GENERATORS OF JACOBIANS OF GENUS TWO CURVES

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. We prove that in most cases relevant to cryptography, the Frobenius endomorphism on the Jacobian of a genus two curve is represented by a diagonal matrix with respect to an appropriate basis of the subgroup of ℓ-torsion points. From this fact we get an explicit description of the Weil-pairing on the subgroup of ℓ-torsion points. Finally, the explicit description of the Weil-pairing provides us with an efficient, probabilistic algorithm to find generators of the subgroup of ℓ-torsion points on the Jacobian of a genus two curve.

1. Introduction

In [9], 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 [10] then proposed using Jacobians of hyperelliptic curves. After Boneh and Franklin [1] proposed an identity based cryptosystem by using the Weil-pairing on an elliptic curve, pairings have been of great interest to cryptography [5]. The next natural step was to consider pairings on Jacobians of hyperelliptic curves. Galbraith *et al* [6] survey the recent research on pairings on Jacobians of hyperelliptic curves.

Miller [12] uses the Weil-pairing to determine generators of $E(\mathbb{F}_q)$, where E is an elliptic curve defined over a finite field $\mathbb{F}_q$. Let $\mathcal{J}_C$ be the Jacobian of a genus two curve defined over $\mathbb{F}_q$. In [14], the author describes an algorithm based on the Tate-pairing to determine generators of the subgroup $\mathcal{J}_C(\mathbb{F}_q)[m]$ of points of order m on the Jacobian, where m is a number dividing $q-1$. The key ingredient of the algorithm is a "diagonalization" of a set of randomly chosen points $\{P_1,\dots,P_4,Q_1,\dots,Q_4\}$ on the Jacobian with respect to the (reduced) Tate-pairing ε; i.e. a modification of the set such that $\varepsilon(P_i,Q_j)\neq 1$ if and only if $i=j$. This procedure is based on solving the discrete logarithm problem in $\mathcal{J}_C(\mathbb{F}_q)[m]$. Contrary to the special case when m divides $q-1$, this is infeasible in general. Hence, in general the algorithm in [14] does not apply.

In the present paper, we generalize the algorithm in [14] to subgroups of points of prime order ℓ, where ℓ does not divide $q-1$. In order to do so, we must somehow alter the diagonalization step. We show and exploit the fact that the q-power Frobenius endomorphism on $\mathcal{J}_C$ has a diagonal representation on $\mathcal{J}_C[\ell]$. Hereby, computations of discrete logarithms are avoided, yielding the desired altering of the diagonalization step.

2000 *Mathematics Subject Classification.* 11G20 (Primary) 11T71, 14G50, 14H45 (Secondary).

Key words and phrases. Jacobians, genus two curves, Frobenius endomorphism, diagonal representation, pairings, embedding degree.

Research supported in part by a PhD grant from CRYPTOMAThIC.

Setup. Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Let ℓ be an odd prime number dividing the number of $\mathbb{F}_q$-rational points on the Jacobian $\mathcal{J}_C$, and with ℓ dividing neither q nor $q-1$. Assume that the $\mathbb{F}_q$-rational subgroup $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ of points on the Jacobian of order ℓ is cyclic. Let k be the multiplicative order of q modulo ℓ. Write the characteristic polynomial of the q^k-power Frobenius endomorphism on $\mathcal{J}_C$ as

$$P_k(X) = X^4 + 2\sigma_k X^3 + (2q^k + \sigma_k^2 - \tau_k)X^2 + 2\sigma_k q^k X + q^{2k},$$

where $2\sigma_k, 4\tau_k \in \mathbb{Z}$. Let $\omega_k \in \mathbb{C}$ be a root of $P_k(X)$. Finally, if ℓ divides $4\tau_k$, we assume that ℓ is unramified in $\mathbb{Q}(\omega_k)$.

Remark. Notice that in most cases relevant to cryptography, the considered genus two curve C fulfills these assumptions. Cf. Remark 7 and 14.

The algorithm. First of all, we notice that in the above setup, the q-power Frobenius endomorphism φ on $\mathcal{J}_C$ can be represented on $\mathcal{J}_C[\ell]$ by a diagonal matrix with respect to an appropriate basis $\mathcal{B}$ of $\mathcal{J}_C[\ell]$; cf. Theorem 11. (In fact, to show this we do not need the $\mathbb{F}_q$-rational subgroup $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ of points on the Jacobian of order ℓ to be cyclic.) From this observation it follows that all non-degenerate, bilinear, anti-symmetric and Galois-invariant pairings on $\mathcal{J}_C[\ell]$ are given by the matrices

$$\mathcal{E}_{a,b} = \begin{bmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & -b & 0 \end{bmatrix}, \qquad a, b \in (\mathbb{Z}/\ell\mathbb{Z})^\times$$

with respect to $\mathcal{B}$; cf. Theorem 12. By using this description of the pairing, the desired algorithm is given as follows.

Algorithm 17. *On input the considered curve C, the numbers ℓ, q, k and τ_k and a number $n \in \mathbb{N}$, the following algorithm outputs a generating set of $\mathcal{J}_C[\ell]$ or "failure".*

(1) *If ℓ does not divide $4\tau_k$, then do the following.*
  (a) *Choose points $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, $x_2 \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \backslash \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and $x_3' \in U := \mathcal{J}_C[\ell] \backslash \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$; compute $x_3 = x_3' - \varphi^k(x_3')$. If $\varepsilon(x_3, \varphi(x_3)) \neq 1$, then output $\{x_1, x_2, x_3, \varphi(x_3)\}$ and stop.*
  (b) *Let $i = j = 0$. While $i < n$ do the following*
    (i) *Choose a random point $x_4 \in U$.*
    (ii) *$i := i + 1$.*
    (iii) *If $\varepsilon(x_3, x_4) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
  (c) *If $j = 0$ then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*

(2) *If ℓ divides $4\tau_k$, then do the following.*
  (a) *Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$*
  (b) *Let $i = j = 0$. While $i < n$ do the following*
    (i) *Choose random points $y_3, y_4 \in \mathcal{J}_C[\ell]$; compute $x_\nu := q(y_\nu - \varphi(y_\nu)) - \varphi(y_\nu - \varphi(y_\nu))$ for $\nu = 3, 4$.*
    (ii) *If $\varepsilon(x_3, x_4) = 1$ then $i := i + 1$. Else $i := n$ and $j := 1$.*
  (c) *If $j = 0$ then output "failure" and stop.*
  (d) *Let $i = j = 0$. While $i < n$ do the following*
    (i) *Choose a random point $x_2 \in \mathcal{J}_C[\ell]$.*
    (ii) *If $\varepsilon(x_1, x_2) = 1$ then $i := i + 1$. Else $i := n$ and $j := 1$.*
  (e) *If $j = 0$ then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$ and stop.*

Algorithm 17 finds generators of $\mathcal{J}_C[\ell]$ with probability at least $(1-{}^1/\ell^n)^2$ and in expected running time $O(\log \ell)$; cf. Theorem 18.

Remark. To implement Algorithm 17, we need to find a q^k-*Weil number* (cf. Definition 2). On Jacobians generated by the *complex multiplication method* [17, 7, 3], we know the Weil numbers in advance. Hence, Algorithm 17 is particularly well suited for such Jacobians.

Assumption. In this paper, a *curve* is an irreducible nonsingular projective variety of dimension one.

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. [2, 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

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

The Jacobian is an abelian group. We write the group law additively, and denote the zero element of the Jacobian by $\mathcal{O}$.

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. [11, 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. [8].

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 $q^k \equiv 1 \pmod{\ell}$.

3. The Frobenius endomorphism

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; cf. [11, pp. 109–110]. $P(X)$ 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 [11, pp. 109–110]); i.e. the number of $\mathbb{F}_q$-rational points on the Jacobian is $P(1)$.

Definition 2 (Weil number)**.** Let notation be as above. Let $P_k(X)$ be the characteristic polynomial of the q^m-power Frobenius endomorphism φ_m on $\mathcal{J}_C$. A complex number $\omega_m \in \mathbb{C}$ with $P_m(\omega_m) = 0$ is called a q^m-*Weil number* of $\mathcal{J}_C$.

Remark 3. Note that $\mathcal{J}_C$ has four q^m-Weil numbers. If $P_1(X) = \prod_i (X - \omega_i)$, then $P_m(X) = \prod_i (X - \omega_i^m)$. Hence, if ω is a q-Weil number of $\mathcal{J}_C$, then ω^m is a q^m-Weil number of $\mathcal{J}_C$.

4. Non-cyclic subgroups

Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Let $P_m(X)$ be the characteristic polynomial of the q^m-power Frobenius endomorphism φ_m on the Jacobian $\mathcal{J}_C$. $P_m(X)$ is of the form $P_m(X) = X^4 + sX^3 + tX^2 + sq^m X + q^{2m}$, where $s, t \in \mathbb{Z}$. Let $\sigma = \frac{s}{2}$ and $\tau = 2q^m + \sigma^2 - t$. Then

$$P_m(X) = X^4 + 2\sigma X^3 + (2q^m + \sigma^2 - \tau)X^2 + 2\sigma q^m X + q^{2m},$$

and $2\sigma, 4\tau \in \mathbb{Z}$. In [15], the author proves the following Theorem 4 and 5.

Theorem 4. *Consider a genus two curve C defined over a finite field $\mathbb{F}_q$. Write the characteristic polynomial of the q^m-power Frobenius endomorphism on the Jacobian $\mathcal{J}_C$ as $P_m(X) = X^4+2\sigma X^3+(2q^m+\sigma^2-\tau)X^2+2\sigma q^m X+q^{2m}$, where $2\sigma, 4\tau \in \mathbb{Z}$. Let ℓ be an odd prime number dividing the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, and with $\ell \nmid q$ and $\ell \nmid q-1$. If $\ell \nmid 4\tau$, then*

1. *$\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ is of rank at most two as a $\mathbb{Z}/\ell\mathbb{Z}$-module, and*
2. *$\mathcal{J}_C(\mathbb{F}_{q^m})[\ell]$ is bicyclic if and only if ℓ divides $q^m - 1$.*

Theorem 5. *Let notation be as in Theorem 4. Furthermore, let ω_m be a q^m-Weil number of $\mathcal{J}_C$, and assume that ℓ is unramified in $\mathbb{Q}(\omega_m)$. Now assume that $\ell \mid 4\tau$. Then the following holds.*

1. *If $\omega_m \in \mathbb{Z}$, then $\ell \mid q^m - 1$ and $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^m})$.*
2. *If $\omega_m \notin \mathbb{Z}$, then $\ell \nmid q^m - 1$, $\mathcal{J}_C(\mathbb{F}_{q^m})[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ and $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{mk}})$ if and only if $\ell \mid q^{mk} - 1$.*

Inspired by Theorem 4 and 5 we introduce the following notation.

Definition 6. Consider a curve C with Jacobian $\mathcal{J}_C$. We call C a $\mathcal{C}(\ell, q, k, \tau_k)$-curve, and write $C \in \mathcal{C}(\ell, q, k, \tau_k)$, if the following holds.

1. C is of genus two and defined over the finite field $\mathbb{F}_q$.
2. ℓ is an odd prime number dividing the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, ℓ divides neither q nor $q - 1$, and $\mathcal{J}_C(\mathbb{F}_q)$ is of embedding degree k with respect to ℓ.
3. The characteristic polynomial of the q^k-power Frobenius endomorphism on $\mathcal{J}_C$ is given by $P_k(X) = X^4+2\sigma_k X^3+(2q^k+\sigma_k^2-\tau_k)X^2+2\sigma_k q^k X+q^{2k}$, where $2\sigma_k, 4\tau_k \in \mathbb{Z}$.
4. Let ω_k be a q^k-Weil number of $\mathcal{J}_C$. If ℓ divides $4\tau_k$, then ℓ is unramified in $\mathbb{Q}(\omega_k)$.

Remark 7. Since ℓ is ramified in $\mathbb{Q}(\omega_k)$ if and only if ℓ divides the discriminant of $\mathbb{Q}(\omega_k)$, ℓ is unramified in $\mathbb{Q}(\omega_k)$ with probability approximately $1 - 1/\ell$. Hence, in most cases relevant to cryptography a genus two curve C is a $\mathcal{C}(\ell, q, k, \tau_k)$-curve.

5. Matrix representation of the Frobenius endomorphism

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 $M \in \mathrm{Mat}_4(\mathbb{Z}/\ell\mathbb{Z})$ on $\mathcal{J}_C[\ell]$. If ψ can be represented on $\mathcal{J}_C[\ell]$ by a diagonal matrix with respect to an appropriate basis of $\mathcal{J}_C[\ell]$, then we say that ψ is *diagonalizable* or has a *diagonal representation* on $\mathcal{J}_C[\ell]$.

Let $f \in \mathbb{Z}[X]$ be the characteristic polynomial of ψ (see [11, 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 [11, Theorem 3, p. 186],

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

We wish to show that in most cases, the q-power Frobenius endomorphism φ is diagonalizable on $\mathcal{J}_C[\ell]$. To do this, we need to describe the matrix representation in the case when φ is not diagonalizable on $\mathcal{J}_C[\ell]$.

Lemma 8. *Consider a curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$. Let φ be the q-power Frobenius endomorphism on the Jacobian $\mathcal{J}_C$. If φ is not diagonalizable on $\mathcal{J}_C[\ell]$, then φ is represented on $\mathcal{J}_C[\ell]$ by a matrix of the form*

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix} \tag{1}$$

with respect to an appropriate basis of $\mathcal{J}_C[\ell]$.

Proof. Let $\bar{P}_k \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ be the characteristic polynomial of the restriction of the q^k-power Frobenius endomorphism φ_k to $\mathcal{J}_C[\ell]$. Since ℓ divides the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, 1 is a root of $\bar{P}_k$. Assume that 1 is an root of $\bar{P}_k$ with multiplicity ν. Then

$$\bar{P}_k(X) = (X-1)^\nu \bar{Q}_k(X),$$

where $\bar{Q}_k \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ is a polynomial of degree $4-\nu$, and $\bar{Q}_k(1) \neq 0$. Since the roots of $\bar{P}_k$ occur in pairs $(\alpha, 1/\alpha)$, ν is an even number. Let $U_k = \ker(\varphi_k - 1)^\nu$ and $W_k = \ker(\bar{Q}_k(\varphi_k))$. Then U_k and W_k are φ_k-invariant submodules of the $\mathbb{Z}/\ell\mathbb{Z}$-module $\mathcal{J}_C[\ell]$, $\operatorname{rank}_{\mathbb{Z}/\ell\mathbb{Z}}(U_k) = \nu$, and $\mathcal{J}_C[\ell] \simeq U_k \oplus W_k$.

Assume at first that ℓ does not divide $4\tau_k$. Then $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic and $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ bicyclic; cf. Theorem 4. By [16, Theorem 3.1], $\nu = 2$. Choose points $x_1, x_2 \in \mathcal{J}_C[\ell]$, such that $\varphi(x_1) = x_1$ and $\varphi(x_2) = qx_2$. Then $\{x_1, x_2\}$ is a basis of $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. Now, let $\{x_3, x_4\}$ be a basis of W_k, and consider the basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$. If x_3 and x_4 are eigenvectors of φ_k, then φ_k is represented by a diagonal matrix on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. Assume x_3 is not an eigenvector of φ_k. Then $\mathcal{B}' = \{x_1, x_2, x_3, \varphi_k(x_3)\}$ is a basis of $\mathcal{J}_C[\ell]$, and φ_k is represented by a matrix of the form (1).

Now, assume ℓ divides $4\tau_k$. Since ℓ divides $q^k - 1$, it follows that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 5. Let $\bar{P} \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ be the characteristic polynomial of the restriction of φ to $\mathcal{J}_C[\ell]$. Since ℓ divides the number of $\mathbb{F}_q$-rational points on $\mathcal{J}_C$, 1 is a root of $\bar{P}$. Assume that 1 is an root of $\bar{P}$ with multiplicity ν. Since the roots of $\bar{P}$ occur in pairs $(\alpha, q/\alpha)$, it follows that

$$\bar{P}(X) = (X-1)^\nu (X-q)^\nu \bar{Q}(X),$$

where $\bar{Q} \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ is a polynomial of degree $4-2\nu$, $\bar{Q}(1) \neq 0$ and $\bar{Q}(q) \neq 0$. Let $U = \ker(\varphi - 1)^\nu$, $V = \ker(\varphi - q)^\nu$ and $W = \ker(\bar{Q}(\varphi))$. Then U, V and W are φ-invariant submodules of the $\mathbb{Z}/\ell\mathbb{Z}$-module $\mathcal{J}_C[\ell]$, $\operatorname{rank}_{\mathbb{Z}/\ell\mathbb{Z}}(U) = \operatorname{rank}_{\mathbb{Z}/\ell\mathbb{Z}}(V) = \nu$, and $\mathcal{J}_C[\ell] \simeq U \oplus V \oplus W$. If $\nu = 1$, then it follows as above that φ is either diagonalizable on $\mathcal{J}_C[\ell]$ or represented by a matrix of the form (1) with respect to some basis of $\mathcal{J}_C[\ell]$. Hence, we may assume that $\nu = 2$. Now choose $x_1 \in U$, such that $\varphi(x_1) = x_1$, and expand this to a basis (x_1, x_2) of U. Similarly, choose a basis (x_3, x_4) of V with $\varphi(x_3) = qx_3$. With respect to the basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$, φ is represented by a matrix of the form

$$M = \begin{bmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q & \beta \\ 0 & 0 & 0 & q \end{bmatrix}.$$

Notice that

$$M^k = \begin{bmatrix} 1 & k\alpha & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & kq^{k-1}\beta \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Since $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$, we know that $\varphi^k = \varphi_k$ is the identity on $\mathcal{J}_C[\ell]$. Hence, $M^k = I$. So $\alpha \equiv \beta \equiv 0 \pmod{\ell}$, i.e. φ is represented by a diagonal matrix with respect to $\mathcal{B}$. □

The next step is to determine when the Weil polynomial splits modulo ℓ.

Lemma 9. *Consider a curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$. Let φ be the q-power Frobenius endomorphism on the Jacobian $\mathcal{J}_C$. Assume that φ is not diagonalizable on $\mathcal{J}_C[\ell]$, and let φ be represented on $\mathcal{J}_C[\ell]$ by the matrix*

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & 0 & -q \\ 0 & 0 & 1 & c \end{bmatrix}$$

with respect to an appropriate basis of $\mathcal{J}_C[\ell]$. Let $P_n(X)$ be the characteristic polynomial of the q^n-power Frobenius endomorphism on $\mathcal{J}_C$. Then $P_n(X)$ splits modulo ℓ if and only if $c^2 - 4q$ is a quadratic residue modulo ℓ. In particular, if $P_n(X)$ splits modulo ℓ for some *$n \in \mathbb{N}$, then $P_n(X)$ splits modulo ℓ for* any *$n \in \mathbb{N}$.*

Proof. Let $M_1 = \left[\begin{smallmatrix} 0 & -q \\ 1 & c \end{smallmatrix}\right]$, and write

$$M_1^n = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}.$$

Since $M_1^n M_1 = M_1 M_1^n$, it follows that $m_{12} = -qm_{21}$ and $m_{22} = m_{11} + cm_{21}$. But then $P_n(X) \equiv (X-1)(X-q^n)F_n(X) \pmod{\ell}$, where

$$F_n(X) \equiv X^2 - (2m_{11} + cm_{21})X + m_{11}^2 + qm_{21}^2 + cm_{11}m_{21} \pmod{\ell}.$$

The discriminant of $F_n(X)$ is given by $\Delta \equiv (c^2 - 4q)m_{21}^2 \pmod{\ell}$; hence the lemma. □

Theorem 10. *The Weil polynomial of the Jacobian $\mathcal{J}_C$ of a curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$ splits modulo ℓ.*

Proof. For some $n \in \mathbb{N}$, $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^n})$. But then φ^n acts as the identity on $\mathcal{J}_C[\ell]$, i.e. $P_n(X) \equiv (X-1)^4 \pmod{\ell}$. In particular, $P_n(X)$ splits modulo ℓ. But then $P(X)$ splits modulo ℓ by Lemma 9. □

We are now ready to prove the desired result.

Theorem 11. *The q-power Frobenius endomorphism on the Jacobian $\mathcal{J}_C$ of a curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$ is diagonalizable on $\mathcal{J}_C[\ell]$.*

Proof. Cf. Theorem 10, we may write the Weil polynomial of $\mathcal{J}_C$ as

$$P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell}.$$

If $\alpha \not\equiv 1, q, q/\alpha \pmod{\ell}$, then the theorem follows. If $\alpha \equiv 1, q \pmod{\ell}$, then

$$P(X) \equiv (X-1)^2(X-q)^2 \pmod{\ell};$$

in this case, the theorem follows by the last part of the proof of Lemma 8.

Assume that $\alpha \equiv q/\alpha \pmod{\ell}$, i.e. that $\alpha^2 \equiv q \pmod{\ell}$. Then the q-power Frobenius endomorphism is represented on $\mathcal{J}_C[\ell]$ by a matrix of the form

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & q & 0 & 0 \\ 0 & 0 & \alpha & \beta \\ 0 & 0 & 0 & \alpha \end{bmatrix}$$

with respect to an appropriate basis of $\mathcal{J}_C[\ell]$. Notice that

$$M^{2k} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2k\alpha^{2k-1}\beta \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Thus, $P_{2k}(X) \equiv (X-1)^4 \pmod{\ell}$. By Theorem 5, it follows that $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^{2k}})$. But then $M^{2k} = I$, i.e. $\beta \equiv 0 \pmod{\ell}$. Hence, the q-power Frobenius endomorphism on $\mathcal{J}_C$ is diagonalizable on $\mathcal{J}_C[\ell]$ also in this case. The theorem is proved. □

6. Anti-symmetric pairings on the Jacobian

On $\mathcal{J}_C[\ell]$, a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing

$$\varepsilon : \mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell] \to \mu_\ell = \langle \zeta \rangle \subseteq \mathbb{F}_{q^k}^\times.$$

exists, e.g. the Weil-pairing. Here, μ_ℓ is the group of ℓ^{th} roots of unity. Since ε is bilinear, it is given by

$$\varepsilon(x, y) = \zeta^{x^T \mathcal{E} y},$$

for some matrix $\mathcal{E} \in \mathrm{Mat}_4(\mathbb{Z}/\ell\mathbb{Z})$ with respect to a basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$. Let φ denote the q-power Frobenius endomorphism on $\mathcal{J}_C$. Since ε is Galois-invariant,

$$\forall x, y \in \mathcal{J}_C[\ell] : \varepsilon(x, y)^q = \varepsilon(\varphi(x), \varphi(y)).$$

This is equivalent to

$$\forall x, y \in \mathcal{J}_C[\ell] : q(x^T \mathcal{E} y) = (Mx)^T \mathcal{E}(My),$$

where M is the matrix representation of φ on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. Since $(Mx)^T \mathcal{E}(My) = x^T M^T \mathcal{E} M y$, it follows that

$$\forall x, y \in \mathcal{J}_C[\ell] : x^T q \mathcal{E} y = x^T M^T \mathcal{E} M y,$$

or equivalently, that $q\mathcal{E} = M^T \mathcal{E} M$.

Now, let $\varepsilon(x_i, x_j) = \zeta^{a_{ij}}$. By anti-symmetry,

$$\mathcal{E} = \begin{bmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & a_{23} & a_{24} \\ -a_{13} & -a_{23} & 0 & a_{34} \\ -a_{14} & -a_{24} & -a_{34} & 0 \end{bmatrix}.$$

Assume that φ is represented by a diagonal matrix $\operatorname{diag}(1, q, \alpha, q/\alpha)$ with respect to $\mathcal{B}$. Then it follows from $M^T \mathcal{E} M = q\mathcal{E}$, that

$$a_{13}(\alpha - q) \equiv a_{14}(\alpha - 1) \equiv a_{23}(\alpha - 1) \equiv a_{24}(\alpha - q) \equiv 0 \pmod{\ell}.$$

If $\alpha \equiv 1, q \pmod{\ell}$, then $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is bi-cyclic. Hence the following theorem holds.

Theorem 12. *Consider a curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$. Let φ be the q-power Frobenius endomorphism on the Jacobian $\mathcal{J}_C$. Now choose a basis $\mathcal{B}$ of $\mathcal{J}_C[\ell]$, such that φ is represented by a diagonal matrix $\operatorname{diag}(1, q, \alpha, q/\alpha)$ with respect to $\mathcal{B}$. If the $\mathbb{F}_q$-rational subgroup $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ of points on the Jacobian of order ℓ is cyclic, then all non-degenerate, bilinear, anti-symmetric and Galois-invariant pairings on $\mathcal{J}_C[\ell]$ are given by the matrices*

$$\mathcal{E}_{a,b} = \begin{bmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & -b & 0 \end{bmatrix}, \qquad a, b \in (\mathbb{Z}/\ell\mathbb{Z})^\times$$

with respect to $\mathcal{B}$.

Remark 13. Let notation and assumptions be as in Theorem 12. Let ε be a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing on $\mathcal{J}_C[\ell]$, and let ε be given by $\mathcal{E}_{a,b}$ with respect to a basis $\{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$. Then ε is given by $\mathcal{E}_{1,1}$ with respect to $\{a^{-1}x_1, x_2, b^{-1}x_3, x_4\}$.

Remark 14. In most cases relevant to cryptography, we consider a prime divisor ℓ of size q^2. Assume ℓ is of size q^2. Then ℓ divides neither q nor $q-1$. The number of $\mathbb{F}_q$-rational points on the Jacobian is approximately q^2. Thus, $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ is cyclic in most cases relevant to cryptography.

7. Generators of $\mathcal{J}_C[\ell]$

Consider a curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$ with Jacobian $\mathcal{J}_C$. Assume the $\mathbb{F}_q$-rational subgroup $\mathcal{J}_C(\mathbb{F}_q)[\ell]$ of points on the Jacobian of order ℓ is cyclic. Let φ be the q-power Frobenius endomorphism on $\mathcal{J}_C$. Let ε be a non-degenerate, bilinear, anti-symmetric and Galois-invariant pairing

$$\varepsilon : \mathcal{J}_C[\ell] \times \mathcal{J}_C[\ell] \to \mu_\ell = \langle \zeta \rangle \subseteq \mathbb{F}_{q^k}^\times.$$

We consider the cases $\ell \nmid 4\tau_k$ and $\ell \mid 4\tau_k$ separately.

7.1. The case $\ell \nmid 4\tau_k$.

If ℓ does not divide $4\tau_k$, then $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$ is bicyclic; cf. Theorem 4. Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, and expand $\{x_1\}$ to a basis $\{x_1, y_2\}$ of $\mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$, where $\varphi(y_2) = qy_2$. Let $x_2' \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \setminus \mathcal{J}_C(\mathbb{F}_q)[\ell]$ be a random point. Write $x_2' = \alpha_1 x_1 + \alpha_2 y_2$. Then

$$x_2 = x_2' - \varphi(x_2') = \alpha_2(1 - q)y_2 \in \langle y_2 \rangle,$$

i.e. $\varphi(x_2) = qx_2$. Now, let $\mathcal{J}_C[\ell] \simeq \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \oplus W$, where W is a φ-invariant submodule of rank two. Choose a random point $x_3' \in \mathcal{J}_C[\ell] \setminus \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. Then

$$x_3 = x_3' - \varphi^k(x_3') \in W$$

as above. Notice that

$$\mathcal{J}_C[\ell] = \langle x_1, x_2, x_3, \varphi(x_3)\rangle \quad \text{if and only if} \quad \varepsilon(x_3, \varphi(x_3)) \neq 1;$$

cf. Theorem 12.

Assume $\varepsilon(x_3, \varphi(x_3)) = 1$. Then x_3 is an eigenvector of φ. Expand $\{x_1, x_2, x_3\}$ to a basis $\mathcal{B} = \{x_1, x_2, x_3, x_4\}$ of $\mathcal{J}_C[\ell]$, such that φ is represented by a diagonal matrix on $\mathcal{J}_C[\ell]$ with respect to $\mathcal{B}$. We may assume that ε is given by $\mathcal{E}_{1,1}$ with respect to $\mathcal{B}$; cf. Remark 13.

Now, choose a random point $x \in \mathcal{J}_C[\ell] \setminus \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$. Write $x = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4$. Then $\varepsilon(x_3, x) = \zeta^{\alpha_4}$. So $\varepsilon(x_3, x) \neq 1$ if and only if ℓ does not divide α_4. On the other hand, $\{x_1, x_2, x_3, x\}$ is a basis of $\mathcal{J}_C[\ell]$ if and only ℓ does not divide α_4. Hence, $\{x_1, x_2, x_3, x\}$ is a basis of $\mathcal{J}_C[\ell]$ if and only if ℓ does not divide α_4. Thus, if ℓ does not divide $4\tau_k$, then the following Algorithm 15 outputs generators of $\mathcal{J}_C[\ell]$ with probability $1 - 1/\ell^n$.

Algorithm 15. *The following algorithm takes as input a $\mathcal{C}(\ell, q, k, \tau_k)$-curve C, the numbers ℓ, q, k and τ_k and a number $n \in \mathbb{N}$.*

1. *Choose points $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, $x_2 \in \mathcal{J}_C(\mathbb{F}_{q^k})[\ell] \setminus \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and $x_3' \in U := \mathcal{J}_C[\ell] \setminus \mathcal{J}_C(\mathbb{F}_{q^k})[\ell]$; compute $x_3 = x_3' - \varphi^k(x_3')$. If $\varepsilon(x_3, \varphi(x_3)) \neq 1$, then output $\{x_1, x_2, x_3, \varphi(x_3)\}$ and stop.*
2. *Let $i = j = 0$. While $i < n$ do the following*
   - (a) *Choose a random point $x_4 \in U$.*
   - (b) *$i := i + 1$.*
   - (c) *If $\varepsilon(x_3, x_4) = 1$, then $i := i + 1$. Else $i := n$ and $j := 1$.*
3. *If $j = 0$ then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*

7.2. **The case $\ell \mid 4\tau_k$.** Assume ℓ divides $4\tau_k$. Then $\mathcal{J}_C[\ell] \subseteq \mathcal{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 5. Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$, and let $y_2 \in \mathcal{J}_C[\ell]$ be a point with $\varphi(y_2) = qy_2$. Write $\mathcal{J}_C[\ell] = \langle x_1, y_2\rangle \oplus W$, where W is a φ-invariant submodule of rank two; cf. the proof of Lemma 8. Let $\{y_3, y_4\}$ be a basis of W, such that φ is represented on $\mathcal{J}_C[\ell]$ by a diagonal matrix $M = \operatorname{diag}(1, q, \alpha, q/\alpha)$ on $\mathcal{J}_C[\ell]$ with respect to the basis

$$\mathcal{B} = \{x_1, y_2, y_3, y_4\}.$$

Now, choose a random point $z \in \mathcal{J}_C[\ell] \setminus \mathcal{J}_C(\mathbb{F}_q)[\ell]$. Since $z - \varphi(z) \in \langle y_2, y_3, y_4\rangle$, we may assume that $z \in \langle y_2, y_3, y_4\rangle$. Write $z = \alpha_2 y_2 + \alpha_3 y_3 + \alpha_4 y_4$. Then

$$\begin{aligned} qz - \varphi(z) &= \alpha_2 q y_2 + \alpha_3 q y_3 + \alpha_4 q y_4 - (\alpha_2 q y_2 + \alpha_3 \alpha y_3 + \alpha_4 (q/\alpha) y_4) \\ &= \alpha_3 (q - \alpha) y_3 + \alpha_4 (q - q/\alpha) y_4; \end{aligned}$$

so $qz - \varphi(z) \in \langle y_3, y_4\rangle$. If $qz - \varphi(z) = 0$, then it follows that $q \equiv 1 \pmod{\ell}$. This contradicts the choice of the curve $C \in \mathcal{C}(\ell, q, k, \tau_k)$. Hence, we have a procedure to choose a point $\mathcal{O} \neq w \in W$.

Choose two random points $w_1, w_2 \in W$. Write $w_i = \alpha_{i3} y_3 + \alpha_{i4} y_4$ for $i = 1, 2$. We may assume that ε is given by $\mathcal{E}_{1,1}$ with respect to $\mathcal{B}$; cf. Remark 13. But then

$$\varepsilon(w_1, w_2) = \zeta^{\alpha_{13}\alpha_{24} - \alpha_{14}\alpha_{23}}.$$

Hence, $\varepsilon(w_1, w_2) = 1$ if and only if $\alpha_{13}\alpha_{24} \equiv \alpha_{14}\alpha_{23} \pmod{\ell}$. If $\alpha_{13} \not\equiv 0 \pmod{\ell}$, then $\varepsilon(w_1, w_2) = 1$ if and only if $\alpha_{24} \equiv \frac{\alpha_{14}\alpha_{23}}{\alpha_{13}} \pmod{\ell}$. So $\varepsilon(w_1, w_2) \neq 1$ with probability $1 - 1/\ell$. Hence, we have a procedure to find a basis of W.

Until now, we have found points $x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$ and $w_3, w_4 \in W$, such that $W = \langle w_3, w_4 \rangle$. Now, choose a random point $x_2 \in \mathcal{J}_C[\ell]$. Write $x_2 = \alpha_1 x_1 + \alpha_2 y_2 + \alpha_3 y_3 + \alpha_4 y_4$. Then $\varepsilon(x_1, x_2) = \zeta^{\alpha_2}$, i.e. $\varepsilon(x_1, x_2) = 1$ if and only if $\alpha_2 \equiv 0 \pmod{\ell}$. Thus, with probability $1 - \ell^3/\ell^4 = 1 - 1/\ell$, the set $\{x_1, x_2, w_3, w_4\}$ is a basis of $\mathcal{J}_C[\ell]$.

Summing up, if ℓ divides $4\tau_k$, then the following Algorithm 15 outputs generators of $\mathcal{J}_C[\ell]$ with probability $(1 - 1/\ell^n)^2$.

Algorithm 16. *The following algorithm takes as input a $\mathcal{C}(\ell, q, k, \tau_k)$-curve C, the numbers ℓ, q, k and τ_k and a number $n \in \mathbb{N}$.*

1. *Choose a random point $\mathcal{O} \neq x_1 \in \mathcal{J}_C(\mathbb{F}_q)[\ell]$*
2. *Let $i = j = 0$. While $i < n$ do the following*
   - (a) *Choose random points $y_3, y_4 \in \mathcal{J}_C[\ell]$; compute $x_\nu := q(y_\nu - \varphi(y_\nu)) - \varphi(y_\nu - \varphi(y_\nu))$ for $\nu = 3, 4$.*
   - (b) *If $\varepsilon(x_3, x_4) = 1$ then $i := i + 1$. Else $i := n$ and $j := 1$.*
3. *If $j = 0$ then output "failure" and stop.*
4. *Let $i = j = 0$. While $i < n$ do the following*
   - (a) *Choose a random point $x_2 \in \mathcal{J}_C[\ell]$.*
   - (b) *If $\varepsilon(x_1, x_2) = 1$ then $i := i + 1$. Else $i := n$ and $j := 1$.*
5. *If $j = 0$ then output "failure". Else output $\{x_1, x_2, x_3, x_4\}$.*

7.3. **The complete algorithm.** Combining Algorithm 15 and 16 yields the desired algorithm to find generators of $\mathcal{J}_C[\ell]$.

Algorithm 17. *The following algorithm takes as input a $\mathcal{C}(\ell, q, k, \tau_k)$-curve C, the numbers ℓ, q, k and τ_k and a number $n \in \mathbb{N}$.*

1. *If $\ell \nmid \tau_k$, run Algorithm 15 on input $(C, \ell, q, k, \tau_k, n)$.*
2. *If $\ell \mid \tau_k$, run Algorithm 16 on input $(C, \ell, q, k, \tau_k, n)$.*

Theorem 18. *Let C be a $\mathcal{C}(\ell, q, k, \tau_k)$-curve. On input (C, ℓ, τ_k, n), Algorithm 17 outputs generators of $\mathcal{J}_C[\ell]$ with probability at least $(1 - 1/\ell^n)^2$ and in expected running time $O(\log \ell)$.*

Proof. We may assume that the time necessary to perform an addition of two points on the Jacobian, to multiply a point with a number or to evaluate the q-power Frobenius endomorphism on the Jacobian is small compared to the time necessary to compute the (Weil-) pairing of two points on the Jacobian. By [4], the pairing can be evaluated in time $O(\log \ell)$. Hence, the expected running time of Algorithm 17 is of size $O(\log \ell)$. □

8. Implementation issues

A priori, to implement Algorithm 17, we need to find a q^k-Weil number ω_k of the Jacobian $\mathcal{J}_C$, in order to check if ℓ ramifies in $\mathbb{Q}(\omega_k)$ in the case when ℓ divides $4\tau_k$. On Jacobians generated by the *complex multiplication method* [17, 7, 3], we know the Weil numbers in advance. Hence, Algorithm 17 is particularly well suited for such Jacobians.

Fortunately, in most cases ℓ does not divide $4\tau_k$, and then we do not have to find a q^k-Weil number. And in fact, we do not even have to compute $4\tau_k$. To see this, notice that by Theorem 10, the Weil polynomial of $\mathfrak{J}_C$ is of the form

$$P(X) \equiv (X-1)(X-q)(X-\alpha)(X-q/\alpha) \pmod{\ell}.$$

Let φ be the q-power Frobenius endomorphism on $\mathfrak{J}_C$, and let $P_k(X)$ be the characteristic polynomial of φ^k. Since φ is diagonalizable on $\mathfrak{J}_C[\ell]$, it follows that

$$P_k(X) \equiv (X-1)^2(X-\alpha^k)(X-1/\alpha^k) \pmod{\ell}.$$

If ℓ divides $4\tau_k$, then $\mathfrak{J}_C[\ell] \subseteq \mathfrak{J}_C(\mathbb{F}_{q^k})$; cf. Theorem 5. But then $P_k(X) \equiv (X-1)^4 \pmod{\ell}$. Hence,

$$\ell \text{ divides } 4\tau_k \text{ if and only if } \alpha^k \equiv 1 \pmod{\ell}. \tag{2}$$

Assume $\alpha^k \equiv 1 \pmod{\ell}$. Then $P_k(X) \equiv (X-1)^4 \pmod{\ell}$. Hence,

$$\ell \text{ ramifies in } \mathbb{Q}(\omega^k) \text{ if and only if } \omega^k \notin \mathbb{Z}; \tag{3}$$

cf. [13, Proposition 8.3, p. 47]. Here, ω is a q-Weil number of $\mathfrak{J}_C$.

Consider the case when $\alpha^k \equiv 1 \pmod{\ell}$ and $\omega^k \in \mathbb{Z}$. Then $\omega = \sqrt{q}e^{\frac{in\pi}{k}}$ for some $n \in \mathbb{Z}$ with $0 < n < k$. Assume k divides mn for some $m < k$. Then $\omega^{2m} = q^m \in \mathbb{Z}$. Since the q-power Frobenius endomorphism is the identity on the $\mathbb{F}_q$-rational points on the Jacobian, it follows that $\omega^{2m} \equiv 1 \pmod{\ell}$. Hence, $q^m \equiv 1 \pmod{\ell}$, i.e. k divides m. This is a contradiction. So n and k has no common divisors. Let $\xi = \omega^2/q = e^{\frac{in2\pi}{k}}$. Then ξ is a primitive k^{th} root of unity, and $\mathbb{Q}(\xi) \subseteq K$. Since $[K:\mathbb{Q}] \leq 4$ and $[\mathbb{Q}(\xi):\mathbb{Q}] = \phi(k)$, where ϕ is the Euler phi function, it follows that $k \leq 12$. Hence,

$$\text{if } \alpha^k \equiv 1 \pmod{\ell}, \text{ then } \omega^k \in \mathbb{Z} \text{ if and only if } k \leq 12. \tag{4}$$

The criteria (2), (3) and (4) provides the following efficient Algorithm 19 to check whether a given curve is of type $\mathcal{C}(\ell, q, k, \tau_k)$, and whether ℓ divides $4\tau_k$.

Algorithm 19. *Let $\mathfrak{J}_C$ be the Jacobian of a genus two curve C. Assume the odd prime number ℓ divides the number of $\mathbb{F}_q$-rational points on $\mathfrak{J}_C$, and that ℓ divides neither q nor $q-1$. Let k be the multiplicative order of q modulo ℓ.*

(1) *Compute the Weil polynomial $P(X)$ of $\mathfrak{J}_C$. Let $P(X) \equiv \prod_{i=1}^4 (X-\alpha_i) \pmod{\ell}$.*
(2) *If $\alpha_i^k \not\equiv 1 \pmod{\ell}$ for an $i \in \{1,2,3,4\}$, then output "$C \in \mathcal{C}(\ell, q, k, \tau_k)$ and ℓ does not divide $4\tau_k$" and stop.*
(3) *If $k > 12$ then output "$C \notin \mathcal{C}(\ell, q, k, \tau_k)$" and stop.*
(4) *Output "$C \in \mathcal{C}(\ell, q, k, \tau_k)$ and ℓ divides $4\tau_k$" and stop.*

References

[1] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *SIAM J. Computing*, 32(3):586–615, 2003.
[2] 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.
[3] K. Eisenträger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields, 2007. To appear in *Proceedings of AGCT-10*. Available at `http://arxiv.org`.
[4] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.
[5] 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.

[6] S.D. Galbraith, F. Hess, and F. Vercauteren. Hyperelliptic pairings. In *Pairing 2007*, Lecture Notes in Computer Science, pages 108–131. Springer, 2007.
[7] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The p-adic cm-method for genus 2, 2005.
[8] F. Hess. A note on the tate pairing of curves over finite fields. *Arch. Math.*, 82:28–32, 2004.
[9] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203–209, 1987.
[10] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1:139–150, 1989.
[11] S. Lang. *Abelian Varieties*. Interscience, 1959.
[12] V.S. Miller. The weil pairing, and its efficient calculation. *J. Cryptology*, 17:235–261, 2004.
[13] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.
[14] C.R. Ravnshøj. Generators of Jacobians of hyperelliptic curves, 2007. Preprint, available at `http://arxiv.org`. Submitted to *Math. Comp.*
[15] C.R. Ravnshøj. Non-cyclic subgroups of Jacobians of genus two curves, 2007. Preprint, available at `http://arxiv.org`. Submitted to *Design, Codes and Cryptography*.
[16] K. Rubin and A. Silverberg. Supersingular abelian varieties in cryptology. In M. Yung, editor, *CRYPTO 2002*, Lecture Notes in Computer Science, pages 336–353. Springer, 2002.
[17] 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`