NON-CYCLIC SUBGROUPS OF JACOBIANS OF GENUS TWO CURVES WITH COMPLEX MULTIPLICATION

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. Let E be an elliptic curve defined over a finite field. Balasubramanian and Koblitz have proved that if the ℓ^{th} roots of unity μ_ℓ is not contained in the ground field, then a field extension of the ground field contains μ_ℓ if and only if the ℓ-torsion points of E are rational over the same field extension. We generalize this result to Jacobians of genus two curves with complex multiplication. In particular, we show that the Weil- and the Tate-pairing on such a Jacobian are non-degenerate over the same field extension of the ground field.

1. Introduction

In [11], Koblitz described how to use elliptic curves to construct a public key cryptosystem. To get a more general class of curves, and possibly larger group orders, Koblitz [12] then proposed using Jacobians of hyperelliptic curves.

In elliptic curve cryptography it is essential to know the number of points on the curve. Cryptographically we are interested in elliptic curves with large cyclic subgroups. Such elliptic curves can be constructed. The construction is based on the theory of complex multiplication, studied in detail by [1]. It is referred to as the *CM method*. The CM method for constructing elliptic curves has been generalized to genus two curves by [22], and efficient algorithms have been proposed by [23] and [9]. Both algorithms take as input a primitive, quartic CM field K (see section 5), and give as output a genus two curve C defined over a prime field $\mathbb{F}_p$.

After Boneh and Franklin [3] proposed an identity based cryptosystem by using the Weil pairing on an elliptic curve, pairings have been of great interest to cryptography [7]. The next natural step was to consider pairings on Jacobians of hyperelliptic curves. Galbraith *et al* [8] survey the recent research on pairings on Jacobians of hyperelliptic curves.

The pairing in question is usually the Weil- or the Tate-pairing; both pairings can be computed with Miller's algorithm [14]. The Tate-pairing can be computed more efficiently than the Weil-pairing, cf. [6]. Let C be a smooth curve defined over a finite field $\mathbb{F}_q$, and let $\mathcal{J}_C$ be the Jacobian of C. Let ℓ be a prime number dividing the number of $\mathbb{F}_q$-rational points on the Jacobian, and let k be the multiplicative order of q modulo ℓ. By [10], the Tate-pairing is non-degenerate on $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. By [21, Proposition 8.1, p. 96], the Weil-pairing is non-degenerate on $\mathcal{J}_C[\ell]$. So if $\mathcal{J}_C[\ell]$ is not contained in $\mathcal{J}_C(\mathbb{F}_{q^k})$, then the Tate pairing is non-degenerate over a possible smaller field extension than the Weil-pairing. For elliptic curves, in most cases relevant to cryptography, the Weil-pairing and the Tate-pairing are non-degenerate

2000 *Mathematics Subject Classification.* Primary 14H40; Secondary 11G15, 14Q05, 94A60.
Key words and phrases. Jacobians, hyperelliptic curves, embedding degree, complex multiplication, cryptography.
Research supported in part by a PhD grant from CRYPTOMAThIC.

over the same field: let E be an elliptic curve defined over $\mathbb{F}_p$, and consider a prime number ℓ dividing the number of $\mathbb{F}_p$-rational points on E. Balasubramanian and Koblitz [2] proved that

$$\text{(1)} \qquad \text{if } \ell \nmid p-1, \text{ then } E[\ell] \subseteq E(\mathbb{F}_{p^k}) \text{ if and only if } \ell \mid p^k - 1.$$

By Rubin and Silverberg [19], this result also holds for Jacobians of genus two curves in the following sense: *if $\ell \nmid p-1$, then the Weil-pairing is non-degenerate on $U \times V$, where $U = \mathcal{J}_C(\mathbb{F}_p)[\ell]$, $V = \ker(\varphi - p) \cap \mathcal{J}_C[\ell]$ and φ is the p-power Frobenius endomorphism on $\mathcal{J}_C$.*

The result (1) can also be stated as: *if $\ell \nmid p-1$, then $E(\mathbb{F}_{p^k})[\ell]$ is bicyclic if and only if $\ell \mid p^k - 1$.* In this paper, we show that in most cases, this result also holds for Jacobians of genus two curves with complex multiplication. More precisely, the following theorem is established.

Theorem 9. *Consider a genus two curve C defined over $\mathbb{F}_p$ with $\mathrm{End}(\mathcal{J}_C) \simeq \mathfrak{O}_K$, where K is a primitive, quartic CM field (cf. section 5). Let ω_m be a p^m-Weil number of the Jacobian $\mathcal{J}_C$. Let ℓ be an odd prime number dividing the number of $\mathbb{F}_p$-rational points on $\mathcal{J}_C$, and with ℓ unramified in K, $\ell \nmid p$ and $\ell \nmid p-1$. Let p be of multiplicative order k modulo ℓ. Then the following holds.*

(i) If $\omega_m^2 \not\equiv 1 \pmod{\ell}$, then $\mathcal{J}_C(\mathbb{F}_{p^m})[\ell]$ is bicyclic if and only if ℓ divides $p^m - 1$.
(ii) The Weil-pairing is non-degenerate on $\mathcal{J}_C(\mathbb{F}_{p^k})[\ell] \times \mathcal{J}_C(\mathbb{F}_{p^k})[\ell]$.

Notation and assumptions. In this paper we only consider smooth curves. If F is an algebraic number field, then $\mathfrak{O}_F$ denotes the ring of integers of F, and $F_0 = F \cap \mathbb{R}$ denotes the real subfield of F.

2. Genus two curves

A hyperelliptic curve is a projective curve $C \subseteq \mathbb{P}^n$ of genus at least two with a separable, degree two morphism $\phi : C \to \mathbb{P}^1$. It is well known, that any genus two curve is hyperelliptic. Throughout this paper, let C be a curve of genus two defined over a finite field $\mathbb{F}_q$ of characteristic p. By the Riemann-Roch Theorem there exists a birational map $\psi : C \to \mathbb{P}^2$, mapping C to a curve given by an equation of the form

$$y^2 + g(x)y = h(x),$$

where $g, h \in \mathbb{F}_q[x]$ are of degree $\deg(g) \leq 3$ and $\deg(h) \leq 6$; cf. [4, chapter 1].

The set of principal divisors $\mathcal{P}(C)$ on C constitutes a subgroup of the degree zero divisors $\mathrm{Div}_0(C)$. The Jacobian $\mathcal{J}_C$ of C is defined as the quotient

$$\mathcal{J}_C = \mathrm{Div}_0(C)/\mathcal{P}(C).$$

Let $\ell \neq p$ be a prime number. The ℓ^n-torsion subgroup $\mathcal{J}_C[\ell^n] \subseteq \mathcal{J}_C$ of points of order dividing ℓ^n is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank four, i.e.

$$\mathcal{J}_C[\ell^n] \simeq \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z};$$

cf. [13, Theorem 6, p. 109].

The multiplicative order k of q modulo ℓ plays an important role in cryptography, since the (reduced) Tate-pairing is non-degenerate over $\mathbb{F}_{q^k}$; cf. [10].

Definition 1 (Embedding degree)**.** Consider a prime number $\ell \neq p$ dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$. The embedding degree of $\mathcal{J}_C(\mathbb{F}_q)$ with respect to ℓ is the least number k, such that $q^k \equiv 1 \pmod{\ell}$.

Closely related to the embedding degree, we have the *full* embedding degree.

Definition 2 (Full embedding degree)**.** Consider a prime number $\ell \neq p$ dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$. The full embedding degree of $\mathcal{J}_C(\mathbb{F}_q)$ with respect to ℓ is the least number $\varkappa$, such that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^\varkappa})$.

Remark 3. If $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^\varkappa})$, then $\ell \mid q^\varkappa - 1$; cf. [5, Corollary 5.77, p. 111]. Hence, the full embedding degree is a multiple of the embedding degree.

A priori, the Weil-pairing is only non-degenerate over $\mathbb{F}_{q^\varkappa}$. But in fact, as we shall see, the Weil-pairing is also non-degenerate over $\mathbb{F}_{q^k}$.

3. The Weil- and the Tate-pairing

Let $\mathbb{F}$ be an algebraic extension of $\mathbb{F}_q$. Let $x \in \mathcal{J}_C(\mathbb{F})[\ell]$ and $y = \sum_i a_i P_i \in \mathcal{J}_C(\mathbb{F})$ be divisors with disjoint supports, and let $\bar{y} \in \mathcal{J}_C(\mathbb{F})/\ell\mathcal{J}_C(\mathbb{F})$ denote the divisor class containing the divisor y. Furthermore, let $f_x \in \mathbb{F}(C)$ be a rational function on C with divisor $\operatorname{div}(f_x) = \ell x$. Set $f_x(y) = \prod_i f(P_i)^{a_i}$. Then $e_\ell(x, \bar{y}) = f_x(y)$ is a well-defined pairing

$$e_\ell : \mathcal{J}_C(\mathbb{F})[\ell] \times \mathcal{J}_C(\mathbb{F})/\ell\mathcal{J}_C(\mathbb{F}) \longrightarrow \mathbb{F}^\times/(\mathbb{F}^\times)^\ell,$$

it is called the *Tate-pairing*; cf. [7]. Raising the result to the power $\frac{|\mathbb{F}^\times|}{\ell}$ gives a well-defined element in the subgroup $\mu_\ell \subseteq \bar{\mathbb{F}}$ of the ℓ^{th} roots of unity. This pairing

$$\hat{e}_\ell : \mathcal{J}_C(\mathbb{F})[\ell] \times \mathcal{J}_C(\mathbb{F})/\ell\mathcal{J}_C(\mathbb{F}) \longrightarrow \mu_\ell$$

is called the *reduced* Tate-pairing. If the field $\mathbb{F}$ is finite and contains the ℓ^{th} roots of unity, then the Tate-pairing is bilinear and non-degenerate; cf. [10].

Now let $x, y \in \mathcal{J}_C[\ell]$ be divisors with disjoint support. The Weil-pairing

$$e_\ell : \mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell] \to \mu_\ell$$

is then defined by $e_\ell(x, y) = \frac{\hat{e}_\ell(x,\bar{y})}{\hat{e}_\ell(y,\bar{x})}$. The Weil-pairing is bilinear, anti-symmetric and non-degenerate on $\mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell]$; cf. [15].

4. Matrix representation of the endomorphism ring

An endomorphism $\psi : \mathcal{J}_C \to \mathcal{J}_C$ induces a linear map $\bar{\psi} : \mathcal{J}_C[\ell] \to \mathcal{J}_C[\ell]$ by restriction. Hence, ψ is represented by a matrix $M \in \operatorname{Mat}_4(\mathbb{Z}/\ell\mathbb{Z})$ on $\mathcal{J}_C[\ell]$. Let $f \in \mathbb{Z}[X]$ be the characteristic polynomial of ψ (see [13, pp. 109–110]), and let $\bar{f} \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ be the characteristic polynomial of $\bar{\psi}$. Then f is a monic polynomial of degree four, and by [13, Theorem 3, p. 186],

$$f(X) \equiv \bar{f}(X) \pmod{\ell}.$$

Since C is defined over $\mathbb{F}_q$, the mapping $(x, y) \mapsto (x^q, y^q)$ is a morphism on C. This morphism induces the q-power Frobenius endomorphism φ on the Jacobian $\mathcal{J}_C$. Let $P(X)$ be the characteristic polynomial of φ. $P(X)$ is called the *Weil polynomial* of $\mathcal{J}_C$, and

$$|\mathcal{J}_C(\mathbb{F}_q)| = P(1)$$

by the definition of $P(X)$ (see [13, pp. 109–110]); i.e. the number of $\mathbb{F}_q$-rational points on the Jacobian is $P(1)$.

Definition 4 (Weil number)**.** Let notation be as above. Let $P_m(X)$ be the characteristic polynomial of the q^m-power Frobenius endomorphism φ_m on $\mathcal{J}_C$. Consider a number $\omega_m \in \mathbb{C}$ with $P_m(\omega_m) = 0$. If $P_m(X)$ is reducible, assume furthermore that ω_m and φ_m are roots of the same irreducible factor of $P_m(X)$. We identify φ_m with ω_m, and we call ω_m a *q^m-Weil number* of $\mathcal{J}_C$.

Remark 5. A q^m-Weil number is not necessarily uniquely determined. In general, $P_m(X)$ is irreducible, in which case $\mathcal{J}_C$ has four q^m-Weil numbers.

Assume $P_m(X)$ is reducible. Write $P_m(X) = f(X)g(X)$, where $f, g \in \mathbb{Z}[X]$ are of degree at least one. Since $P_m(\varphi_m) = 0$, either $f(\varphi_m) = 0$ or $g(\varphi_m) = 0$; if not, then either $f(\varphi_m)$ or $g(\varphi_m)$ has infinite kernel, i.e. is not an endomorphism of $\mathcal{J}_C$. So a q^m-Weil number is well-defined.

5. CM fields

An elliptic curve E with $\mathbb{Z} \neq \mathrm{End}(E)$ is said to have *complex multiplication*. Let K be an imaginary, quadratic number field with ring of integers $\mathfrak{O}_K$. K is a *CM field*, and if $\mathrm{End}(E) \simeq \mathfrak{O}_K$, then E is said to have *CM by $\mathfrak{O}_K$*. More generally a CM field is defined as follows.

Definition 6 (CM field)**.** A number field K is a CM field, if K is a totally imaginary, quadratic extension of a totally real number field K_0.

In this paper only CM fields of degree $[K : \mathbb{Q}] = 4$ are considered. Such a field is called a *quartic* CM field.

Let C be a genus two curve. We say that C has CM by $\mathfrak{O}_K$, if $\mathrm{End}(\mathcal{J}_C) \simeq \mathfrak{O}_K$. The structure of K determines whether $\mathcal{J}_C$ is simple, i.e. does not contains an abelian subvariety other than $\{\mathcal{O}\}$ and itself. More precisely, the following theorem holds.

Theorem 7. *Let C be a genus two curve with $\mathrm{End}(\mathcal{J}_C) \simeq \mathfrak{O}_K$, where K is a quartic CM field. Then $\mathcal{J}_C$ is simple if and only if $K/\mathbb{Q}$ is Galois with Galois group $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. [20, proposition 26, p. 61]. □

Theorem 7 motivates the following definition.

Definition 8 (Primitive, quartic CM field)**.** A quartic CM field K is called primitive if either $K/\mathbb{Q}$ is not Galois, or $K/\mathbb{Q}$ is Galois with cyclic Galois group.

6. Non-cyclic subgroups of $\mathcal{J}_C$

Let K be a primitive, quartic CM field. By the CM method (see [23, 9]), we can construct a genus two curve C with $\mathrm{End}(\mathcal{J}_C) \simeq \mathfrak{O}_K$. The following theorem concerns such a curve.

Theorem 9. *Consider a genus two curve C defined over $\mathbb{F}_p$ with $\operatorname{End}(\mathfrak{J}_C) \simeq \mathfrak{O}_K$, where K is a primitive, quartic CM field. Let ω_m be a p^m-Weil number of the Jacobian $\mathfrak{J}_C$. Let ℓ be an odd prime number dividing the number of $\mathbb{F}_p$-rational points on $\mathfrak{J}_C$, and with ℓ unramified in K, $\ell \nmid p$ and $\ell \nmid p-1$. Let p be of multiplicative order k modulo ℓ. Then the following holds.*

- *(i) If $\omega_m^2 \not\equiv 1 \pmod{\ell}$, then $\mathfrak{J}_C(\mathbb{F}_{p^m})[\ell]$ is bicyclic if and only if ℓ divides $p^m - 1$.*
- *(ii) The Weil-pairing is non-degenerate on $\mathfrak{J}_C(\mathbb{F}_{p^k})[\ell] \times \mathfrak{J}_C(\mathbb{F}_{p^k})[\ell]$.*

In the following, let $\bar{P}_m \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ be the characteristic polynomial of the restriction of φ_m to $\mathfrak{J}_C[\ell]$. The proof of Theorem 9 uses a number of lemmas.

Lemma 10. *Let notation and assumptions be as in Theorem 9. Let $\imath : \mathfrak{O}_K \to \operatorname{End}(\mathfrak{J}_C)$ be an isomorphism. Consider a number $\alpha \in \mathfrak{O}_K$. If $\ker[\ell] \subseteq \ker(\imath(\alpha)^n)$ for some number $n \in \mathbb{N}$, then $\ker[\ell] \subseteq \ker(\imath(\alpha))$.*

Proof. Since $\ker[\ell] \subseteq \ker(\imath(\alpha)^n)$, it follows that $\imath(\alpha)^n = \ell\tilde{\beta}$ for some endomorphism $\tilde{\beta} \in \operatorname{End}(\mathfrak{J}_C)$; see e.g. [16, Remark 7.12, p. 37]. Notice that $\tilde{\beta} = \frac{\imath(\alpha)^n}{\ell} = \imath(\beta)$ for some number $\beta \in \mathfrak{O}_K$. Hence, $\alpha^n = \ell\beta \in \ell\mathfrak{O}_K$. Since ℓ is unramified in K, it follows that $\alpha \in \ell\mathfrak{O}_K$. So $\ker[\ell] \subseteq \ker(\imath(\alpha))$. □

Lemma 11. *Let notation and assumptions be as in Theorem 9. If $\omega_m \not\equiv 1 \pmod{\ell}$, then $\mathfrak{J}_C(\mathbb{F}_{p^m})[\ell]$ is of rank at most two as a $\mathbb{Z}/\ell\mathbb{Z}$-module.*

Proof. Since $\ell \mid |\mathfrak{J}_C(\mathbb{F}_p)|$, 1 is a root of $\bar{P}_m$. Assume that 1 is a root of $\bar{P}_m$ of multiplicity ν. Since the roots of $\bar{P}_m$ occur in pairs $(\alpha, p^m/\alpha)$, also p^m is a root of $\bar{P}_m$ of multiplicity ν.

If $\mathfrak{J}_C(\mathbb{F}_{q^m})[\ell]$ is of rank three as a $\mathbb{Z}/\ell\mathbb{Z}$-module, then ℓ divides $q^m - 1$ by [5, Proposition 5.78, p. 111]. Choose a basis $\mathcal{B}$ of $\mathfrak{J}_C[\ell]$. With respect to $\mathcal{B}$, φ_m is represented by a matrix of the form

$$M = \begin{bmatrix} 1 & 0 & 0 & m_1 \\ 0 & 1 & 0 & m_2 \\ 0 & 0 & 1 & m_3 \\ 0 & 0 & 0 & m_4 \end{bmatrix}.$$

Now, $m_4 = \det M \equiv \deg \varphi_m = p^{2m} \equiv 1 \pmod{\ell}$, so $\bar{P}_m(X) = (X-1)^4$. Since ℓ is unramified in K, it follows that $\omega_m \equiv 1 \pmod{\ell}$; cf. Lemma 10. This is a contradiction. So $\mathfrak{J}_C(\mathbb{F}_{p^m})[\ell]$ is of rank at most two as a $\mathbb{Z}/\ell\mathbb{Z}$-module. □

Lemma 12. *Let notation and assumptions be as in Theorem 9. If $\omega_m^2 \not\equiv 1 \pmod{\ell}$, then $P(X)$ is irreducible.*

Proof. The Jacobian $\mathfrak{J}_C$ is simple by Theorem 7. Assume $P_m(X)$ is reducible. Then $P_m(X) = f(X)^e$ for some integer $e \in \mathbb{Z}$ and some irreducible polynomial $f \in \mathbb{Z}[X]$ by [17, Theorem 8, p. 58]. Notice that $e \in \{2, 4\}$. If $\omega_m \notin \mathbb{R}$, then $\mathbb{Q}(\omega_m) \subset K$ is an imaginary, quadratic number field and K is the composition of K_0 and $\mathbb{Q}(\omega_m)$, i.e. $\operatorname{Gal}(K/\mathbb{Q})$ is bicyclic. This is a contradiction. So $\omega_m \in \mathbb{R}$, i.e. $\omega_m^2 = p^m$. If $\omega_m \in \mathbb{Q}$, then $f(X) \equiv X - 1 \pmod{\ell}$ because $\bar{P}_m(1) = 0$. But then $\omega_m \equiv 1 \pmod{\ell}$. This is a contradiction. So $\omega_m \notin \mathbb{Q}$, $e = 2$ and $f(X) = X^2 - p^m$. Hence, $\bar{P}_m(X) = (X^2 - p^m)^2$. Since $\bar{P}_m(1) = 0$, it follows that $\omega_m^2 = p^m \equiv 1 \pmod{\ell}$. This is a contradiction. So $P_m(X)$ is irreducible. □

Proof of Theorem 9. Assume that $\mathcal{J}_C(\mathbb{F}_{p^m})[\ell]$ is bicyclic. If $p^m \not\equiv 1 \pmod{\ell}$, then 1 is a root of $\bar{P}_m$ of multiplicity two, i.e. $\bar{P}_m(X) = (X-1)^2(X-p^m)^2$. $P(X)$ is irreducible by Lemma 12. Hence, by [18, Proposition 8.3, p. 47] it follows that ℓ ramifies in K. This is a contradiction. So $p^m \equiv 1 \pmod{\ell}$, i.e. $\ell \mid p^m - 1$.

On the other hand, if $\ell \mid p^m - 1$, then the Tate pairing is non-degenerate on $\mathcal{J}_C(\mathbb{F}_{p^m})[\ell]$. So $\mathcal{J}_C(\mathbb{F}_{p^m})[\ell]$ must be of rank at least two as a $\mathbb{Z}/\ell\mathbb{Z}$-module, since $\ell \nmid p-1$. Hence, $\mathcal{J}_C(\mathbb{F}_{p^m})[\ell]$ is bicyclic by Lemma 11. The proof of Theorem 9, part (i) is established.

Now let $m = k$. If $\omega_k \equiv 1 \pmod{\ell}$, then $\mathcal{J}_C[\ell] = \mathcal{J}_C(\mathbb{F}_{p^k})[\ell]$, and (ii) follows. Assume that $\omega_k \not\equiv 1 \pmod{\ell}$. Let $U = \mathcal{J}_C(\mathbb{F}_p)[\ell]$ and $V = \ker(\varphi - p) \cap \mathcal{J}_C[\ell]$, where φ is the p-power Frobenius endomorphism on $\mathcal{J}_C$. Then $V = \mathcal{J}_C(\mathbb{F}_{p^k})[\ell] \setminus \mathcal{J}_C(\mathbb{F}_p)[\ell]$ by Lemma 11, and

$$\mathcal{J}_C(\mathbb{F}_{p^k})[\ell] \simeq U \oplus V \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

By [19], the Weil-pairing e_W is non-degenerate on $U \times V$. Now let $x \in \mathcal{J}_C(\mathbb{F}_{p^k})[\ell]$ be an arbitrary $\mathbb{F}_{p^k}$-rational point of order ℓ. Write $x = x_U + x_V$, where $x_U \in U$ and $x_V \in V$. Choose $y \in V$ and $z \in U$, such that $e_W(x_U, y) \neq 1$ and $e_W(x_V, z) \neq 1$. We may assume that $e_W(x_U, y) \cdot e_W(x_V, z) \neq 1$; if not, replace z by $2z$. Since the Weil-pairing is anti-symmetric, $e_W(x_U, z) = e_W(x_V, y) = 1$. Hence,

$$e_W(x, y+z) = e_W(x_U, y) \cdot e_W(x_V, z) \neq 1.$$

$\square$

References

[1] A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61:29–68, 1993.

[2] R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the menezes-okamoto-vanstone algorithm. *J. Cryptology*, 11:141–145, 1998.

[3] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *SIAM J. Computing*, 32(3):586–615, 2003.

[4] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2. London Mathematical Society Lecture Note Series. Cambridge University Press, 1996.

[5] G. Frey and T. Lange. Varieties over special fields. In H. Cohen and G. Frey, editors, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, pages 87–113. Chapman & Hall/CRC, 2006.

[6] S.D. Galbraith. Supersingular curves in cryptography. In *Advances in Cryptology – Asiacrypt 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 495–513. Springer, 2001.

[7] S.D. Galbraith. Pairings. In I.F. Blake, G. Seroussi, and N.P. Smart, editors, *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*, pages 183–213. Cambridge University Press, 2005.

[8] S.D. Galbraith, F. Hess, and F. Vercauteren. Hyperelliptic pairings. In *Pairing 2007*, Lecture Notes in Computer Science, pages 108–131. Springer, 2007.

[9] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The p-adic cm-method for genus 2, 2005.

[10] F. Hess. A note on the tate pairing of curves over finite fields. *Arch. Math.*, 82:28–32, 2004.

[11] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.
[12] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1:139–150, 1989.
[13] S. Lang. *Abelian Varieties.* Interscience, 1959.
[14] V.S. Miller. Short programs for functions on curves, 1986. Unpublished manuscript, available at `http://crypto.stanford.edu/miller/miller.pdf`.
[15] V.S. Miller. The weil pairing, and its efficient calculation. *J. Cryptology*, 17:235–261, 2004.
[16] J.S. Milne. Abelian varieties, 1998. Available at `http://www.jmilne.org`.
[17] J.S. Milne and W.C. Waterhouse. Abelian varieties over finite fields. *Proc. Symp. Pure Math.*, 20:53–64, 1971.
[18] J. Neukirch. *Algebraic Number Theory.* Springer, 1999.
[19] K. Rubin and A. Silverberg. Using abelian varieties to improve pairing-based cryptography, 2007. Preprint, available at `http://www.math.uci.edu/~asilverb/bibliography/`.
[20] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions.* Princeton University Press, 1998.
[21] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.
[22] A.-M. Spallek. *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen.* PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.
[23] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, 72:435–458, 2003.

Department of Mathematical Sciences, University of Aarhus, Ny Munkegade, Building 1530, DK-8000 Aarhus C

E-mail address: `cr@imf.au.dk`