CONSTRUCTING PAIRING-FRIENDLY HYPERELLIPTIC CURVES USING WEIL RESTRICTION

DAVID MANDELL FREEMAN AND TAKAKAZU SATOH

Abstract. A *pairing-friendly curve* is a curve over a finite field whose Jacobian has small embedding degree with respect to a large prime-order subgroup. In this paper we construct pairing-friendly genus 2 curves over finite fields $\mathbb{F}_q$ whose Jacobians are ordinary and simple, but not absolutely simple. We show that constructing such curves is equivalent to constructing elliptic curves over $\mathbb{F}_q$ that become pairing-friendly over a finite extension of $\mathbb{F}_q$. Our main proof technique is Weil restriction of elliptic curves. We describe adaptations of the Cocks-Pinch and Brezing-Weng methods that produce genus 2 curves with the desired properties. Our examples include a parametric family of genus 2 curves whose Jacobians have the smallest recorded ρ-value for simple, non-supersingular abelian surfaces.

1. Introduction

Let q be a prime power and $\mathbb{F}_q$ be a finite field of q elements. In this paper we study two types of abelian varieties:

- Elliptic curves E, defined over $\mathbb{F}_{q^d}$, with $j(E) \in \mathbb{F}_q$.
- Genus 2 curves C, defined over $\mathbb{F}_q$, whose Jacobians are isogenous over $\mathbb{F}_{q^d}$ to a product of two isomorphic elliptic curves defined over $\mathbb{F}_q$.

Both types of abelian varieties have recently been proposed for use in cryptography. In the first case, Galbraith, Lin, and Scott [16] showed that arithmetic operations on certain elliptic curves E as above can be up to 30% faster than arithmetic on generic elliptic curves over prime fields. In the second case, Satoh [27] showed that point counting on Jacobians of certain genus 2 curves C as above can be executed much faster than point counting on Jacobians of generic genus 2 curves.

We consider the construction of these two types of abelian varieties for use in *pairing-based cryptography* [24]. To be suitable for this application, the variety must be *pairing-friendly*, which means that it must have

- a subgroup of large prime order r, and
- a small *embedding degree* $k = [\mathbb{F}_q(\zeta_r) : \mathbb{F}_q]$.

Our main result is to show that constructing pairing-friendly abelian varieties of the above two types is in a sense equivalent. Specifically, if we can construct an elliptic curve $E/\mathbb{F}_q$ whose base extension to $\mathbb{F}_{q^d}$ is pairing-friendly (and d is minimal with this property), then there is a simple pairing-friendly abelian variety $A/\mathbb{F}_q$ that is isogenous over $\mathbb{F}_{q^d}$ to E^e, where $e = \varphi(d)$ or $\varphi(d)/2$. If $e = 2$ and certain further conditions are met, then we can construct a genus 2 curve C over $\mathbb{F}_q$ whose Jacobian is isogenous to A. Conversely, given certain genus 2 curves $C/\mathbb{F}_q$ as above whose Jacobians are simple and pairing-friendly, we can construct elliptic

Date: September 28, 2009.

curves $E/\mathbb{F}_q$ whose base extensions to $\mathbb{F}_{q^d}$ are pairing-friendly. (We focus on simple abelian surfaces A because we can replace a non-simple A by one of its elliptic curve factors in any application.)

In our principal application of the main result, we take previous methods that construct pairing-friendly *elliptic* curves and adapt them to produce *genus 2* curves with pairing-friendly Jacobians. Our technique has the advantage that the fields $\mathbb{F}_q$ over which the resulting abelian surfaces are defined can be made much smaller relative to the group orders r than previous techniques would allow. This ratio is measured by the *ρ-value*, defined as $\rho(A) = \dim A \cdot \log q / \log r$. Our construction produces pairing-friendly abelian surfaces with ρ-values that are generically around 4, and we achieve a "record" ρ-value of approximately 2.2 in the case $k = 27$. (The corresponding figures when A is absolutely simple are $\rho \approx 8$ generically [13] and $\rho \approx 4$ for certain examples [11]. When A is supersingular we can achieve $\rho \approx 1$ but are restricted to $k \leq 12$ [26].)

Our constructions properly contain those of Kawazoe and Takahashi [21], who consider a single isomorphism class of genus 2 curves with split Jacobians.

Outline. In Section 2 we introduce notation and recall some basic facts about abelian varieties. In Section 3 we introduce and study *Weil restriction*, which is the process by which, given a finite extension of fields L/K, we can interpret a variety V over L as a higher-dimensional variety V' over K. Our main result is that Jacobians that split over $\mathbb{F}_{q^d}$ into a product of isomorphic elliptic curves $E/\mathbb{F}_q$ are isogenous to subvarieties of the Weil restriction of E from $\mathbb{F}_{q^d}$ down to $\mathbb{F}_q$. We also study when these subvarieties are simple.

In Section 4 we study two specific families of genus 2 curves with split Jacobians, paying careful attention to the minimal field over which this splitting occurs. We apply the theory developed in Section 3 to determine precisely the subvarieties of Weil restrictions to which these Jacobians are isogenous.

In Section 5 we put the theory to work in the form of algorithms that can be used to produce genus 2 curves with pairing-friendly Jacobians. We give two algorithms that produce a pairing-friendly *Frobenius element*: one modeled on the algorithm of Cocks and Pinch [8] that is very flexible, and one modeled on the algorithm of Brezing and Weng [6] that is more restrictive but leads to smaller ρ-values. Section 6 gives examples of pairing-friendly genus 2 curves produced by our algorithms.

In Section 7 we describe an extension of our techniques that generalizes a method of Freeman, Scott, and Teske [12, Section 6.4], and give some examples produced by this method. Finally we conclude in Section 8 with some open questions.

2. Abelian varieties

We assume throughout that all fields are perfect. We first recall some background on abelian varieties. An *abelian variety* is a smooth, projective, geometrically irreducible group variety. An *elliptic curve* is a one-dimensional abelian variety, and an *abelian surface* is a two-dimensional abelian variety.

Let $\mathbb{F}_q$ be a finite field of q elements. An abelian variety $A/\mathbb{F}_q$ is *ordinary* if $\#A(\overline{\mathbb{F}}_q)[p] = p^{\dim A}$, where $p = \operatorname{char}(\mathbb{F}_q)$, and A is *supersingular* if it is isogenous over $\overline{\mathbb{F}}_q$ to a product of non-ordinary elliptic curves. If $\dim A \geq 2$ then it is possible that A is neither ordinary nor supersingular.

If A is an abelian variety over a field F we use $\operatorname{End}(A)$ to denote the ring of endomorphisms of A that are defined over F, and we use $\operatorname{End}_{\overline{F}}(A)$ to denote the ring of endomorphisms of A that are defined over the algebraic closure $\overline{F}$. If A is an ordinary abelian variety over a finite field, then these two rings are equal.

An *isogeny* of abelian varieties is a surjective morphism of varieties that is a group homomorphism. Two varieties A, A' over F are *isogenous* if there is an isogeny between them that is defined over F. (If there is an isogeny defined over an extension field F' then the two varieties are *isogenous over* F'.) An abelian variety A over F is *simple* if it is not isogenous (over F) to a product of two abelian varieties of positive dimension. We say A is *absolutely simple* if it remains simple when base-extended to $\overline{F}$.

A *twist* of an abelian variety A over F is an abelian variety A' that is isomorphic to A over $\overline{F}$. The *degree* of the twist is the degree of the smallest field extension F'/F such that there is an isomorphism $\phi : A \to A'$ defined over F'.

If A is an abelian variety over $\mathbb{F}_q$, we let $f_{A,q}(x)$ denote the characteristic polynomial of the q-power Frobenius endomorphism of A. This is a *q-Weil polynomial*: a monic polynomial in $\mathbb{Z}[x]$ all of whose roots have absolute value $\sqrt{q}$. If $\dim A = g$ then $\deg f_{A,q} = 2g$. A *q-Weil number* is a root of an irreducible q-Weil polynomial. We will make extensive use of the following facts.

Theorem 2.1.

(a) *Two abelian varieties A, B are isogenous over $\mathbb{F}_q$ if and only if $f_{A,q} = f_{B,q}$.*
(b) *If A, B are abelian varieties over $\mathbb{F}_q$ then $f_{A\times B,q} = f_{A,q} f_{B,q}$.*
(c) *There is a bijection*

$$\left\{\begin{matrix}\textit{isogeny classes of}\\ \textit{simple abelian varieties over } \mathbb{F}_q\end{matrix}\right\} \to \left\{\begin{matrix}\textit{irreducible}\\ q\textit{-Weil polynomials}\end{matrix}\right\}$$

$$\textit{isogeny class of } A/\mathbb{F}_q \mapsto (f_{A,q})^{1/e},$$

where e is the largest integer such that $(f_{A,q})^{1/e} \in \mathbb{Z}[x]$.
(d) *If $A/\mathbb{F}_q$ is ordinary and simple, the integer e from (a) is equal to 1, and* $\operatorname{End}(A) \otimes \mathbb{Q} \cong \mathbb{Q}[x]/(f_{A,q}(x))$.

Proof.

(a) This is [30, Theorem 1].
(b) This follows from the fact that the Tate module $V_\ell(A \times B)$ is equal to $V_\ell(A) \times V_\ell(B)$.
(c) This is the main result of Honda-Tate theory [31, Théorème 1 (i)].
(d) By [31, Théorème 1 (ii)], $\mathbb{Q}[x]/(f_{A,q}(x)^{1/e})$ is isomorphic to the center of $\operatorname{End}(A) \otimes \mathbb{Q}$, and if e is as in part (a) then e^2 is the degree of $\operatorname{End}(A) \otimes \mathbb{Q}$ over its center. By [33, Theorem 7.2], if A is ordinary then $\operatorname{End}(A)$ is commutative, and the result follows. □

If $A/\mathbb{F}_q$ is ordinary and simple, then the middle coefficient of $f_{A,q}$ is prime to q. In this case we say that $f_{A,q}$ is an ordinary q-Weil polynomial, and its roots are ordinary q-Weil numbers.

3. Weil restrictions

We now recall the concept of *Weil restriction*, also known as *restriction of scalars*. Let L/K be a finite (separable) extension of fields. The Weil restriction from L to K, denoted $\operatorname{Res}_{L/K}$, is a functor from varieties over L to varieties over K. On the level of affine varieties, the Weil restriction of a variety X defined over L can be obtained by the following process:

(1) Choose a K-basis $\{\alpha_i\}$ of L.
(2) Expand the equations defining X in terms of this basis, with each variable over L becoming $[L:K]$ variables over K.
(3) Collect terms with matching basis elements to obtain $[L:K]$ equations over K from each equation over L. These equations define $X' = \mathrm{Res}_{L/K}(X)$.

It holds that $\dim X' = [L:K]\dim X$. For projective varieties X we can apply this procedure on affine open subsets and glue the results together to obtain X'. If X is an abelian variety, then X' is as well, since on affine patches we can apply the same process to the equations defining the group law. For further details see [34, Section 1.3].

In this paper we focus on abelian varieties described by the following proposition, whose proof was shown to us by Marco Streng.

Proposition 3.1. *Let A be a g-dimensional simple abelian variety defined over a perfect field K. Let L be a finite extension of K, and suppose A is isogenous over L to a product of g isomorphic simple abelian varieties B defined over K. Then A is isogenous over K to a subvariety of the Weil restriction $\mathrm{Res}_{L/K}(B)$.*

Proof. By the functoriality of Weil restriction, any map $\phi : A \to B^g$ defined over L descends to a map $\phi' : \mathrm{Res}_{L/K}(A) \to \mathrm{Res}_{L/K}(B^g) \cong (\mathrm{Res}_{L/K}(B))^g$. Furthermore, there is an abelian subvariety $B \subset \mathrm{Res}_{L/K}(A)$ isomorphic to A: let $\alpha_1, \ldots, \alpha_d$ be a basis of L as a K-vector space, with $\alpha_1 \in K$, and let x_i be the variables defining A/L on some affine open subset U. Then $B \cap U$ is defined by writing $x_i = y_{i1}\alpha_1 + \cdots + y_{id}\alpha_d$ and intersecting $\mathrm{Res}_{L/K}(A)$ with the hyperplanes defined by $y_{ij} = 0$ for all i and $j = 2, \ldots, d$, and these patches can be glued to obtain all of B. Thus A is isogenous to a subvariety of $(\mathrm{Res}_{L/K}(B))^g$, and since A is simple it must be isogenous to a subvariety of $\mathrm{Res}_{L/K}(B)$. $\square$

When L and K are finite fields, we wish to know how the characteristic polynomials of Frobenius of A and $\mathrm{Res}_{L/K}(A)$ are related. It is known that for any prime $\ell \neq \mathrm{char}\, K$, the ℓ-adic representation of $\mathrm{Gal}(\overline{K}/K)$ on the Tate module $V_\ell(X')$ is the induced representation of $\mathrm{Gal}(\overline{K}/L)$ on $V_\ell(X)$. The next proposition is an immediate consequence of this fact (see [9, Proposition 1.21]). We give here a direct elementary proof starting from the fact that for any variety X and any K-algebra R, we have

$$\mathrm{Res}_{L/K}(X)(R) \cong X(L \otimes_K R) \tag{3.1}$$

scheme-theoretically [4, Section 7.6]. Furthermore, if X is a group variety then (3.1) is a group isomorphism.

Proposition 3.2. *Let A be an abelian variety over a finite field $\mathbb{F}_{q^d}$, and let $A' = \mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(A)$. Then $f_{A',q}(x) = f_{A,q^d}(x^d)$.*

Proof. Our proof uses the properties of resultants. If K is a perfect field and $f, g \in K[x]$, the resultant of f and g is

$$R_x(f(x), g(x)) = \prod_{\substack{\alpha \in \overline{K} \\ f(\alpha)=0}} g(\alpha) = (-1)^{\deg f \deg g} \prod_{\substack{\beta \in \overline{K} \\ g(\beta)=0}} f(\beta). \tag{3.2}$$

Let X be an abelian variety over $\mathbb{F}_q$ and let π be the q-power Frobenius morphism. Since $X(\mathbb{F}_q)$ is the kernel of $\pi - 1$, then $\#X(\mathbb{F}_q) = f_{X,q}(1)$. Furthermore, since π^m is the q^m-power Frobenius morphism for any $m \geq 1$, we have

$$\#X(\mathbb{F}_{q^m}) = R_x\left(f_{X,q}(x), x^m - 1\right). \tag{3.3}$$

The expression on the right-hand side is the *mth cyclic resultant* of f. In addition, observe that

$$\mathbb{F}_{q^d} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m} \cong (\mathbb{F}_{q^{\mathrm{lcm}(d,m)}})^{\gcd(d,m)} = (\mathbb{F}_{q^{abc}})^a, \tag{3.4}$$

where $a = \gcd(m, d)$, $m = ab$, and $d = ac$. We thus have

$$\begin{aligned}
\#A'(\mathbb{F}_{q^m}) &= \#A(\mathbb{F}_{q^{abc}})^a \quad \text{by (3.1) and (3.4)}, \\
&= R_x\left(f_{A,q^d}(x), x^b - 1\right)^a \quad \text{by (3.3)}, \\
&= \prod_{\zeta^b = 1} f_{A,q^d}(\zeta)^a \quad \text{by (3.2)}, \\
&= \prod_{\zeta^b = 1} f_{A,q^d}(\zeta^c)^a \quad \text{since } \gcd(b,c) = 1, \\
&= \prod_{\eta^{ab} = 1} f_{A,q^d}(\eta^{ac}) \quad \text{by taking } a\text{th roots}, \\
&= R_x\left(f_{A,q^d}(x^d), x^m - 1\right) \quad \text{by (3.2)}, \\
&= R_x(f_{A',q}(x), x^m - 1) \quad \text{by (3.1)}.
\end{aligned}$$

(Note that we can ignore the minus signs arising in (3.2) since f_{A,q^d} has even degree.) By an argument of Kedlaya [22, Section 8], a q-Weil polynomial is determined uniquely by its sequence of cyclic resultants. Thus we conclude that $f_{A,q^d}(x^d) = f_{A',q}(x)$. □

3.1. **Primitive subgroups.** Our main construction involves taking an abelian variety defined over a field K, base extending to a field L, and then taking the Weil restriction back down to K. If L/K is cyclic, then this Weil restriction decomposes nicely into factors that correspond to the subfields of L containing K. The factor which is "new" for L, in other words, which does not appear as a factor in the Weil restrictions for proper subfields of L, was studied by Frey, Kani and Völklein [14], and in cryptographic contexts by Rubin and Silverberg [26]. This factors, known as a *primitive subgroup*, is defined as follows.

Definition 3.3 ([26, Definition 8.1])**.** *Let A be an abelian variety defined over a field K, and let L be a finite, nontrivial extension of K. Define the* primitive subgroup *of* $\mathrm{Res}_{L/K}(A)$ *to be*

$$V_{L/K} = \bigcap_{K \subseteq F \subsetneq L} \ker\left(\mathrm{Res}_{L/K}(A) \xrightarrow{\mathrm{Tr}_{L/F}} \mathrm{Res}_{F/K}(A)\right),$$

where $\mathrm{Tr}_{L/F} : \mathrm{Res}_{L/K}(A) \to \mathrm{Res}_{F/K}(A)$ *is the Weil restriction of the usual trace map from $A(L)$ to $A(F)$ defined on $x \in A(L)$ by*

$$x \mapsto \sum_{\sigma \in \mathrm{Gal}(L/F)} \sigma(x).$$

Define $V_{K/K}(A) = A$.

Diem [9, Theorem 5] has shown that there is an isogeny decomposition

$$\mathrm{Res}_{L/K}(A) \sim \bigoplus_{K\subseteq F\subseteq L} V_{F/K}(A). \tag{3.5}$$

See [9, Section 2.1.3] for further details.

Now suppose K is a finite field $\mathbb{F}_q$; in this case we use $V_d(A)$ or V_d (when A is obvious from context) to denote $V_{\mathbb{F}_{q^d}/\mathbb{F}_q}(A)$. Let π be the q-power Frobenius endomorphism of A. Since $A(\mathbb{F}_{q^d}) = \ker(\pi^d - 1)$, we can decompose $A(\mathbb{F}_{q^d})$ into subgroups corresponding to cyclotomic factors of $\pi^d - 1$. The subgroup $\ker(\Phi_d(\pi))$ is exactly the intersection of the kernels of the trace maps on A from $\mathbb{F}_{q^d}$ to proper subfields. It follows from Definition 3.3 and property (3.1) of Weil restriction that there is a group isomorphism $V_d(A)(\mathbb{F}_q) \cong \ker(\Phi_d(\pi))$. We now determine the characteristic polynomial of Frobenius of $V_d(A)$.

Proposition 3.4. *Let A be a g-dimensional ordinary abelian variety over $\mathbb{F}_q$, and write*

$$f_{A,q}(x) = \prod_{i=1}^{2g}(x - \alpha_i).$$

Then the characteristic polynomial of Frobenius of $V_d(A)$ is

$$f_{V_d(A),q}(x) = \prod_{i=1}^{2g} \alpha_i^{\varphi(d)}\Phi_d(x/\alpha_i) = \prod_{i=1}^{2g}\prod_{\substack{1\le j\le d\\(d,j)=1}}(x - \zeta^j\alpha_i),$$

where ζ is a primitive dth root of unity.

Proof. The result is obvious for $d = 1$. Let $X = \mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q} A$ and let $\zeta \in \mathbb{C}$ be a primitive dth root of unity. By Proposition 3.2 we have

$$f_{X,q}(x) = \prod_{i=1}^{2g}(x^d - \alpha_i^d) = \prod_{i=1}^{2g}\prod_{j=1}^{d}\alpha_i(x/\alpha_i - \zeta^j) = \prod_{e|d}\left(\prod_{i=1}^{2g}\alpha_i^{\varphi(e)}\Phi_e(x/\alpha_i)\right).$$

The result now follows inductively from the base case $d = 1$ and equation (3.5). $\square$

Remark 3.5. If d is odd, then since $\Phi_{2d}(x) = \Phi_d(-x)$, Proposition 3.4 implies that V_{2d} is isogenous to the quadratic twist of V_d. In particular, V_2 is isogenous to the quadratic twist A' of A, with A' defined over $\mathbb{F}_q$ and isomorphic to A over $\mathbb{F}_{q^2}$.

Furthermore, it follows from our observations above that when d is even, the group $V_d(\mathbb{F}_q)$ is isomorphic to a subgroup of $A'(\mathbb{F}_{q^{d/2}})$, where A' is the quadratic twist of A over $\mathbb{F}_{q^d}$; that is, a variety defined over $\mathbb{F}_{q^d}$ that is isomorphic to A over $\mathbb{F}_{q^{2d}}$. If d is a power of 2 then this subgroup is the entire group $A'(\mathbb{F}_{q^{d/2}})$.

Proposition 3.6. *Let A be an ordinary, absolutely simple abelian variety over $\mathbb{F}_q$. Let $K = \mathrm{End}(A)\otimes\mathbb{Q}$. The primitive subgroup $V_d(A)$ is simple if and only if $K \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$.*

Diem [9, Theorem 5] proves the statement using representation theory; we give an alternative proof.

Proof. Let α be the q-power Frobenius element of A (so $K = \mathbb{Q}(\alpha)$) and let ζ be a primitive dth root of unity. Since α^d is the q^d-power Frobenius element of A, our hypotheses on A imply that $\mathbb{Q}(\alpha^d)$ has degree $2\cdot\dim A$, and therefore $\mathbb{Q}(\alpha^d) = \mathbb{Q}(\alpha)$.

Since $\mathbb{Q}(\alpha^d) \subset \mathbb{Q}(\zeta\alpha)$, this implies that $\alpha \in \mathbb{Q}(\zeta\alpha)$ and thus $\mathbb{Q}(\zeta\alpha) = \mathbb{Q}(\zeta, \alpha)$. Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois, we have

$$[\mathbb{Q}(\zeta\alpha) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta) : \mathbb{Q}][\mathbb{Q}(\alpha) : \mathbb{Q}]}{[\mathbb{Q}(\zeta) \cap \mathbb{Q}(\alpha) : \mathbb{Q}]} = \frac{2 \cdot \dim A \cdot \varphi(d)}{[\mathbb{Q}(\zeta) \cap \mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

By Proposition 3.4, the algebraic integer $\zeta\alpha$ is a root of $f_{V_d,q}$, which has degree $2 \cdot \dim A \cdot \varphi(d)$. We conclude that $f_{V_d,q}$ is irreducible, and thus $V_d(A)$ is simple, if and only if $\mathbb{Q}(\zeta) \cap \mathbb{Q}(\alpha) = \mathbb{Q}$. □

We will use the result $\mathbb{Q}(\zeta\alpha) = \mathbb{Q}(\zeta, \alpha)$ in subsequent proofs, so we state it here as a lemma.

Lemma 3.7. *Let A be an abelian variety over $\mathbb{F}_q$. Let α be the q-power Frobenius endomorphism of A, and let ζ be a root of unity. If A is ordinary and absolutely simple, then $\mathbb{Q}(\zeta\alpha) = \mathbb{Q}(\zeta, \alpha)$.* □

In the case of elliptic curves we can determine the structure of V_d precisely in the cases where it splits; see also [9, Corollary 8].

Proposition 3.8. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve, and let $d \geq 3$ be an integer. Let $K = \mathrm{End}(E) \otimes \mathbb{Q}$. If $K \subset \mathbb{Q}(\zeta_d)$, then $V_d(E)$ is isogenous to the product of two simple, non-isogenous abelian varieties of dimension $\varphi(d)/2$.*

Proof. Let $\alpha \in K$ be a root of $f_{E,q}$. By Proposition 3.4 the roots of $f_{V_d,q}$ are $\{\alpha\zeta_d^i, \overline{\alpha}\zeta_d^i\}$ for $1 \leq i \leq d$ with $(i, d) = 1$. If these are not all distinct then $\alpha/\overline{\alpha} = \alpha^2/q$ is a root of unity and therefore E is supersingular, a contradiction. By Lemma 3.7 we have $\mathbb{Q}(\alpha\zeta_d) = \mathbb{Q}(\alpha, \zeta_d) = \mathbb{Q}(\zeta_d)$. Thus $\alpha\zeta_d$ is a q-Weil number of degree $\varphi(d)$. It follows from Theorem 2.1 that $V_d(E)$ is isogenous to the product of two simple abelian varieties of dimension $\varphi(d)/2$. Since the roots of $f_{V_d,q}$ are distinct these factors are not isogenous. □

4. Non-simple abelian surfaces.

We now give some examples of genus 2 curves whose Jacobians are isogenous over an extension field to a product of isomorphic elliptic curves. We will see that in certain cases, the Jacobians of these curves realize, up to isogeny, the primitive subgroups discussed in the previous section.

In the following we let K be a perfect field of characteristic not equal to 2 or 3. Our first example was described by Satoh [27] and Gaudry and Schost [19, Section 4]; we give an alternative construction that allows us to determine explicitly the field of definition of the various maps.

Proposition 4.1. *Let $C : y^2 = x^5 + ax^3 + bx$ be a hyperelliptic curve over K, let $c = a/\sqrt{b} \in \overline{K}$, and let $i \in \overline{K}$ be a primitive fourth root of unity. Then $\mathrm{Jac}(C)$ is isogenous over $K(b^{1/4}, i)$ to $E \times E$, where*

$$E : y^2 = (c + 2)u^3 - (3c - 10)u^2 + (3c - 10)u - (c + 2) \tag{4.1}$$

is an elliptic curve defined over $K(b^{1/2})$ with

$$j(E) = 2^6 \frac{(3c - 10)^3}{(c - 2)(c + 2)^2}. \tag{4.2}$$

Proof. The curve C is isomorphic to $C' : y^2 = x^5 + cx^3 + x$ by the map $\phi : (x, y) \mapsto (b^{1/4}x, b^{5/8}y)$. The map ϕ is defined over $K(b^{1/8})$, and the curve C' is defined over $K(b^{1/2})$. Writing C' in weighted projective coordinates $[x : y : z]$ and substituting $u = (x + z)/2$, $v = (x - z)/2$ gives a map ρ defined over K to the curve

$$C'' : y^2 = (c + 2)u^6 - (3c - 10)u^4v^2 + (3c - 10)u^2v^4 - (c + 2)v^6,$$

which is also defined over $K(b^{1/2})$. The functions $\psi_1 : [u : y : v] \mapsto [u^2 : y : v^2]$ and $\psi_2 : [u, y, v] \mapsto [v^2 : iy : u^2]$ give maps from C'' to E defined over K and $K(i)$, respectively. Thus the map $\psi_1\rho\phi \times \psi_2\rho\phi : C \to E \times E$ is defined over $K(b^{1/8}, i)$ and induces an isogeny $\lambda : \mathrm{Jac}(C) \to E \times E$. The discriminant of E is $(c - 2)(c + 2)^2$; the fact that C is nonsingular implies $c \neq \pm 2$ and thus E is nonsingular. The calculation of $j(E)$ is straightforward. $\square$

We now consider an analogous family of degree 6 curves. These curves have also been studied by Duursma and Kiyavash [10, Section 4.2] and Gaudry and Schost [19, Section 3]. As before, our construction allows us to keep track of the field of definition over which the various maps are defined.

Proposition 4.2. *Let $C : y^2 = x^6 + ax^3 + b$ be a hyperelliptic curve over K, let $c = a/\sqrt{b} \in \overline{K}$, and let $\zeta_3 \in \overline{K}$ be a primitive cube root of unity. Then $\mathrm{Jac}(C)$ is isogenous over $K(b^{1/6}, \zeta_3)$ to $E \times E$, where*

$$E : y^2 = (c + 2)u^3 - (3c - 30)u^2 + (3c + 30)u - (c - 2) \tag{4.3}$$

is an elliptic curve defined over $K(b^{1/2})$ with

$$j(E) = 2^8 3^3 \frac{(2c - 5)^3}{(c - 2)(c + 2)^3}. \tag{4.4}$$

Proof. The curve C is isomorphic to $C' : y^2 = x^6 + cx^3 + 1$ by the map $\phi\colon (x, y) \mapsto (b^{1/6}x, b^{1/2}y)$. The map ϕ is defined over $K(b^{1/6})$, and the curve C' is defined over $K(b^{1/2})$. Writing C' in weighted projective coordinates $[x : y : z]$ and substituting $u = (x + z)/2$, $v = (x - z)/2$ gives a map ρ defined over K to the curve

$$C'' : y^2 = (c + 2)u^6 - (3c - 30)u^4v^2 + (3c + 30)u^2v^4 - (c - 2)v^6,$$

with C'' also defined over $K(b^{1/2})$. The function $\psi_1\colon [u : y : v] \mapsto [u^2 : y : v^2]$ maps C'' to E. The discriminant of E is $(c - 2)(c + 2)^3$; the fact that C is nonsingular implies $c \neq \pm 2$ and thus E is nonsingular. The calculation of $j(E)$ is straightforward.

Let E_c be the elliptic curve of (4.3), parametrized by c. Then the function $\psi_2\colon [u : y : v] \mapsto [v^2 : y : u^2]$ maps C'' to the elliptic curve E_{-c}. Both ψ_1 and ψ_2 are defined over K. Thus the map $\psi_1\rho\phi \times \psi_2\rho\phi\colon C \to E_c \times E_{-c}$ is defined over $K(b^{1/6})$ and induces an isogeny $\lambda\colon \mathrm{Jac}(C) \to E_c \times E_{-c}$.

It remains to show that E_c and E_{-c} are isogenous over $K(b^{1/6}, \zeta_3)$. By taking the second derivative of the equation for E_c, we find that E_c has rational 3-torsion points at $(1, \pm 8)$. Taking the quotient of E_c by the order-3 subgroup generated by these points gives a curve

$$E'_c : y^2 = x^3 - (3c - 30)x^2 + (3c^2 - 924c - 1860)x - (c^3 + 834c^2 + 30972c + 58616).$$

The curve E'_c is isomorphic to E_{-c} over $K(\zeta_3)$ by the map

$$(x, y) \mapsto \left(\frac{x + 2c + 40}{3c - 6}, -\frac{y}{(3c - 6)\sqrt{-3}} \right).$$

We conclude that E_c and E_{-c} are 3-isogenous over $K(b^{1/6}, \zeta_3)$. □

Remark 4.3. If x^6+ax^3+b has a root in K, then we can move that root to infinity to obtain a degree 5 model for C. In general, arithmetic and pairing operations on a hyperelliptic curve with an imaginary (i.e., odd-degree) model are faster than the same operations on a curve with a real (i.e., even-degree) model, though there have been some recent advances in the latter case [17, 18]. However, to unify our presentation we will continue to use the degree 6 model when working with the curves of Proposition 4.2.

For the remainder of this section we let $K = \mathbb{F}_q$ be a finite field of characteristic greater than 3. Combining Propositions 4.1 and 4.2 with the results of Section 3 gives the following.

Theorem 4.4. *Let $C : y^2 = x^5 + ax^3 + bx$ be a hyperelliptic curve over $\mathbb{F}_q$, and suppose $\mathrm{Jac}(C)$ is ordinary. Let E be the elliptic curve given by (4.1), with $c = a/\sqrt{b}$. If $b \in (\mathbb{F}_q^*)^2 \setminus (\mathbb{F}_q^*)^4$ and $\mathrm{End}(E) \otimes \mathbb{Q} \not\cong \mathbb{Q}(i)$, then $\mathrm{Jac}(C)$ is simple and isogenous over $\mathbb{F}_q$ to $V_4(E)$.*

Proof. The hypothesis on b implies that $i \in \mathbb{F}_q$ and $\mathbb{F}_q(b^{1/8}) = \mathbb{F}_{q^4}$. By Proposition 4.1, $\mathrm{Jac}(C)$ is isogenous over $\mathbb{F}_{q^4}$ to $E \times E$. Let $\phi : C \to C'$, $\rho : C' \to C''$, and $\psi_1, \psi_2 : C'' \to E$ be as in Proposition 4.1. Since $i \in \mathbb{F}_q$, the maps $\psi_1\rho, \psi_2\rho : C' \to E$ are both defined over $\mathbb{F}_q$. Thus the map $\psi_1\rho \times \psi_2\rho : C' \to E \times E$ induces an isogeny from $\mathrm{Jac}(C')$ to $E \times E$ defined over $\mathbb{F}_q$. By Theorem 2.1 we have $f_{\mathrm{Jac}(C'),q}(x) = f_{E,q}(x)^2$.

Write $f_{E,q}(x) = (x-\alpha)(x-\overline{\alpha})$. Since the map $\phi : C \to C'$ is a twist of degree 4, the eigenvalues of Frobenius on $\mathrm{Jac}(C)$ are primitive fourth roots of unity times eigenvalues of Frobenius on $\mathrm{Jac}(C')$. In particular, one of $\pm i\alpha$ is an eigenvalue of Frobenius on $\mathrm{Jac}(C)$, i.e., a root of $f_{\mathrm{Jac}(C),q}$. Since $\mathrm{Jac}(C)$ is ordinary, we may apply Lemma 3.7 to deduce that $\mathbb{Q}(i\alpha) = \mathbb{Q}(i, \alpha)$. Since $\alpha \notin \mathbb{Q}(i)$, the field $\mathbb{Q}(i, \alpha)$ has degree 4 over $\mathbb{Q}$. Thus $f_{\mathrm{Jac}(C),q}$ is a degree 4 polynomial with a root that defines a degree 4 number field, so it is irreducible. By Theorem 2.1, $\mathrm{Jac}(C)$ is simple.

By Proposition 3.1, $\mathrm{Jac}(C)$ is isogenous over $\mathbb{F}_q$ to a subvariety of $X = \mathrm{Res}_{\mathbb{F}_{q^4}/\mathbb{F}_q}(E)$. By equation (3.5), the variety X is isogenous to $V_1(E) \times V_2(E) \times V_4(E)$, where $\dim V_d(E) = \varphi(d)$. Since $\mathrm{Jac}(C)$ is simple, it must be isogenous to $V_4(E)$. □

Theorem 4.5. *Let $C : y^2 = x^6 + ax^3 + b$ be a hyperelliptic curve over $\mathbb{F}_q$, and suppose $\mathrm{Jac}(C)$ is ordinary. Let E be the elliptic curve given by (4.3), with $c = a/\sqrt{b}$. If $b \in (\mathbb{F}_q^*)^2 \setminus (\mathbb{F}_q^*)^6$ and $\mathrm{End}(E) \otimes \mathbb{Q} \not\cong \mathbb{Q}(\zeta_3)$, then $\mathrm{Jac}(C)$ is simple and isogenous over $\mathbb{F}_q$ to $V_3(E)$.*

Proof. The hypothesis on b implies that $\zeta_3 \in \mathbb{F}_q$ and $\mathbb{F}_q(b^{1/6}) = \mathbb{F}_{q^3}$. By Proposition 4.2, $\mathrm{Jac}(C)$ is isogenous over $\mathbb{F}_{q^3}$ to $E \times E$. By Proposition 3.1, $\mathrm{Jac}(C)$ is isogenous over $\mathbb{F}_q$ to a subvariety of $X = \mathrm{Res}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(E)$. By (3.5), X is isogenous to $V_1(E) \times V_3(E)$, where $V_d(E)$ has dimension $\varphi(d)$. Since $\mathrm{End}(E) \otimes \mathbb{Q} \not\cong \mathbb{Q}(\zeta_3)$, $V_3(E)$ is simple by Proposition 3.6. Since $\mathrm{Jac}(C)$ is two-dimensional, it must be isogenous to $V_3(E)$. □

In both of the above cases, the condition that $\mathrm{Jac}(C)$ is ordinary is easy to test: if $\mathrm{Jac}(C)$ is not ordinary then the elliptic curve E given by (4.1) or (4.3) is supersingular and has $q + 1 - t$ points over $\mathbb{F}_q$, with $t \in \{0, \pm\sqrt{q}, \pm 2\sqrt{q}\}$ (since

$\operatorname{char}\mathbb{F}_q > 3$). Choosing a random point $P \in E(\mathbb{F}_q)$ and multiplying by the possible group order(s) will quickly determine whether E, and thus $\operatorname{Jac}(C)$, is ordinary.

If b is not a square, we can perform the same analysis as in Theorems 4.4 and 4.5, but in this case we see from (4.2) and (4.4) that the elliptic curve E usually has j-invariant outside of $\mathbb{F}_q$. In the cases where $j(E) \in \mathbb{F}_q$, we have the following results:

Proposition 4.6. *Let $C : y^2 = x^5 + ax^3 + bx$ be a hyperelliptic curve over $\mathbb{F}_q$, and let $p = \operatorname{char}\mathbb{F}_q$. Let E be the elliptic curve given by* (4.1) *(with $c = a/\sqrt{b}$). If $b \notin (\mathbb{F}_q^*)^2$ and $j(E) \in \mathbb{F}_q$, then one of the following holds:*

1. *$a = 0$, $j(E) = 8000$, and* $\operatorname{Jac}(C)$ *is:*
   - *supersingular, if $p \equiv 5, 7 \pmod 8$.*
   - *ordinary, simple, and isogenous to $V_4(E)$, if $q \equiv 3 \pmod 8$, or*
   - *ordinary, simple, and isogenous to a subvariety of $V_8(E)$, otherwise.*
2. *$a/\sqrt{b} = \pm\frac{10}{9}\sqrt{-7}$, $j(E) = -3375$, and* $\operatorname{Jac}(C)$ *is supersingular.*

Proof. Set $c = a/\sqrt{b}$ and let $j(c)$ denote the right hand side of (4.2). Since the nontrivial element $\sigma \in \operatorname{Gal}(\mathbb{F}_q(\sqrt{b})/\mathbb{F}_q)$ satisfies $\sigma(\sqrt{b}) = -\sqrt{b}$ (and thus $\sigma(c) = -c$), solving $j(c) = j(-c)$ gives all values of c for which $j(c) \in \mathbb{F}_q$. We find the solutions $\{0, \pm 2, \pm\frac{10}{9}\sqrt{-7}\}$. The solutions $c = \pm 2$ give singular curves so we can ignore them.

If $c = 0$, then Propositions 4.1 and 3.1 imply that $j(E) = 8000$ and $\operatorname{Jac}(C)$ is isogenous over $\mathbb{F}_q$ to a subvariety of $\operatorname{Res}_{\mathbb{F}_{q^8}/\mathbb{F}_q}(E)$. Since C is isomorphic over $\overline{\mathbb{F}}_q$ to the curve $y^2 = x^5 + x$, we can apply [15, Theorem 3] to conclude that $\operatorname{Jac}(C)$ is ordinary if $p \equiv 1, 3 \pmod 8$ and supersingular otherwise. In the ordinary case the fact that $j(E) = 8000$ implies $\operatorname{End}(E) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{-2})$.

Let C' be as in Proposition 4.1. If $q \equiv 1 \pmod 8$ then $\mathbb{F}_q(b^{1/8}, i) = \mathbb{F}_{q^8}$. In this case C' is a degree 8 twist of C and $\operatorname{Jac}(C')$ is isogenous over $\mathbb{F}_q$ to $E \times E$. If $f_{E,q}(x) = (x - \alpha)(x - \overline{\alpha})$, then there is some primitive 8th root of unity $\zeta_8 \in \overline{\mathbb{Q}}$ such that $\zeta_8\alpha$ is an eigenvalue of Frobenius for $\operatorname{Jac}(C)$, i.e., a root of $f_{\operatorname{Jac}(C),q}$. Since $\operatorname{Jac}(C)$ is ordinary, we may apply Lemma 3.7 to deduce that $\mathbb{Q}(\zeta_8\alpha) = \mathbb{Q}(\zeta_8, \alpha) = \mathbb{Q}(\zeta_8)$, with the last equality following from $\alpha \in \mathbb{Q}(\sqrt{-2}) \subset \mathbb{Q}(\zeta_8)$. Taking the $\operatorname{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$-conjugates of $\zeta_8\alpha$, we see that

$$f_{\operatorname{Jac}(C),q} = (x - \zeta_8\alpha)(x - \zeta_8^3\alpha)(x - \zeta_8^5\overline{\alpha})(x - \zeta_8^7\overline{\alpha}).$$

It follows from Proposition 3.4 that $f_{\operatorname{Jac}(C),q}$ divides $f_{V_8(E),q}$, and thus $\operatorname{Jac}(C)$ is isogenous to a subvariety of $V_8(E)$. By Proposition 3.8, $\operatorname{Jac}(C)$ is simple.

If $q \equiv 3 \pmod 4$, then $\mathbb{F}_q(b^{1/8}, i) = \mathbb{F}_{q^4}$. In this case $\operatorname{Jac}(C')$ is isogenous over $\mathbb{F}_q$ to $E \times E'$, where E and E' are quadratic twists of each other. Let α be an eigenvalue of Frobenius for E; then $-\alpha$ is an eigenvalue of Frobenius for E'. Since C and C' are degree 4 twists of each other, one of $\pm i\alpha$ is an eigenvalue of Frobenius for $\operatorname{Jac}(C')$. Continuing the analysis as in Theorem 4.4, we conclude that $\operatorname{Jac}(C)$ is simple and isogenous to $V_4(E)$.

Finally, if $c = \pm\frac{10}{9}\sqrt{-7}$ then from (4.2) we have $j(E) = -3375$, so E is the reduction of the curve over $\mathbb{Q}$ with CM by $\mathbb{Z}[\sqrt{-7}]$ (see [28, Section A.3]). If $c = 0$ then $p = 5$ or 7 and $\operatorname{Jac}(C)$ is supersingular by the analysis above. If $c \neq 0$ then our assumption on b implies that -7 is a non-square in $\mathbb{F}_q^*$, and therefore p is inert in $\mathbb{Q}(\sqrt{-7})$. By a standard result of CM theory (see [23, Theorem 13.12]), this implies that E is supersingular, and thus $\operatorname{Jac}(C)$ is as well. $\square$

Remark 4.7. If $a = 0$ and $q \equiv 1 \pmod 4$ we have obtained the "Type I" case of Kawazoe and Takahashi [21], while if $a = 0$ and $q \equiv 3 \pmod 4$ we have obtained the "Type II" case. Further analysis of the special case $a = 0$, including a formula for $f_{\mathrm{Jac}(C),q}$ in terms of b and q only, can be found in [15].

Proposition 4.8. *Let $C : y^2 = x^6 + ax^3 + b$ be a hyperelliptic curve over $\mathbb{F}_q$. Let E be the elliptic curve given by* (4.3) *(with $c = a/\sqrt{b}$). If $b \notin (\mathbb{F}_q^*)^2$ and $j(E) \in \mathbb{F}_q$, then one of the following holds:*

(1) *$a = 0$, $j(E) = 54000$, and either* $\mathrm{Jac}(C)$ *is supersingular or* $\mathrm{Jac}(C)$ *is ordinary and not simple;*
(2) *$a/\sqrt{b} = \pm 5\sqrt{-2}$, $j(E) = 8000$, and* $\mathrm{Jac}(C)$ *is supersingular; or*
(3) *$a/\sqrt{b} = \pm\frac{1}{2}\sqrt{-11}$, $j(E) = -32768$, and* $\mathrm{Jac}(C)$ *is supersingular.*

Proof. We set $c = a/\sqrt{b}$ and let $j(c)$ be defined by the right hand side of (4.4). The solutions to $j(c) = j(-c)$ are $\{0, \pm 2, \pm 5\sqrt{-2}, \pm\frac{1}{2}\sqrt{-11}\}$. The solutions $c = \pm 2$ give singular curves so we can ignore them.

If $c = 0$, then Propositions 4.2 and 3.1 imply that $\mathrm{Jac}(C)$ is isogenous to a subvariety of $\mathrm{Res}_{\mathbb{F}_{q^6}/\mathbb{F}_q}(E')$ with $j(E') = 54000$. If E' is supersingular then $\mathrm{Jac}(C)$ is supersingular. If E' is ordinary then $\mathrm{End}(E') \otimes \mathbb{Q} \cong \mathbb{Q}(\zeta_3)$ (see [28, Section A.3]). Thus by Proposition 3.8 $V_3(E)$ and $V_6(E)$ are not simple, and thus $\mathrm{Jac}(C)$ is ordinary and not simple.

If $c = \pm 5\sqrt{-2}$ or $c = \pm\frac{1}{2}\sqrt{-11}$ then we can perform the same analysis as in case (2) of Proposition 4.6. If $c \neq 0$ then in both cases E is the reduction of a curve over $\mathbb{Q}$ with CM by $\mathbb{Z}[\sqrt{-D}]$ with $-D$ a non-square in $\mathbb{F}_q^*$, so $\mathrm{Jac}(C)$ is supersingular. If $c = 0$ then either p $(= \operatorname{char}\mathbb{F}_q) = 5$ and $j(E) = 0$, or $p = 11$ and $j(E) = 1728$. In both cases the curve E has an automorphism that does not commute with the p-power Frobenius endomorphism, so E is supersingular. $\square$

5. Constructing Pairing-Friendly Curves

We now turn our attention to constructing pairing-friendly abelian varieties, which informally are abelian varieties that have small embedding degree with respect to a large prime-order subgroup. We call a curve pairing-friendly if its Jacobian is so. We first define the embedding degree, which is the degree of the field extension of $\mathbb{F}_q$ in which the Weil and Tate pairings take their values.

Definition 5.1. *Let A be an abelian variety defined over $\mathbb{F}_q$, where $q = p^m$ for some prime p and integer m. Let $r \neq p$ be a prime dividing $\#A(\mathbb{F}_q)$. The* embedding degree of A with respect to r *is the smallest integer k such that r divides $q^k - 1$.*

Let A be a simple (though not necessarily absolutely simple) abelian variety over $\mathbb{F}_q$. Let π be the Frobenius endomorphism of A; we will also use π to refer to a root of $f_{A,q}$. From this point on we will assume that $K = \mathbb{Q}(\pi)$ is the full endomorphism algebra $\mathrm{End}(A) \otimes \mathbb{Q}$; in particular, this is the case when A is ordinary. Under these assumptions, we have $[K : \mathbb{Q}] = 2 \cdot \dim A$ (see Theorem 2.1), and the number of $\mathbb{F}_q$-rational points of A is given by

$$\#A(\mathbb{F}_q) = f_{A,q}(1) = \mathrm{N}_{K/\mathbb{Q}}(\pi - 1).$$

We can thus express the conditions for A being pairing-friendly as follows.

Proposition 5.2. *Let $A/\mathbb{F}_q$ be a simple abelian variety with Frobenius endomorphism π, and assume $K = \mathbb{Q}(\pi)$ equals $\mathrm{End}(A) \otimes \mathbb{Q}$. Let k be a positive integer, let Φ_k be the kth cyclotomic polynomial, and let r be a prime not dividing kq. If*

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

then A has embedding degree k with respect to r. □

It follows from Proposition 5.2 that the property of being pairing-friendly depends only on the isogeny of class of A.

The following theorem relates the "pairing-friendliness" properties of elliptic curves over extension fields and primitive subgroups of Weil restrictions.

Proposition 5.3. *Let A be an ordinary, simple abelian variety defined over a finite field $\mathbb{F}_q$. Let r be prime and k, d be integers with $r \nmid kq$. Assume that*

(1) *d is the smallest integer such that $A(\mathbb{F}_{q^d})$ has a point of order r, and*
(2) *$\Phi_k(q) \equiv 0 \pmod{r}$.*

Then A base extended to $\mathbb{F}_{q^d}$ has embedding degree $k/\gcd(k,d)$ with respect to r, and $V_d/\mathbb{F}_q$ has embedding degree k with respect to r.

Proof. Assumption (1) implies that $V_d(\mathbb{F}_q)$ has a point of order r. Assumption (2) thus implies directly that $V_d/\mathbb{F}_q$ has embedding degree k with respect to r. Furthermore, one can show (see e.g. [26, Lemma 5.2]) that $\Phi_k(x)$ divides $\Phi_{k/\gcd(k,d)}(x^d)$ as polynomials. Given this fact, assumption (2) implies that $\Phi_k(q^d) \equiv 0 \pmod{r}$, and thus $A/\mathbb{F}_{q^d}$ has embedding degree $k/\gcd(k,d)$ with respect to r. □

Remark 5.4. If $A/\mathbb{F}_q$ has embedding degree k with respect to r and q is not prime, then the Weil and Tate pairings on E may take values in a proper subfield of $\mathbb{F}_{q^k}$, called the *minimal embedding field* [20]. If $p = \mathrm{char}(\mathbb{F}_q)$, then the minimal embedding field is $\mathbb{F}_p(\zeta_r)$. In this case, the security of cryptosystems based on A will be determined not by the embedding degree but by the size of the minimal embedding field. For example, if A is as in Proposition 5.3 and $d \nmid k$, then $A/\mathbb{F}_{q^d}$ has embedding degree $k' = k/\gcd(k,d)$ but the minimal embedding field is $\mathbb{F}_{q^k}$, which is a proper subfield of $\mathbb{F}_{(q^{k'd})}$. For the remainder of our discussion we will have q prime and $d \mid k$, so we may safely continue to work with the embedding degree only.

Combining Proposition 5.3 with the results of Section 3.1, we see that for any integer d, we can construct simple pairing-friendly abelian varieties $V_d/\mathbb{F}_q$ of dimension $\varphi(d)$ (or dimension $\varphi(d)/2$ if $\mathrm{End}(E) \otimes \mathbb{Q} \subset \mathbb{Q}(\zeta_d)$) by constructing elliptic curves $E/\mathbb{F}_q$ that become pairing-friendly when base extended to $\mathbb{F}_{q^d}$. In general the variety V_d will not be the Jacobian of a curve, so one will have to use the "compression" technique of Rubin and Silverberg [26, Section 10] to do arithmetic on V_d.

However, in Theorems 4.4 and 4.5 and Proposition 4.6 we have seen explicit examples of genus 2 curves whose Jacobians are isogenous to a subvariety of V_d for $d = 4$, 3, and 8, respectively. If we start with an elliptic curve over $\mathbb{F}_q$ whose base-extension to $\mathbb{F}_{q^d}$ is pairing-friendly, then we can work backwards from $j(E)$ to find the equation for a curve C whose Jacobian is simple and pairing-friendly.

5.1. **Elliptic curves whose base extensions are pairing-friendly.** We now turn to the problem of constructing an elliptic curve E that has the two properties given in Proposition 5.3. Fix a prime r and integers k, d with $d \mid k$. Let K be a quadratic imaginary field and let $\pi \in K$ be the Frobenius endomorphism of $E/\mathbb{F}_q$. Suppose further that r splits in $\mathcal{O}_K$. We consider each property of Proposition 5.3 in turn:

Condition (1) holds if and only if $\mathrm{N}_{K/\mathbb{Q}}(\pi^d - 1) \equiv 0 \pmod{r}$ and $\mathrm{N}_{K/\mathbb{Q}}(\pi^e - 1) \not\equiv 0 \pmod{r}$ for all $e < d$. These two conditions, in turn, hold if and only if there is a prime $\mathfrak{r}$ of $\mathcal{O}_K$ over r such that $\pi^d \equiv 1 \pmod{\mathfrak{r}}$ and both $\pi^e \not\equiv 1$ and $\overline{\pi}^e \not\equiv 1 \pmod{\mathfrak{r}}$ for all $e < d$. It follows that we must have

$$\pi \equiv \zeta_d \pmod{\mathfrak{r}} \tag{5.1}$$

for some primitive dth root of unity $\zeta_d \in \mathbb{F}_r$ and some prime $\mathfrak{r} \mid r$ in $\mathcal{O}_K$.

Condition (2) holds if and only if $\pi\overline{\pi}$ is a primitive kth root of unity ζ_k mod r; without loss of generality we may assume that this congruence is modulo the same $\mathfrak{r}$ as above. This implies that

$$\overline{\pi} \equiv \zeta_k/\zeta_d \pmod{\mathfrak{r}}. \tag{5.2}$$

Since condition (1) requires $\overline{\pi}^e \not\equiv 1 \pmod{\mathfrak{r}}$ for all $e < d$, we must also require that the order of ζ_k/ζ_d be at least d. The order of ζ_k/ζ_d may depend on the specific kth and dth roots of unity chosen, but if we assume $k > d$ then ζ_k/ζ_d always has order k.

We can use the congruences (5.1) and (5.2) as the basis for either a Cocks-Pinch type algorithm or a Brezing-Weng type algorithm to construct π. The former has the advantage of applying to arbitrary embedding degree k and imposing few conditions on the subgroup size r; the latter has the advantage of producing smaller field sizes q relative to r for certain embedding degrees k and a more restricted set of subgroup sizes r.

Our first algorithm is based on Freeman, Stevenhagen, and Streng's generalization of the Cocks-Pinch algorithm [13], and is as follows:

Algorithm 5.5. Input: integers k, d with $d \mid k$ and $d < k$, a quadratic imaginary field K, and a real number b. Output: a q-Weil number $\pi \in K$, with q prime, and a prime r.

(1) Choose a prime $r > 2^b$ such that $r \equiv 1 \pmod{k}$, $r > 2\,\mathrm{disc}(\mathcal{O}_K)$, and r splits in $\mathcal{O}_K$.
(2) Choose a primitive kth root of unity $\zeta_k \in \mathbb{F}_r$ and a primitive dth root of unity $\zeta_d \in \mathbb{F}_r$.
(3) Write $r\mathcal{O}_K = \mathfrak{r}\overline{\mathfrak{r}}$.
(4) Compute a $\pi \in \mathcal{O}_K$ such that
$$\pi \equiv \zeta_d \pmod{\mathfrak{r}}, \quad \pi \equiv \zeta_k/\zeta_d \pmod{\overline{\mathfrak{r}}}$$
and $q = \pi\overline{\pi}$ is prime.
(5) Output π and r.

The method of Brezing and Weng [6] has the same structure as the Cocks-Pinch algorithm, except we replace the ring of integers $\mathcal{O}_K$ with the polynomial ring $K[x]$. The algorithm generates polynomials $\pi(x)$ and $r(x)$ and searches for values of x for which $q(x) = \pi(x)\overline{\pi}(x)$ is prime and $r(x)$ is prime or has a large prime factor.

For this to be possible $q(x)$ must satisfy certain conditions, incorporated in the following definition.

Definition 5.6. *Let $f(x) \in \mathbb{Q}[x]$ be a non-constant, irreducible polynomial with positive leading coefficient. We say f is a* Bateman-Horn polynomial *if (1) $f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$, and (2) $\gcd(\{f(x) : x, f(x) \in \mathbb{Z}\}) = 1$.*

Definition 5.6 derives its nomenclature from the conjecture of Bateman and Horn [2], which says that if $f \in \mathbb{Q}[x]$ satisfies conditions (1) and (2), then $f(x)$ takes on an infinite number of prime values, and furthermore gives a heuristic asymptotic formula for the number of prime values. In previous work (e.g. [12, 11]) such a polynomial was said to *represent primes*. Since it is not known whether any such polynomial of degree at least 2 does in fact take an infinite number of prime values, some may find this terminology misleading.

Our algorithm is based on Freeman's generalization of the Brezing-Weng algorithm [11], and is as follows:

Algorithm 5.7. Input: integers k, d with $d \mid k$ and $d < k$, a quadratic imaginary field K, and a real number b. Output: a q-Weil number $\pi \in K$, with q prime, and a prime r.

(1) Choose an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ such that $L = \mathbb{Q}[x]/(r(x))$ contains K and a primitive kth root of unity.
(2) Choose a primitive kth root of unity $\zeta_k \in L$ and a primitive dth root of unity $\zeta_d \in L$.
(3) Write $r(x) = \mathfrak{r}(x)\overline{\mathfrak{r}(x)}$ in $K[x]$.
(4) Compute a $\pi(x) \in K[x]$ such that

$$\pi(x) \equiv \zeta_d \bmod \mathfrak{r}(x), \quad \pi(x) \equiv \zeta_k/\zeta_d \bmod \overline{\mathfrak{r}(x)}$$

and $q(x) = \pi(x)\overline{\pi}(x) \in \mathbb{Q}[x]$ is a Bateman-Horn polynomial.
(5) Find an integer x_0 such that $\pi(x_0)\overline{\pi(x_0)}$ is prime and $r(x_0)$ has a prime factor greater than $\max(2^b, 2\,\mathrm{disc}(\mathcal{O}_K))$.
(6) Output $\pi(x_0)$ and the largest prime factor of $r(x_0)$.

If $\pi(x)$ and $r(x)$ are as produced by Algorithm 5.7, we say that $(\pi(x), r(x))$ *parametrizes a family of pairing-friendly Frobenius elements*, and we often refer to $(\pi(x), r(x))$ as a *family*.

Theorem 5.8. *Suppose π, r are output by Algorithm 5.5 or 5.7, on inputs k, d, and K. Let $q = \pi\overline{\pi}$ and assume $r \neq q$. Let $E/\mathbb{F}_q$ be an elliptic curve with Frobenius endomorphism π. Then E is ordinary, E base extended to $\mathbb{F}_{q^d}$ has embedding degree k/d with respect to r, and $V_d(E)$ has embedding degree k with respect to r.*

Furthermore, if d is even then the quadratic twist of E over $\mathbb{F}_{q^{d/2}}$ has embedding degree $2k/d$ with respect to r.

Proof. To prove the statements in the first paragraph it suffices to show that E satisfies the hypotheses of Proposition 5.3. To start, the assumption $r > 2\,\mathrm{disc}(K)$ implies that $q > \mathrm{disc}(K)$, and thus q is unramified in $\mathcal{O}_K$. Since q is prime, the curve E is supersingular if and only if $\pi = \pm\sqrt{-q}$, so we deduce that E is ordinary. Since E is an elliptic curve it is necessarily simple. Next, in both cases we have $r \equiv 1 \pmod{k}$ and thus $r \nmid k$, and by assumption $r \nmid q$. By construction, since $r \nmid d$ and $k > d$, d is the smallest integer such that $\mathrm{N}_{K/\mathbb{Q}}(\pi^d - 1) \equiv 0 \pmod{r}$ and thus the smallest integer such that $E(\mathbb{F}_{q^d})$ has a point of order r. Finally, the fact that

$\Phi_k(q) \equiv 0 \pmod r$ follows immediately from the construction. The "furthermore" statement follows from Remark 3.5. □

Remark 5.9. The "furthermore" clause of Theorem 5.8 shows that when $d = 4$, we can use our algorithms to construct pairing-friendly elliptic curves of the type considered by Galbraith, Lin, and Scott [16], i.e., curves E over $\mathbb{F}_{q^2}$ with $j(E) \in \mathbb{F}_q$. This answers an open question posed by Benger et al. [3, Section 5].

Let π be a q-Weil number output by Algorithm 5.5 or 5.7. We can use the *complex multiplication method* (or *CM method*) to construct an ordinary elliptic curve E with Frobenius endomorphism π. This method, developed originally by Atkin and Morain [1], constructs an elliptic curve $\mathcal{E}$ whose endomorphism ring is isomorphic to a given order $\mathcal{O}$ in a quadratic imaginary field K. If H is the Hilbert class field of $\mathcal{O}$ then $j(\mathcal{E}) \in H$. Since $\mathfrak{p} = (\pi)$ is a principal degree one prime of K over q, the prime $\mathfrak{p}$ splits completely in H. It follows that $\mathcal{E}$ has good ordinary reduction at all primes of H over $\mathfrak{p}$, any reduction E' also has endomorphism ring isomorphic to $\mathcal{O}$, and the Frobenius endomorphism of any such E' is equal to $\zeta\pi$ for some root of unity $\zeta \in \mathcal{O}$. (See [7, Section 3] for further details.)

This discussion leads naturally to the issue of twisting. Algorithms 5.5 and 5.7 produce q-Weil numbers π, but the CM method produces an elliptic curve E' whose Frobenius endomorphism is $\zeta\pi$ for some root of unity ζ. The curve E is a degree e twist of E', where e is the order of ζ. Thus for any order $\mathcal{O} \neq \mathbb{Z}[i]$ or $\mathbb{Z}[\zeta_3]$, the desired curve E is isomorphic to the constructed curve E' over at most a quadratic extension of $\mathbb{F}_q$. In this case the integer e is usually determined by taking a random point $P \in E'$ and multiplying it by $(p + 1 - \mathrm{Tr}_{K/\mathbb{Q}}(\pi))$. If the result is O then $e = 1$; otherwise $e = 2$. (Rubin and Silverberg [25] have offered an alternative, deterministic method for determining the correct twist.)

We will return to the special cases of $\mathcal{O} = \mathbb{Z}[i]$ or $\mathbb{Z}[\zeta_3]$ in Section 5.4 below. For now we note the following result, which we will apply when we use the outputs of Algorithms 5.5 or 5.7 to construct pairing-friendly curves of the types discussed in Section 4.

Proposition 5.10. *Suppose E and E' are elliptic curves over $\mathbb{F}_q$ that are quadratic twists of each other.*

(1) *If $4 \mid d$, then $V_d(E)$ is isogenous over $\mathbb{F}_q$ to $V_d(E')$.*
(2) *If d is odd, then $V_d(E)$ and $V_d(E')$ are quadratic twists of each other.*

Proof. If π and π' are the Frobenius elements of E and E' respectively, then since E and E' are quadratic twists of each other we have $\pi = -\pi'$. The statement now follows from Proposition 3.4 and properties of cyclotomic polynomials. □

5.2. **Constructing pairing-friendly genus 2 curves.** In the previous section we showed how to construct the Frobenius element of an elliptic curve E such that $V_d(E)$ is pairing-friendly for a given d. If $\varphi(d) = 2$, then $V_d(E)$ is isogenous to the Jacobian of a genus 2 curve. We now describe step-by-step the method for finding a curve whose Jacobian is isogenous to $V_d(E)$.

Again let K be a quadratic imaginary field and let $\pi \in K$ be output by Algorithm 5.5 or 5.7, with $q = \pi\overline{\pi}$ prime. Let E be an elliptic curve over $\mathbb{F}_q$ with Frobenius endomorphism π. For future reference, we let j_0 be the j-invariant of E. By construction, E satisfies conditions (1) and (2) of Proposition 5.3, and therefore $V_d(E)$ has embedding degree k with respect to r. If $V_d(E)$ is simple let $A = V_d(E)$;

if $V_d(E)$ is not simple let A be the simple factor of $V_d(E)$ that has a point of order r.

We now consider the case where A has dimension 2. By Propositions 3.6 and 3.8, this occurs if and only if

$$[\mathbb{Q}(\zeta_d) : \mathbb{Q}(\zeta_d) \cap K] = 2. \tag{5.3}$$

In most cases where (5.3) holds, we can use the following algorithm to construct a genus 2 curve whose Jacobian is isogenous over $\mathbb{F}_q$ to $V_d(E)$.

Algorithm 5.11. Input: a q-Weil number $\pi \in K$, where $q \equiv 1 \pmod{d}$ is prime and K is a quadratic imaginary field; and an integer $d \in \{3, 4, 8\}$, with $d = 8$ only allowed if $K = \mathbb{Q}(\sqrt{-2})$. Output: a genus 2 curve over $\mathbb{F}_q$ or the symbol $\perp$.

(1) Use the CM method to find the j-invariant j_0 of an ordinary elliptic curve $E/\mathbb{F}_q$ with $\mathrm{End}(E) \cong \mathcal{O}_K$.
(2) Compute $c \in \mathbb{F}_q$ satisfying equation (4.2) (if $d = 4, 8$) or (4.4) (if $d = 3$) with $j(E) = j_0$. If there is no such $c \in \mathbb{F}_q$, output $\perp$ and terminate.
(3) Choose $a, b \in \mathbb{F}_q$ such that
   - a/c is a nonsquare, $b = (a/c)^2$, if $d = 4$ and $c \neq 0$;
   - $a = 0$, b is a square and not a fourth power, if $d = 4$ and $c = 0$;
   - $a = 0$, b is a nonsquare, if $d = 8$;
   - a/c is a noncube, $b = (a/c)^2$, if $d = 3$.
(4) Define the curve $C : y^2 = x^5 + ax^3 + bx$ (if $d = 4, 8$) or $C : y^2 = x^6 + ax^3 + b$ (if $d = 3$).
(5) If $d = 4$ or 8, output C.
(6) If $d = 3$, do the following:
   (a) Choose a random point $P \in \mathrm{Jac}(C)(\mathbb{F}_q)$.
   (b) Let $n = \Phi_d(\pi)\Phi_d(\overline{\pi})$.
   (c) If $[n]P = O$, output C. Otherwise output a quadratic twist C' of C.

We see from this description that the "Type I" curves of Kawazoe and Takahashi [21] are produced by our algorithm when $K = \mathbb{Q}(\sqrt{-2})$, $d = 4$ or 8, and $c = 0$. The "Type II" curves can be produced by a similar procedure when $K = \mathbb{Q}(\sqrt{-2})$, $d = 4$, and $q \equiv 3 \pmod{4}$: in Step (3) we set $a = 0$ and choose b to be a nonsquare.

Theorem 5.12. *Suppose π, r are output by Algorithm 5.5 or 5.7 on inputs k, d, and K, with K not isomorphic to $\mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$. Assume $\pi\overline{\pi} \neq r$. Suppose Algorithm 5.11 is run on inputs π and d. If the algorithm outputs a curve C, then* $\mathrm{Jac}(C)$ *is ordinary and simple and (with high probability) has embedding degree k with respect to r.*

Proof. The requirement $q \equiv 1 \pmod{d}$ guarantees that we can choose a, b as specified in Step (3). With this choice of a, b, the curve C satisfies the hypotheses of Theorem 4.4 (if $d = 4$), Theorem 4.5 (if $d = 3$), or Proposition 4.6 (if $d = 8$). (The fact that $\mathrm{Jac}(C)$ is ordinary is guaranteed by Theorem 5.8.) It follows from these results that $\mathrm{Jac}(C)$ is isogenous over $\mathbb{F}_q$ to a subvariety of $V_d(E)$, where E is an elliptic curve over $\mathbb{F}_q$ with j-invariant as computed in Step (1). Since K is not isomorphic to $\mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$, any elliptic curve over $\mathbb{F}_q$ with this j-invariant is either E or its quadratic twist E'.

By Theorem 5.8, either $V_d(E)$ or $V_d(E')$ has embedding degree k with respect to r. If $d = 4$ or 8, then by Proposition 5.10, $V_d(E)$ and $V_d(E')$ are isogenous and $\mathrm{Jac}(C)$ necessarily has the stated properties. If $d = 3$, then by Proposition 5.10, either $\mathrm{Jac}(C)$ or $\mathrm{Jac}(C')$ has the stated properties. Testing whether $[n]P = O$ in Step (6) allows us to determine the correct twist with high probability. □

Remark 5.13. If we want to guarantee that Algorithm 5.11 does not output $\perp$ in Step (2), we must ensure that the appropriate equation (4.2) or (4.4) has a root in $\mathbb{F}_q$. To find inputs where this is the case, we substituted j-invariants of CM elliptic curves over $\mathbb{Q}$ into the two equations and determined when the appropriate polynomial has a root c in either $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$. The results appear in the following table:

d	K	j_0	c
3	$\mathbb{Q}(i)$	1728	$7 \pm 3\sqrt{3}$
3	$\mathbb{Q}(\sqrt{-2})$	8000	$\pm 5\sqrt{-2}$
3	$\mathbb{Q}(\sqrt{-11})$	-32768	$\pm\frac{1}{2}\sqrt{-11}$
4	$\mathbb{Q}(\zeta_3)$	0	$\pm\frac{10}{3}$
4	$\mathbb{Q}(\sqrt{-2})$	8000	$0, -\frac{130}{49} \pm \frac{160}{49}\sqrt{2}$
4	$\mathbb{Q}(\sqrt{-7})$	-3375	$\frac{130}{63}, \pm\frac{10}{9}\sqrt{-7}$
8	$\mathbb{Q}(\sqrt{-2})$	8000	0

If we use the values d and K from a row of the table as input to Algorithm 5.5 or 5.7, then we can use the corresponding values of j_0 and c in Steps (1) and (2) of Algorithm 5.11. The facts that π is an ordinary q-Weil number (i.e., $\mathrm{Tr}_{K/\mathbb{Q}}(\pi) \neq 0$) and $q \equiv 1 \pmod{d}$ guarantee that $c \in \mathbb{F}_q$ in each case. (See also Propositions 4.6 and 4.8.)

Note that Theorem 5.12 does not guarantee correctness of Algorithm 5.11 when $(d, K) = (3, \mathbb{Q}(i))$ or $(4, \mathbb{Q}(\zeta_3))$; see Section 5.4 for further discussion.

5.3. **Measuring efficiency: ρ-values.** Let $A/\mathbb{F}_q$ be a g-dimensional abelian variety that has embedding degree k with respect to a subgroup of order r. If we are using A in a cryptographic protocol, then the cryptographic elements (e.g., keys, ciphertexts, signatures) usually include points on $A(\mathbb{F}_q)$, while security depends on the size r of the pairing-friendly subgroup. Since points on $A(\mathbb{F}_q)$ are described in terms of elements of $\mathbb{F}_q$, then to minimize bandwidth and storage space we want q to be as small as possible. Since $\#A(\mathbb{F}_q) = q^g + O(q^{g-1/2})$, the "optimal" size of q is approximately $r^{1/g}$. To measure how far A strays from this optimum, we define a parameter ρ as follows:

$$\rho(A) = \frac{g \log q}{\log r}. \tag{5.4}$$

Now suppose we are given a pair of polynomials $(\pi(x), r(x))$ as in Algorithm 5.7 that parametrize Frobenius elements and group orders. If $\pi \in K[x]$ we set $g = \frac{1}{2}[K : \mathbb{Q}]$ and define

$$\rho(\pi(x), r(x)) = \lim_{x\to\infty} \frac{g \log \pi(x)\overline{\pi}(x)}{\log r(x)} = \frac{2g \deg \pi(x)}{\deg r(x)}.$$

Thus if A is an abelian variety with Frobenius element $\pi(x_0)$, if x_0 is large then $\rho(A) \approx \rho(\pi(x), r(x))$.

We now examine the ρ-values of the abelian varieties produced using Algorithms 5.5 and 5.7. We start with Algorithm 5.5. That algorithm takes as input a CM field $K = \mathbb{Q}(\sqrt{-D})$ and constructs a $\pi = u + v\sqrt{-D} \in \mathcal{O}_K$ with a prescribed residue modulo a factor $\mathfrak{r}$ of r. We have no way *a priori* to control the size of u and v, so heuristically we expect π to be randomly distributed in $\mathcal{O}_K/\mathfrak{r}$. Since $\mathfrak{r}$ has norm r, we expect $|\pi|$ to be on average around the size of r. Thus heuristically we expect $q = \pi\overline{\pi}$ to be roughly the size of r^2. If C is output by Algorithm 5.11 on input π produced by Algorithm 5.5, then we expect $\rho(\mathrm{Jac}(C)) \approx 4$. Indeed, this is what we observe in practice; see Section 6.

On the other hand, we may do better with Algorithm 5.7. Here $\pi(x)$ and $r(x)$ are polynomials where $r(x)$ has a prescribed residue modulo $r(x)$. We can thus always find a $\pi(x)$ with the desired residues and degree strictly less than $\deg r$. Setting $q(x) = \pi(x)\overline{\pi}(x)$, for large values of x we will have $\deg q < 2 \deg r$, and thus ρ-values of varieties produced by Algorithm 5.11 will be less than 4. Note that in this case $2\rho(\pi(x), r(x))$ is a good estimate of the ρ-values of varieties produced by Algorithm 5.11, where the factor of 2 comes from the increase in dimension when taking the Weil restriction. See Section 6 for examples.

While the optimal ρ-value is ≈ 1, in certain cases we have larger lower bounds for the ρ-value. Specifically, we have the following, which generalizes [12, Proposition 2.9 and Remark 2.10].

5.4. **CM fields with extra roots of unity.** In Theorem 5.12, which proves the correctness of Algorithm 5.11, we specifically excluded the CM fields $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(i)$, corresponding to (the isogeny classes of) elliptic curves with j-invariant 0 and 1728, respectively. The difficulty with these fields stems from the fact that the fields have more than two roots of unity, and thus over any given field $\mathbb{F}_q$ there are more than two isogeny classes of elliptic curves with these j-invariants.

We first consider the case $K = \mathbb{Q}(i)$. Fix an elliptic curve $E/\mathbb{F}_q$ with j-invariant 1728. By Propositions and 3.6 and 3.8, if (5.3) holds then $d = 3, 6, 8$, or 12. For the case $d = 8$, it follows from Propositions 4.1, 4.2, 4.6, and 4.8 that no genus 2 curve having one of the forms considered in Section 4 can be defined over $\mathbb{F}_q$ and isogenous over $\mathbb{F}_q$ to a subvariety of $V_8(E)$. It is thus an open question to construct a genus 2 curve over $\mathbb{F}_q$ with this property.

For the remaining values of d, we first observe that $V_{12}(E)$ has four simple two-dimensional factors. It follows from Proposition 3.4 that each of these factors is isogenous to $V_3(E_a)$ for a distinct twist E_a of E. Suppose π is a q-Weil number output by Algorithm 5.5 or 5.7 on inputs $K = \mathbb{Q}(i)$, $d = 3$, and any k divisible by 3. Then the curve C output by Algorithm 5.11 will be isogenous over $\mathbb{F}_q$ to $V_3(E_a)$ for one of the twists E_a, but it may not be the twist with Frobenius endomorphism π. By Proposition 5.10 we can take the quadratic twist of C to get V_3 of the quadratic twist of E_a. However, if the correct curve is a quartic twist of E_a then we cannot twist C to get V_3 of the correct curve — the quartic twist is defined over $\mathbb{F}_{q^4}$ but all twisting isomorphisms of C are defined over $\mathbb{F}_{q^6}$.

If $K = \mathbb{Q}(i)$ and $d = 3$ we can still run Algorithm 5.11 and hope to produce a curve with embedding degree k, but even if $\mathrm{Jac}(C)$ is simple the algorithm is not guaranteed to output a curve with the desired properties. The above discussion suggests that heuristically, given a sufficiently random set of elements π we should expect Algorithm 5.11 to output the correct curve half the time. Indeed, this is what we find in practice: we ran Algorithm 5.5 2000 times with $K = \mathbb{Q}(i)$, $d = 3$, and k a random multiple of 3 in $[6, 99]$. We produced 1000 pairs π, r with r 160 bits, and 1000 pairs π, r with r 256 bits. Running Algorithm 5.11 on the outputs produced 507 pairing-friendly genus 2 curves in the first case and 519 pairing-friendly genus 2 curves in the second case.

The analysis is similar for the case $K = \mathbb{Q}(\zeta_3)$. Fix an elliptic curve $E/\mathbb{F}_q$ with j-invariant 0. By Propositions and 3.6 and 3.8, if (5.3) holds then $d = 4$ or 12. For the case $d = 12$, we see that no genus 2 curve that has one of the forms considered in Section 4 and is defined over $\mathbb{F}_q$ can be isogenous over $\mathbb{F}_q$ to a subvariety of $V_{12}(E)$. It is thus an open question to construct a genus 2 curve over $\mathbb{F}_q$ with this property.

For the case $d = 4$ the analysis is as above: there are six twists of the curve E, grouped into three pairs of quadratic twists (E_a, E'_a), and the curve C output by Algorithm 5.11 is not necessarily isogenous to $V_4(E_a)$ for the twist E_a with Frobenius endomorphism π. As before, we can still run Algorithm 5.11 and hope to find a curve with the desired properties; here we expect (heuristically) to find the correct curve one third of the time. The same experiment as above supports this reasoning: we found 332 pairing-friendly curves with a 160-bit r and 333 pairing-friendly curves with a 256-bit r, out of 1000 Frobenius elements π in each case.

6. Examples

6.1. **Cocks-Pinch curves.** We begin with examples of Cocks-Pinch type curves constructed using Algorithm 5.5.

Example 6.1. Input to Algorithm 5.5: $k = 8$, $d = 4$, $K = \mathbb{Q}(\sqrt{-7})$.
Output from Algorithm 5.5:

$$\begin{aligned} \pi &= 1314477132061358983885556245278266383885541313109 \\ &\quad + 4469363578043653387037313202346701830329373640556\sqrt{-7} \\ r &= 2^{160} - 47 \end{aligned}$$

Output from Algorithm 5.11:

$$\begin{aligned} C:&\quad y^2 = x^5 + ax^3 + bx, \text{ where} \\ a &= 3 \\ b &= 10373909867685157511938903196035769724563494435174040510940201200830700576\\ &\quad 442512041837790917528748 \\ \rho &= 4.076 \end{aligned}$$

Example 6.2. Input to Algorithm 5.5: $k = 15$, $d = 3$, $K = \mathbb{Q}(\sqrt{-2010})$.
Output from Algorithm 5.5:

$$\begin{aligned} \pi &= -1678660572854406197005072337476013708314561165592117087229107334822409768\\ &\quad 5844127695445482158304014329394513915325463871680883338187529758899142951111\\ &\quad 88643523 + 2087758604208696186561202475993423618555089317872195249350214064\\ &\quad 9758206963504315821129860786118047615001452934536945729348722321591445778884\\ &\quad 78905215290201195\sqrt{-2010} \\ r &= 2^{512} - 975 \end{aligned}$$

Output from Algorithm 5.11:

$$\begin{aligned} C: &\quad y^2 = x^6 + ax^3 + b, \text{ where} \\ a &= 3 \\ b &= 1968348365836456065974381950021235277530777821861852053543547774641662136 16\\ &\quad 984778389936993413153955376136984353070795595196392582393435044914727006741\\ &\quad 891809646067442467350068290456274838175167955502877772412208131414454806932\\ &\quad 858537851070061634315466276333183856839732803580435434609693925915577343591\\ &\quad 53873275746138 \\ \rho &= 4.074 \end{aligned}$$

Examples of the Cocks-Pinch method with $d = 8$ and $K = \mathbb{Q}(\sqrt{-2})$ can be found in [21].

6.2. **Brezing-Weng families.** We implemented Algorithm 5.7 in Magma [5] and did a systematic search for families with embedding degree $k \leq 100$. For each k we did the following:

- If $3 \mid k$, do the following for each $D \in \{1, 2, 5, 6, 7, 10, 11, 13, 14, 15\}$:
  1. Let $K = \mathbb{Q}(\sqrt{-D})$.
  2. Let $\ell = \operatorname{lcm}(k, D)$ if $D \equiv 3 \pmod 4$, $\ell = \operatorname{lcm}(k, 4D)$ otherwise. If $\varphi(\ell) > 60$ then go to the next D.
  3. Let $A = \{i\ell/k : 1 \leq i \leq k, \gcd(i, k) = 1\}$
  4. Let $B = \{i\ell/d : 1 \leq i \leq d, \gcd(i, d) = 1\}$
  5. For each $a \in A$ and $b \in B$, run Algorithm 5.7, with
     - $r(x) = \Phi_\ell(x)$ in Step (1),
     - $\zeta_k = x^a \bmod r(x)$ and $\zeta_d = x^b \bmod r(x)$ in Step (2).
- If $4 \mid k$, repeat the above for each $D \in \{2, 3, 5, 6, 7, 10, 11, 13, 14, 15\}$.
- If $8 \mid k$, repeat the above with $D = 2$.

Observe that the ℓ computed in Step (2) is such that $\mathbb{Q}(\zeta_\ell)$ is the smallest cyclotomic field containing a primitive kth root of unity and the field K. We ignore values ℓ with $\varphi(\ell) > 60$ because for such ℓ it will difficult to find values of $r(x)$ with a large prime factor of cryptographic size. (See the discussion of [12, Section 8].) The sets A and B are constructed so that x^a and x^b range over primitive kth and dth roots of unity mod $r(x)$, respectively.

Table 1 lists all the embedding degrees for which we found families with $\rho < 3.5$. For each such embedding degree we list the smallest ρ-value of a family that we could use to produce an explicit curve, and the corresponding value of D. Embedding degrees marked with * indicate that the corresponding families were already found by Kawazoe and Takahashi. A list of the values of $\pi(x)$ for each k can be found in the Appendix.

We now give some specific examples.

Example 6.3. Let $\alpha = \sqrt{-7}$.

Input to Algorithm 5.7: $k = 6$, $d = 3$, $K = \mathbb{Q}(\alpha)$.

TABLE 1. Best ρ-values for families produced by Algorithm 5.7.

k	d	D	$r(x)$	$2\rho(\pi(x), r(x))$	k	d	D	$r(x)$	$2\rho(\pi(x), r(x))$
6	3	7	$\Phi_{42}(x)$	3.00	42	3	7	$\Phi_{42}(x)$	3.00
9	3	1	$\Phi_{36}(x)$	2.67	44	4	11	$\Phi_{44}(x)$	3.00
12	4	3	$\Phi_{12}(x)$	3.00	45	3	1	$\Phi_{180}(x)$	2.67
18	3	1	$\Phi_{36}(x)$	3.33	54	3	1	$\Phi_{108}(x)$	2.44
21	3	1	$\Phi_{84}(x)$	2.67	64*	8	2	$\Phi_{64}(x)$	3.13
24*	4	2	$\Phi_{24}(x)$	3.00	66	3	1	$\Phi_{132}(x)$	2.60
27	3	1	$\Phi_{108}(x)$	2.22	78	3	1	$\Phi_{156}(x)$	2.83
32*	8	2	$\Phi_{32}(x)$	3.25	80	4	5	$\Phi_{80}(x)$	3.13
33	3	1	$\Phi_{132}(x)$	2.80	88*	8	2	$\Phi_{88}(x)$	3.40
39	3	1	$\Phi_{156}(x)$	2.33	90	3	1	$\Phi_{180}(x)$	2.83
40	4	5	$\Phi_{40}(x)$	3.25	100	4	5	$\Phi_{100}(x)$	3.10

Output from Algorithm 5.7:

$$\begin{aligned} \pi(x) &= \tfrac{1}{14}(2\alpha x^9 + (-\alpha+7)x^7 + 2\alpha x^4 - 2\alpha x^2 - 2\alpha x - 14) \\ r(x) &= \Phi_{42}(x) \\ 2\rho(\pi(x), r(x)) &= 3 \\ x_0 &= 614418 \end{aligned}$$

With x_0 as above, we compute a 342-bit prime $q(x_0)$ and a 230-bit prime group order $r(x_0)$. The output from Algorithm 5.11 is

$$\begin{aligned} C:\quad & y^2 = 2x^6 + 6x^3 + b, \text{ where} \\ b \quad = \quad & 324171225620076869571188623794759633701424533679792906824955935054498501314 \\ & 6192267340219164093362942895. \end{aligned}$$

Since q^k has 2047 bits, this curve is suitable for applications at a security level equivalent to a 112-bit symmetric-key system. The precise ρ-value of Jac(C) is 2.976. $\square$

Example 6.4. Let $\alpha = \sqrt{-5}$.

Input to Algorithm 5.7: $k = 20$, $d = 4$, $K = \mathbb{Q}(\alpha)$.

Output from Algorithm 5.7:

$$\begin{aligned} \pi(x) &= \tfrac{1}{10}(2\alpha x^7 + (2\alpha+5)x^6 - (2\alpha+5)x^5 - 2\alpha x^4 - \alpha x - \alpha) \\ r(x) &= \Phi_{20}(x) \\ 2\rho(\pi(x), r(x)) &= 7/2 \\ x_0 &= 16915738899553523459 \end{aligned}$$

With x_0 as above, we compute a 892-bit prime $q(x_0)$ and a 512-bit prime group order $r(x_0)$. The output from Algorithm 5.11 is

$$\begin{aligned} C:\quad & y^2 = x^5 + 2x^3 + bx, \text{ where} \\ b \quad = \quad & 628251615243589193596440571791700247856145963459257227129804674856286600398 \\ & 898676314154498737832883390780288650315378271801413491072526640295077133022 \\ & 376579357249696250246041156465818149048348953057323584016154656213825316772 \\ & 2942322526487325733134709477134661258549165 \end{aligned}$$

Since q^k has 17839 bits, this curve is suitable for applications at a security level equivalent to a 256-bit symmetric-key system. The precise ρ-value of $\mathrm{Jac}(C)$ is 3.491. □

As discussed in Section 5.4, we can run Algorithms 5.5 or 5.7 with $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$, but it is not guaranteed that we can use the output to find a genus 2 curve using Algorithm 5.11.

Example 6.5. Input to Algorithm 5.7: $k = 9$, $d = 3$, $K = \mathbb{Q}(i)$.

Output from Algorithm 5.7:

$$\begin{aligned} \pi(x) &= -\tfrac{1}{2}(x^8 - x^6 - ix^5 - ix^3 - x^2 + 1) \\ r(x) &= \Phi_{36}(x) \\ 2\rho(\pi(x), r(x)) &= 8/3 \\ x_0 &= 2877297 \end{aligned}$$

With x_0 as above, we compute a 342-bit prime $q(x_0)$ and a 258-bit prime group order $r(x_0)$. The output from Algorithm 5.11 is

$$C: \quad y^2 = x^5 + 2x^3 + bx, \text{ where}$$

$$\begin{aligned} b \quad = \quad & 46906541885948759306109827163399172347890838862957594954891419596825499666 \\ & 56054399024630888562947585 23 \end{aligned}$$

Since q^k has 3072 bits, this curve is suitable for applications at a security level equivalent to a 128-bit symmetric-key system. The precise ρ-value of $\mathrm{Jac}(C)$ is 2.651. □

Let $\pi(x), r(x)$ be as in Example 6.5. A sampling of a large number of values of x_0 such that $\pi(x_0)\overline{\pi}(x_0)$ and $r(x_0)$ are both prime suggests that Algorithm 5.11 will output a pairing-friendly curve in approximately one third of such cases. This finding contradicts the reasoning of Section 5.4, which suggests we should expect to find a pairing-friendly curve one half of the time, and we have no explanation of this phenomenon. However, we will see in the next section how to improve this probability.

7. Varying the CM field

Freeman, Scott, and Teske [12, Section 6.4] showed that if the polynomials $\pi(x) \in K[x]$ and $r(x) \in \mathbb{Z}[x]$ generated in the Brezing-Weng method have a certain form, then one can perform a substitution to produce polynomials $\pi'(x) \in K'[x]$ and $r'(x) \in \mathbb{Z}[x]$ that have the same embedding degree properties but make use of a different CM field K'. They suggest that one might wish to make such a change for reasons of security — being able to change the CM field K might foil any potential attacks on the discrete logarithm problem that are effective for specific CM fields (though at present we know of no such attacks). They also use the substitution in some cases where $\pi(x)\overline{\pi}(x)$ never takes on prime values; after the substitution $\pi'(x)\overline{\pi}'(x)$ may take on prime values.

In this section we describe how the observation of Freeman, Scott, and Teske applies to the polynomials constructed in Algorithm 5.7. We then apply this result to Example 6.5. By replacing the CM field $\mathbb{Q}(i)$ with a field K' that has only two roots of unity, whenever $\pi(x_0)\overline{\pi}(x_0)$ is prime we can use Algorithm 5.11 to find a genus 2 curve whose Jacobian has the specified embedding degree.

Our construction uses the following result.

Proposition 7.1. *Let $u(x) \in \mathbb{Z}[x]$ be an irreducible polynomial that is not even, and let $L = \mathbb{Q}[x]/(u(x))$. Suppose $\eta(x) \in \mathbb{Q}[x]$ satisfies*

$$\eta(x) \equiv \sigma \bmod u(x), \quad \eta(-x) \equiv \tau \bmod u(x)$$

for some $\sigma, \tau \in L$. Let $K = \mathbb{Q}(\alpha)$ be a quadratic imaginary field with $\alpha^2 \in \mathbb{Q}$ and $\alpha \notin L$. Define $\pi(x) = \eta(\alpha x) \in K[x]$ and $r(x) = u(\alpha x)u(-\alpha x) \in \mathbb{Q}[x]$. Then $r(x)$ is irreducible, and

$$\pi(x) \equiv \sigma \bmod u(\alpha x), \quad \overline{\pi}(x) \equiv \tau \bmod u(\alpha x).$$

Proof. Let θ be a root of $u(x)$, so $L = \mathbb{Q}(\theta)$. Then $K(\theta) = L(\alpha)$, and since $\alpha \notin L$ this field is a quadratic extension of L. It follows that $u(x)$ is irreducible in $K[x]$, and thus $u(\alpha x)$ is as well. Since $u(x)$ is not even, $u(\alpha x) \notin \mathbb{Q}[x]$, and thus $r(x)$ is irreducible in $\mathbb{Q}[x]$. We have an field inclusion $\mathbb{Q}[x]/(u(x)) \hookrightarrow K[y]/(u(\alpha y))$ given by $x \mapsto \alpha y$, and the properties of $\pi(x)$ follow immediately. □

We apply this result in the following construction, which generalizes Example 6.5.

Proposition 7.2. *Let $k \equiv 9$ or $15 \pmod{18}$, let $u(x) = \Phi_k(x)$, and define*

$$\eta(x) = -\tfrac{1}{2}(x^{2k/3+2} + x^{2k/3} + x^{k/3+2} - x^{k/3} + x^2 + 1).$$

Let $K = \mathbb{Q}(\alpha)$ be a quadratic number field with $\alpha^2 \in \mathbb{Z}$ square free and $\alpha^2 \nmid k$. Define $\pi(x) = \eta(\alpha x) \in K[x]$ and $r(x) = u(\alpha x)u(-\alpha x) \in \mathbb{Q}[x]$. Then $r(x)$ is irreducible, and

$$\pi(x) \equiv \zeta_3 \bmod u(\alpha x), \quad \pi(x)\overline{\pi}(x) \equiv \zeta_k \bmod u(\alpha x).$$

where ζ_3, ζ_k are primitive 3rd and kth roots of unity, respectively.

Proof. Let $h(x) = \Phi_3(x^{k/3}) = x^{2k/3} + x^{k/3} + 1$, and note that $h(x)$ is divisible by $u(x) = \Phi_k(x)$. Then we have

$$\begin{aligned} \eta(x) &\equiv \eta(x) + \tfrac{1}{2}(x^2+1)h(x) = x^{k/3} \bmod u(x) \\ \eta(-x) &\equiv \eta(-x) + \tfrac{1}{2}(x^2+1)h(x) = x^{k/3+2} \bmod u(x) \end{aligned}$$

Since k is a multiple of 3, $x^{k/3}$ is a primitive cube root of unity mod $u(x)$. Since $\gcd(k/3+2, k) = 1$ if and only if $k \equiv 0$ or $6 \pmod 9$, we see that $\pi(x)\overline{\pi}(x) \equiv x^{2k/3+2} \bmod u(x)$ is a primitive kth root of unity mod $u(x)$. The fact that $\alpha^2 \nmid k$ implies that $\alpha \notin \mathbb{Q}[x]/(u(x)) \cong \mathbb{Q}(\zeta_k)$. The result now follows from Proposition 7.1. □

Fix k and let $\eta(x)$ be as in Proposition 7.2. Computations with Magma [5] show that $\eta(x)$ is irreducible for all $k < 1000$ divisible by 3, and we conjecture $\eta(x)$ is irreducible for all such k. For any α as in the theorem, let $\pi_\alpha(x) = \eta(\alpha x)$; then $\pi_\alpha(x) \notin \mathbb{Q}[x]$ (since $k/3$ is odd), so $q_\alpha(x) = \pi_\alpha(x)\overline{\pi_\alpha}(x)$ is irreducible if and only if $\eta(x)$ is. In addition, if α^2 is odd then $q_\alpha(x)$ is an odd integer, so there is hope that $q(x)$ will take on prime values. However, without checking each value of α individually we do cannot say whether $q_\alpha(x)$ is a Bateman-Horn polynomial.

Let $r_\alpha(x) = \Phi_k(\alpha x)\Phi_k(-\alpha x)$. In the case where $q_\alpha(x)$ is a Bateman-Horn polynomial, we have $\rho(\pi_\alpha(x), r_\alpha(x)) = (2k/3+2)/\varphi(k)$ (note that this is independent of α). The entries in Table 1 with $k \in \{9, 15, 27, 33, 45\}$ are exactly these families with $\alpha = \sqrt{-1}$. (See the Appendix for the explicit values of $\pi_\alpha(x)$.) The smallest

ρ-value for an abelian surface constructed using these families is for $k = 27$, in which case $2\rho(\pi(x), r(x)) = 20/9$. Performing a search over α and x found the following example.

Example 7.3. Fix $k = 27$, and let $\pi_\alpha(x)$ and $r_\alpha(x)$ be as above. Let $\alpha = \sqrt{-188765}$ and $x_0 = 49$. Then $q_\alpha(x_0)$ is a 569-bit prime and $r_\alpha(x_0)$ is a 514-bit prime. The output from Algorithm 5.11 is

$$\begin{aligned} C: &\quad y^2 = x^5 + 2x^3 + bx, \text{ where} \\ b \;=&\quad 1355348487374045268415613952356994872682750156069391853919778351061273767 21 \\ &\quad 548255877742176038099282483607627708802571292467474279112671395811904432026 \\ &\quad 9189906985882976108477 2 \end{aligned}$$

Since q^k has 15342 bits, this curve is suitable for applications at a security level equivalent to a 256-bit symmetric-key system. The precise ρ-value of $\mathrm{Jac}(C)$ is 2.214. The improvement in ρ-value by a factor of 1.5 over Example 6.4 means that computations on this curve will run much faster than computations on the curve of Example 6.4, which has the same security level. $\square$

If we fix $\alpha = \sqrt{-1}$, the closest we are able to get to the parameters of Example 7.3 is a 510-bit value for r and a 579-bit value for q ($q^{27} = 15608$ bits), with $x_0 = 23205$. Thus to specify the bit sizes precisely it is necessary to vary the field $K = \mathbb{Q}(\alpha)$ in the search. Current methods to compute Hilbert class polynomials (required for Step (1) of Algorithm 5.11) are feasible for discriminants D with $|D| < 10^{12}$ [29]; the field of Example 7.3 is well within this range.

8. Open Questions

Our algorithms in Section 5 produce an algebraic integer π in a quadratic imaginary field K such that an elliptic curve E with Frobenius element π is pairing-friendly over some extension field $\mathbb{F}_{q^d}$ (where $q = \pi\overline{\pi}$ and we assume d is minimal). The theory developed in Section 3 tells us that there is a simple subvariety A of the Weil restriction $\mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(E)$ that is also pairing-friendly. If A is two-dimensional and certain conditions hold, then we can realize A (up to isogeny) as the Jacobian of one of the genus 2 curves described in Section 4.

It is an open question to efficiently realize A as the Jacobian of a genus 2 curve in *all* cases where it has dimension 2. One obstacle to our method is that we cannot always find an elliptic curve E with Frobenius element π; this occurs when equations (4.2) or (4.4) have no solutions in $\mathbb{F}_q$ for any root j of the Hilbert class polynomial for $\mathcal{O}_K$. One avenue for further research is to find conditions on q and K that guarantee that these equations have a solution in $\mathbb{F}_q$.

Even when we can find an elliptic curve E with Frobenius element π, we cannot use the genus 2 curves discussed in Section 4 in the following cases:

- $d = 3$ and $q \equiv 2 \pmod 3$,
- $d = 4$ and $q \equiv 3 \pmod 4$.

The problem in both these cases is that the Jacobians of the curves discussed in Section 4 either split over the base field or split over an extension field into products of elliptic curves defined over $\mathbb{F}_{p^2}$. Thus beyond a few exceptional cases (cf. Propositions 4.6 and 4.8) there is no "middle ground" where the Jacobian is simple over the base field yet splits over an extension field into a product of elliptic curves defined over $\mathbb{F}_p$. It is thus an open question to find genus 2 curves whose Jacobians are isogenous over $\mathbb{F}_q$ to a simple subvariety of $V_d(E)$ when d and q are as above.

One idea for solving this problem is to investigate genus 2 curves constructed by gluing elliptic curves along ℓ-torsion subgroups with $\ell > 2$. The genus 2 curves in Section 4 come from elliptic curves glued along 2-torsion; gluing elliptic curves along higher torsion subgroups is considerably more complicated.

Another idea is to use the genus 2 CM method [32], which, given an order $\mathcal{O}$ in a quartic CM field K and a prime p, produces all abelian surfaces over $\overline{\mathbb{F}}_p$ with endomorphism ring isomorphic to $\mathcal{O}$. If $\pi \in \mathcal{O}$ is the Frobenius endomorphism of $V_d(E)$, then any Jacobian produced by the CM method will solve our problem. However, it may happen that for all orders $\mathcal{O}$ small enough for the CM method to be inefficient, all abelian surfaces A with $\mathrm{End}(A) \cong \mathcal{O}$ are products of elliptic curves. This is especially likely to happen if K has small class number and the primes dividing $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ are all large. In a few test cases we found that the CM method does not help us find Jacobians where we could find none via our other methods; however, the method requires more study.

The curves of Section 4 also cannot be used when $d = 8$ and $K = \mathbb{Q}(i)$, or when $d = 12$ and $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$. It is also an open question to find genus 2 curves whose Jacobians are isogenous to a simple subvariety of $V_d(E)$ in these cases.

Finally, when $d = 3$ and $K = \mathbb{Q}(i)$ or $d = 4$ and $K = \mathbb{Q}(\zeta_3)$, the fact that the elliptic curve E is isogenous to a curve with extra automorphisms means we can only sometimes use the curves of Section 4. The heuristic reasoning and experiments discussed in Section 5.4 indicate that the curves of Section 4 realize the variety A half of the time when $d = 3$ and $K = \mathbb{Q}(i)$ and one third of the time when $d = 4$ and $K = \mathbb{Q}(\zeta_3)$. It is an open question to find a genus 2 curve realizing A in the remainder of the cases.

Acknowledgments. The first author thanks Bas Edixhoven, Kiran Kedlaya, Peter Stevenhagen, and Edlyn Teske for helpful discussions, and Marco Streng for many detailed comments on an earlier draft of this work. The first author is supported by a National Science Foundation International Research Fellowship, with additional support from the Office of Multidisciplinary Activities in the NSF Directorate for Mathematical and Physical Sciences.

References

[1] A. Atkin and F. Morain. "Elliptic curves and primality proving." *Mathematics of Computation* **61** (1993), 29–68.

[2] P. Bateman and R. Horn. "A heuristic asymptotic formula concerning the distribution of prime numbers." *Mathematics of Computation* **16** (1962), 363–367.

[3] N. Benger, M. Charlemagne, and D. Freeman. "On the security of pairing-friendly abelian varieties over non-prime fields." In *Pairing-Based Cryptography — Pairing 2009*, Springer LNCS **5671** (2009), 52–65.

[4] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)] **21**. Springer, Berlin (1990).

[5] W. Bosma, J. Cannon, and C. Playoust. "The Magma algebra system. I. The user language." *Journal of Symbolic Computation* **24** (1997), 235–265.

[6] F. Brezing and A. Weng. "Elliptic curves suitable for pairing based cryptography." *Designs, Codes and Cryptography* **37** (2005), 133–141.

[7] R. Bröker. *Constructing elliptic curves of prescribed order*. Ph.D. dissertation, Universiteit Leiden (2006). Available at `http://math.leidenuniv.nl/~reinier/thesis.pdf`.

[8] C. Cocks and R. Pinch. "Identity-based cryptosystems based on the Weil pairing." Unpublished manuscript (2001). While this manuscript is generally unavailable, the main result appears as Theorem 4.1 of [12].

[9] C. Diem. *A Study on Theoretical and Practical Aspects of Weil-Restrictions of Varieties*. Ph.D. dissertation, Universität-Gesamthochschule Essen (2001). Available at `http://www.math.uni-leipzig.de/~diem/preprints/dissertation_diem.ps`.

[10] I. Duursma and N. Kiyavash. "The vector decomposition problem for elliptic and hyperelliptic curves." *Journal of the Ramanujan Mathematical Society* **20** (2005), 59–76.

[11] D. Freeman. "A generalized Brezing-Weng algorithm for constructing pairing-friendly ordinary abelian varieties." In *Pairing-Based Cryptography — Pairing 2008*, Springer LNCS **5209**. Springer (2008), 146–163.

[12] D. Freeman, M. Scott, and E. Teske. "A taxonomy of pairing-friendly elliptic curves." To appear in *Journal of Cryptology* (2009). Available at `http://eprint.iacr.org/2006/372`.

[13] D. Freeman, P. Stevenhagen, and M. Streng. "Abelian varieties with prescribed embedding degree." In *Algorithmic Number Theory — ANTS-VIII*, Springer LNCS **5011** (2008), 60–73.

[14] G. Frey, E. Kani, and H. Völklein. "Curves with infinite K-rational geometric fundamental group." In *Aspects of Galois theory*, London Math. Soc. Lecture Note Ser. **256**. Cambridge Univ. Press, Cambridge (1999). 85–118.

[15] E. Furukawa, M. Kawazoe, and T. Takahashi. "Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields." In *Selected Areas in Cryptography — SAC 2003*, Springer LNCS **3006** (2004), 26–41.

[16] S. Galbraith, X. Lin, and M. Scott. "Endomorphisms for faster elliptic curve cryptography on a large class of curves." In *Advances in Cryptology — EUROCRYPT 2009*, Springer LNCS **5479** (2009), 518–535.

[17] S. D. Galbraith, M. Harrison, and D. J. M. Morales. "Efficient hyperelliptic arithmetic using balanced representation for divisors." In *Algorithmic Number Theory Symposium — ANTS-VIII*, Springer LNCS **5011** (2008), 342–356.

[18] S. D. Galbraith, X. Lin, and D. J. M. Morales. "Pairings on hyperelliptic curves with a real model." In *Pairing-Based Cryptography — Pairing 2008*, Springer LNCS **5209** (2008), 265–281.

[19] P. Gaudry and E. Schost. "On the invariants of the quotients of the Jacobian of a curve of genus 2." In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes — AAECC-14*, Springer LNCS **2227** (2001), 373–386.

[20] L. Hitt. "On the minimal embedding field." In *Pairing-Based Cryptography — Pairing 2007*, Springer LNCS **4575** (2007), 294–301.

[21] M. Kawazoe and T. Takahashi. "Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$." In *Pairing-Based Cryptography — Pairing 2008*, Springer LNCS **5209**. Springer (2008), 164–177.

[22] K. S. Kedlaya. "Quantum computation of zeta functions of curves." *Computational Complexity* **15** (2006), 1–19.

[23] S. Lang. *Elliptic Functions*, Graduate Texts in Mathematics **112**. Second edition. Springer-Verlag, New York (1987).

[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. "Choosing the correct elliptic curve in the CM method." To appear in *Mathematics of Computation* (2009). Available at `http://math.uci.edu/~asilverb/bibliography/RubSilcmmethod.pdf`.

[26] K. Rubin and A. Silverberg. "Using abelian varieties to improve pairing-based cryptography." *Journal of Cryptology* **22** (2009), 330–364.

[27] T. Satoh. "Generating genus two hyperelliptic curves over large characteristic finite fields." In *Advances in Cryptology — EUROCRYPT 2009*, Springer LNCS **5479** (2009), 536–553.

[28] J. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**. Springer-Verlag, New York (1994).

[29] A. Sutherland. "Computing Hilbert class polynomials with the Chinese remainder theorem." ArXiV preprint 0903.2785 (2009). Available at `http://arxiv.org/abs/0903.2785`.

[30] J. Tate. "Endomorphisms of abelian varieties over finite fields." *Inventiones Mathematicae* **2** (1966).
[31] J. Tate. "Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)." In *Séminaire Bourbaki 1968/69*, Springer Lect. Notes in Math. **179** (1971), 95–110.
[32] P. van Wamelen. "Examples of genus two CM curves defined over the rationals." *Mathematics of Computation* **68** (1999), 307–320.
[33] W. C. Waterhouse. "Abelian varieties over finite fields." *Annales Scientifiques de l'École Normale Supérieure. Quatrième Série* **2** (1969), 521–560.
[34] A. Weil. *Adeles and algebraic groups*, Progress in Mathematics **23**. Birkhäuser, Boston (1982). With appendices by M. Demazure and Takashi Ono.

Appendix: Values of $\pi(x)$ for families in Table 1

$$\begin{aligned}
k = 6, &\quad \alpha = \sqrt{-7} \\
\pi(x) &= \tfrac{1}{7}\left(\alpha x^9 + \tfrac{-\alpha+7}{2}x^7 + \alpha x^4 - \alpha x^2 - \alpha x - 7\right) \\
k = 9, &\quad \alpha = \sqrt{-1} \\
\pi(x) &= \tfrac{1}{2}(-x^8 + x^6 + \alpha x^5 + \alpha x^3 + x^2 - 1) \\
k = 12, &\quad \alpha = \sqrt{-3} \\
\pi(x) &= \tfrac{1}{3}\left(\tfrac{\alpha-3}{2}x^3 + \tfrac{-\alpha-3}{2}x^2 - \alpha x + \alpha\right) \\
k = 18, &\quad \alpha = \sqrt{-1} \\
\pi(x) &= \tfrac{1}{2}\left(-x^{10} + \alpha x^7 + x^6 + x^4 + \alpha x^3 - 1\right) \\
k = 21, &\quad \alpha = \sqrt{-1} \\
\pi(x) &= \tfrac{1}{2}\left(-x^{16} + x^{14} + \alpha x^9 + \alpha x^7 + x^2 - 1\right) \\
k = 24, &\quad \alpha = \sqrt{-2} \\
\pi(x) &= \tfrac{1}{4}\left(2x^6 + (\alpha - 2)x^5 + \alpha x^4 - \alpha x^3 - \alpha x^2 - \alpha x - \alpha\right) \\
k = 27, &\quad \alpha = \sqrt{-1} \\
\pi(x) &= \tfrac{1}{2}\left(-x^{20} + x^{18} + \alpha x^{11} + \alpha x^9 + x^2 - 1\right) \\
k = 32, &\quad \alpha = \sqrt{-2} \\
\pi(x) &= \tfrac{1}{4}\left(2x^{13} + 2x^{12} - \alpha x^9 + \alpha x^8 - \alpha x + \alpha\right) \\
k = 33, &\quad \alpha = \sqrt{-1} \\
\pi(x) &= \tfrac{1}{2}\left(-x^{28} + x^{22} + \alpha x^{17} + \alpha x^{11} + x^6 - 1\right) \\
k = 39, &\quad \alpha = \sqrt{-1} \\
\pi(x) &= \tfrac{1}{2}\left(-x^{28} + x^{26} - \alpha x^{15} - \alpha x^{13} + x^2 - 1\right) \\
k = 40, &\quad \alpha = \sqrt{-5} \\
\pi(x) &= \tfrac{1}{10}\left(2\alpha x^{13} - 2\alpha x^{12} + 5x^{11} + 5x^{10} - 2\alpha x^9 + 2\alpha x^8 - \alpha x + \alpha\right) \\
k = 42, &\quad \alpha = \sqrt{-7} \\
\pi(x) &= \tfrac{1}{7}\left(-\alpha x^9 + \alpha x^8 + \tfrac{\alpha-7}{2}x^7 + \tfrac{-\alpha-7}{2}x^6 - \alpha x^4 + \alpha x^3 + \alpha x^2 - \alpha\right)
\end{aligned}$$

$$k = 44, \qquad \alpha = \sqrt{-11}$$
$$\pi(x) = \tfrac{1}{11}\left(\alpha x^{15} + \alpha x^{14} + \tfrac{\alpha-11}{2}x^{11} + \tfrac{\alpha+11}{2}x^{10} - \alpha x^9 - \alpha x^8 - \alpha x^5 - \alpha x^4 + \alpha x^3 + \alpha x^2 - \alpha x - \alpha\right)$$

$$k = 45, \qquad \alpha = \sqrt{-1}$$
$$\pi(x) = \tfrac{1}{2}\left(-x^{32} + x^{30} - \alpha x^{17} - \alpha x^{15} + x^2 - 1\right)$$

$$k = 54, \qquad \alpha = \sqrt{-1}$$
$$\pi(x) = \tfrac{1}{2}\left(-x^{22} + x^{18} + \alpha x^{13} + \alpha x^9 + x^4 - 1\right)$$

$$k = 64, \qquad \alpha = \sqrt{-2}$$
$$\pi(x) = \tfrac{1}{4}\left(-2x^{25} - 2x^{24} + \alpha x^{17} - \alpha x^{16} + \alpha x - \alpha\right)$$

$$k = 66, \qquad \alpha = \sqrt{-1}$$
$$\pi(x) = \tfrac{1}{2}\left(-x^{26} + x^{22} + \alpha x^{15} + \alpha x^{11} + x^4 - 1\right)$$

$$k = 78, \qquad \alpha = \sqrt{-1}$$
$$\pi(x) = \tfrac{1}{2}\left(-x^{34} + x^{26} - \alpha x^{21} - \alpha x^{13} + x^8 - 1\right)$$

$$k = 80, \qquad \alpha = \sqrt{-5}$$
$$\pi(x) = \tfrac{1}{10}\left(-2\alpha x^{25} + 2\alpha x^{24} - 5x^{21} - 5x^{20} + 2\alpha x^{17} - 2\alpha x^{16} + \alpha x - \alpha\right)$$

$$k = 88, \qquad \alpha = \sqrt{-2}$$
$$\pi(x) = \tfrac{1}{4}\left(2x^{34} + 2x^{33} + \alpha x^{23} - \alpha x^{22} + \alpha x - \alpha\right)$$

$$k = 90, \qquad \alpha = \sqrt{-1}$$
$$\pi(x) = \tfrac{1}{2}\left(-x^{34} + x^{30} - \alpha x^{19} - \alpha x^{15} + x^4 - 1\right)$$

$$k = 100, \qquad \alpha = \sqrt{-5}$$
$$\pi(x) = \tfrac{1}{10}\left(-2\alpha x^{31} + 2\alpha x^{30} - 5x^{26} - 5x^{25} + 2\alpha x^{21} - 2\alpha x^{20} + \alpha x - \alpha\right)$$

CWI Amsterdam and Universiteit Leiden, Netherlands, freeman@cwi.nl

Tokyo Institute of Technology, Japan, satohcgn@mathpc-satoh.math.titech.ac.jp