q})$ and $\epsilon' = (-3/\sqrt{q})$

C_v	v	p	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^5 - x$	(x, y)	$p > 5$ $p = 5$	$(-4\epsilon\sqrt{q}, 6q)$	no	48 240
$y^2 = x^5 - t^2x, \quad t \notin (k^*)^2$	$(-x, iy)$		$(0, 2q)$	yes	8
$y^2 = x^5 - tx, \quad t \notin (k^*)^2$	$(ix, \frac{1+i}{\sqrt{2}}y)$		$(0, 0)$	no	8
$y^2 = (x^2 - t)(x^4 + 6tx^2 + t^2),$ $t \notin (k^*)^2$	$(\frac{i}{x}, \frac{i-1}{\sqrt{2}x^3}y)$	$p > 5$ $p = 5$	$(0, -2q)$	yes	4 12
$y^2 = (x^3 - t)(x^3 - (15\sqrt{3} - 26)t),$ $t \notin (k^*)^3$	$(\frac{x-i}{x+i}, \frac{2(1-i)y}{(x+i)^3})$	$p > 5$ $p = 5$	$(2\epsilon'\sqrt{q}, 3q)$	no	6 12
$y^2 = x^5 - x - t, \quad \text{tr}_{k/\mathbb{F}_5}(t) = 1$	$(x+1, y)$	$p = 5$	(\sqrt{q}, q)	no	10
$y^2 = x^6 + tx^5 + (1-t)x + 2, \quad \text{irred.}$	$(\frac{3}{x-1}, \frac{\sqrt{2}y}{(x+1)^3})$	$p = 5$	$(0, q)$	no	12

 TABLE 9. Twists of the curve $y^2 = x^6 - 1$ when $q \equiv -1 \pmod{3}$, $p \neq 5$. Here $\epsilon = (-1/p)$

C_v	v	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^6 - 1$	(x, y)	$(0, 2q)$	iff $\epsilon = -1$	$6 + 2\epsilon$
$y^2 = x^6 - t, \quad t \notin (k^*)^2$	$(-x, -y)$	$(0, 2q)$	iff $\epsilon = 1$	$6 - 2\epsilon$
$y^2 = x(x^2 - 1)(x^2 - 9)$	$(\frac{1}{x}, \frac{iy}{x^3})$	$(0, -2\epsilon q)$	yes	12
$y^2 = (x^4 - 2stx^3 + (7s+1)x^2 + 2tsx + 1) \cdot$ $(x^2 - \frac{4}{t}x - 1), \quad t^2 + 4 \in k^* \setminus (k^*)^2, \quad s^{-1} = t^2 + 3$	$(-\frac{1}{x}, \frac{iy}{x^3})$	$(0, 2\epsilon q)$	yes	12
$y^2 = x^6 + 6tx^5 + 15sx^4 + 20tsx^3 + 15s^2x^2 +$ $+ 6ts^2x + s^3, \quad s = t^2 - 4 \notin (k^*)^2,$ $\gcd(x^{(q+1)/3} - 1, x^2 - tx + 1) = 1$	$(\frac{\eta}{x}, \frac{iy}{x^3})$	$(0, \epsilon q)$	yes	6
$y^2 = x^6 + 6x^5 + 15sx^4 + 20sx^3 + 15s^2x^2 +$ $+ 6s^2x + s^3, \quad s = t^2/(t^2 + 4) \notin (k^*)^2,$ $\gcd(x^{(q+1)/3} + 1, x^2 - tx - 1) = 1$	$(-\frac{\eta}{x}, \frac{iy}{x^3})$	$(0, -\epsilon q)$	yes	6

 TABLE 10. Twists of the curve $y^2 = x^6 - 1$ when $p \equiv -1 \pmod{3}$, $p \neq 5$ and q is a square. Here $\epsilon = (-3/\sqrt{q})$

C_v	v	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^6 - 1$	(x, y)	$(-4\epsilon\sqrt{q}, 6q)$	no	24
$y^2 = x^6 - t^3, \quad t \notin (k^*)^2$	$(-x, y)$	$(0, -2q)$	yes	12
$y^2 = x^6 - t^2, \quad t \notin (k^*)^3$	$(\eta x, y)$	$(2\epsilon\sqrt{q}, 3q)$	no	12
$y^2 = x^6 - t, \quad t \notin ((k^*)^2 \cup (k^*)^3)$	$(-\eta x, -y)$	$(0, q)$	no	12
$y^2 = x(x^2 + 3t)(x^2 + \frac{t}{3}), \quad t \notin (k^*)^2$	$(\frac{1}{x}, \frac{iy}{x^3})$	$(0, 2q)$	yes	4
$y^2 = x^6 + 15tx^4 + 15t^2x^2 + t^3, \quad t \notin (k^*)^2$	$(-\frac{1}{x}, \frac{iy}{x^3})$	$(0, -2q)$	yes	4

TABLE 11. Twists of the supersingular curve $y^2 = x^6 + x^3 + a$, $a \neq 0, 1/4, -1/50$, when $q \equiv -1 \pmod{3}$. Here $\epsilon = \nu_2(a)$ and A is the cubic root of a in k

C_v	v	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^6 + x^3 + a$	(x, y)	$(0, 2q)$	iff $\epsilon = -1$	$3 + \epsilon$
$y^2 = \theta^{-3}(x - \theta)^6 - g(x)^3 + a\theta^3(x - \theta^\sigma)^6$ $g(x)$ min. polyn. of $\theta \in k_2 \setminus k$, $N_{k_2/k}(\theta) = A^{-1}$	$(\frac{A}{x}, \frac{\sqrt{a}}{x^3}y)$	$(0, 2\epsilon q)$	iff $\epsilon = -1$	$9 + 3\epsilon$
$y^2 = \theta(x - \eta)^6 - g(x)^3 + a\theta^{-1}(x - \eta^2)^6$ $g(x) = x^2 + x + 1$, $\theta \in k_2 \setminus (k_2^*)^3$, $N_{k_2/k}(\theta) = a$	$(\eta\frac{A}{x}, \frac{\sqrt{a}}{x^3}y)$	$(0, -\epsilon q)$	no	6

TABLE 12. Twists of the supersingular curve $y^2 = x^6 + x^3 + a$, $a \neq 0, 1/4, -1/50$, when $q \equiv 1 \pmod{3}$ and q is nonsquare. Here A is a cubic root of a in k and $n = 3$, if $a \in (k^*)^3$, whereas $A = a$, $n = 1$, if $a \notin (k^*)^3$

C_v	v	$\nu_3(a)$	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^6 + x^3 + a$	(x, y)	1 -1	$(0, -2q)$ $(0, q)$	yes no	6
$y^2 = x^6 + tx^3 + t^2a$, $t \notin (k^*)^3$ $y^2 = x^6 + ax^3 + a^3$	$(t\frac{a-1}{3}x, y)$	1 -1	$(0, q)$ $(0, -2q)$	no yes	6
$y^2 = \theta^{-n}(x - \theta)^6 - g(x)^3 + a\theta^n(x - \theta^\sigma)^6$ $g(x)$ min. polyn. of $\theta \in k_2 \setminus k$, $N_{k_2/k}(\theta) = A^{-1}$	$(\frac{\sqrt[3]{a}}{x}, \frac{\sqrt{a}}{x^3}y)$		$(0, 2q)$	yes	2

TABLE 13. Twists of the supersingular curve $y^2 = x^6 + x^3 + a$, $a \neq 0, 1/4, -1/50$, when q is a square. Here $\epsilon = (-3/\sqrt{q})$. Also, A is a cubic root of a in k and $n = 3$, if $a \in (k^*)^3$, whereas $A = a$, $n = 1$, if $a \notin (k^*)^3$

C_v	v	$\nu_3(a)$	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^6 + x^3 + a$	(x, y)	1 -1	$(-4\epsilon\sqrt{q}, 6q)$ $(2\epsilon\sqrt{q}, 3q)$	no	12 6
$y^2 = x^6 + tx^3 + t^2a$, $t \notin (k^*)^3$ $y^2 = x^6 + ax^3 + a^3$	$(t\frac{a-1}{3}x, y)$	1 -1	$(2\epsilon\sqrt{q}, 3q)$ $(-4\epsilon\sqrt{q}, 6q)$	no	6 12
$y^2 = \theta^{-n}(x - \theta)^6 - g(x)^3 + a\theta^n(x - \theta^\sigma)^6$ $g(x)$ min. polyn. of $\theta \in k_2 \setminus k$, $N_{k_2/k}(\theta) = A^{-1}$	$(\frac{\sqrt[3]{a}}{x}, \frac{\sqrt{a}}{x^3}y)$		$(0, -2q)$	no	4

TABLE 14. Twists of the supersingular curve $y^2 = x^5 + x^3 + ax$, $a \neq 0, 1/4, 9/100$, when q is a square. The last row provides two inequivalent twists according to the two values of \sqrt{a} . Here $\epsilon = -(-1/\sqrt{q})\nu_4(z)$ and $\epsilon' = -(-1/\sqrt{q})\nu_4(tz)$, where $z^2 + z + a = 0$

C_v	v	$\nu_4(a)$	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^5 + x^3 + ax$	(x, y)	1 -1	$(4\epsilon\sqrt{q}, 6q)$ $(0, 2q)$	no yes	8 4
$y^2 = x^5 + tx^3 + at^2x$, $t \notin (k^*)^2$	$(-x, t\frac{a-1}{4}y)$	1 -1	$(0, 2q)$ $(4\epsilon'\sqrt{q}, 6q)$	yes no	4 8
$y^2 = g(x)(\theta^2(x - \theta^\sigma)^4 + g(x)^2 + a\theta^{-2}(x - \theta)^4)$, $N_{k_2/k}(\theta) = \sqrt{a}$ $g(x)$ min. polyn. of $\theta \in k_2 \setminus k$	$(\frac{\sqrt{a}}{x}, \frac{\sqrt[4]{a^3}}{x^3}y)$		$(0, -2q)$	yes	4

TABLE 15. Twists of the supersingular curve $y^2 = x^5 + x^3 + ax$, $a \neq 0, 1/4, 9/100$, when q is nonsquare and $a \notin (k^*)^2$

C_v	v	$(-1/p)$	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^5 + x^3 + ax$	(x, y)	1 -1	$(0, 0)$ $(0, 2q)$	no yes	4 2
$y^2 = (x^2 - a)(\theta(x - \sqrt{a})^4 + (x^2 - a)^2 + a\theta^{-1}(x + \sqrt{a})^4)$, $\theta \in k_2$, $N_{k_2/k}(\theta) = a$	$(\frac{\sqrt{a}}{x}, \frac{\sqrt[4]{a^3}}{x^3}y)$	1 -1	$(0, 2q)$ $(0, 0)$	yes no	2 4

TABLE 16. Twists of the supersingular curve $y^2 = x^5 + x^3 + ax$, $a \neq 0, 1/4, 9/100$, when q is nonsquare and $a \in (k^*)^2$. Here $\epsilon = (-1/p)$. If $p \equiv -1 \pmod{4}$ we assume that \sqrt{a} belongs to $(k^*)^2$

C_v	v	$\nu_4(a)$	(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^5 + x^3 + ax$	(x, y)	1 -1	$(0, 2q)$ $(0, -2q)$	iff $\epsilon = -1$ yes	$6 + 2\epsilon$ 4
$y^2 = x^5 + tx^3 + at^2x$, $t \notin (k^*)^2$	$(-x, t^{\frac{q-1}{4}}y)$	1 -1	$(0, -2\epsilon q)$ $(0, 2q)$	yes no	4 8
$y^2 = g(x)(\theta^2(x - \theta^\sigma)^4 + g(x)^2 + a\theta^{-2}(x - \theta)^4)$, $N_{k_2/k}(\theta) = \sqrt{a}$ $g(x)$ min. polyn. of $\theta \in k_2 \setminus k$	$(\frac{\sqrt{a}}{x}, \frac{\sqrt[4]{a^3}}{x^3}y)$		$(0, 2q)$	iff $\epsilon = 1$	$6 - 2\epsilon$
$y^2 = g(x)(\theta^2(x - \theta^\sigma)^4 + g(x)^2 + a\theta^{-2}(x - \theta)^4)$, $N_{k_2/k}(\theta) = -\sqrt{a}$ $g(x)$ min. polyn. of $\theta \in k_2 \setminus k$	$(\frac{-\sqrt{a}}{x}, \frac{\sqrt[4]{a^3}}{x^3}y)$		$(0, 2\epsilon q)$	yes	4

TABLE 17. Twists of the supersingular curve $y^2 = x^6 + ax^4 + bx^2 + 1$ satisfying (5)

C_v	v		(r, s)	s.d.	$ \text{Aut}(C_v) $
$y^2 = x^6 + ax^4 + bx^2 + 1$	(x, y)	q nonsq. q square	$(0, 2q)$ $(\pm 4\sqrt{q}, 6q)$	no	4
$y^2 = x^6 + atx^4 + bt^2x^2 + t^3$ $t \notin (k^*)^2$	$(-x, -y)$	q nonsq. q square	$(0, 2q)$ $(0, -2q)$	no	4

an application one gets a direct computation of the cryptographic exponent of the Jacobian of these curves. Also, the computation of the zeta function is necessary to determine the structure of the endomorphism ring of the Jacobian and to compute distortion maps for the Weil and Tate pairings.

Acknowledgement. It is a pleasure to thank Christophe Ritzenthaler for his help in finding some of the equations of the twisted curves.

REFERENCES

- [Car03] G. Cardona, *On the number of curves of genus 2 over a finite field*, Finite Fields and Their Applications **9** (2003), 505-526.
- [CQ05] G. Cardona, J. Quer, *Field of moduli and field of definition for curves of genus 2*, in Computational aspects of algebraic curves (T. Shaska, ed.) pp. 71-83., Lecture Notes Series on Computing 13 (World Scientific).
- [Car06] G. Cardona, *Representations of G_K -groups and the genus 2 curve $y^2 = x^5 - x$* , Journal of Algebra **303** (2006), 707-721.
- [CQ06] G. Cardona, J. Quer, *Curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12}* , Trans. Amer. Math. Soc. to appear.
- [FR94] G. Frey, H.-G. Rück, *A remark concerning m -divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation **62** (1994), 865-874.
- [Gal01] S. D. Galbraith, *Supersingular curves in cryptography*, In ASIACRYPT 2001, volume 2248 of Lecture Notes in Computer Science, 495-513. Springer-Verlag 2001.
- [GPRS06] S. D. Galbraith, J. Pujolàs, C. Ritzenthaler, B. Smith, *Distortion maps for genus two curves*, <http://eprint.iacr.org/2006/375>.
- [HNR06] E.W. Howe, E. Nart, C. Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, [arXiv:math.NT/0607515](https://arxiv.org/abs/math.NT/0607515).
- [IKO86] T. Ibukiyama, T. Katsura, F. Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), 127-152.
- [Igu60] J.-I. Igusa, *Arithmetic variety of moduli for genus two*, Annals of Mathematics, **72** (1960) 612-649.
- [MN02] D. Maisner, E. Nart, with an appendix by Everett W. Howe, *Abelian surfaces over finite fields as jacobians*, Experimental Mathematics, **11** (2002), 321-337.

- [MN06] D. Maisner, E. Nart, *Zeta functions of supersingular curves of genus 2*, Canadian Journal of Mathematics **59** (2007), 372-392.
- [MOV93] A.J. Menezes, T. Okamoto, S.A. Vanstone, *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*, IEEE Trans. on Information Theory **39** (1993), 1639-1646.
- [RS04] K. Rubin, A. Siverberg, *Supersingular abelian varieties in cryptology*, In Advances in Cryptology-Crypto'2002, volume 2442 of Lecture Notes in Computer Science, 336-353. Springer-Verlag 2004.
- [VV92] G. van der Geer, M. van der Vlugt, *Supersingular curves of genus 2 over finite fields of characteristic 2*, Math. Nachrichten **159** (1992), 73-81.
- [Wat69] W.C. Waterhouse, *Abelian varieties over finite fields*, Annales Scientifiques de l'École Normale Supérieure (4) **2** (1969), 521-560.
- [Xin96] C.P. Xing, *On supersingular abelian varieties of dimension two over finite fields*, Finite Fields and Their Applications **2** (1996), 407-421.
- [Yui78] N. Yui, *On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$* , Journal of Algebra **52** (1978), 378-410.
- [Zhu00] H.J. Zhu, *Group Structures of Elementary Supersingular Abelian Varieties over Finite Fields*, Journal of Number Theory **81** (2000), 292-309.

DEPT. CIÈNCIES MATEMÀTIQUES I INFORMÀTICA, UNIVERSITAT DE LES ILLES BALEARS, 07122,
PALMA DE MALLORCA, SPAIN
E-mail address: `gabriel.cardona@uib.es`

DEPARTAMENT DE MATEMÀTIQUES, UNIVERSITAT AUTÒNOMA DE BARCELONA, EDIFICI C, 08193
BELLATERRA, BARCELONA, SPAIN
E-mail address: `nart@mat.uab.cat`