# Abelian varieties with prescribed embedding degree

David Freeman[1], Peter Stevenhagen[2], and Marco Streng[2]

[1] University of California, Berkeley**
dfreeman@math.berkeley.edu
[2] Mathematisch Instituut, Universiteit Leiden
psh,streng@math.leidenuniv.nl

**Abstract.** We present an algorithm that, on input of a CM-field $K$, an integer $k \geq 1$, and a prime $r \equiv 1 \bmod k$, constructs a $q$-Weil number $\pi \in \mathcal{O}_K$ corresponding to an abelian variety $A$ over the field $\mathbf{F}$ of $q$ elements that has an $\mathbf{F}$-rational point of order $r$ and embedding degree $k$ with respect to $r$. We then show how CM-methods over $K$ can be used to explicitly construct $A$.

## 1 Introduction

Let $A$ be an abelian variety defined over a finite field $\mathbf{F}$, and $r \neq \mathrm{char}(\mathbf{F})$ a prime number dividing the order of the group $A(\mathbf{F})$. Then the *embedding degree* of $A$ with respect to $r$ is the degree of the field extension $\mathbf{F} \subset \mathbf{F}(\zeta_r)$ obtained by adjoining a primitive $r$-th root of unity $\zeta_r$ to $\mathbf{F}$.

The embedding degree is a natural notion in pairing-based cryptography, where $A$ is taken to be the Jacobian of a curve defined over $\mathbf{F}$. In this case, $A$ is principally polarized and we have the non-degenerate *Weil pairing*

$$e_r : A[r] \times A[r] \longrightarrow \mu_r$$

on the subgroup scheme $A[r]$ of $r$-torsion points of $A$ with values in the $r$-th roots of unity. If $\mathbf{F}$ contains $\zeta_r$, we also have the non-trivial *Tate pairing*

$$t_r : A[r](\mathbf{F}) \times A(\mathbf{F})/rA(\mathbf{F}) \to \mathbf{F}^*/(\mathbf{F}^*)^r.$$

The Weil and Tate pairings can be used to 'embed' $r$-torsion subgroups of $A(\mathbf{F})$ in the multiplicative group $\mathbf{F}(\zeta_r)^*$, and this has immediate consequences for the discrete logarithm problem in $A(\mathbf{F})[r]$, which forms the basis for several cryptographic protocols. In pairing-based cryptographic protocols [4], one chooses the prime $r$ and the embedding degree $k$ such that the discrete logarithm problems in $A(\mathbf{F})[r]$ and $\mathbf{F}(\zeta_r)^*$ are computationally infeasible, and of roughly equal difficulty. This means that $r$ is typically large, whereas $k$ is small. Jacobians of curves meeting such requirements are often said to be *pairing-friendly.*

** The first author is supported by a National Defense Science and Engineering Graduate Fellowship

If $\mathbf{F}$ has order $q$, the embedding degree $k = [\mathbf{F}(\zeta_r) : \mathbf{F}]$ is simply the multiplicative order of $q$ in $(\mathbf{Z}/r\mathbf{Z})^*$. As 'most' elements in $(\mathbf{Z}/r\mathbf{Z})^*$ have large order, the embedding degree of $A$ with respect to a large prime divisor $r$ of $\#A(\mathbf{F})$ will usually be of the same size as $r$, and $A$ will not be pairing-friendly. One is therefore led to the question of how to efficiently construct $A$ and $\mathbf{F}$ such that $A(\mathbf{F})$ has a (large) prime factor $r$ and the embedding degree of $A$ with respect to $r$ has a prescribed (small) value $k$. The current paper addresses this question on two levels: the *existence* and the actual *construction* of $A$ and $\mathbf{F}$.

Section 2 focuses on the question whether, for given $r$ and $k$, there exist abelian varieties $A$ that are defined over a finite field $\mathbf{F}$, have an $\mathbf{F}$-rational point of order $r$, and have embedding degree $k$ with respect to $r$. Here we restrict to *ordinary* abelian varieties $A$, i.e., those $A$ for which the endomorphism ring $\mathrm{End}(A)$ over $\overline{\mathbf{F}}$ is isomorphic to an order of rank $2g = 2\dim(A)$ in a number field $K$. This restriction is very mild, as in any dimension $g$, 'most' abelian varieties are ordinary: they make up a Zariski-open part of the moduli spaces involved. It also frees us from unwanted restrictions on embedding degrees such as those occurring for supersingular $A$ [5]. Ordinary abelian varieties $A$ can be characterized up to isogeny by their CM-field $K = \mathrm{End}(A)\otimes\mathbf{Q}$ and the Frobenius element $\pi \in K$, which is a *$q$-Weil number* in $K$, with $q = \#\mathbf{F}$. The existence of abelian varieties with the properties we want is therefore tantamount to the existence of suitable Weil numbers in CM-fields $K$. What our Algorithm 2.10 achieves is the construction of suitable $q$-Weil numbers $\pi$ in a given CM-field $K$ of degree $2g$ in time polynomial in $\log r$. It exhibits $\pi$ as a *type norm* of an element in the *reflex field* of $K$ satisfying certain congruences modulo $r$. The abelian varieties $A$ in the isogeny classes over $\mathbf{F}$ that correspond to these Weil numbers have an $\mathbf{F}$-rational point of order $r$ and embedding degree $k$ with respect to $r$.

For an abelian variety of dimension $g$ over the field $\mathbf{F}$ of $q$ elements, the group $A(\mathbf{F})$ has about $q^g$ elements, and one traditionally compares this size to $r$ by putting

$$\rho = \frac{g \log q}{\log r}. \tag{1.1}$$

In cryptographic terms, $\rho$ measures the ratio of a pairing-based system's required bandwidth to its security level, so small $\rho$-values are desirable. In Section 3, we show that for fixed $K$, the expected run time of our algorithm is heuristically polynomial in $\log r$, and we discuss the distribution of the $\rho$-values it yields.

In Section 4, we address the issue of the actual construction of abelian varieties corresponding to the Weil numbers found by our algorithm. This is accomplished via the construction in characteristic zero of the abelian varieties having CM by the ring of integers $\mathcal{O}_K$ of $K$, a hard problem that is far from being algorithmically solved. Part of the problem is that in dimension $g > 3$, only few abelian varieties arise as Jacobians of curves, and we only have efficient group operations for Jacobians of hyperelliptic curves. In Section 4, we discuss the elliptic case $g = 1$, for which reasonable algorithms exist, and the case $g = 2$, for which such algorithms are still in their infancy. For genus $g \geq 3$, we restrict attention to a few families of curves that we can handle at this point. Our final Section 5 provides numerical examples.

## 2 Weil numbers yielding prescribed embedding degrees

In this section, we determine which $q$-Weil numbers $\pi$ correspond to abelian varieties with prescribed embedding degrees, and provide an algorithm to find such $\pi$.

Let $A$ be a $g$-dimensional ordinary abelian variety over the field $\mathbf{F} = \mathbf{F}_q$ of $q$ elements, and $K = \mathrm{End}(A) \otimes \mathbf{Q}$ its associated CM-field. This is a totally complex number field of degree $2g$, and a quadratic extension of a totally real subfield $K_0 \subset K$. The Frobenius endomorphism $\pi \in \mathrm{End}(A)$ is an algebraic integer in $K$, and if we denote the complex conjugation automorphism of $K$ over $K_0$ by $\overline{\cdot}$, we have

$$N_{K/K_0}(\pi) = \pi\overline{\pi} = q.$$

It follows that $\pi$ is a *$q$-Weil number* in $K$: an algebraic integer with the property that all of its embeddings in $\overline{\mathbf{Q}}$ have complex absolute value $\sqrt{q}$. The $q$-Weil number $\pi \in \mathrm{End}(A) \subset K$ determines the group order of $A(\mathbf{F})$: as the $\mathbf{F}$-rational points of $A$ form the kernel of the endomorphism $\pi - 1$, we have

$$\#A(\mathbf{F}) = \mathrm{N}_{K/\mathbf{Q}}(\pi - 1).$$

**Proposition 2.1.** *Let $A$ be an ordinary abelian variety over $\mathbf{F} = \mathbf{F}_q$ with CM-field $K$, and $\pi \in \mathcal{O}_K$ the Frobenius endomorphism of $A$. Let $k$ be a positive integer, $\Phi_k$ the $k$-th cyclotomic polynomial, and $r \nmid qk$ a prime number. If we have*

$$\begin{aligned} \mathrm{N}_{K/\mathbf{Q}}(\pi - 1) &\equiv 0 \pmod{r}, \\ \Phi_k(\pi\overline{\pi}) &\equiv 0 \pmod{r}, \end{aligned}$$

*then $A$ has embedding degree $k$ with respect to $r$.*

**Proof**. The first condition tells us that $r$ divides $\#A(\mathbf{F}_q)$, the second that the order of $\pi\overline{\pi} = q$ in $(\mathbf{Z}/r\mathbf{Z})^*$, which is the embedding degree of $A$ with respect to $r$, equals $k$. □

If we fix a CM-field $K$, i.e., a totally complex quadratic extension $K$ of some totally real number field $K_0$, we can search for $q$-Weil numbers $\pi \in \mathcal{O}_K$ meeting the conditions of Proposition 2.1. By a theorem of Honda and Tate [7], all such $q$-Weil numbers arise as Frobenius elements of abelian varieties defined over $\mathbf{F} = \mathbf{F}_q$ having $K$ as their CM-field, and we can prove the *existence* of an abelian variety $A$ as in Proposition 2.1 by exhibiting a $q$-Weil number $\pi \in K$ as in the proposition.

**Example 2.2.** Our general construction is motivated by the case where $K$ is a Galois CM-field of degree $2g$, with cyclic Galois group generated by $\sigma$. Here

$\sigma^g$ is complex conjugation, so we can construct an element $\pi \in \mathcal{O}_K$ satisfying $\pi\sigma^g(\pi) = \pi\overline{\pi} \in \mathbf{Z}$ by choosing any $\xi \in \mathcal{O}_K$ and letting $\pi = \prod_{i=1}^g \sigma^i(\xi)$. Then we have $\pi\overline{\pi} = N_{K/\mathbf{Q}}(\xi)$, which is an integer. If this integer is a prime (or prime power) $q$, then $\pi$ is a $q$-Weil number in $K$.

Now we wish to impose the conditions of Proposition 2.1 on $\pi$. Let $r$ be a rational prime that splits completely in $K$, and $\mathfrak{r}$ a prime of $\mathcal{O}_K$ over $r$. For $i = 1, \ldots, 2g$, put $\mathfrak{r}_i = \sigma^{-i}(\mathfrak{r})$; then the factorization of $r$ in $\mathcal{O}_K$ is $r\mathcal{O}_K = \prod_{i=1}^{2g} \mathfrak{r}_i$. If $\alpha_i \in \mathbf{F}_r = \mathcal{O}_K/\mathfrak{r}_i$ is the residue class of $\xi$ modulo $\mathfrak{r}_i$, then we see that the residue class of $\pi$ modulo $\mathfrak{r}$ is $\prod_{i=1}^g \alpha_i$, and furthermore, the residue class of $\pi\overline{\pi}$ modulo $\mathfrak{r}$ is $\prod_{i=1}^{2g} \alpha_i$. If we choose $\xi$ to satisfy

$$\textstyle\prod_{i=1}^g \alpha_i = 1 \in \mathbf{F}_r, \tag{2.3}$$

we find $\pi \equiv 1 \pmod{\mathfrak{r}}$ and thus $N_{K/\mathbf{Q}}(\pi - 1) \equiv 0 \pmod{r}$. By choosing $\xi$ such that in addition

$$\zeta = \textstyle\prod_{i=1}^{2g} \alpha_i = \prod_{i=g+1}^{2g} \alpha_i \tag{2.4}$$

is a primitive $k$-th root of unity in $\mathbf{F}_r^*$, we guarantee that $\pi\overline{\pi} = q$ is a primitive $k$-th root of unity modulo $r$. Thus, we can try to find a Weil number as in Proposition 2.1 by picking residue classes $\alpha_i \in \mathbf{F}_r^*$ for $i = 1, \ldots, 2g$ meeting the two conditions above, computing some 'small' lift $\xi \in \mathcal{O}_K$ with $(\xi \bmod \mathfrak{r}_i) = \alpha_i$ and testing whether $\pi = \prod_{i=1}^g \sigma^i(\xi)$ has prime power norm. As numbers of moderate size have a high probability of being prime by the prime number theorem, a small number of choices $(\alpha_i)_i$ should suffice. There are $(r-1)^{2g-2}\varphi(k)$ possible choices for $(\alpha_i)_{i=1}^{2g}$, where $\varphi$ is the Euler totient function, so for $g > 1$ and $r$ large we are very likely to succeed. For $g = 1$, there are only a few choices $(\alpha_1, \alpha_2) = (1, \zeta)$, but one can try various lifts and thus recover what is known as the Cocks-Pinch algorithm [2, Theorem 4.1] for finding pairing-friendly elliptic curves.

For arbitrary CM-fields $K$, the appropriate generalization of the map

$$\xi \mapsto \textstyle\prod_{i=1}^g \sigma^i(\xi)$$

in Example 2.2 is provided by the *type norm*. A *CM-type* of a CM-field $K$ of degree $2g$ is a set $\Phi = \{\phi_1, \ldots, \phi_g\}$ of embeddings of $K$ into its normal closure $L$ such that $\Phi \cup \overline{\Phi} = \{\phi_1, \ldots, \phi_g, \overline{\phi_1}, \ldots, \overline{\phi_g}\}$ is the complete set of embeddings of $K$ into $L$. The *type norm* $N_\Phi : K \to L$ with respect to $\Phi$ is the map

$$N_\Phi : x \longmapsto \textstyle\prod_{i=1}^g \phi_i(x),$$

which clearly satisfies

$$N_\Phi(x)\overline{N_\Phi(x)} = N_{K/\mathbf{Q}}(x) \in \mathbf{Q}. \tag{2.5}$$

If $K$ is not Galois, the type norm $N_\Phi$ does not map $K$ to itself, but to its *reflex field* $\widehat{K}$ with respect to $\Phi$. To end up in $K$, we can however take the type norm with respect to the *reflex type* $\Psi$, which we will define now.

Let $G$ be the Galois group of $L/\mathbf{Q}$, and $H$ the subgroup fixing $K$. Then the $2g$ left cosets of $H$ in $G$ can be viewed as the embeddings of $K$ in $L$, and this makes the CM-type $\Phi$ into a set of $g$ left cosets of $H$ for which we have $G/H = \Phi \cup \overline{\Phi}$. Let $S$ be the union of the left cosets in $\Phi$, and put $\widehat{S} = \{\sigma^{-1} : \sigma \in S\}$. Let $\widehat{H} = \{\gamma \in G : \gamma S = S\}$ be the stabilizer of $S$ in $G$. Then $\widehat{H}$ defines a subfield $\widehat{K}$ of $L$, and as we have $\widehat{H} = \{\gamma \in G : \widehat{S}\gamma = \widehat{S}\}$ we can interpret $\widehat{S}$ as a union of left cosets of $\widehat{H}$ inside $G$. These cosets define a set of embeddings $\Psi$ of $\widehat{K}$ into $L$. We call $\widehat{K}$ the *reflex field* of $(K, \Phi)$ and we call $\Psi$ the *reflex type.*

**Lemma 2.6.** *The field $\widehat{K}$ is a CM-field. It is generated over $\mathbf{Q}$ by the sums $\sum_{\phi\in\Phi} \phi(x)$ for $x \in K$, and $\Psi$ is a CM-type of $\widehat{K}$. The type norm $N_\Phi$ maps $K$ to $\widehat{K}$.*

**Proof**. The first two statements are proved in [6, Chapter II, Proposition 28] (though the definition of $\widehat{H}$ differs from ours, because Shimura lets $G$ act from the right). For the last statement, notice that for $\gamma \in \widehat{H}$, we have $\gamma S = S$, so $\gamma \prod_{\phi\in\Phi} \phi(x) = \prod_{\phi\in\Phi} \phi(x)$. □

A CM-type $\Phi$ of $K$ is *induced* from a CM-subfield $K' \subset K$ if it is of the form $\Phi = \{\phi : \phi|_{K'} \in \Phi'\}$ for some CM-type $\Phi'$ of $K'$. In other words, $\Phi$ is induced from $K'$ if and only if $S$ as above is a union of left cosets of $\mathrm{Gal}(L/K')$. We call $\Phi$ *primitive* if it is not induced from a strict subfield of $K$. Notice that the reflex type $\Psi$ is primitive by definition of $\widehat{K}$ and that $(K, \Phi)$ is induced from the reflex of its reflex. In particular, if $\Phi$ is primitive, then the reflex of its reflex is $(K, \Phi)$ itself. For $K$ Galois and $\Phi$ primitive we have $\widehat{K} = K$, and the reflex type of $\Phi$ is $\Psi = \{\phi^{-1} : \phi \in \Phi\}$.

For primitive CM-fields $K$ of degree 2 or 4, the reflex field $\widehat{K}$ has the same degree as $K$. This fails to be so for $g \geq 3$.

**Lemma 2.7.** *If $K$ has degree $2g$, then the degree of $\widehat{K}$ divides $2^g g!$.*

**Proof**. We have $K = K_0(\sqrt{\eta})$, with $K_0$ totally real and $\eta \in K$ totally negative. The normal closure $L$ of $K$ is obtained by adjoining to the normal closure $\widetilde{K_0}$ of $K_0$, which has degree dividing $g!$, the square roots of the $g$ conjugates of $\eta$. Thus $L$ is of degree dividing $2^g g!$, and $\widehat{K}$ is a subfield of $L$. □

For a 'generic' CM field $K$ the degree of $L$ is exactly $2^g g!$, and $\widehat{K}$ is a field of degree $2^g$ generated by $\sum_\sigma \sqrt{\sigma(\eta)}$, with $\sigma$ ranging over $\mathrm{Gal}(K_0/\mathbf{Q})$.

From (2.5) and Lemma 2.6, we find that for every $\xi \in \mathcal{O}_{\widehat{K}}$, the element $\pi = N_\Psi(\xi)$ is an element of $\mathcal{O}_K$ that satisfies $\pi\overline{\pi} \in \mathbf{Z}$. To make $\pi$ satisfy the conditions in Proposition 2.1, we need to impose conditions modulo $r$ on $\xi$ in $\widehat{K}$. Suppose $r$ splits completely in $K$, and therefore in its normal closure $L$ and in the reflex field $\widehat{K}$ with respect to $\Phi$. Pick a prime $\mathfrak{R}$ over $r$ in $L$, and write $\mathfrak{r}_\psi = \psi^{-1}(\mathfrak{R}) \cap \mathcal{O}_{\widehat{K}}$ for $\psi \in \Psi$. Then the factorization of $r$ in $\mathcal{O}_{\widehat{K}}$ is

$$r\mathcal{O}_{\widehat{K}} = \prod_{\psi\in\Psi} \mathfrak{r}_\psi \overline{\mathfrak{r}_\psi}. \tag{2.8}$$

**Theorem 2.9.** *Let $(K, \varPhi)$ be a CM-type and $(\widehat{K}, \varPsi)$ its reflex. Suppose the prime $r \equiv 1 \pmod{k}$ splits completely in $K$, and write its factorization in $\mathcal{O}_{\widehat{K}}$ as in (2.8). Given $\xi \in \mathcal{O}_{\widehat{K}}$, write $(\xi \bmod \mathfrak{r}_\psi) = \alpha_\psi \in \mathbf{F}_r$ and $(\xi \bmod \overline{\mathfrak{r}_\psi}) = \beta_\psi \in \mathbf{F}_r$ for $\psi \in \varPsi$. If we have*

$$\prod_{\psi \in \varPsi} \alpha_\psi = 1 \qquad \text{and} \qquad \prod_{\psi \in \varPsi} \beta_\psi = \zeta$$

*for some primitive $k$-th root of unity $\zeta \in \mathbf{F}_r^*$, then $\pi = N_\varPsi(\xi) \in \mathcal{O}_K$ satisfies $\pi\overline{\pi} \in \mathbf{Z}$ and*

$$\begin{aligned} \mathrm{N}_{K/\mathbf{Q}}(\pi - 1) &\equiv 0 \pmod{r}, \\ \varPhi_k(\pi\overline{\pi}) &\equiv 0 \pmod{r}. \end{aligned}$$

**Proof**. After our preparations, and with the correct notation in place, the proof is a more or less straightforward generalization of the argument in Example 2.2. The conditions imposed are analogous to (2.3) and (2.4), and they imply $\pi - 1$ and $\varPhi_k(\pi\overline{\pi})$ are in the prime $\mathfrak{R}$ underlying the factorization (2.8). □

If the complex absolute value of the element $\pi$ constructed in Theorem 2.9 is a prime power $q$, then $\pi$ is a $q$-Weil number corresponding to an abelian variety $A/\mathbf{F}_q$ with CM by $K$ and Frobenius element $\pi$. By Proposition 2.1, $A$ will have embedding degree $k$ with respect to $r$. This gives rise to the following algorithm.

**Algorithm 2.10.**

Input: a CM-field $K$ of degree $2g \geq 4$, a primitive CM-type $\varPhi$ of $K$, a positive integer $k$, and a prime $r \equiv 1 \pmod{k}$ that splits completely in $K$.

Output: a prime power $q$ and a $q$-Weil number $\pi \in K$ such that an abelian variety $A/\mathbf{F}_q$ with Frobenius endomorphism $\pi$ has embedding degree $k$ with respect to $r$.

1. Compute a Galois closure $L$ of $K$ and the reflex $(\widehat{K}, \varPsi)$ of $(K, \varPhi)$. Set $\widehat{g} \leftarrow \frac{1}{2} \deg \widehat{K}$ and write $\varPsi = \{\psi_1, \psi_2, \ldots, \psi_{\widehat{g}}\}$.
2. Fix a prime $\mathfrak{R} \mid r$ of $\mathcal{O}_L$, and compute the factorization of $r$ in $\mathcal{O}_{\widehat{K}}$ as in (2.8).
3. Compute a primitive $k$-th root of unity $\zeta \in \mathbf{F}_r$.
4. Choose random $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1} \in \mathbf{F}_r$.
5. Set $\alpha_{\widehat{g}} \leftarrow \prod_{i=1}^{\widehat{g}-1} \alpha_i^{-1} \in \mathbf{F}_r$ and $\beta_{\widehat{g}} \leftarrow \zeta \prod_{i=1}^{\widehat{g}-1} \beta_i^{-1} \in \mathbf{F}_r$.
6. Compute $\xi \in \mathcal{O}_{\widehat{K}}$ such that $(\xi \mod \mathfrak{r}_{\psi_i}) = \alpha_i$ and $(\xi \mod \overline{\mathfrak{r}_{\psi_i}}) = \beta_i$ for $i = 1, 2, \ldots, \widehat{g}$.
7. Set $q \leftarrow \mathrm{N}_{\widehat{K}/\mathbf{Q}}(\xi)$. If $q$ is not a prime power, go to Step (4).
8. Set $\pi \leftarrow N_\varPsi(\xi)$.
9. Return $q$ and $\pi$.

**Remark 2.11.** We require $g \geq 2$ in Algorithm 2.10, as the case $g = 1$ is already covered by Example 2.2, and requires a slight adaptation.

The condition that $r$ be prime is for simplicity of presentation only; the algorithm easily extends to square-free values of $r$ that are products of splitting primes. Such $r$ are required, for example, by the cryptosystem of [1].

## 3 Performance of the algorithm

Algorithm 2.10 consists of a precomputation for the field $K$ (Steps (1)–(3)) followed by a loop (Steps (4)–(7)) that is performed until an element $\xi$ of prime power norm $q$ is found in Step (7). In order to maximize the likelihood of finding prime power norms, and also to minimize the $\rho$-value (1.1), one should try to minimize the norm of the lift $\xi$ computed in the Chinese Remainder Step (6). This involves minimizing a norm function of degree $2\widehat{g}$ in $2\widehat{g}$ integral variables, which is already infeasible for $\widehat{g} = 2$ as Step (6) may have to be executed many times.

It is better in practice to lift a standard basis of $\mathcal{O}_{\widehat{K}}/r\mathcal{O}_{\widehat{K}} \cong (\mathbf{F}_r)^{2\widehat{g}}$ to $\mathcal{O}_{\widehat{K}}$ once and for all, and then multiply those lifts by integer representatives for $\alpha_i$ and $\beta_i$. To get upper bounds on the norms of such lifts, we fix a basis of $\mathcal{O}_{\widehat{K}}$ and let $F$ be the fundamental parallelotope in $\widehat{K} \otimes \mathbf{R}$ consisting of those elements that have coefficients in $(-\frac{1}{2}, \frac{1}{2}]$ with respect to our chosen basis. Then there is a unique lift $\xi$ inside $rF$ in Step (6), which is obtained from any lift by expressing it in terms of the basis and reducing the coordinates modulo $r$ to bring them in $(-r/2, r/2]$. If we denote the maximum on $F \cap \widehat{K}$ of all complex absolute values of $\widehat{K}$ by $M_{\widehat{K}}$, we have

$$q = N_{\widehat{K}/\mathbf{Q}}(\xi) \leq (rM_{\widehat{K}})^{2\widehat{g}},$$

and for the $\rho$-value (1.1) we find

$$\rho \leq 2g\widehat{g}(1 + \log M_{\widehat{K}}/\log r),$$

which is approximately $2g\widehat{g}$ if $r$ gets large with respect to $M_{\widehat{K}}$. By the prime number theorem, a random integer below a bound $B$ is prime with probability $1/\log(B)$, so if we view the value $q = N_{\widehat{K}/\mathbf{Q}}(\xi)$ as a random integer below its upper bound, the expected number of executions of Steps (4)–(7) before finding a prime $q$ is heuristically at most $2\widehat{g}\log(rM_{\widehat{K}})$. The probability of finding prime *powers* $q$ is very small, and this hardly ever happens in practice.

**Theorem 3.1.** *If the field $K$ is fixed, then the heuristic running time of Algorithm 2.10 is polynomial in $\log r$.* □

Let $H_{r,k}$ be the subset of the parallelotope $rF$ consisting of those $\xi \in rF \cap \mathcal{O}_{\widehat{K}}$ that satisfy the two congruence conditions of Theorem 2.9 for a given embedding degree $k$. Heuristically, we will treat the elements of $H_{r,k}$ as random elements of $rF \cap \mathcal{O}_{\widehat{K}}$ with respect to the distributions of complex absolute values and norm functions. This yields expected values for the probability that $q = N_{\widehat{K}/\mathbf{Q}}(\xi)$ is in a given range for randomly chosen $\alpha_i$ and $\beta_i$ in Step (4) of Algorithm 2.10, and also tells us what the best $\rho$-value is that we can expect to exist.

**Theorem 3.2.** *If the field $K$ is fixed and $r$ gets large, we expect the output $q$ of Algorithm 2.10 to yield $\rho \approx 2g\widehat{g}$. Furthermore, we expect the element $\xi \in \mathcal{O}_{\widehat{K}}$ of smallest norm satisfying the conditions of Theorem 2.9 to yield $\rho \approx 2g$.*

**Open problem 3.3.** *Find an efficient algorithm to compute the element $\xi \in \mathcal{O}_{\widehat{K}}$ of smallest norm satisfying the conditions of Theorem 2.9.*

We have already proven an upper bound on $\rho$, so it remains to give a lower bound for $\rho$ on the output of our algorithm and to give the estimates for the best possible $\xi$. We start with the latter.

As $\widehat{K}$ is totally complex of degree $2\widehat{g}$, the $\mathbf{R}$-algebra $\widehat{K} \otimes \mathbf{R}$ is naturally isomorphic to $\mathbf{C}^{\widehat{g}}$. Let $Q_{\widehat{K}} > 0$ be a lower bound on $\widehat{K} \setminus F$ for the maximum of all complex absolute values, so the box $V_X \subset \widehat{K} \otimes \mathbf{R}$ consisting of those elements that have all absolute values below $X$ lies completely inside $(X/Q_{\widehat{K}})F$. The standard volume of $V_X$ in $\widehat{K} \otimes \mathbf{R}$ is $(\pi X^2)^{\widehat{g}}$, while $rF$ has volume $(r^2/2)^{\widehat{g}}\sqrt{|\Delta_{\widehat{K}}|}$, where $\Delta_{\widehat{K}}$ is the discriminant of $\widehat{K}$. If $X$ is a real number between 0 and $rQ_{\widehat{K}}$, then $V_X$ is completely contained inside $rF$, so the expected number of $\xi \in H_{r,k}$ with all absolute values below $X$ is $\#H_{r,k} = r^{2\widehat{g}-2}\varphi(k)$ times the quotient of these volumes, which is

$$\frac{(2\pi)^{\widehat{g}} X^{2\widehat{g}}}{r^{2\widehat{g}}\sqrt{|\Delta_{\widehat{K}}|}}. \tag{3.4}$$

Since every such $\xi$ has norm at most $X^{2\widehat{g}}$, we get the following result.

**Lemma 3.5.** *Given a real number $Y \in (0, (rQ_{\widehat{K}})^{2\widehat{g}})$, the expected number of $\xi \in H_{r,k}$ satisfying $N_{\widehat{K}/\mathbf{Q}}(\xi) < Y$ is at least*

$$\frac{(2\pi)^{\widehat{g}}\varphi(k)}{\sqrt{|\Delta_{\widehat{K}}|}}\left(\frac{Y}{r^2}\right).$$

If we fix our field $K$ and take any $\varepsilon > 0$, then for sufficiently large $r$ there will be many choices of $\alpha_i, \beta_i$ that give $q = N_{\widehat{K}/\mathbf{Q}}(\xi) < Y = r^{2+\varepsilon}$, so we have $\rho < (2+\varepsilon)g$ for the optimal $\xi$.

We now find a lower bound on $\rho$ for the optimal $\xi$. Let $\mathcal{O}_0$ be the ring of integers of the maximal real subfield of $\widehat{K}$. Let $U$ be the subgroup of norm one elements of $\mathcal{O}_0^*$. Notice that the conditions of Theorem 2.9, as well as the norm of $\xi$, are invariant under multiplication by elements of $U$. We embed $\mathcal{O}_0^*$ into $\mathbf{R}^{\widehat{g}}$ by mapping $u$ to the vector of logarithms of absolute values of $u$. The image forms a complete lattice in the $(\widehat{g}-1)$-dimensional space of vectors with coordinate sum 0. Fix a fundamental parallelotope $F'$ for the index-2 sublattice $U$. Without loss of generality, the vector of logarithms of absolute values of the optimal $\xi$ is inside $F' + \mathbf{C}(1,\ldots,1)$, so every difference of two logarithms of absolute values is bounded, hence every quotient of absolute values of $\xi$ is bounded from below by a positive constant $c'$, depending only on $K$. In particular, if $|\xi|$ is the maximum of all absolute values of $\xi$, then $N_{\widehat{K}/\mathbf{Q}}(\xi) > (c'|\xi|)^{2\widehat{g}}$, so if $\xi$ has norm below $X^{2\widehat{g}}$, then it is inside $V_{X/c'}$. As we have seen in (3.4), if $X/c'$ is between 0 and $rQ_{\widehat{K}}$, then the expected number of $\xi$ in $V_{X/c'} \cap H_{k,r}$ is $c''X^{2\widehat{g}}r^{-2}$ for some positive constant $c''$ depending only on the field $K$. In particular, if we fix $\varepsilon > 0$ and take $X^{2\widehat{g}} = r^{2-\varepsilon}$, then for sufficiently large $r$, we expect such $\xi$ not to exist, hence we expect $\rho > g(2-\varepsilon)$ for the optimal $\xi$, and therefore $\rho \approx 2$ as claimed.

For simplicity, we prove the lower bound for random $\xi$ only for $g = 2$, so suppose that $g = \widehat{g} = 2$.

**Lemma 3.6.** *Fix the field $K$. Under our heuristic assumption, there exist constants $c_3, c_4 > 0$ such that for all $\varepsilon > 0$, if $r$ is sufficiently large, then the probability that a random $\xi \in H_{r,k}$ satisfies $q < r^{2\widehat{g}-\varepsilon}$ is less than $c_3 r^{-c_4\varepsilon}$.*

**Proof** *(for $g = 2$).* Let $V_b \subset \widehat{K} \otimes \mathbf{R}$ be the set of those elements that have all absolute values below $b$ and for which the product of the absolute values is below 1. If $b \geq 1$, then the volume of this set is $\pi^2(1 + 4\log(b))$. If $b = M_{\widehat{K}} r^{\varepsilon/4}$, then $r^{1-\varepsilon/4}V_b$ contains all $\xi$ inside $rF$ of norm at most $r^{4-\varepsilon}$, so the probability of $\xi \in rF$ to have norm at most $r^{4-\varepsilon}$ is smaller than

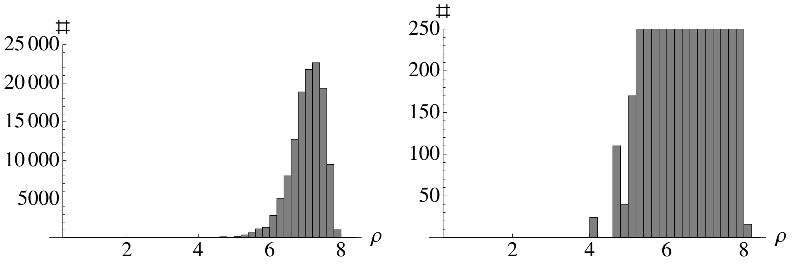
$$\frac{(2\pi)^2}{\sqrt{|\Delta_{\widehat{K}}|}}(1 + 4\log(M_{\widehat{K}}) + \log(r^{\varepsilon}))r^{-\varepsilon} < \frac{(2\pi)^2}{\sqrt{|\Delta_{\widehat{K}}|}}(2 + 4\log(M_{\widehat{K}}))r^{-\frac{1}{2}\varepsilon}$$

if $r^{\varepsilon}$ is larger than $\max\{1, M_{\widehat{K}}^{-4}\}$. □

If we fix $K$ and $\varepsilon > 0$, then this shows that for large $r$, we have $\rho > g(2\widehat{g} - \varepsilon)$ with high probability. This finishes the proof of Theorem 3.2.

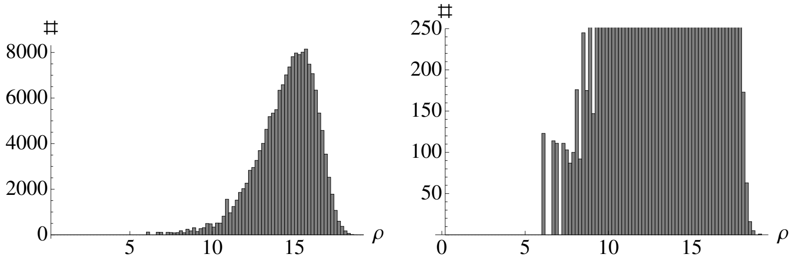
For very small values of $r$ we are able to do a brute-force search for the smallest $q$ by testing all possible values of $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1}$ in Step 4 of Algorithm 2.10. We performed two such searches, one in dimension 2 and one in dimension 3. The experimental results support our heuristic evidence that $\rho \approx 2g$ is possible with a smart choice in the algorithm, and that $\rho \approx 2g\widehat{g}$ is achieved with a randomized algorithm.

**Example 3.7.** Take $K = \mathbf{Q}(\zeta_5)$, and let $\Phi = \{\phi_1, \phi_2\}$ be the CM-type of $K$ defined by $\phi_n(\zeta_5) = e^{2\pi i n/5}$. We ran Algorithm 2.10 with $r = 1021$ and $k = 2$, and tested all possible values of $\alpha_1, \beta_1$. The total number of primes $q$ found was 125578, and the corresponding $\rho$-values were distributed as follows:



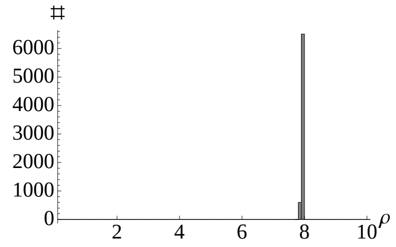
The smallest $q$ found was 2023621, giving a $\rho$-value of 4.19. The curve over $\mathbf{F}_q$ for which the Jacobian has this $\rho$-value is $y^2 = x^5 + 18$, and the number of points on its Jacobian is 4092747290896.

**Example 3.8.** Take $K = \mathbf{Q}(\zeta_7)$, and let $\Phi = \{\phi_1, \phi_2, \phi_3\}$ be the CM-type of $K$ defined by $\phi_i(\zeta_7) = e^{2\pi i/7}$. We ran Algorithm 2.10 with $r = 29$ and $k = 4$, and tested all possible values of $\alpha_1, \alpha_2, \beta_1, \beta_2$. The total number of primes $q$ found was 162643, and the corresponding $\rho$-values were distributed as follows:



The smallest $q$ found was 911, giving a $\rho$-value of 6.07. The curve over $\mathbf{F}_q$ for which the Jacobian has this $\rho$-value is $y^2 = x^7 + 34$, and the number of points on its Jacobian is 778417333.

**Example 3.9.** Take $K = \mathbf{Q}(\zeta_5)$, and let $\Phi = \{\phi_1, \phi_2\}$ be the CM-type of $K$ defined by $\phi_i(\zeta_5) = e^{2\pi i/5}$. We ran Algorithm 2.10 with $r = 2^{160} + 685$ and $k = 10$, and tested $2^{20}$ random values of $\alpha_1, \beta_1$. The total number of primes $q$ found was 6939, and the corresponding $\rho$-values were distributed as follows:



The smallest $q$ found has 621 binary digits, giving a $\rho$-value of 7.76.

## 4 Construction of abelian varieties with prescribed Weil numbers

Our Algorithm 2.10 yields $q$-Weil numbers $\pi \in K$ that correspond, in the sense of the theorem of Honda and Tate [7], to isogeny classes of abelian varieties that have a point of order $r$ and embedding degree $k$ with respect to $r$. It does not give a method to explicitly construct an abelian variety $A$ with Frobenius $\pi \in K$. In this section we focus on the problem of explicitly constructing such varieties using complex multiplication techniques.

We will assume throughout that $q$ is a prime number, as this is what our algorithm yields with very high probability, and that the $q$-Weil number $\pi$ we find is an algebraic integer of degree $2g = [K : \mathbf{Q}]$ in $K$. It then corresponds to the isogeny class of a *simple* abelian variety over $\mathbf{F}_q$. In all interesting cases, $q$ will not be a very small prime, so there is no harm in assuming that the $q$-Weil number $\pi$ we are dealing with corresponds to an isogeny class of *ordinary* abelian varieties; these are the abelian varieties for which the minimal polynomial of $\pi$ has middle coefficient relatively prime to $q$.

The key point of the complex multiplication construction is the fact that every ordinary abelian variety over $\mathbf{F}_q$ with Frobenius $\pi \in K$ arises as the reduction at a prime over $q$ of some abelian variety $A_0$ in characteristic zero that has CM by the ring of integers of $K$. Thus, if we have fixed our $K$ as in Algorithm 2.10, we can solve the construction problem for all ordinary Weil numbers coming out of the algorithm by compiling the finite list of $\overline{\mathbf{Q}}$-isogeny classes of abelian varieties in characteristic zero having CM by $\mathcal{O}_K$. There will be one class for each equivalence class of primitive CM-types of $K$, where $\Phi$ and $\Phi'$ are said to be equivalent if we have $\Phi = \Phi' \circ \sigma$ for an automorphism $\sigma$ of $K$. These abelian varieties will not in general be defined over $K$, but over some extension field of $K$. As we can choose our favorite field $K$ of degree $2g$ to produce abelian varieties of dimension $g$, we can pick fields $K$ for which such lists already occur in the literature.

From representatives of our list of isogeny classes of abelian varieties in characteristic zero having CM by $\mathcal{O}_K$, we obtain a list $\mathcal{A}$ of abelian varieties over $\mathbf{F}_q$ with CM by $\mathcal{O}_K$ by reducing at some fixed prime $\mathfrak{q}$ over $q$. Changing the choice of the prime $\mathfrak{q}$ amounts to taking the reduction at $\mathfrak{q}$ of a conjugate abelian variety which also has CM by $\mathcal{O}_K$ and hence is isogenous to one already in the list.

For every abelian variety $A \in \mathcal{A}$, we compute the set of its twists, i.e., all the varieties up to $\mathbf{F}_q$-isomorphism that become isomorphic to $A$ over $\overline{\mathbf{F}}_q$. There is at least one twist $B$ of an element $A \in \mathcal{A}$ satisfying $\#B(\mathbf{F}_q) = \mathrm{N}_{K/\mathbf{Q}}(\pi - 1)$, and this $B$ has a point of order $r$ and the desired embedding degree.

Note that while efficient point-counting algorithms do not exist for varieties of dimension $g > 1$, we can determine probabilistically whether an abelian variety has a given order by choosing a random point, multiplying by the expected order, and seeing if the result is the identity.

The complexity of the construction problem rapidly increases with the genus $g = [K : \mathbf{Q}]/2$, and it is fair to say that we only have satisfactory general methods at our disposal in very small genus.

In genus one, we are dealing with elliptic curves, which are isomorphic to their own Jacobians. The $j$-invariants of elliptic curves over $\mathbf{C}$ with CM by $\mathcal{O}_K$ are the roots of the *Hilbert class polynomial* of $K$, which lies in $\mathbf{Z}[X]$. The degree of this polynomial is the class number $h_K$ of $K$, and it can be computed in time $\tilde{O}(|\Delta_K|)$.

For genus 2, we have to construct abelian surfaces. Any principally polarized abelian surface is the Jacobian of a genus 2 curve, and all genus 2 curves are hyperelliptic. There is a theory of class polynomials analogous to that for elliptic curves, as well as several algorithms to compute these polynomials, which lie in $\mathbf{Q}[X]$. The genus 2 algorithms are not as well-developed as those for elliptic curves; at present they can handle only very small quartic CM-fields, and there exists no rigorous running time estimate.

Any three-dimensional abelian variety is isogenous to the Jacobian of a genus 3 curve. There are two known families of genus 3 curves over $\mathbf{C}$ whose Jacobians have CM by an order of dimension 6. The first family, due to Weng [10], gives hyperelliptic curves whose Jacobians have CM by a degree-6 field containing $\mathbf{Q}(i)$. The second family, due to Koike and Weng [3], gives Picard curves (curves of the form $y^3 = f(x)$ with $\deg f = 4$) whose Jacobians have CM by a degree-6 field containing $\mathbf{Q}(\zeta_3)$.

Explicit CM-theory is mostly undeveloped for dimension $\geq 3$. Moreover, most abelian varieties of dimension $\geq 4$ are not Jacobians, as the moduli space of Jacobians has dimension $3g-3$ while the moduli space of abelian varieties has dimension $g(g+1)/2$. For implementation purposes we prefer Jacobians or even hyperelliptic Jacobians, as these are the only abelian varieties for which group operations can be computed efficiently. Due to index-calculus attacks on the discrete logarithm problem, Jacobians of dimension $g \geq 5$ are of more theoretical than practical interest.

In cases where we cannot compute every abelian variety in characteristic zero with CM by $\mathcal{O}_K$, we can use a single such variety $A$ and run Algorithm 2.10 for each different CM-type of $K$ until it yields a prime $q$ for which the reduction of $A$ mod $q$ is in the correct isogeny class. An example for $K = \mathbf{Q}(\zeta_{2p})$ with $p$ prime is given by the Jacobian $A$ of $y^2 = x^p + a$, which has $g = (p-1)/2$.

## 5 Numerical examples

We implemented Algorithm 2.10 in MAGMA and used it to compute examples of hyperelliptic curves of genus 2 and 3 over fields of cryptographic size for which the Jacobians are pairing-friendly. The subgroup size $r$ is chosen so that the discrete logarithm problem in $A[r]$ is expected to take roughly $2^{80}$ steps. The embedding degree $k$ is chosen so that $r^{k/g} \approx 1024$; this would be the ideal embedding degree for the 80-bit security level if we could construct varieties with $\#A(\mathbf{F}_q) \approx r$. Space constraints prevent us from giving the group orders for each Jacobian, but we note that a set of all possible $q$-Weil numbers in $K$, and hence all possible group orders, can be computed from the factorization of $q$ in $K$.

**Example 5.1.** Let $\eta = \sqrt{-2+\sqrt{2}}$ and let $K$ be the degree-4 Galois CM field $\mathbf{Q}(\eta)$. Let $\Phi = \{\phi_1, \phi_2\}$ be the CM type of $K$ such that $\mathrm{Im}(\phi_i(\eta)) > 0$. We ran Algorithm 2.10 with CM type $(K, \Phi)$, $r = 2^{160} - 1679$, and $k = 13$. The algorithm output the following field size:

$$\begin{aligned} q = {} & 31346057808293157913762344531005275715544680219641338497449500238872300350617165 \backslash \\ & 40892530853973205578151445285706963588204818794198739264123849002104890399459807 \backslash \\ & 4631327324771546515176667557021 67 \quad \text{(640 bits)} \end{aligned}$$

There is a single $\overline{\mathbf{F}}_q$-isomorphism class of curves over $\mathbf{F}_q$ whose Jacobians have CM by $\mathcal{O}_K$; the desired twist is given by $C : y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$ [8]. The $\rho$-value of $\mathrm{Jac}(C)$ is 7.99.

**Example 5.2.** Let $\eta = \sqrt{-30 + 2\sqrt{5}}$ and let $K$ be the degree-4 non-Galois CM field $\mathbf{Q}(\eta)$. The reflex field $\widehat{K}$ is $\mathbf{Q}(\omega)$ where $\omega = \sqrt{-15 + 2\sqrt{55}}$. Let $\varPsi$ be the CM type of $K$ such that $\mathrm{Im}(\phi_i(\eta)) > 0$. We ran Algorithm 2.10 with the CM type $(K, \varPhi)$, subgroup size $r = 2^{160} - 1445$, and embedding degree $k = 13$. The algorithm output the following field size:

$$
\begin{aligned}
q = {} & 11091654887169512971365407040293599579976378158973405181635081379157078302130927 \ \backslash \\
& 51652003623786192531077127388944453303584091334492452752693094089192986541533819 \ \backslash \\
& 3551886616778340023118130834598146 1 \quad (645 \text{ bits})
\end{aligned}
$$

The Igusa class polynomials for $K$ can be found in the preprint version of [9]. We used the roots of the Igusa class polynomials mod $q$ to construct curves over $\mathbf{F}_q$ with CM by $\mathcal{O}_K$. As $K$ is non-Galois with class number 4, there are 8 isomorphism classes of curves in 2 isogeny classes. We found a curve $C$ in the correct isogeny class with equation $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$, with

$$
\begin{aligned}
a_3 = {} & 37909827361040902434390338072754918705969566622865244598340785379492062293493023 \ \backslash \\
& 07887220632471591953460261515915189503199574055791975955834407879578484212700263 \ \backslash \\
& 26004014371084570321085865481897 69 \\
a_2 = {} & 18960350992731066141619447121681062843951822341216980089632110294900985267348927 \ \backslash \\
& 56700435114431697785479098782721806327279074708206429263751983109351250831853735 \ \backslash \\
& 19012820004210701825726715060564 32 \\
a_1 = {} & 69337488142924022910219499907432470174331183248226721112535199929650663260487281 \ \backslash \\
& 50177351432967251207037416196614255668796808046612641767922273749125366541534440 \ \backslash \\
& 58824657313765233049070410064645 04 \\
a_0 = {} & 31678142561939596895646021753607012342277658384169880961095701825776704126204818 \ \backslash \\
& 48230687778916790603969757571449880417861689471274167016388608712966941178120424 \ \backslash \\
& 38133326172720384940201785611195 64
\end{aligned}
$$

The $\rho$-value of $\mathrm{Jac}(C)$ is 8.06.

**Example 5.3.** Let $K$ be the degree-6 Galois CM field $\mathbf{Q}(\zeta_7)$, and let $\varPhi = \{\phi_1, \phi_2, \phi_3\}$ be the CM type of $K$ such that $\phi_n(\zeta_7) = e^{2\pi i n/7}$. We used the CM type $(K, \varPhi)$ to construct a curve $C$ whose Jacobian has embedding degree 17 with respect to $r = 2^{180} - 7427$. Since $K$ has class number 1 and one equivalence class of primitive CM types, there is a unique isomorphism class of curves in characteristic zero whose Jacobians are simple and have CM by $K$; these curves are given by $y^2 = x^7 + a$. Algorithm 2.10 ran in 51 seconds and output the following field size:

$$
\begin{aligned}
q = {} & 15755584138119771535917878020143687930577769468671374639550678761402500812175974 9 \ \backslash \\
& 72634937716254216816917600718698808129260457040637146802812702044068612772692590 \ \backslash \\
& 77188966205156107806823000096120874915612017184924206843204621759232946263357637 \ \backslash \\
& 19251697987740263891168971441085531481109276328740299111531260484082698571214310 \ \backslash \\
& 33499 \quad (1077 \text{ bits})
\end{aligned}
$$

The equation of the curve $C$ is $y^2 = x^7 + 10$. The $\rho$-value of $\mathrm{Jac}(C)$ is 17.95.

We conclude with an example of an 8-dimensional abelian variety found using our algorithms. We started with a single CM abelian variety $A$ in characteristic zero and searched for primes and CM types for which the reduction of $A$ is pairing-friendly.

**Example 5.4.** Let $K = \mathbf{Q}(\zeta_{17})$. We set $r = 1021$ and $k = 10$ and ran Algorithm 2.10 repeatedly with different CM types for $K$. Given the output, we tested the Jacobian of (twists of) $y^2 = x^{17} + 1$ for the specified number of points. We found that the curve $y^2 = x^{17} + 30$ has embedding degree 10 with respect to $r$ over the field $\mathbf{F}_q$, with

$$q = 686960350832243461485490853554520897803881943 7$$

The CM type was

$$\varPhi = \{\phi_1, \phi_3, \phi_5, \phi_6, \phi_8, \phi_{10}, \phi_{13}, \phi_{15}\},$$

where $\phi_n(\zeta_{17}) = e^{2\pi i n/17}$. The $\rho$-value of $\mathrm{Jac}(C)$ is 121.9.

## References

1. D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2- DNF formulas on ciphertexts," in *TCC '05*, Springer LNCS **3378**, 2005, 325–341.
2. D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," Cryptology eprint 2006/371, available at `http://eprint.iacr.org`.
3. K. Koike and A. Weng, "Construction of CM Picard curves," *Math. Comp.* **74** (2004), 499–518.
4. K. Paterson, "Cryptography from pairings," in *Advances in Elliptic Curve Cryptography*, ed. I. F. Blake, G. Seroussi, and N. P. Smart, Cambridge University Press, 2005, 215–251.
5. K. Rubin and A. Silverberg, "Supersingular abelian varieties in cryptology," in *CRYPTO '02*, Springer LNCS **2442**, 2002, 336–353.
6. G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, 1998.
7. J. Tate, "Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)," Séminaire Bourbaki 1968/69, Springer Lect. Notes in Math. **179** (1971) exposé 352, 95–110.
8. P. van Wamelen, "Examples of genus two CM curves defined over the rationals," *Math. Comp.* **68** (1999), 307–320.
9. A. Weng, "Constructing hyperelliptic curves of genus 2 suitable for cryptography," *Math. Comp.* **72** (2003), 435–458.
10. A. Weng, "Hyperelliptic CM-curves of genus 3," *Journal of the Ramanujan Mathematical Society* **16**:4 (2001), 339–372.