Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians

David Freeman

University of California, Berkeley
dfreeman@math.berkeley.edu

Abstract. We provide the first explicit construction of genus 2 curves over finite fields whose Jacobians are ordinary, have large prime-order subgroups, and have small embedding degree. Our algorithm works for arbitrary embedding degrees k and prime subgroup orders r. The resulting abelian surfaces are defined over prime fields $\mathbb{F}_q$ with $q \approx r^4$. We also provide an algorithm for constructing genus 2 curves over prime fields $\mathbb{F}_q$ with ordinary Jacobians J having the property that $J[r] \subset J(\mathbb{F}_q)$ or $J[r] \subset J(\mathbb{F}_{q^k})$ for any even k.

1 Introduction

In the last few years, many cryptographic protocols have been proposed that make use of bilinear pairings [24]. While the protocols are described in the language of abstract groups, in practice the pairings used are the Weil and Tate pairings on abelian varieties over finite fields. These pairings take as input two points on an abelian variety A defined over a finite field $\mathbb{F}_q$ and give as output an element of an extension field $\mathbb{F}_{q^k}$. The degree k of the extension field is known as the "embedding degree" of the abelian variety.

For pairing-based cryptosystems to be both efficient and secure, the embedding degree k should be chosen so that the discrete logarithm problem is equally difficult on the abelian variety (where only exponential-time discrete logarithm algorithms are known) and in the multiplicative group of the extension field (where there exist subexponential-time discrete logarithm algorithms). Since the optimal embedding degree will vary according to the desired level of security, in order to build systems with a variety of security levels we wish to have a supply of abelian varieties with various embedding degrees.

The abelian varieties originally proposed for use in pairing-based protocols were supersingular elliptic curves, which are restricted to embedding degree $k \leq 6$. The problem of constructing ordinary elliptic curves with prescribed embedding degree was first treated by Miyaji, Nakabayashi, and Takano [22] and remains an active area of research. Freeman, Scott, and Teske [8] provide an overview of the best current constructions for all embedding degrees $k \leq 50$.

While elliptic curves remain the most common choice of a family of abelian varieties for cryptographic protocols, Bernstein [2] and Lange [17] have recently shown that for certain applications Jacobians of genus 2 curves are now competitive with elliptic curves in terms of performance and security. In addition,

Frey and Lange [9] have shown that in many applications the Tate pairing can be computed more efficiently on Jacobians of hyperelliptic curves of genus $g > 1$ than on elliptic curves. It is thus only natural that we should seek to construct "pairing-friendly" genus 2 curves, i.e. curves whose Jacobians have small embedding degree.

At present there exist very few constructions of pairing-friendly genus 2 curves. Rubin and Silverberg [25] showed that any supersingular Jacobian of a genus 2 curve has embedding degree at most 12. Galbraith, McKee, and Valença [11] and Hitt [13] have demonstrated the existence of isogeny classes of ordinary abelian surfaces with small embedding degree, but to date there exist no equations of genus 2 curves over fields of cryptographic size whose Jacobians are ordinary and have small embedding degree.

In this paper we provide the first explicit construction of genus 2 curves whose Jacobians are ordinary, have large prime-order subgroups, and have prescribed embedding degree. Our construction is modeled on the Cocks-Pinch method for constructing pairing-friendly elliptic curves [5], and makes use of the Complex Multiplication (CM) method of curve construction. The outline of our algorithm is as follows:

1. Find primes q and r and a polynomial $h(x)$ such that if $h(x)$ is the characteristic polynomial of Frobenius of an abelian surface A over $\mathbb{F}_q$, then A has a subgroup of order r with embedding degree k.
2. Use the Igusa class polynomials for the quartic CM field $K = \mathbb{Q}[x]/(h(x))$ to construct a genus 2 curve C over $\mathbb{F}_q$ such that the Jacobian of C has characteristic polynomial of Frobenius $h(x)$.

The difficult part of the construction is ensuring that the polynomial $h(x)$ defines a CM field K for which the Igusa class polynomials can be computed efficiently using current methods. The solution to this problem is our most important theoretical contribution.

Our paper is structured as follows. Section 2 addresses Step 1 of the algorithm. In this section we give a precise definition of embedding degree, and we give a set of explicit conditions necessary for the prime q and the polynomial $h(x)$ to have the desired properties. We give separate sets of conditions that address two different notions of embedding degree: the standard notion as described above, and a new notion we call the "full embedding degree," which indicates the field over which the full set of r-torsion points of A is defined.

Section 3 addresses Step 2 of the algorithm. We find explicit formulas that relate the CM field K to the characteristic polynomial of Frobenius $h(x)$. We then use the theory of ordinary abelian varieties over finite fields to give conditions on $h(x)$ such that the desired genus 2 curve C exists over $\mathbb{F}_q$. Construction of C from roots of the Igusa class polynomials modulo q is then a standard procedure.

In Section 4 we give a complete algorithm for constructing genus 2 curves whose Jacobians are ordinary and have prescribed embedding degree. In Section 5 we give an analogous algorithm for constructing genus 2 curves whose Jacobians are ordinary and have prescribed full embedding degree; i.e. all r-torsion points

of the Jacobian are defined over a specified field extension. Examples of curves of cryptographic size constructed using these algorithms appear in the Appendices.

Finally, in Section 6 we consider possible extensions of our constructions. We show that our algorithms extend readily to produce abelian varieties that have small embedding degree with respect to subgroups of composite order; such varieties are required by a number of recent protocols. We also consider methods of generalizing the algorithm to improve the ratio between the sizes of the primes q and r. Our method produces varieties with $\log q / \log r \approx 4$; our hope is that the techniques presented here will lead to constructions that reduce this ratio to its theoretical minimum of $1/2$.

Acknowledgments. The problem of constructing pairing-friendly genus 2 curves was first suggested to me by Kristin Lauter. The results presented in this paper were inspired by discussions with Dan Boneh and Edward Schaefer in the winter of 2006-07. I thank Ken Ribet for useful discussions, and I thank Steven Galbraith, Tanja Lange, Edward Schaefer, and Edlyn Teske for helpful feedback on early drafts. This research was supported by a National Defense Science and Engineering Graduate Fellowship.

2 Pairing-friendly abelian varieties

In this section we gather together facts about abelian varieties relevant to our construction. Good overviews of the subject can be found in the articles of Waterhouse and Milne [29], which focuses on varieties over finite fields, and Milne [21], which treats varieties over arbitrary fields.

An *abelian variety* A is a complete algebraic variety with a group structure whose operations are given by algebraic morphisms. An *elliptic curve* is a one-dimensional abelian variety, and an *abelian surface* is a two-dimensional abelian variety. If A is an abelian variety defined over a field K, we denote by $A(K)$ the set of K-rational points of A. If r is an integer, then $A[r]$ denotes the set of all r-torsion points of A, defined over an algebraic closure of K. We denote by $A(K)[r]$ the set of r-torsion points of A defined over K. If A has dimension g and r is prime to the characteristic of K, then $A[r] \cong (\mathbb{Z}/r\mathbb{Z})^{2g}$.

Every abelian variety A defined over a finite field $\mathbb{F}_q$ has an endomorphism called the *Frobenius endomorphism*, which operates by raising the coordinates of a point to the qth power. The Frobenius endomorphism satisfies an integer polynomial $h(x)$ known as the *characteristic polynomial of Frobenius*. By a theorem of Weil [21, Theorem 19.1], all of the complex roots of $h(x)$ have absolute value $\sqrt{q}$; such a polynomial is called a *q-Weil polynomial*. If A has dimension g, then this polynomial is of the form

$$\begin{aligned} h(x) = x^{2g} + a_1 x^{2g-1} + \ldots + a_{g-1} x^{g+1} + a_g x^g \\ + a_{g-1} q x^{g-1} + \ldots + a_1 q^{g-1} x + q^g, \end{aligned} \tag{2.1}$$

By Honda-Tate theory [27], q-Weil polynomials are in one-to-one correspondence with isogeny classes of abelian varieties over $\mathbb{F}_q$.

If A is an abelian variety with characteristic polynomial of Frobenius $h(x)$, then $\#A(\mathbb{F}_q) = h(1)$. We say that A is *ordinary* if the middle coefficient a_g of $h(x)$ is relatively prime to q, and A is *supersingular* if all of the complex roots of $h(x)$ are roots of unity times $\sqrt{q}$. (For other equivalent definitions of ordinary and supersingular, see [15, Definition 3.1] or [10, Theorem 1].) If $g \geq 2$ then there are g-dimensional abelian varieties that are neither ordinary nor supersingular.

The most common abelian varieties used in cryptography are Jacobians of hyperelliptic curves of genus $g \geq 1$. A hyperelliptic curve of genus g is the normal projective closure of a nonsingular affine curve of the form $y^2 = f(x)$, with $\deg f = 2g + 1$ or $2g + 2$. (If the characteristic of the ground field is 2, the left hand side becomes $y^2 + h(x)y$ with $\deg h \leq g + 1$.) The Jacobian of a projective curve C, denoted $\mathrm{Jac}(C)$, is a principally polarized abelian variety whose points are degree zero divisors on C modulo principal divisors. If C is a curve of genus g, then $\mathrm{Jac}(C)$ has dimension g

2.1 Pairings and embedding degrees

The two most common pairings on abelian varieties used in cryptography are the Weil and Tate pairings. Let A be an abelian variety defined over a field K, and let r be a positive integer. Let μ_r be the rth roots of unity in an algebraic closure of K. The Weil pairing is a nondegenerate bilinear map

$$e_{weil,r} : A[r] \times A[r] \to \mu_r,$$

while the Tate pairing is a nondegenerate bilinear map

$$e_{tate,r} : A(K)[r] \times A(K)/rA(K) \to K^\times/(K^\times)^r.$$

If $\mu_r \subset K$, then the target group $K^\times/(K^\times)^r$ is isomorphic to μ_r; otherwise it is isomorphic to μ_s for some $s \mid r$. Thus to obtain Weil or Tate pairing values of order r, we must work over a field containing the rth roots of unity. We define the embedding degree to be the extension degree of the smallest such field.

Definition 2.1. Let A be an abelian variety defined over a field K, and let r be a positive integer relatively prime to $\mathrm{char}(K)$. We say that A has *embedding degree k with respect to r* if

1. A has a K-rational point of order r, and
2. k is the smallest integer such that μ_r is contained in a degree-k extension of K.

If C is a projective nonsingular curve, then we say that C has embedding degree k with respect to r if and only if the Jacobian of C does.

Remark 2.2. If A is an abelian variety over a finite field $\mathbb{F}_q$ with an $\mathbb{F}_q$-rational point of order r, then the following conditions are equivalent:

1. A has embedding degree k with respect to r.

2. k is the smallest integer such that r divides $q^k - 1$.
3. k is the multiplicative order of q modulo r.

Furthermore, if r is square-free these conditions are equivalent to

4. $\Phi_k(q) \equiv 0 \pmod{r}$, where Φ_k is the kth cyclotomic polynomial. (Cf. [8, Proposition 2.4].)

The embedding degree gets its name because we can use a pairing to "embed" a cyclic subgroup of A of order r into the multiplicative group of the degree-k extension of K. The MOV attack on the discrete logarithm problem on supersingular elliptic curves [19] makes use of such an "embedding." If A is an abelian variety over a prime field $\mathbb{F}_q = \mathbb{F}_p$ then the embedding degree is a good measure of the security of cryptosystems based on A; if $q = p^d$ is a prime power, then the appropriate measure of security is $k/\gcd(k, d)$ [14].

In general we expect a "random" abelian variety over $\mathbb{F}_q$ with a point of order r to have embedding degree $k \sim r$; this statement has been made more precise in the case of elliptic curves by Balasubramanian and Koblitz [1] and Luca, Mireles, and Shparlinski [18]. In cryptographic applications r will be at least 2^{160}, so computing pairings on random abelian varieties over $\mathbb{F}_q$ appears hopeless. Thus we wish to construct abelian varieties over finite fields that have points of large order r and small embedding degree with respect to r; such varieties are called "pairing-friendly." We refrain from giving a more precise definition of "pairing-friendly" here because it is not yet clear what "large order" and "small embedding degree" should mean for general abelian varieties. For a formal definition in the case of elliptic curves, see [8, Definition 2.3].

Our first task is to give some conditions on the characteristic polynomial of Frobenius that are sufficient for A to have embedding degree k.

Proposition 2.3. *Let A be an abelian variety over $\mathbb{F}_q$, and let $h(x)$ be the characteristic polynomial of Frobenius of A. Let $r \nmid q$ be a prime number and k a positive integer, and suppose the following hold:*

$$\begin{aligned} h(1) &\equiv 0 \pmod{r}, \\ \Phi_k(q) &\equiv 0 \pmod{r}, \end{aligned}$$

where Φ_k is the kth cyclotomic polynomial. Then A has embedding degree k with respect to r.

Furthermore, if $k > 1$ then $A(\mathbb{F}_{q^k})$ contains two linearly independent r-torsion points.

Proof. The condition $r \mid h(1)$ guarantees that A has an $\mathbb{F}_q$-rational point of order r, and by Remark 2.2 the condition $r \mid \Phi_k(q)$ implies that A has embedding degree k with respect to r.

The proof of the "furthermore" clause follows the argument of [1, Theorem 1]. Let $\tilde{h}(x)$ be the reduction of $h(x)$ modulo r. The roots of $\tilde{h}(x)$ are the eigenvalues of the Frobenius endomorphism F on $A[r]$. From equation (2.1) we see that $h(x) = (x^2/q)^g h(q/x)$, so roots of $\tilde{h}(x)$ come in pairs $(\alpha, q/\alpha)$. The hypothesis

$h(1) \equiv 0 \pmod{r}$ thus implies that $\tilde{h}(q)$ is also zero. The hypotheses $\tilde{h}'(1) \neq 0$ and $k > 1$ imply that 1 and q are distinct roots with multiplicity 1, so $A[r]$ has a one-dimensional eigenspace with eigenvalue 1, and a one-dimensional eigenspace with eigenvalue q. Since $q^k = 1 \pmod{r}$, F^k acts trivially on the two-dimensional span of these eigenspaces, so $\dim A[r](\mathbb{F}_{q^k}) \geq 2$. □

If $\dim A = 1$ (i.e. A is an elliptic curve) and the "furthermore" clause of Proposition 2.3 holds, then since $A[r]$ is two-dimensional we must have $A[r] \subset A(\mathbb{F}_{q^k})$. However, if $\dim A > 1$, then in general $A[r]$ will not be contained in $A(\mathbb{F}_{q^k})$. Thus we define a second type of embedding degree, which indicates the extension degree of the smallest field over which all r-torsion points of A are defined.

Definition 2.4. Let A be an abelian variety defined over a field K, and let r be a positive integer relatively prime to $\mathrm{char}(K)$. We say that A has *full embedding degree k with respect to r* if

1. A has a K-rational point of order r, and
2. k is the smallest integer such that *all* r-torsion points of A are defined over a degree-k extension of K.

If C is a projective nonsingular curve, then we say that C has full embedding degree k with respect to r if and only if the Jacobian of C does.

Remark 2.5. The non-degeneracy of the Weil pairing [21, §16] implies that the full embedding degree is a multiple of the embedding degree.

We next give a criterion that determines when all of the r-torsion points are defined over a given extension field.

Proposition 2.6. *Let A be a g-dimensional abelian variety over $\mathbb{F}_q$, let R be the endomorphism ring of A, and suppose R is a Dedekind domain. Let F be the Frobenius endomorphism of A, and for $k \geq 1$ let $h_k(x)$ be the characteristic polynomial of F^k. Let $r \nmid q$ be a rational prime unramified in R, and suppose that for some k, $h_k(x) \equiv (x-1)^{2g} \pmod{r}$. Then $A[r] \subset A(\mathbb{F}_{q^k})$.*

Proof. Let $\pi \in R$ be the Frobenius endomorphism of A. By [6, Fact 10], $A[r] \subset A(\mathbb{F}_{q^k})$ if and only if $\pi^k - 1 \in rR$. Since R is a Dedekind domain and r is unramified in R, it suffices to show that $\pi^k - 1 \in \mathfrak{p}$ for every prime $\mathfrak{p}$ of R dividing r. Since π^k is a root of $h_k(x)$, the hypothesis $h_k(x) \equiv (x-1)^{2g} \pmod{r}$ implies that $(\pi^k - 1)^{2g} \in \mathfrak{p}$ for every $\mathfrak{p} \mid r$, and since $R/\mathfrak{p}$ is a field we conclude that $\pi^k - 1 \in \mathfrak{p}$ for every $\mathfrak{p} \mid r$. □

Using Proposition 2.6, we can now give a statement analogous to Proposition 2.3 that gives us sufficient conditions for A to have full embedding degree k.

Proposition 2.7. *Let A be an abelian variety over $\mathbb{F}_q$, and let $h(x)$ be the characteristic polynomial of Frobenius of A. Let $r \nmid q$ be a prime number, let $\tilde{h}(x) \in \mathbb{F}_r[x]$ be $h(x)$ modulo r, and suppose $\tilde{h}(1) = 0$. Let $\{\alpha_i\}$ be the roots of $\tilde{h}(x)$ in $\overline{\mathbb{F}}_r$, and suppose that k is the least common multiple of the multiplicative orders of all the α_i. Suppose at least one of the following conditions holds:*

– $\gcd(\tilde{h}(x), \tilde{h}'(x)) = 1$, *or*
– $\mathrm{End}(A)$ *is a Dedekind domain and* r *is unramified in* $\mathrm{End}(A)$.

Then A *has full embedding degree* k *with respect to* r.

Proof. The condition $\tilde{h}(1) = 0$ guarantees that A has an $\mathbb{F}_q$-rational point of order r. The α_i are the eigenvalues of the Frobenius endomorphism F on $A[r]$. Since $\alpha_i^k = 1$, all of the $2g$ eigenvalues of F^k are 1, and by assumption k is the smallest integer with this property.

If $\gcd(\tilde{h}(x), \tilde{h}'(x)) = 1$, then all the eigenvalues of F are distinct, so F is diagonalizable. Thus F^k is the identity on $A[r]$, and we conclude that $A[r] \subset A(\mathbb{F}_{q^k})$. If $\mathrm{End}(A)$ is a Dedekind domain and r is unramified in $\mathrm{End}(A)$, then since the characteristic polynomial of F^k modulo r is $(x-1)^{2g}$, we may apply Proposition 2.6 to deduce that $A[r] \subset A(\mathbb{F}_{q^k})$. Thus in both cases we see that A has full embedding degree k with respect to r. □

The security of pairing-based cryptographic protocols depends on both the size r of the subgroup involved in the pairing and the size q^k of the finite field into which the pairing maps. Ideally r is very close to the total number of points on the abelian variety. However, many of the constructions of pairing-friendly varieties give values of r whose size is some fraction of the total number of points on the variety. We define a parameter ρ that measures this ratio. Since the Weil conjectures [21, Theorem 19.1] imply that $\#A(\mathbb{F}_q) = q^g + O(q^{g-1/2})$, it is reasonable to use q^g as an approximation to $\#A(\mathbb{F}_q)$ in our definition.

Definition 2.8. Let $A/\mathbb{F}_q$ be a g-dimensional abelian variety, and suppose r divides $\#A(\mathbb{F}_q)$. The *ρ-value of* A (with respect to r) is defined to be

$$\rho(A) = \frac{g \log q}{\log r}.$$

Varieties with a prime number of points, such as MNT elliptic curves [22], will have ρ-value very close to 1; this is the "ideal" case. The expression $k\rho/g$ measures the ratio of the size of the field into which the pairing maps to the size of the prime-order subgroup on the variety. Recommended values of this expression to achieve "balanced" security levels comparable to standard sizes of keys for symmetric encryption have been given by several authors; for a summary, see [8, Table 1.1].

3 Constructing abelian surfaces via the genus 2 CM method

In this section we consider the problem of generating a genus 2 curve C such that the characteristic polynomial of Frobenius of $\mathrm{Jac}(C)$ is equal to a specified q-Weil polynomial $h(x)$.

Let A be an absolutely simple ordinary g-dimensional abelian variety over a finite field $\mathbb{F}_q$. The ring of endomorphisms of A is a rank-$2g$ $\mathbb{Z}$-module that is

isomorphic as a $\mathbb{Z}$-algebra to an order in the ring of integers in a number field K. We say that such a variety has *complex multiplication by K* or *CM by K*. The field K has degree $2g$ and is an imaginary quadratic extension of a totally real number field of degree g; a field with these properties is called a *CM field*. A CM field K is *primitive* if it contains no proper CM subfields.

The fundamental fact we will use in our construction of pairing-friendly abelian surfaces is the following, which relates the CM field to the characteristic polynomial of Frobenius.

Fact 3.1 ([29, Theorem 8]). *Let K be a CM field. An ordinary abelian variety $A/\mathbb{F}_q$ has CM by K if and only if $K \cong \mathbb{Q}[x]/(h(x))$, where $h(x)$ is the characteristic polynomial of Frobenius of A.*

In the case of abelian surfaces, we can give a more explicit relation between the CM field and the characteristic polynomial of Frobenius.

Lemma 3.2. *Let $h(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients of the form*

$$h(x) = x^4 - sx^3 + tx^2 - sqx + q^2. \tag{3.1}$$

Then the four complex roots of $h(x)$ are

$$\frac{s}{4} + \frac{1}{2}\sqrt{\frac{s^2}{4} - t + 2q} \pm \frac{1}{2}\sqrt{\left(\frac{s^2}{2} - t - 2q\right) + s\sqrt{\frac{s^2}{4} - t + 2q}},$$
$$\frac{s}{4} - \frac{1}{2}\sqrt{\frac{s^2}{4} - t + 2q} \pm \frac{1}{2}\sqrt{\left(\frac{s^2}{2} - t - 2q\right) - s\sqrt{\frac{s^2}{4} - t + 2q}}.$$

Proof. An easy calculation shows that if α is a root of $h(x)$, then $\alpha + q/\alpha$ is a root of $x^2 - sx + t - 2q$. The result then follows from two successive applications of the quadratic formula. □

Proposition 3.3. *Let $h(x)$ be a polynomial of the form* (3.1). *Let $\delta = s^2/4 - t + 2q$. Suppose the following hold:*

$$\delta > 0 \tag{3.2}$$

$$\frac{s^2}{2} - t - 2q \pm s\sqrt{\delta} < 0 \tag{3.3}$$

Then there is an abelian surface A such that the characteristic polynomial of Frobenius of A is equal to $h(x)$. Furthermore, A has CM by $\mathbb{Q}(\eta)$, where

$$\eta = \sqrt{\left(\frac{s^2}{2} - t - 2q\right) + s\sqrt{\frac{s^2}{4} - t + 2q}}. \tag{3.4}$$

Proof. By Lemma 3.2, $h(x)$has a root in $K = \mathbb{Q}(\eta)$, so $K \cong \mathbb{Q}[x]/(h(x))$. Conditions (3.2) and (3.3) ensure that K is a purely imaginary quadratic extension of the real quadratic field $\mathbb{Q}(\sqrt{\delta})$. Under this hypothesis, one can compute that all four of the roots of $h(x)$ given by Proposition 4.1 have complex absolute value $\sqrt{q}$. Thus $h(x)$ is a q-Weil polynomial, so by Honda-Tate theory [27] there is an isogeny class $\mathcal{A}$ of abelian varieties over $\mathbb{F}_q$ with characteristic polynomial of Frobenius $h(x)$. By Fact 3.1, any $A \in \mathcal{A}$ has CM by K. □

If the CM field $K = \mathbb{Q}(\eta)$ is primitive and the isogeny class $\mathcal{A}$ is ordinary, then we can go one step further and say that there is an abelian surface $A \in \mathcal{A}$ such that A is the Jacobian of a genus 2 curve over $\mathbb{F}_q$ and $\mathrm{End}(A)$ is the ring of integers of K.

Proposition 3.4. *Let $h(x)$ be a polynomial of the form* (3.1) *satisfying the conditions of Proposition 3.3, and suppose that* $\gcd(t, q) = 1$. *Let η be defined by equation* (3.4)*, and suppose that the number field $K = \mathbb{Q}(\eta)$ is a primitive quartic CM field. Then there is a genus 2 curve $C/\mathbb{F}_q$ such that* $\mathrm{Jac}(C)$ *has characteristic polynomial of Frobenius $h(x)$ and* $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$*, the ring of integers of K.*

Proof. Let $A \in \mathcal{A}$ be an abelian surface in the isogeny class of abelian varieties given by Proposition 3.3. Since $\gcd(t, q) = 1$, A is ordinary. Since K is primitive and A is ordinary, it follows from the Honda-Tate theorem [27] that A is absolutely simple. By a theorem of Weil (cf. [23]), an absolutely simple principally polarized abelian surface is the Jacobian of a genus 2 curve. It thus suffices to show that we can find an $A \in \mathcal{A}$ that is principally polarized and has endomorphism ring isomorphic to $\mathcal{O}_K$.

Let K_0 be the real quadratic subfield of K. By the work of Howe [15, Propositions 5.7 and 10.1], it suffices to show that there is a finite prime $\mathfrak{p}$ of K_0 that ramifies in K. A variation of Howe's proof of [15, Lemma 12.1] shows that if there is no finite prime $\mathfrak{p}$ of K_0 that ramifies in K, then K contains an imaginary quadratic subfield, contradicting the assumption that K is primitive. □

Our algorithms in Sections 4 and 5 for generating pairing-friendly abelian surfaces will produce primes q and q-Weil polynomials $h(x)$ satisfying the hypotheses of Proposition 3.4. To construct the genus 2 curves specified by the proposition, we turn to genus 2 invariant theory.

If $\mathbb{F}$ is a field with $\mathrm{char}(\mathbb{F}) \neq 2$, then $\overline{\mathbb{F}}$-isomorphism classes of genus 2 curves defined over $\mathbb{F}$ are in one-to-one correspondence with triples $(j_1, j_2, j_3) \in \mathbb{F}^3$. The triple (j_1, j_2, j_3) corresponding to a curve C is called the curve's *absolute invariants*. Let K be a primitive quartic CM field, and let $\mathscr{C}_K$ be the set of isomorphism classes of genus 2 curves over $\mathbb{C}$ such that $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$, the ring of integers in K. The *Igusa class polynomials* of K are defined to be

$$H_i(x) = \prod_{C \in \mathscr{C}_K} (x - j_i(C))$$

for $i = 1, 2, 3$; these polynomials have rational coefficients. There are currently several methods for computing the Igusa class polynomials: a complex-analytic

algorithm involving modular functions [26], [28], [30]; a Chinese Remainder Theorem algorithm that computes the $H_i(x)$ modulo many small primes [6], [7]; and a p-adic lifting algorithm [12]. All three methods are currently limited to CM fields K with small discriminant and class number.

By the Serre-Tate theory of canonical liftings [16], any ordinary abelian variety A over a finite field is the reduction modulo a suitable prime $\mathfrak{p}$ of an abelian variety $\tilde{A}$ over $\mathbb{C}$ with $\mathrm{End}(\tilde{A}) \cong \mathrm{End}(A)$. Furthermore, if A is the Jacobian of a genus 2 curve C, then $\tilde{A}$ is the Jacobian of a genus 2 curve $\tilde{C}$, and the absolute invariants of C are the reduction modulo $\mathfrak{p}$ of the absolute invariants of $\tilde{C}$. Combining these facts gives the following statement.

Fact 3.5. *Let K be a primitive quartic CM field, and let $H_i(x)$ be the Igusa class polynomials of K. Let $q = p^d$ be a prime power, and let $C/\mathbb{F}_q$ be a genus 2 curve. Suppose that $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathcal{O}_K$. Then p does not divide the denominator of any coefficient of any $H_i(x)$, and for each i the absolute invariant j_i of C is a root of $H_i(x)$ modulo p.*

Thus given a q-Weil polynomial $h(x)$ satisfying the hypotheses of Proposition 3.4 with q prime, we can construct the curve C by computing the Igusa class polynomials for K and finding roots of the polynomials modulo q. A step by step procedure for this construction is given in Algorithm 4.3 below.

4 Constructing genus 2 curves with prescribed embedding degree

We have seen in Sections 2 and 3 that to construct an abelian surface with prescribed embedding degree k, it suffices to find a q-Weil polynomial $h(x)$ satisfying the conditions of Propositions 2.3 and 3.4. Given such an $h(x)$, Fact 3.5 says that we can use the Igusa class polynomials of $K = \mathbb{Q}[x]/(h(x))$ to find a genus 2 curve C such that $\mathrm{Jac}(C)$ has the desired properties. Since current methods of computing the Igusa class polynomials are limited to a small range of quartic CM fields K, we will specify K as an input to our algorithm, and assume that K is chosen such that the Igusa class polynomials for K are known or can be easily computed.

Recall that a CM field is a purely imaginary quadratic extension of a totally real field. Thus all primitive CM fields K of degree 4 can be written in the form $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$ for some integers $a, b, d > 0$ with $a^2 - b^2 d > 0$. If $a^2 - b^2 d$ is not a square then K is primitive.

If we fix an element $\xi = \sqrt{-a + b\sqrt{d}}$ generating our CM field K and require that the element η given by Proposition 3.3 is equal to ξ, then we have three equations in the three variables q, s, t. By Proposition 2.3, requiring that an abelian surface with characteristic polynomial $h(x)$ has embedding degree k imposes two additional constraints on q, s, t, and it will almost certainly be impossible to find q, s, t satisfying all five equations. Thus we wish to add at least two degrees of freedom to our description of the CM field so that instead of

requiring $\xi = \eta$, we only require $\mathbb{Q}(\xi) \cong \mathbb{Q}(\eta)$. The following proposition achieves this goal.

Proposition 4.1. *Suppose $K = \mathbb{Q}(\sqrt{-a+b\sqrt{d}})$ is a primitive quartic CM field. Let u, v, w be integers, and let*

$$\alpha = w^2(au^2 + adv^2 + 2bduv), \tag{4.1}$$
$$\beta = bu^2 + bdv^2 + 2auv, \tag{4.2}$$
$$\delta = dw^4. \tag{4.3}$$

Then K is isomorphic to $\mathbb{Q}(\sqrt{-\alpha+\beta\sqrt{\delta}})$.

Proof. Let $L = \mathbb{Q}(\sqrt{-\alpha+\beta\sqrt{\delta}})$. Since K is primitive it contains a unique quadratic subfield K_0 isomorphic to $\mathbb{Q}(\sqrt{d})$. Since $\delta = dw^4$, K_0 is a quadratic subfield of L, so it suffices to show that K and L are isomorphic as quadratic extensions of K_0; that is to say,

$$K_0\left(\sqrt{-a+b\sqrt{d}}\right) \cong K_0\left(\sqrt{-\alpha+\beta\sqrt{\delta}}\right).$$

One can check that the choices of α, β, δ above satisfy

$$-\alpha + \beta\sqrt{\delta} = (-a+b\sqrt{d})(u - v\sqrt{d})^2 w^2,$$

so $(-a+b\sqrt{d})/(-\alpha+\beta\sqrt{\delta})$ is a square in K_0, and K and L are isomorphic. □

We now turn to the task of constructing the characteristic polynomial of Frobenius of a pairing-friendly abelian surface A. We will fix throughout a prime r and an embedding degree k, and look for a polynomial $h(x)$ satisfying the conditions of Proposition 2.3. As remarked above, we will also fix a CM field $K = \mathbb{Q}(\sqrt{-a+b\sqrt{d}})$ and require that $K \cong \mathbb{Q}[x]/(h(x))$.

Recall that $h(x)$ has the form

$$h(x) = x^4 - sx^3 + tx^2 - sqx + q^2. \tag{4.4}$$

If we are given $\eta = \sqrt{-a+b\sqrt{d}}$, Propositions 3.3 and 4.1 give a set of conditions sufficient for A to have CM by $\mathbb{Q}(\eta)$, namely, that for some u, v, w, the following hold:

$$\frac{s^2}{2} - t - 2q = -w^2(au^2 + adv^2 + 2bduv) \tag{4.5}$$
$$s = bu^2 + bdv^2 + 2auv \tag{4.6}$$
$$\frac{s^2}{4} - t + 2q = dw^4. \tag{4.7}$$

By Proposition 2.3, the condition that A has embedding degree k with respect to r is equivalent to

$$q^2 + 1 - s(q+1) + t \equiv 0 \pmod{r} \tag{4.8}$$
$$\Phi_k(q) \equiv 0 \pmod{r}, \tag{4.9}$$

where Φ_k is the kth cyclotomic polynomial.

Conditions (4.5) through (4.9) together comprise five equations in six variables over $\mathbb{F}_r$, so we can expect to find solutions (q', s', t', u', v', w') in $\mathbb{F}_r^6$ for some positive fraction of all primes r. Since we have an extra degree of freedom, we can loop on one variable and search for solutions to the five equations in the remaining five variables. When a solution is found, we can then lift u', v', w' to integers u, v, w and use equations (4.5) through (4.7) to compute q, s, t congruent to q', s', t' modulo r. Explicitly, we have s given by equation (4.6) and

$$t = \frac{1}{2}w^2(au^2 + adv^2 + 2bduv) - \frac{1}{2}dw^4 + \frac{3}{8}(bu^2 + bdv^2 + 2auv)^2 \quad (4.10)$$

$$q = \frac{1}{4}w^2(au^2 + adv^2 + 2bduv) + \frac{1}{4}dw^4 + \frac{1}{16}(bu^2 + bdv^2 + 2auv)^2. \quad (4.11)$$

We can choose different lifts u, v, w until the value of q computed is prime. (In theory we could allow q to be a prime power, but since almost all prime powers of a given size are prime, in practice we find q will always be prime.) We summarize the procedure in the following algorithm.

Algorithm 4.2. The following algorithm takes as input five positive integers a, b, d, k, r and a (finite) interval $I \subset \mathbb{Z}$, such that $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$ is a primitive quartic CM field, and r is a prime congruent to 1 (mod k). The algorithm outputs either the symbol $\perp$ or a prime q and a polynomial $h(x)$ of the form (4.4). If the output is not $\perp$, then there is a genus 2 curve $C/\mathbb{F}_q$ such that

- Jac(C) has characteristic polynomial of Frobenius $h(x)$,
- Jac(C) has endomorphism ring isomorphic to $\mathcal{O}_K$, and
- Jac(C) has embedding degree k with respect to r.

1. Set $v' \leftarrow 0$.
2. Using v' as the value of the variable v, find a simultaneous solution $(q', s', t', u', w') \in \mathbb{F}_r^5$ to equations (4.5) through (4.9) modulo r. If none exists, go to Step 5.
3. Let u_0, v_0, w_0 be the unique integers in $[0, r)$ congruent to u', v', w' respectively.
4. For each triple $(i_1, i_2, i_3) \in I^3$, do the following:
   (a) Set $u \leftarrow u_0 + i_1 r$, $v \leftarrow v_0 + i_2 r$, $w \leftarrow w_0 + i_3 r$.
   (b) Compute q, s, and t by equations (4.11), (4.6), and (4.10), respectively.
   (c) If t and q are integers, q is prime, and $q \nmid t$, go to Step 6.
5. Set $v' \leftarrow v' + 1$. If $v \equiv 0 \pmod{r}$ then output $\perp$; otherwise go to Step 2.
6. Output q and the polynomial $h(x) = x^4 - sx^3 + tx^2 - sqx + q^2$.

By Fact 3.5, if q and $h(x)$ are outputs of Algorithm 4.2, we can construct the desired curve C by the following procedure:

Algorithm 4.3. The following algorithm takes as input a prime q and a q-Weil polynomial $h(x)$. Let $K = \mathbb{Q}[x]/(h(x))$. With high probability, the algorithm outputs a genus 2 curve $C/\mathbb{F}_q$ such that

– $\mathrm{Jac}(C)$ has characteristic polynomial of Frobenius $h(x)$, and
– $\mathrm{Jac}(C)$ has endomorphism ring isomorphic to $\mathcal{O}_K$.

1. Compute the Igusa class polynomials $H_i(x)$ for K, via e.g. [30], [6], or [12].
2. Let S_i for $i = 1, 2, 3$ be the sets of roots in $\mathbb{F}_q$ of the $H_i(x) \pmod q$.
3. Let $n_1 = h(1)$ and $n_2 = h(-1)$. For each $(j_i, j_2, j_3) \in S_1 \times S_2 \times S_3$, do the following:
   (a) Use Mestre's algorithm [20] to compute a curve $C/\mathbb{F}_q$ with absolute Igusa invariants (j_1, j_2, j_3).
   (b) Choose a random point $P \in \mathrm{Jac}(C)(\mathbb{F}_q)$.
   (c) If $[n_1]P = O$, return C.
   (d) If $[n_2]P = O$, return the quadratic twist of C.
   (e) If $K \cong \mathbb{Q}(\zeta_5)$, repeat Steps 3b through 3d for each quintic twist of C.

We note that if the correct triple of invariants is tested in Step 3 then the algorithm will output the correct curve C. The algorithm will only output an incorrect curve C if the random point P has order dividing both $\#\,\mathrm{Jac}(C)$ and one of n_1 or n_2. If q is reasonably large then this event occurs with negligible probability; to further reduce the probability of error one could choose more random points P.

We have run Algorithm 4.2 for various prime values r of cryptographic size and various embedding degrees k, and used Algorithm 4.3 to generate pairing-friendly genus 2 curves C. Some examples appear in Appendix A.

Since u_0, v_0, and w_0 are essentially random integers in $[0, r)$, we see from equation (4.11) that we can expect q to be roughly the same size as r^4, so by Definition 2.8 the ρ-values of the varieties generated will be roughly 8. The examples in Appendix A bear this heuristic observation out in practice. As a consequence, to achieve comparable levels of security on the abelian surface A and in the finite field $\mathbb{F}_{q^k}$, the chosen embedding degree k should be one eighth of the embedding degree of an "ideal" abelian surface of prime order $r \sim q^2$.

Remark 4.4. An analysis of the formula for q given by equation (4.11) shows that in most cases in order for q to be prime the value of b input into Algorithm 4.2 must be odd. In practice this restriction does not pose a problem, since if $b = 2^\ell b'$ then $\mathbb{Q}(\sqrt{-a + b\sqrt{d}})$ is isomorphic to $\mathbb{Q}(\sqrt{-a + b'\sqrt{4^\ell d}})$.

Finally, we note that it may happen that for a given r any solution (q', s', t', u', v', w') produced in Step 2 gives values for q that are always either not integers or not prime. Instead of trying all possible v', one may wish to abort the algorithm when v' reaches a certain value and try again with a different r. This is the method we used to find Example 2 of Appendix A.

5 Constructing genus 2 curves with prescribed full embedding degree

Algorithm 4.2 constructs abelian surfaces $A/\mathbb{F}_q$ that have prescribed embedding degree k with respect to a subgroup of a given size r. By Proposition 2.3, this

guarantees that two roots of the characteristic polynomial of Frobenius have order dividing k, so if $k > 1$ then two dimensions of $A[r]$ are contained in $A(\mathbb{F}_{q^k})$. However, the algorithm makes no claim about the remaining two roots of the characteristic polynomial, so we have no control over the full embedding degree of A, i.e. the field over which all of the points of $A[r]$ are defined. Such control would be necessary, for instance, in a protocol that required pairings involving three or four linearly independent r-torsion points. We thus seek a method of producing abelian surfaces with prescribed full embedding degree.

As in the previous section, we fix a prime r and an embedding degree k. To construct an abelian variety with prescribed full embedding degree k with respect to r, by Proposition 2.7 it suffices to produce a characteristic polynomial of Frobenius with four distinct roots, all of which have order dividing k in $\mathbb{F}_r^\times$. There are many possibilities for such a polynomial; for our construction we will choose the polynomial to have the form

$$h(x) \equiv x^4 - (q^2+1)x^2 + q^2 \pmod{r} \tag{5.1}$$

This polynomial has roots $1, -1, q, -q$, so choosing q to be a primitive kth root of unity modulo r will give us the desired condition on the orders of the roots. To ensure that all four roots are distinct we require $k \geq 3$. Since -1 has order 2, the full embedding degree k must be even.

Now suppose as in the previous section that the characteristic polynomial of Frobenius (over the integers) is given by

$$h(x) = x^4 - sx^3 + tx^2 - sqx + q^2. \tag{5.2}$$

Equation (5.1) and the requirement that q be a primitive kth root of unity modulo r tell us that

$$\Phi_k(q) \equiv 0 \pmod{r} \tag{5.3}$$
$$s \equiv 0 \pmod{r} \tag{5.4}$$
$$t \equiv -q^2 - 1 \pmod{r}, \tag{5.5}$$

where Φ_k is the kth cyclotomic polynomial.

As before, due to the limitations of the genus 2 CM method we will fix a quartic CM field $K = \mathbb{Q}(\sqrt{-a+b\sqrt{d}})$, and look for a polynomial $h(x)$ such that $K \cong \mathbb{Q}[x]/(h(x))$. By Propositions 3.3 and 4.1 it suffices to find u, v, and w satisfying equations (4.5) through (4.7). These three equations together with equations (5.3) through (5.5) give six relations in six variables, so we can expect to find a valid solution (q', s', t', u', v', w') modulo r for some positive fraction of all r. As in Algorithm 4.2, if a solution exists we can then lift u', v', w' to integers u, v, w and use equations (4.11), (4.6), and (4.10) to compute q, s, t congruent to q', s', t' modulo r. We choose different lifts u, v, w until the value of q computed is prime. We summarize the procedure in the following algorithm.

Algorithm 5.1. The following algorithm takes as input five positive integers a, b, d, k, r and a (finite) interval $I \subset \mathbb{Z}$, such that $K = \mathbb{Q}(\sqrt{-a+b\sqrt{d}})$ is a

primitive quartic CM field, $k \geq 4$ is even, and r is a prime congruent to 1 (mod k). The algorithm outputs either the symbol $\perp$ or a prime q and a polynomial $h(x)$ of the form (5.2). If the output is not $\perp$, then there is a genus 2 curve $C/\mathbb{F}_q$ such that

- Jac(C) has characteristic polynomial of Frobenius $h(x)$,
- Jac(C) has endomorphism ring isomorphic to $\mathcal{O}_K$, and
- Jac(C) has full embedding degree k with respect to r.

1. Find a simultaneous solution $(q', s', t', u', v', w') \in \mathbb{F}_r^6$ to equations (4.5) through (4.7) and (5.3) through (5.5). If none exists, output $\perp$.
2. Let u_0, v_0, w_0 be the unique integers in $[0, r)$ congruent to u', v', w' respectively.
3. For each triple $(i_1, i_2, i_3) \in I^3$, do the following:
   (a) Set $u \leftarrow u_0 + i_1 r$, $v \leftarrow v_0 + i_2 r$, $w \leftarrow w_0 + i_3 r$.
   (b) Compute q, s, and t by equations (4.11), (4.6), and (4.10), respectively.
   (c) If t and q are integers, q is prime, and $q \nmid t$, go to Step 4.
   (d) If every triple (i_1, i_2, i_3) has been tested, output $\perp$.
4. Output q and the polynomial $h(x) = x^4 - sx^3 + tx^2 - sqx + q^2$.

If q and $h(x)$ are outputs of Algorithm 5.1, we can use Algorithm 4.3 to construct the desired curve C. As noted in Remark 4.4, the value of b input into Algorithm 5.1 should be odd. Since the algorithm requires solving six equations in six variables, there is no extra degree of freedom that we can use for a loop as in Algorithm 4.2. Thus if no solution to the system exists for a given r, we must try again with a different r.

We have run Algorithm 5.1 for various prime values r of cryptographic size and various embedding degrees k, and used Algorithm 4.3 to generate pairing-friendly genus 2 curves C. An example with a 512-bit r and $k = 18$ appears in Appendix B. As before, the ρ-values of the varieties generated are roughly 8.

Remark 5.2. Since the endomorphism rings of the abelian varieties constructed by Algorithm 4.3 are Dedekind domains, by Proposition 2.6 if r is unramified in $\mathcal{O}_K$ then the variety constructed has full embedding degree k even if the characteristic polynomial of Frobenius has multiple roots. Thus while Algorithm 5.1 is stated for $k \geq 4$, it also works for $k = 2$.

5.1 Constructing genus 2 curves C with Jac(C)[r] $\subset$ Jac(C)($\mathbb{F}_q$)

It may happen that for some protocols we require all of the r-torsion points of our pairing-friendly abelian surface A to be defined over a prime field, i.e. A to have full embedding degree 1. Since Algorithm 5.1 requires k to be even, we must find a different means of constructing such abelian surfaces.

The abelian surfaces we construct via Algorithm 4.3 have endomorphism rings equal to rings of integers in number fields. Thus we may apply Proposition 2.6 to determine when such a surface has embedding degree 1. Given a prime r, we seek characteristic polynomial $h(x)$ such that $h(x) \equiv (x-1)^4 \pmod{r}$.

In the notation of (5.2), this means that we have $q \equiv 1$, $s \equiv 4$, and $t \equiv 6 \pmod{r}$. Substituting into expressions (4.5), (4.6), and (4.7), we see that the left hand sides of equations (4.5) and (4.7) both become zero. Thus if we set $w \equiv 0 \pmod{r}$, we need only find a solution (u, v) to

$$bu^2 + bdv^2 + 2auv = 4 \pmod{r}. \tag{5.6}$$

This single equation in two variables gives an extra degree of freedom as in Algorithm 4.2, allowing us to loop on the value of v until a solution is found. The complete algorithm is as follows.

Algorithm 5.3. The following algorithm takes as input four positive integers a, b, d, r and a (finite) interval $I \subset \mathbb{Z}$, such that $K = \mathbb{Q}(\sqrt{-a + b\sqrt{d}})$ is a primitive quartic CM field, and r is prime. The algorithm outputs either the symbol $\perp$ or a prime q and a polynomial $h(x)$ of the form (5.2). If the output is not $\perp$, then there is a genus 2 curve $C/\mathbb{F}_q$ such that

- $\mathrm{Jac}(C)$ has characteristic polynomial of Frobenius $h(x)$,
- $\mathrm{Jac}(C)$ has endomorphism ring isomorphic to $\mathcal{O}_K$, and
- $\mathrm{Jac}(C)[r] \subset \mathrm{Jac}(C)(\mathbb{F}_q)$.

1. Set $v' \leftarrow 0$.
2. Using v' as the value of the variable v, find a solution u' to equation (5.6) modulo r. If none exists, go to Step 5.
3. Let u_0, v_0 be the unique integers in $[0, r)$ congruent to u', v' respectively.
4. For each triple $(i_1, i_2, i_3) \in I \times I \times (I \cap \mathbb{Z}_{>0})$, do the following:
   (a) Set $u \leftarrow u_0 + i_1 r$, $v \leftarrow v_0 + i_2 r$, $w \leftarrow i_3 r$.
   (b) Compute q, s, and t by equations (4.11), (4.6), and (4.10), respectively.
   (c) If t and q are integers, q is prime, and $q \nmid t$, go to Step 6.
5. Set $v' \leftarrow v' + 1$. If $v \equiv 0 \pmod{r}$ then output $\perp$; otherwise go to Step 2.
6. Output q and the polynomial $h(x) = x^4 - sx^3 + tx^2 - sqx + q^2$.

We can then use Algorithm 4.3 to construct the genus 2 curve C whose Jacobian has the desired properties. An example with a prime r of cryptographic size appears in Appendix B.

We note that Proposition 2.6 requires that the prime r be unramified in the specified CM field K. Since r is large (currently at least 2^{160}) and current methods only allow us to work with CM fields with very small discriminant, this condition will always be satisfied in practice.

6 Extending the algorithms

6.1 Composite-order subgroups

Recently, a number of protocols have been proposed that require a pairing-friendly abelian variety with a subgroup r whose order is a large composite number that is presumed to be infeasible to factor, such as an RSA modulus

(see e.g. [3]). We observe that our algorithms extend readily to produce such varieties. If we choose the desired subgroup size $r = r_1 r_2$ and find appropriate $(q_i', s_i', t_i', u_i', v_i', w_i')$ modulo r_i for $i = 1, 2$, we can use the Chinese Remainder Theorem to compute the values of the parameters modulo r, which we then lift to the integers in the usual manner. An example where r is a product of 512-bit primes appears in Appendix A.

6.2 Improving the ρ-values

Algorithms 4.2 and 5.1 produce pairing-friendly abelian varieties with ρ-values around 8. This ρ-value means that computations on the abelian variety A must be done over a field whose size (in bits) is four times the size of the prime-order subgroup. Since the fields of definition of abelian surfaces can have as little as half as many bits as group sizes, our large ρ-value implies that arithmetic in the order-r subgroup of A will be significantly less efficient than if r were the full order of $A(\mathbb{F}_q)$.

An important open problem is thus to produce genus 2 curves $C/\mathbb{F}_q$ whose Jacobians are ordinary and pairing-friendly with respect to subgroups of order $r \sim q$ (i.e. $\rho \sim 2$) or even $r \sim q^2$ (i.e. $\rho \sim 1$). Just as there are a multitude of techniques for producing elliptic curves with $\rho < 2$ [8], there may be many different ways to generate abelian surfaces with $\rho < 2$. The results presented in this paper suggest two possible approaches; these ideas are the basis of ongoing research.

The Brezing-Weng extension. Our construction of pairing-friendly genus 2 curves is modeled on the Cocks-Pinch method for constructing pairing-friendly elliptic curves [5], which produces curves with $\rho \approx 2$. Brezing and Weng [4] generalized the Cocks-Pinch method to produce elliptic curves with $\rho < 2$ by working over a number field L instead of modulo the prime r. Our method invites a similar generalization.

A Brezing-Weng-like construction for abelian surfaces would look something like the following: choose an embedding degree k and a primitive quartic CM field K. Let $L = \mathbb{Q}[x]/(r(x))$ be an extension of K that contains the kth roots of unity. Consider equations (4.5) through (4.10) as having coefficients in L, and find a simultaneous solution (q', s', t', u', v', w') in L^6. Represent these solutions as polynomials modulo $r(x)$ and lift to $\mathbb{Q}[x]$ to compute polynomials $q(x)$, $s(x)$, and $t(x)$. Then for any x_0 for which $q(x_0)$, $r(x_0)$, $s(x_0)$, and $t(x_0)$ take on integer values and $q = q(x_0)$ is prime, we can use Algorithm 4.3 to produce a genus 2 curve C over $\mathbb{F}_q$ whose Jacobian has embedding degree k with respect to $r(x_0)$.

While the setup is straightforward, it is far from obvious how to choose a number field L so that the relevant equations have solutions in L. It is also unclear what ρ-values the construction would produce.

The MNT extension. The first construction of pairing-friendly ordinary elliptic curves was given by Miyaji, Nakabayashi, and Takano [22], who constructed

curves of prime order with embedding degree $k = 3$, 4, or 6. While the MNT method is fundamentally different from our approach in this paper, our hope is that the results established here – in particular the relationship between the CM field and the characteristic polynomial of Frobenius described by Proposition 3.3 – will lead to a generalization of the MNT equations that produces abelian surfaces of prime order with small embedding degree.

A Appendix: Examples of abelian surfaces with prescribed embedding degree

Example 1. We used the CM field $K = \mathbb{Q}(\sqrt{-2+\sqrt{2}})$ to construct a curve whose Jacobian has embedding degree 2 with respect to $r = 2^{160} + 7$. The Igusa class polynomials for K can be found in [28]. The outputs of Algorithm 4.2 are:

$q = 795006611640170109396940876005774396116863415419758542983000866861998633580771737$
$977185988060481042862469026090643969667638364464302415656507943863305115226587117$
$936072460021623269435928862304096161$ (651 bits)

$s = 241065221491947514428541310368448574139558370891656283357513064453386954760732987$
4103585110310902524

$t = 273597961733915219746412647988034912157244791593900712761392170842037137177036567$
$553396874299843349115422505366307475408332787349620259128899954674524332906359097$
$803745841721962697398843910255646496 6.$

The equation of curve C is $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$, with

$a_3 = 781556463828009280287360245134696723363334003262680019563373246663399403283036487$
$052339182967247341574259440091198071796180846063637213566649478498289206351995367$
$383165038349582750830436766970252305$

$a_2 = 758207154481521945617036644682392283114949510705878088132268608920626188933438797$
$483381881227773991187422405413699207810216146066184913867557690015136357020025837$
$900328984724486510381446751384612338$

$a_1 = 381808951735164961606343137842255716037080566877126178262494866125561180403110477$
$284125164818374722166481062194047594839530155014907766656596628159270771565309427$
$394435679890448998428239238224064322$

$a_0 = 451779311338035547603652098531473867669756697104795270896070777348303213918152607$
$191913806375610710451208277338640573029091063844390090090252467380128482742811397$
$752085484204533726326846152147956130.$

The ρ-value of $\mathrm{Jac}(C)$ is 8.135.

Example 2. We used the CM field $K = \mathbb{Q}(\sqrt{-13+3\sqrt{13}})$ to construct a curve whose Jacobian has embedding degree 5 with respect to $r = 2^{256} + 1935$. The Igusa class polynomials for K can be found in [28]. The outputs of Algorithm 4.2 are:

$q = 187054417300272888829081758103622625251800135275434297468834634921946092469113092$
$072159086600150762181774510677124635515553318814158762548930085510167332573217$
$544127058975207752200665843226201646820828198496166224560964119189956499885464717$
$184898469850033563781542203078552721104019920165985151959421583842811009334897$
(1041 bits)

$s = 162199757807017422228350792714313053133505577989736208331668193062343780270127547$
$403350534399231454670007427706569357326380036236554853105131100557790566935123636$

$t = 102914421945590709871634847034773414016461147763347283126606718257050049926149417$
$299439075333629448439722939787041228399008950947622539751018938730195127459579417$
$610834128227506849921568088716062947169430812232436972062283451594387535690527317$
$828826073700791264227305233330675683512084945877473304419543733527614996293734.$

The equation of curve C is $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$, with

$a_3 = 17711932034826598918283689493771517557773876172909860411136075106337245263908578 \backslash$
$38130632676662412318317995526768766016156509218023316817809243032636104864542135 \backslash$
$90450974675151214252356394141967359391373046477845725484335245940593602161185522 \backslash$
$99407180726519279323555530065745247279169841864254113262083113263075718295$

$a_2 = 15986676510291987692234115367676532911850944091016679833071471047947234683585606 \backslash$
$97115034669874820450535884159056843728249225669815188505386944583659138080162909 \backslash$
$05967274844595441965601950514813102729723644095411071587133554049011997599748427 \backslash$
$04612514672592478589233445454956670634552105995792263972845133993646857289$

$a_1 = 47201942823478063845886098041135725187242793436198889585030352165809645065572147 \backslash$
$21227820016294216571118639320025552488751294747094636654493682076253265791893965 \backslash$
$45479038178461819213500842438576057436074730626945979688825026746690602467861501 \backslash$
$22818186813590260409963846589232079707065644640692839018443390682626873 54$

$a_0 = 78304034375067256115734447740946659290071046170720112481596930213348431536496457 \backslash$
$55121110421815824365159812788162205652367009731948183507741581532695550495070587 \backslash$
$92454247668794075954692123006270938295625578774958097004925464585575953412442322 \backslash$
$12289080772802589930714322619719426885901604420229918101878858983346214 34.$

The ρ-value of $\mathrm{Jac}(C)$ is 8.130.

Example 3. We used the CM field $\mathbb{Q}(\zeta_5) \cong \mathbb{Q}(\sqrt{-5+2\sqrt{5}})$ to construct a curve whose Jacobian has embedding degree 2 with respect to a subgroup whose order is the product of two randomly chosen 512-bit primes. The subgroup order is $r = r_1r_2$, where

$r_1 = 11803978689777937943630606482916630610771262360451038998055839540326529770667084 \backslash$
$06269543834843695797198684768241171539117202195745798379916447981602904255 1$

$r_2 = 10562148112423020416524404694757877364214379304398742300462810766190994206554837 \backslash$
$20780297868333829273713418161532710655057765890930005617506414340761220117 1.$

The curve parameters output by the algorithm are

$q = 14925756484395620588340828961670838257513478706661565697246822452504566552140574742756687061841 \backslash$
$83327230608483783712366474758540746217028667487640911962140986093599037808756022247012327215177 \backslash$
$55213629155759198095454310558027874214652820897780483388060586066488218687181212452307625483349 \backslash$
$76366496124554483981483373801822503187587258063660086229410727117641415988467013231363616630609 \backslash$
$26784565678664538250238747181160671009774739859107546715830372244678085964167497584751497133190 \backslash$
$62473743991047642606208174057522050397949460193159461788663737303870370025595086798914435773073 \backslash$
$30957441034733183449830042687670076702702427197376791183936276832204167560500941974369069329083 \backslash$
$59708670235808387177041310855024858768884436834008663686434547994549615674931751552305085319169 \backslash$
$66775248336134051351298104896213296602388924453978024513608120925596409216323397648311343976954 \backslash$
$94850608962538593587343311993015139211462964161036467119410583324398159603028447384946960622522 \backslash$
$30770997608659471920286521205949551151597752968638719758638121844984366957688187107935204269465 \backslash$
$43159746899834639602301095209882606155611802028587711772509703238644061650428502599989386107821 \backslash$
$56353856878210524786864051502803963345888644673903158542867892627355727759704273439895981478711 \backslash$
$37491 \quad (4117 \text{ bits})$

$s = 13098746878962436440014430683891336683317189571490505914813272120811614309324444303366871354293 \backslash$
$72830005979537504811319304227876636545294152800886721481194819411446241353532512480738841086280 \backslash$
$05901787542961419689724694687487336334619968682790210396078391235045805526520293911051097509200 \backslash$
$51131450697823896534575237857994830562986932507184751622515815576198264141475009840150514368132 \backslash$
$81177097994456801761971744427560817207874947260618186954355056542820900806005906317355644621334 \backslash$
$64861731628184276806113304191171380570689829907671778827461520756611443418664003201518414345765 \backslash$
$44776360514930087129059147042329322189427488396912 4$

t = 71447874351911649047790586558090993998563268603490200023957371422801555162937685072960026194591 \
694998952798247823234050315812479809544178567369515790041089115191637490664834389911656043491 10 \
44130020633554209704979393260809079217893525464617697539949077675397812340865743118614232705363 \
32570478739783905207633694971163471187578705098554817323471993709158029500477120956863711046179 \
44293443643288015530272249583200203841664579887204015003519212963713250031262059100976431988738 \
31469605908437066772553789354597916412913719959364918891139900756569957522441865629408357922063 \
30830456109046092855847378424606149191959129582443509085118558602795955990660755981192038000549 \
55747149843391833964678178452750359615489740968473577261186810526498627348121318287605849558734 \
73073283842888516880923205533252952679156487993614335873937631278137023958484222652378109937457 \
66579032900411400423678425530874894613633379544708621873764938067722197469475912611967969911573 \
37325106251009118068517774538325440179740638841946741999971551345126799287983731744315849802338 \
31689006680224499487050914376246727166112531962043541974685145515161980670093306648871023302649 \
90769121782534850445620807355896308263404553927025336274119227548353972566258529006993215737180 \
56406.

The equation of the curve C is $y^2 = x^5 + 1$. The ρ-value of $\mathrm{Jac}(C)$ is 8.044.

B Appendix: Examples of abelian surfaces with prescribed full embedding degree

Example 4. We used the CM field $K = \mathbb{Q}(\sqrt{-30 + 2\sqrt{5}})$ to construct a curve whose Jacobian has embedding degree 4 with respect to $r = 2^{224} - 3047$. The field K is non-Galois and has class number 4. The Igusa class polynomials for K can be found in the preprint version of [30]. The outputs of Algorithm 4.2 are:

q = 25875665546464625747483263904141863215223855685631927398442175454186047689727181 \
935477877624034595615954645104592718893686922526984289911563166040265258306653 11 \
737526317236739759816581034931796803081221823586560157806990386975210310942567 55 \
40495783228843733030724545875768981 (912 bits)

s = −49819073164368546886826258467120852760074966205236328690105833376230198398121 96 \
710646403289755093635995976110325660432316004402715132455 36

t = 11315891237651345494483496588271771338331199214236780785739679696556702185995706 \
343720640024960855506245212103174644887087015437031955653461550637913651786406 64 \
146068896590376504023357057659203629511478271064935300988748614890267625575355 30 \
48773420611254748702256459338146056 6.

The equation of curve C is $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$, with

a_3 = 38557522515431718239138775060871205148933533072861261987872384836301846569735691 \
986592038851839717321728951012145525651895863860754634604133003215951636732365 47 \
018580868294026590129299428042217200074345648274635466417334431823899347650135 64 \
81279923766002824202682910288030 21

a_2 = 24361005015196617163667303200244929565396754003199827807036659742558068205679538 \
421600980982608782648429481206395240372659342118807804884635399458201069478773 00 \
191890228594057867422816081676227042279964952528548826178461339965983300429416 38 \
79810835474597261493353081510971860

a_1 = 66320501401668844356948887655622054099995573466241416241541350131153121137993090 \
856352514992833420872425637937410474330719972095158979437861776297341993176200 50 \
788380319047558526192957119225466716725381341896347370652767528334176358987695 01 \
63791039986027798808888128315848257

a_0 = 14382706785238411696604261079830832924182682159103069238604604235474798613117520 \
631729562995904918671161829291441521368707871792618988741217885892105030176041 27 \
073968129467517926771636287512671908365633493330711933386195159910357760869797 57 \
14869063111066962733459404280651443.

The ρ-value of $\mathrm{Jac}(C)$ is 8.139.

Example 5. We used the CM field $\mathbb{Q}(\zeta_5) \cong \mathbb{Q}(\sqrt{-5+2\sqrt{5}})$ to construct a curve whose Jacobian has a full embedding degree 18 with respect to $r = 2^{512} - 21765$. It is well known that if q is a prime congruent to 1 modulo 5, then curves of the form $y^2 = x^5 + a$ over $\mathbb{F}_q$ have ordinary Jacobians with endomorphism ring equal to the ring of integers in $\mathbb{Q}(\zeta_5)$. The outputs of Algorithm 4.2 are:

$q =$ 59074365172249747345684688885799219713686821704312879665133606989966029447850329 \
75230829155311014334779230965118255623420362480778492396721417257747659314786359 \
20795250354731455458038100319688820864862416524698402704757423587857740749579009 \
77252320027663270119406349574563966475722034749556644118761922028294459562833569 \
66240173227513608595794165454204411364337817641757042774322997818908262078473869 \
23136696539919070682511613422539713109290283715297568931260940817111736207365759 \
10384057975422529167443369355635149583367157450916764794128711999113674832682589 \
83922482484396741210910194457900276470627282055231608791065422368495012 (2076 bits)

$s =$ 50198472820463386967952610923013159595056450968496479323073507575708657824814699 \
02090498003872295244854487982241397552440910979091227842831294628034496868814019 \
21791244835548128757898646263309475653445620933881119118480682007865555263873839 \
79370210785664978237527038387490423402089722244461849001568721734735772679169

$t =$ 14067374333890141944513118630814238888086678031154052684224466385886484946580929 \
64165611402257514356534724883654118185716644155788323198490479798592494483708559 \
56033407372393835084136488816919649064994519296700210258212686748715721565437899 \
81232184289343512893913490608476743619200999694075903073932944215131227189317649 \
99294960124852992613543618727026957993353600145226685248887286727306276502269549 \
72507770119555885696497948237993261924120628419697292078175044944442948223566949 \
63615130537634328562711597429371690346222099035125663184763334253731200446863519 \
65849251312439696414819368306735550364910131207053724348955214349177992869.

The equation of the curve C is $y^2 = x^5 + 11^5$. The ρ-value of $\mathrm{Jac}(C)$ is 8.107.

Example 6. We set $r = 2^{192} - 237$ and used the CM field $K = \mathbb{Q}(\sqrt{-13+2\sqrt{13}})$ to construct a curve $C/\mathbb{F}_q$ with $\mathrm{Jac}(C)[r] \subset \mathrm{Jac}(C)(\mathbb{F}_q)$. The Igusa class polynomials for K can be found in [28]. The curve parameters are:

$q =$ 41917988492119141249022446188487568991935922462150808494416316158553598932697733 \
83272842381465331789525955141195441340428996707998134865330379302251402611349723 \
18485837183300638482574886142860696370694527884195065961476308415619112128 1 \
(773 bits)

$s =$ 15760802478557791684911616040057445522031895708186178665984157191280664691164543 \
99383869668163280777796966990248899856

$t =$ 93151085538042536108938769307750153315413161027001796654086997940653311817935243 \
78682802404960938177148354133899993271994641255739054712601215835633030023875323 \
19243748436256787827661246671324707727932944167299366404935886919307341774.

The equation of the curve C is $y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$, with

$$a_3 = 28932282521819038280326666503307020611152548216399078321215512935546100541046 50 \backslash$$
$$02364962806545504432997892720744589983358536928902319593105805009984556203183 82 \backslash$$
$$52471270856385978986255881796236347205721596907069183349632684518889808430$$
$$a_2 = 18519126403250094965953802347785265408499724718736649019824988296072976579694 34 \backslash$$
$$16034423386875812079107032339048677040568945619421747121612569346133509299587 34 \backslash$$
$$16522531237666462484342201598945244051808496141043008227314651611993479002 1$$
$$a_1 = 51004522827135545868055349145766706573208071472631658403414584258886967151621 55 \backslash$$
$$27271154819467166690055569792351605027204302869720462405330228004753949945747 89 \backslash$$
$$94684865345941988652933629587647405581943934960966405623978471953839825408$$
$$a_0 = 33277218609785779101614036830691708370515017230158427310490879303381054908563 00 \backslash$$
$$21075933450284269249263947617171897597598045102922866075405839290140983089035 11 \backslash$$
$$30759428669945350702323198089179219279729580597842288237226415502850187806 2.$$

The ρ-value of $\mathrm{Jac}(C)$ is 8.050.

References

1. R. Balasubramanian and N. Koblitz, "The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm," *Journal of Cryptology* **11** (1998), 141–145.
2. D. Bernstein, "Elliptic vs. hyperelliptic, part 1," talk at ECC 2006, Toronto, Canada, 20 September 2006. Slides available at `http://cr.yp.to/talks/2006.09.20/slides.pdf`.
3. D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," in *TCC '05*, Springer LNCS **3378**, 2005, 325–341.
4. F. Brezing and A. Weng, "Elliptic curves suitable for pairing based cryptography," *Designs, Codes and Cryptography* **37** (2005), 133–141.
5. C. Cocks and R. G. E. Pinch, "Identity-based cryptosystems based on the Weil pairing," Unpublished manuscript, 2001.
6. K. Eisenträger and K. Lauter, "A CRT algorithm for constructing genus 2 curves over finite fields," to appear in *AGCT-11*, 2007, preprint available at `http://arxiv.org/abs/math.NT/0405305`.
7. D. Freeman and K. Lauter, "Computing endomorphism rings of Jacobians of genus 2 curves over finite fields," Cryptology eprint 2007/010, available at `http://eprint.iacr.org`.
8. D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," Cryptology eprint 2006/371, available at `http://eprint.iacr.org`.
9. G. Frey and T. Lange, "Fast bilinear maps from the Tate-Lichtenbaum pairing on hyperelliptic curves," in ANTS-VII, Springer LNCS **4076**, 2006, 466–479.
10. S. Galbraith, "Supersingular curves in cryptography," in *ASIACRYPT '01*, Springer LNCS **2248**, 2001, 495–513.
11. S. Galbraith, J. McKee, and P. Valença, "Ordinary abelian varieties having small embedding degree," to appear in *Finite Fields and Applications*, preprint available at `http://eprint.iacr.org`.
12. P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, "The 2-adic CM method for genus 2 curves with application to cryptography," in *ASIACRYPT '06*, Springer LNCS **4284**, 2006, 114–129.

13. L. Hitt, "Families of genus 2 curves with small embedding degree," Cryptology eprint 2007/001, available at `http://eprint.iacr.org`.
14. L. Hitt, "On an improved definition of embedding degree," Cryptology eprint 2006/415, available at `http://eprint.iacr.org`.
15. E. Howe, "Principally polarized ordinary abelian varieties over finite fields," *Trans. Amer. Math. Soc.* **347** (1995) 2361–2401.
16. N. Katz, "Serre-Tate local moduli," in *Surfaces algébriques (Sém. de géom. algébr. d'Orsay 1976-78)*, Springer Lect. Notes in Math. **868** (1981) exposé V-bis, 138–202.
17. T. Lange, "Elliptic vs. hyperelliptic, part 2," talk at ECC 2006, Toronto, Canada, 20 September 2006. Slides available at `http://hyperelliptic.org/tanja/vortraege/ECC_06.ps`
18. F. Luca, D. Mireles, and I. Shparlinski, "MOV attack in various subgroups on elliptic curves," *Illinois J. Math.* **48** (2004), 1041–1052.
19. A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory* **39** (1993) 1639–1646.
20. J.-F. Mestre, "Construction de courbes de genre 2 à partir de leurs modules," in *Effective methods in algebraic geometry*, Birkhäuser Progr. Math. **94**, 1991, 313–334.
21. J. S. Milne, "Abelian varieties," in *Arithmetic Geometry*, ed. G. Cornell and J. Silverman, Springer, 1986, 103–150.
22. A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals* **E84-A** (2001) 1234–1243.
23. F. Oort and K. Ueno, "Principally polarized abelian varieties of dimension two or three are Jacobian varieties," *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **20** (1973), 377–381.
24. 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.
25. K. Rubin and A. Silverberg, "Supersingular abelian varieties in cryptology," in *CRYPTO '02*, Springer LNCS **2442**, 2002, 336–353.
26. A.-M. Spallek, "Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen," Ph.D. thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.
27. 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.
28. P. van Wamelen, "Examples of genus two CM curves defined over the rationals," *Math. Comp.* **68** (1999), 307–320.
29. W. C. Waterhouse and J. S. Milne, "Abelian varieties over finite fields," *Proc. Symp. Pure Math.* **20** (1971), 53–64.
30. A. Weng, "Constructing hyperelliptic curves of genus 2 suitable for cryptography," *Math. Comp.* **72** (2003), 435–458.