A Generalized Brezing-Weng Algorithm for Constructing Pairing-Friendly Ordinary Abelian Varieties

David Freeman

Department of Mathematics
University of California, Berkeley
Berkeley, CA 94720-3840, USA
dfreeman@math.berkeley.edu

Abstract. We give an algorithm that produces families of Weil numbers for ordinary abelian varieties over finite fields with prescribed embedding degree. The algorithm uses the ideas of Freeman, Stevenhagen, and Streng to generalize the Brezing-Weng construction of pairing-friendly elliptic curves. We discuss how CM methods can be used to construct these varieties, and we use our algorithm to give examples of pairing-friendly ordinary abelian varieties of dimension 2 and 3 that are absolutely simple and have smaller ρ-values than any previous such example.

Keywords. Abelian varieties, hyperelliptic curves, pairing-based cryptosystems, embedding degree, pairing-friendly varieties.

1 Introduction

In recent years, many new and useful cryptographic protocols have been proposed that make use of a bilinear map, or pairing [18]. For secure implementation, these protocols require an easily computable, nondegenerate pairing between finite groups in which the discrete logarithm problem is computationally infeasible. At present, the only known pairings with these properties are the Weil and Tate pairings on abelian varieties over finite fields. These pairings take as input points on an abelian variety defined over the field $\mathbb{F}_q$ and produce as output elements of an extension field $\mathbb{F}_{q^k}$. The degree of this extension is known as the *embedding degree*.

For a pairing-based cryptosystem on an abelian variety $A/\mathbb{F}_q$ to be secure and practical, the group of rational points $A(\mathbb{F}_q)$ should have a subgroup of large prime order r, and the embedding degree k should be large enough so that the discrete logarithm problems in $A[r]$ and $\mathbb{F}_{q^k}^\times$ are of roughly equal difficulty and small enough so that the pairing can be computed efficiently. As the embedding degree of a randomly chosen abelian variety over a field of cryptographic size is expected to be very large (see e.g., [1]), trying varieties at random has a very low chance of finding a variety with small embedding degree. It is in fact a difficult problem to construct "pairing-friendly" abelian varieties: those that have small embedding degree with respect to a large prime-order subgroup.

The problem of constructing pairing-friendly elliptic curves (i.e., pairing-friendly one-dimensional abelian varieties) has been studied extensively; Freeman, Scott, and Teske [8] have provided an exhaustive summary of the known constructions. In higher dimensions much less is known. Galbraith [10] and Rubin and Silverberg [19] have classified supersingular abelian varieties of dimension $g \geq 2$, and the latter have shown that for $g \leq 6$ the ratio of embedding degree k to dimension g always satisfies $k/g \leq 7.5$. Since this ratio roughly measures the security level of pairings on the abelian variety, for high and/or long-term security we require larger k/g ratios, and thus must turn to non-supersingular abelian varieties. The only explicit constructions of pairing-friendly non-supersingular abelian varieties of dimension $g \geq 2$ are those of Freeman [7]; Kawazoe and Takahashi [13]; and Freeman, Stevenhagen, and Streng [9]. The first two constructions produce abelian surfaces ($g = 2$), while the last generalizes to arbitrary dimension the method of Cocks and Pinch [5] for constructing pairing-friendly elliptic curves.

The algorithm of Freeman, Stevenhagen, and Streng produces q-Weil numbers that correspond (in the sense of Honda-Tate theory [21]) to ordinary, absolutely simple abelian varieties having arbitrary embedding degree with respect to a subgroup of (nearly) arbitrary order r. The method works by fixing a CM field K of degree $2g$ and using a primitive CM type Φ on K to construct a q-Weil number $\pi \in K$ that is the Frobenius element of a pairing-friendly ordinary abelian variety A of dimension g. If the CM field K is suitably small, CM methods can then be used to produce A explicitly (see Section 4). If K is Galois, the size $q = \pi\overline{\pi}$ of the field over which this variety is defined is expected to be roughly r^{2g}, and thus $\#A(\mathbb{F}_q)$ will be roughly $q^g \approx r^{2g^2}$. The ratio of the size (in bits) of this group order to the size (in bits) of the subgroup order r is measured by the parameter

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

and can be interpreted as the ratio of the abelian variety's required bandwidth to its security level.

All of the constructions of pairing-friendly elliptic curves can produce curves with $\rho \leq 2$, and in many cases we can come very close to or even achieve the "ideal" of a pairing-friendly curve with a prime number of points (see [8, Table 8.2]). In dimension $g = 2$ the constructions of Freeman and Freeman, Stevenhagen, and Streng both lead to ordinary, absolutely simple abelian varieties with $\rho \approx 8$. The construction of Kawazoe and Takahashi produces ordinary abelian varieties with ρ-values between 3 and 4; however, these varieties are not absolutely simple, and thus the construction can be interpreted as producing pairing-friendly elliptic curves over some extension field of $\mathbb{F}_q$. In dimension $g = 3$ the best ρ-values for ordinary abelian varieties that we can construct efficiently are $\rho \approx 18$, and in general we expect to find $\rho \approx 2g\widehat{g}$, where $2\widehat{g}$ is the degree of the reflex field $\widehat{K}$ of (K, Φ). (If K is Galois then $\widehat{g} = g$, but in general we expect $\widehat{g}$ to be much larger than g.)

In this paper, we demonstrate the first constructions of pairing-friendly ordinary abelian varieties of dimension $g \geq 2$ that are absolutely simple and have ρ-values significantly less than $2g^2$.

In Section 2 we give the technical conditions necessary for an abelian variety to be pairing-friendly and describe the approach of Brezing and Weng [4] to satisfying these conditions for elliptic curves. We then show how the ideas of Freeman, Stevenhagen, and Streng can be used to view the Brezing-Weng construction from a new perspective that admits a generalization to higher dimensions.

We give the details of this generalization in Section 3. The key idea is to parametrize the subgroup order r and the Frobenius element π as polynomials of a single variable $r(x) \in \mathbb{Q}[x]$ and $\pi(x) \in K[x]$. Adapting the method of Freeman, Stevenhagen, and Streng, we construct the polynomial $\pi(x)$ as the *type norm* of an element $\xi \in \widehat{K}[x]$ that is chosen to have specified residues modulo factors of $r(x)$ in $\widehat{K}[x]$.

Section 4 discusses how we use the polynomial $\pi(x)$ to construct explicit pairing-friendly abelian varieties. As in the Brezing-Weng method we compute parameters for these varieties by finding an x_0 for which $q(x_0) = \pi(x_0)\overline{\pi}(x_0)$ is prime and $r(x_0)$ has a large prime factor. Once such an x_0 is found, we can use *CM methods* to construct the abelian variety whose Frobenius element is given by $\pi(x_0)$.

In Section 5 we discuss how to select the parameters in our algorithm to produce the optimal output, and provide a number of examples of families of ordinary abelian varieties produced by our method. These include several families of abelian surfaces ($g = 2$) with $\rho \leq 7$ and one with embedding degree 5 and $\rho \approx 4$, which could be a practical choice for certain security levels and which also answers (in one case) an open problem of Freeman, Stevenhagen, and Streng [9, Open Problem 3.5]. We also demonstrate a family of three-dimensional abelian varieties with $\rho \approx 12$. We conclude by discussing avenues for further research in this area.

Acknowledgments

The author thanks Tanja Lange, Michael Naehrig, Edward Schaefer, and Marco Streng for helpful feedback on earlier drafts of this paper. This research was supported by a National Defense Science and Engineering Graduate Fellowship.

2 Pairing-Friendly Abelian Varieties and the Brezing-Weng Method

Let A be a g-dimensional abelian variety defined over the finite field $\mathbb{F}_q$ of q elements. If the group of $\mathbb{F}_q$-rational points of A, denoted $A(\mathbb{F}_q)$, has a cyclic subgroup of order r, then the *embedding degree of A with respect to r* is the smallest integer k such that the field $\mathbb{F}_{q^k}$ contains all rth roots of unity. Equivalently, the embedding degree is the order of q in $(\mathbb{Z}/r\mathbb{Z})^\times$. The embedding degree

derives its name from the fact that $\mathbb{F}_{q^k}$ is the smallest field over which the Weil and Tate pairings take nontrivial values, and thus these pairings can be used to embed a cyclic, order-r subgroup of $A(\mathbb{F}_q)$ into $\mathbb{F}_{q^k}^\times$. (Note that if q is not prime then the image of these embeddings may be contained in a proper subfield of $\mathbb{F}_{q^k}$ [11].)

The embedding degree of an abelian variety $A/\mathbb{F}_q$ is determined by its *Frobenius endomorphism*. If A is simple then the Frobenius endomorphism, which is denoted by π and which acts by raising the coordinates of points on A to the qth power, satisfies a monic, irreducible polynomial with integer coefficients. We can thus view π as an element of a number field $K = \mathbb{Q}(\pi)$. The field K is either a *CM field*, which is an imaginary quadratic extension of a totally real field, or the field $\mathbb{Q}(\sqrt{q})$ [21]; we will consider only the first case as the second corresponds to supersingular abelian varieties. By a theorem of Weil, all embeddings $K \hookrightarrow \mathbb{C}$ have $\pi\overline{\pi} = q$, where $\overline{\cdot}$ denotes complex conjugation. An algebraic integer π with this property is called a *q-Weil number*.

We will henceforth assume that A is simple, as the case of non-simple A can be reduced to the case of simple abelian varieties of lower dimension. We will further 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 $\deg K = 2 \dim A$, and the number of $\mathbb{F}_q$-rational points of A is given by

$$\#A(\mathbb{F}_q) = N_{K/\mathbb{Q}}(\pi - 1).$$

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

Proposition 2.1 ([9]). *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, Φ_k the kth cyclotomic polynomial, and r a square-free integer not dividing kq. If*

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

then A has embedding degree k with respect to r.

Proof. Since r is prime, the first condition tells us that $A(\mathbb{F}_q)$ has a cyclic subgroup of order r, the second that $\pi\overline{\pi} = q$ has order k in $(\mathbb{Z}/r\mathbb{Z})^\times$. □

The Brezing-Weng Method

If A is an ordinary elliptic curve over $\mathbb{F}_q$ with Frobenius endomorphism π, then $K = \mathbb{Q}(\pi) = \mathrm{End}(A) \otimes \mathbb{Q}$ is a quadratic imaginary field. In this case π can be described by its norm $q = \pi\overline{\pi}$ and its trace $t = \pi + \overline{\pi}$. The two conditions of Proposition 2.1 then become

$$r \mid q + 1 - t, \tag{2.1}$$

$$r \mid \Phi_k(q). \tag{2.2}$$

Furthermore, the condition $\pi \in K$ means that there is some integer y such that

$$t^2 - 4q = -Dy^2, \tag{2.3}$$

where D is the unique square-free positive integer such that $K = \mathbb{Q}(\sqrt{-D})$. Nearly all of the existing methods for constructing pairing-friendly ordinary elliptic curves involve fixing k and D and determining primes r and q and an integer t that satisfy (2.1)–(2.3) for some y.

Many of the methods for constructing pairing-friendly ordinary elliptic curves parametrize t, r, and q as polynomials $t(x)$, $r(x)$, $q(x)$ that produce valid curve parameters for many different inputs x. The advantage of such "families" is that the ρ-values (1.1) produced are often smaller than those produced by more general methods such as that of Cocks and Pinch [5]. One of the most successful approaches to constructing families of pairing-friendly elliptic curves with small ρ-values is the method of Brezing and Weng [4]. Their approach is as follows:

Algorithm 2.2 ([4]).

Input: a positive integer k and a positive square-free integer D.

Output: polynomials $r(x)$, and $q(x)$ such that for any x_0 for which $q(x_0)$ is prime, there is an ordinary elliptic curve E over $\mathbb{F}_{q(x_0)}$ such that $\mathrm{End}(E) \otimes \mathbb{Q} \cong \mathbb{Q}(\sqrt{-D})$ and E has embedding degree k with respect to $r(x_0)$.

1. Find an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ such that $L \cong \mathbb{Q}[x]/(r(x))$ is a number field containing $\sqrt{-D}$ and the cyclotomic field $\mathbb{Q}(\zeta_k)$.
2. Choose a primitive kth root of unity $\zeta \in L$.
3. Let $t(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $\zeta + 1$ in L.
4. Let $y(x) \in \mathbb{Q}[x]$ be a polynomial mapping to $(\zeta - 1)/\sqrt{-D}$ in L.
5. Set $q(x) \leftarrow (t(x)^2 + Dy(x)^2)/4$. Return $r(x)$ and $q(x)$. □

The key idea of the Brezing-Weng algorithm is that since elements of L are represented by polynomials modulo $r(x)$, we can always choose $t(x)$ and $y(x)$ to have degree strictly less than $\deg r(x)$. Thus we can always obtain $\deg q(x) \leq \deg r(x) - 2$, and in some cases we can do much better (see [8, §6]). As x grows, the values of q and r are dominated by their leading terms, so $\deg q / \deg r$ is a good approximation of the ρ-value $\log q(x_0)/\log r(x_0)$. If we call $\deg q / \deg r$ the ρ-value of the *family* $(t(x), r(x), q(x))$, then we see that families generated by the Brezing-Weng method have ρ-values less than 2.

The Brezing-Weng algorithm is itself a generalization of an algorithm of Cocks and Pinch [5], which has the same form but works modulo a prime r instead of a polynomial $r(x)$. Freeman, Stevenhagen, and Streng [9] generalized the Cocks-Pinch algorithm to arbitrary CM fields K by demonstrating how the algorithm constructs a Frobenius element π with specified residues modulo certain primes over r in $\mathcal{O}_K$. We can use the same perspective to view the Brezing-Weng method in a new light.

Our new perspective starts with the fact that since $L = \mathbb{Q}[x]/(r(x))$ contains $K = \mathbb{Q}(\sqrt{-D})$, the polynomial $r(x)$ splits into two irreducible factors when viewed as an element of $K[x]$. We thus have $r(x) = r_1(x)\overline{r_1}(x)$ in $K[x]$, and

$L \cong K[x]/(r_1(x)) \cong K[x]/(\overline{r_1}(x))$. Without loss of generality, we may assume that map implied in Steps (3) and (4) of Algorithm 2.2 sends x to a root of $r_1(x)$.

If we compute $t(x)$ and $y(x)$ as in Algorithm 2.2 and let $\pi(x) = \frac{1}{2}(t(x) + y(x)\sqrt{-D})$, then $\pi(x) \equiv \zeta \bmod r_1(x)$. In addition, we see that $\overline{\pi}(x) = \frac{1}{2}(t(x) - y(x)\sqrt{-D}) \equiv 1 \bmod r_1(x)$, or equivalently, $\pi(x) \equiv 1 \bmod \overline{r}_1(x)$. We thus see that $\pi(x)$ satisfies conditions analogous to those of Proposition 2.1:

$$(\pi(x) - 1)(\overline{\pi}(x) - 1) \equiv 0 \bmod r(x),$$
$$\Phi_k(\pi(x)\overline{\pi}(x)) \equiv 0 \bmod r(x).$$

The expression $\pi(x)\overline{\pi}(x)$ gives the $q(x)$ of the algorithm, so we conclude that for any $x_0 \in \mathbb{Q}$ for which $q(x_0)$ is a prime integer, $\pi(x_0) \in K$ is the Frobenius endomorphism of the elliptic curve E specified in the algorithm's description.

3 Generalizing the Brezing-Weng Method

Before we can use our new perspective to generalize the Brezing-Weng method to arbitrary CM fields K, we must first describe some more complex multiplication theory. If K is a CM field of degree $2g$, a *CM type* Φ of K is a set of g embeddings $\Phi = \{\phi_1, \ldots, \phi_g\}$ of K into its normal closure, one from each complex conjugate pair. A CM type is *primitive* if it is not induced from a CM type on a proper CM subfield of K.

The *reflex type* of (K, Φ) consists of the *reflex field* $\widehat{K}$, which is a certain CM subfield of the normal closure of K, and a CM type Ψ of $\widehat{K}$. (For precise definitions of the reflex field and the reflex type, see [20, Section 8] or [9].) If Φ is primitive then the reflex of the reflex $(\widehat{K}, \Psi)$ is the original CM type (K, Φ). If K is Galois then $\widehat{K} = K$ and $\Psi = \{\phi^{-1} : \phi \in \Phi\}$; however for generic K the degree of $\widehat{K}$ will be much larger than the degree of K [9, Lemma 2.8].

The main algorithm of Freeman, Stevenhagen, and Streng [9, Algorithm 2.12] fixes a prime subgroup size r and uses the *type norm* from $\widehat{K}$ to construct a Frobenius element $\pi \in K$ that has specified residues modulo certain primes over r in $\mathcal{O}_K$. The type norm for a CM type (K, Φ) is the map

$$N_\Phi : \xi \mapsto \textstyle\prod_{\phi \in \Phi} \phi(\xi).$$

The image of the type norm N_Φ is contained in the reflex field $\widehat{K}$ [9, Lemma 2.7], so the image of the reflex type norm N_Ψ is contained in K. If the CM type Φ is primitive, then for generic $\xi \in K$ we have $\widehat{K} = \mathbb{Q}(N_\Phi(\xi))$ (cf. [9, Theorem 3.1]).

To apply the ideas of Freeman, Stevenhagen, and Streng to the Brezing-Weng construction, we extend the type norm to a multiplicative map $\mathcal{N}_\phi$ on polynomials in $K[x]$.

Lemma 3.1. *Let $\xi \in K[x]$, and let Φ be a CM type of K. Define $\mathcal{N}_\Phi(\xi) = \prod_{\phi\in\Phi}\phi(\xi)$, where $\phi(\xi)$ is obtained by applying ϕ to the coefficients of ξ. Then $\mathcal{N}_\Phi(\xi) \in \widehat{K}[x]$.*

Proof. Let L be the normal closure of K, and let $\sigma \in \mathrm{Gal}(L/\widehat{K})$. Then by definition of the reflex type, σ permutes the elements of Φ, so $\sigma(\prod_{\phi\in\Phi}\phi(\xi)) = \prod_{\phi\in\Phi}\phi(\xi)$. (Cf. [9, Lemma 2.7].) □

Remark 3.2. In a similar manner, for any extension of number fields L/K we can extend the norm $N_{L/K}$ to polynomials $f \in L[x]$ by setting $\mathcal{N}_{L/K}(f) = \prod_\phi \phi(f)$, where ϕ ranges over the set of embeddings of L in its normal closure that fix K. An argument analogous to the proof of Lemma 3.1 then shows that the image of $\mathcal{N}_{L/K}$ is contained in $K[x]$.

To generalize the Brezing-Weng construction, we let K be a CM field of degree $2g$ with primitive CM type Φ. Let $(\widehat{K},\Psi)$ be the reflex CM type, and let $\deg\widehat{K} = 2\widehat{g}$. Let $L = \mathbb{Q}[x]/(r(x))$ be a number field containing $\widehat{K}$ and $\mathbb{Q}(\zeta_k)$. In the case where $K = \widehat{K}$ is a quadratic imaginary field, the Brezing-Weng method constructs directly a polynomial $\pi(x)$ parametrizing Frobenius elements by prescribing the residues of $\pi(x)$ modulo each factor of $r(x)$ in $K[x]$. To generalize this construction along the lines of Freeman, Stevenhagen and Streng, we construct $\pi(x)$ as the type norm $\mathcal{N}_\Psi$ of an element $\xi \in \widehat{K}[x]$ with prescribed residues modulo factors of $r(x)$ in $\widehat{K}[x]$. The following proposition allows us to index the factors of $r(x)$ in $\widehat{K}[x]$ in a way that will be useful for our construction.

Proposition 3.3. *Let $\widehat{K}$ be a CM field and Ψ be a CM type on $\widehat{K}$. Let $r(x) \in \mathbb{Q}[x]$ be irreducible, and assume that $L \cong \mathbb{Q}[x]/(r(x))$ is Galois and contains $\widehat{K}$. Let $G = \mathrm{Gal}(L/\mathbb{Q})$ and $H = \mathrm{Gal}(L/\widehat{K})$. For each $\psi \in \Psi$ let $\psi' \in G$ be a representative of the left coset of H that induces the embedding ψ on $\widehat{K}$.*

Fix a root $\gamma \in L$ of $r(x)$. For each $\psi \in \Psi$, define

$$r_\psi(x) = \mathcal{N}_{L/\widehat{K}}(x - \psi'^{-1}(\gamma)), \qquad \overline{r_\psi}(x) = \mathcal{N}_{L/\widehat{K}}(x - \overline{\psi'}^{-1}(\gamma)).$$

Then for each $\psi \in \Psi$, r_ψ and $\overline{r_\psi}$ are irreducible elements of $\widehat{K}[x]$, and the complete factorization of $r(x)$ in $\widehat{K}[x]$ is given by

$$r(x) = \textstyle\prod_{\psi\in\Psi} r_\psi(x)\overline{r_\psi}(x). \tag{3.1}$$

Proof. The fact that r_ψ and $\overline{r_\psi}$ are in $\widehat{K}[x]$ follows from Remark 3.2. Since L is Galois, any root $\delta \in L$ of $r_\psi(x)$ is also a root of $r(x)$, and thus $L = \mathbb{Q}(\delta) = \widehat{K}(\delta)$. It follows that the minimal polynomial of δ over $\widehat{K}$ has degree $[L : \widehat{K}]$, which by construction is the degree of $r_\psi(x)$. Therefore $r_\psi(x)$ is the minimal polynomial of δ over $\widehat{K}$ and is thus irreducible. The proof for $\overline{\psi}$ is analogous.

Since the elements of H induce the complete set of embeddings of $\widehat{K}$ in L, we have

$$r_\psi(x) = \textstyle\prod_{\sigma\in H}(x - \sigma\psi'^{-1}(\gamma)), \qquad \overline{r_\psi}(x) = \prod_{\sigma\in H}(x - \sigma\overline{\psi'}^{-1}(\gamma)).$$

If we let $\Psi' = \{\psi' : \psi \in \Psi\}$, then the set of roots of the right hand side of (3.1) is exactly $\{\tau(\gamma) : \tau \in H(\Psi' \cup \overline{\Psi'})^{-1}\}$. Since $\Psi' \cup \overline{\Psi'}$ is a complete set of left coset representatives of H in G, its inverse is a complete set of *right* coset representatives of H in G, and thus $H(\Psi' \cup \overline{\Psi'})^{-1} = G$. We conclude that $\{\tau(\gamma) : \tau \in H(\Psi' \cup \overline{\Psi'})^{-1}\}$ consists of precisely the roots of $r(x)$ in L. □

We now obtain an analogue of the main theorem of Freeman, Stevenhagen, and Streng [9, Theorem 2.10]:

Theorem 3.4. *Let (K, Φ) be a CM type and $(\widehat{K}, \Psi)$ its reflex. Let $r(x) \in \mathbb{Q}[x]$ be an irreducible (not necessarily monic) polynomial such that $L = \mathbb{Q}[x]/(r(x))$ is a Galois extension of $\mathbb{Q}$ containing $\widehat{K}$ and the cyclotomic field $\mathbb{Q}(\zeta_k)$.*

Let $\gamma \in L$ be a root of $r(x)$, and write the factorization of $r(x)$ in $\widehat{K}[x]$ as in Proposition 3.3. Given $\xi \in \widehat{K}[x]$, for each $\psi \in \Psi$ suppose $\alpha_\psi, \beta_\psi \in \mathbb{Q}[x]$ satisfy

$$\xi \equiv \alpha_\psi \bmod r_\psi(x) \qquad \text{and} \qquad \xi \equiv \beta_\psi \bmod \overline{r_\psi}(x). \tag{3.2}$$

Suppose that

$$\textstyle\prod_{\psi \in \Psi} \alpha_\psi(\gamma) = 1 \qquad \text{and} \qquad \prod_{\psi \in \Psi} \beta_\psi(\gamma) = \zeta, \tag{3.3}$$

where $\zeta \in L$ is a primitive kth root of unity. Then $\pi(x) = \mathcal{N}_\Psi(\xi) \in K[x]$ satisfies

1. *$\pi(x)\overline{\pi}(x) \in \mathbb{Q}[x]$,*
2. *$\mathcal{N}_{K/\mathbb{Q}}(\pi(x) - 1) \equiv 0 \bmod r(x)$, and*
3. *$\Phi_k(\pi(x)\overline{\pi}(x)) \equiv 0 \bmod r(x)$.*

Proof. Statement (1) follows from Remark 3.2 and the fact that $\pi(x)\overline{\pi}(x) = \mathcal{N}_{\widehat{K}/\mathbb{Q}}\xi$. Next, (3.2) implies that $\xi - \alpha_\psi = f r_\psi$ for some $f \in \widehat{K}[x]$, so $\psi'^{-1}(\gamma) \in L$ is a root of $\xi - \alpha_\psi \in \widehat{K}[x]$. Applying ψ' to this expression and using the fact that $\alpha_\psi \in \mathbb{Q}[x]$, we see that γ is a root of $\psi(\xi) - \alpha_\psi \in L[x]$. It follows that $(\psi(\xi))(\gamma) = \alpha_\psi(\gamma)$, and by the same reasoning, $(\overline{\psi}(\xi))(\gamma) = \beta_\psi(\gamma)$. Now since $\pi(\gamma) = \prod_{\psi \in \Psi}(\psi(\xi))(\gamma)$ by definition of the type norm, we conclude from (3.3) that $\pi(\gamma) = 1$ and $\overline{\pi}(\gamma) = \zeta$, from which statements (2) and (3) follow. □

If $\pi(x)$ and $r(x)$ are as in Theorem 3.4, then by Proposition 2.1 for any $x_0 \in \mathbb{Q}$ for which $q = \pi(x_0)\overline{\pi}(x_0)$ is a prime, $\pi(x_0) \in \mathcal{O}_K$ is the Frobenius element of an abelian variety over $\mathbb{F}_q$ that has embedding degree k with respect to $r(x_0)$. We can thus view $\pi(x)$ as defining a one-parameter "family" of pairing-friendly Frobenius elements. The following definitions formalize this concept, generalizing the "families" of Freeman, Scott, and Teske [8, Definition 2.6].

Definition 3.5. Let $f(x) \in \mathbb{Q}[x]$ be a non-constant, irreducible polynomial with positive leading coefficient. We say f *represents primes* 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 3.5 is motivated by the conjecture of Bateman and Horn [3], which gives a heuristic asymptotic formula for the number of prime values taken by a set of polynomials with integer coefficients.

Definition 3.6. Let K be a CM field of degree $2g$, let $\pi(x) \in K[x]$, and let $r(x) \in \mathbb{Z}[x]$. We say that (π, r) *represents a family of g-dimensional abelian varieties with embedding degree k* if:

1. $q(x) = \pi(x)\overline{\pi}(x)$ is in $\mathbb{Q}[x]$.
2. $q(x)$ represents primes (in the sense of Definition 3.5).
3. $r(x)$ is non-constant and irreducible and has positive leading coefficient.
4. $\mathcal{N}_{K/\mathbb{Q}}(\pi(x) - 1) \equiv 0 \bmod r(x)$.
5. $\Phi_k(q(x)) \equiv 0 \bmod r(x)$, where Φ_k is the kth cyclotomic polynomial.

With our setup, we can now adapt [9, Algorithm 2.12] to our new context.

Algorithm 3.7.

Input: a primitive CM type (K, Φ), its reflex type $(\widehat{K}, \Psi)$, a positive integer k, an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ such that $\mathbb{Q}[x]/(r(x))$ is a Galois number field containing K and the cyclotomic field $\mathbb{Q}(\zeta_k)$, and a non-empty set $\Sigma \subset \mathbb{Q}[x]$.

Output: a polynomial $\pi(x) \in K[x]$ such that if $q(x) = \pi(x)\overline{\pi}(x)$ represents primes (in the sense of Definition 3.5), then (π, r) represents a family of abelian varieties with embedding degree k.

1. Set $\widehat{g} \leftarrow \frac{1}{2} \deg \widehat{K}$ and write $\Psi = \{\psi_1, \psi_2, \ldots, \psi_{\widehat{g}}\}$. Set $L \leftarrow \mathbb{Q}[x]/(r(x))$.
2. Let $\gamma \in L$ be a root of $r(x)$. Compute the factorization of $r(x)$ in $\widehat{K}[x]$ as in Proposition 3.3.
3. Choose a primitive kth root of unity $\zeta \in L$.
4. Choose polynomials $\alpha_1, \ldots, \alpha_{\widehat{g}-1}, \beta_1, \ldots, \beta_{\widehat{g}-1} \in \mathbb{Q}[x]$ from Σ.
5. Compute $\alpha_{\widehat{g}} \in \mathbb{Q}[x]$ such that $\prod_{i=1}^{\widehat{g}} \alpha_i(\gamma) = 1$, and compute $\beta_{\widehat{g}} \in \mathbb{Q}[x]$ such that $\prod_{i=1}^{\widehat{g}} \beta_i(\gamma) = \zeta$.
6. Use the Chinese remainder theorem to compute $\xi \in \widehat{K}[x]$ such that $\xi \equiv \alpha_i \bmod r_{\psi_i}(x)$ and $\xi \equiv \beta_i \bmod \overline{r_{\psi_i}}(x)$ for $i = 1, 2, \ldots, \widehat{g}$.
7. Set $\pi(x) \leftarrow \mathcal{N}_{\Psi}(\xi)$, and return $\pi(x)$. □

For any given CM type (K, Φ) and embedding degree k, there are many possible choices for the inputs $r(x)$ (the polynomial that defines L) and Σ (the set of possible choices for the residues of ξ modulo all but two of the factors of $r(x)$ in $\widehat{K}[x]$), as well as the root of unity ζ in Step (3). We will defer our discussion of these choices to Section 5.

We note that if K is a quadratic imaginary field, then Step (4) is empty and setting $q(x) = \pi(x)\overline{\pi}(x)$ and $t(x) = \pi(x) + \overline{\pi}(x)$ recovers the Brezing-Weng algorithm.

4 From Families to Explicit Abelian Varieties

We now consider the problem of constructing the varieties represented by a family (π, r). If K has degree $2g$, to obtain q-Weil numbers corresponding (in the sense of Honda-Tate theory [21]) to ordinary, simple abelian varieties of dimension g, we need to find x_0 such that $\pi(x_0)$ generates K over $\mathbb{Q}$ and $q(x_0)$

is a prime that is unramified in K. (See [9, Lemma 2.2].) In general, we find that if $q(x_0)$ is prime then the other two conditions are satisfied with very high probability. For cryptographic applications, we also need $r(x_0)$ to be prime or very nearly prime. We use the following algorithm to search for an x_0 with the desired properties.

Algorithm 4.1.

Input: a CM field K, a pair of polynomials (π, r) that represents a family of abelian varieties with embedding degree k (in the sense of Definition 3.6), and a positive integer y_0.

Output: integers x_0 and h such that $q(x_0)$ is prime (where $q(x) = \pi(x)\overline{\pi}(x)$) and $r(x_0)$ is h times a prime.

1. Compute integers a, b such that $q(ax + b)$ is integer-valued and represents primes.
2. Compute $h \in \mathbb{Z}$ and $\widetilde{r}(x) \in \mathbb{Q}[x]$ such that $r(x) = h\widetilde{r}(x)$ and there is no prime p dividing $q(ax + b)\widetilde{r}(ax + b)$ for all x.
3. Set $x_1 \leftarrow y_0$.
4. Repeat $x_1 \leftarrow x_1 + 1$ until
   (a) $q(ax_1 + b)$ and $\widetilde{r}(ax_1 + b)$ are prime, and
   (b) $K = \mathbb{Q}(\pi(x_0))$ and $q(x_0)$ is unramified in K.
5. Set $x_0 \leftarrow ax_1 + b$. Return h and x_0.

The input y_0 is the starting point for the search, and should be chosen so that $r(y_0)/h$ is at least the minimum size desired for security. The fact that integers a, b as in Step (1) always exist is a consequence of the following lemma.

Lemma 4.2. *Suppose $q(x) \in \mathbb{Q}[x]$ represents primes in the sense of Definition 3.6. Then there exist integers a, b such that $q(ax + b)$ is integer-valued and represents primes.*

Proof. Write $q(x) = \frac{1}{d}\widetilde{q}(x)$ for some integer d and $\widetilde{q}(x) \in \mathbb{Z}[x]$. For every prime p, let e_p be the integer such that $d = \prod_p p^{e_p}$. Since $q(x)$ represents primes, for each p there exists a b_p such that $q(b_p)$ is an integer not divisible by p, and thus p^{e_p} divides $\widetilde{q}(b_p)$ exactly. Let $a = \prod_{p|d} p^{e_p+1}$, and let b be an integer congruent to b_p mod p^{e_p+1} for every p dividing d. Then $q(ax + b)$ is integer-valued and is nonzero mod p for every p dividing d. For every p not dividing d, $ax + b$ ranges through all residue classes mod p, so there is some residue class of x mod p for which p does not divide $\widetilde{q}(ax + b)$. Thus there is no prime p dividing $q(ax + b)$ for all x, which is equivalent to $q(ax + b)$ representing primes. □

Now suppose $q(x)$ and $r(x)$ have degrees d_1 and d_2 respectively. By the Bateman-Horn conjecture [3] we expect to test roughly $d_1 d_2 (\log ay_0)^2$ values of x_1 before we find one for which $q(ax_1 + b)$ is prime and $r(ax_1 + b)$ is h times a prime. Thus we see that heuristically, the expected number of executions of Step (4) is linear in the degrees of $\pi(x)$ and $r(x)$, and quadratic in the number of bits in y_0. We also note (and find in practice) that the a computed in Step (1) can be smaller than the a produced in the proof of Lemma 4.2.

Once we have found an x_0 such that $q(x_0)$ is prime and $r(x_0)$ is nearly prime, the problem remains to construct an abelian variety over $\mathbb{F} = \mathbb{F}_{q(x_0)}$ whose Frobenius element is $\pi(x_0)$. This is achieved using *CM methods*, which construct varieties in characteristic zero whose endomorphism rings are isomorphic to a specified order $\mathcal{O}$ in a CM field K; for our purposes we can take $\mathcal{O}$ to be the ring of integers $\mathcal{O}_K$. Since any ordinary abelian variety over a finite field arises as the reduction modulo a prime of a variety in characteristic zero with the same endomorphism ring, we can use a CM method to produce a set of abelian varieties over the field $\mathbb{F}$ that includes representatives of all of the $\overline{\mathbb{F}}$-isomorphism classes of varieties A with $\mathrm{End}(A) \cong \mathcal{O}_K$. We test these candidates A, as well as all of their twists (varieties over $\mathbb{F}$ that are $\overline{\mathbb{F}}$-isomorphic to A), to see which is in the correct $\mathbb{F}$-isogeny class; this can be determined by seeing if the number of $\mathbb{F}$-rational points is equal to $N_{K/\mathbb{Q}}(\pi(x_0) - 1)$. Even though counting the number of rational points on a g-dimensional abelian variety A over a field $\mathbb{F}$ of cryptographic size is in general infeasible for $g \geq 2$, we can quickly determine whether the number of points is equal to n by choosing a few random points $P_i \in A(\mathbb{F})$ and seeing if $[n]P_i$ is the identity on A for all i.

Finally, a word is in order about the CM methods. Over an algebraically closed field, all principally polarized abelian varieties of dimension $g \leq 3$ are Jacobians of genus g curves. It thus suffices to produce all curves whose Jacobians have endomorphism ring isomorphic to $\mathcal{O}_K$; we say that these Jacobians have *CM by* $\mathcal{O}_K$. In dimension $g = 1$ we compute the *Hilbert class polynomial*, a polynomial in $\mathbb{Z}[x]$ whose roots are equal to the j-invariants of elliptic curves over $\overline{\mathbb{Q}}$ with CM by $\mathcal{O}_K$. In dimension $g = 2$ we compute the *Igusa class polynomials*, which are three polynomials in $\mathbb{Q}[x]$ whose roots are the *Igusa invariants* of genus 2 curves over $\overline{\mathbb{Q}}$ whose Jacobians have CM by $\mathcal{O}_K$. Methods for $g = 3$ are analogous but have only been developed for fields K containing i or ζ_3 [23, 15]. Methods for $g \geq 4$ are completely undeveloped.

The class polynomials produced by the CM methods are very large: both the degree and the size of the coefficients grow very quickly with the class number of K, and in general the computation is only feasible for very small CM fields K. For $g = 1$ the upper limit is roughly class number 10^5 [6], while for $g = 2$ we can only achieve class numbers around 100 [14], and for $g = 3$ the methods are even more limited. Thus we must be careful to choose a field K as input to Algorithm 3.7 for which we know that the CM method is feasible.

5 Parameter Selection and Examples

The primary advantage of Algorithm 3.7 is that it leads to pairing-friendly ordinary, absolutely simple abelian varieties with smaller ρ-values than any previous construction. Recall that the ρ-value of a g-dimensional abelian variety over $\mathbb{F}_q$ with respect to a subgroup of order r is $\rho = g \log q / \log r$. If $q = q(x)$ and $r = r(x)$ are parametrized as polynomials, then for large x the ρ-value approaches $g \deg q / \deg r$. This motivates the definition of a ρ-value for a family of pairing-friendly abelian varieties.

Definition 5.1. Suppose (π, r) represents a family of g-dimensional abelian varieties with embedding degree k, and let $q(x) = \pi(x)\overline{\pi}(x)$. The *$\rho$-value of the family represented by* (π, r), denoted $\rho(\pi, r)$, is

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

The key feature of Algorithm 3.7 is that the polynomial ξ constructed by the Chinese remainder theorem in Step (6) can always be chosen to have degree strictly less than $\deg r$, and thus $\deg \pi \leq \widehat{g}(\deg r - 1)$. We thus obtain

$$\rho(\pi, r) = 2g\widehat{g}\frac{\deg \xi}{\deg r} \leq 2g\widehat{g}\frac{\deg r - 1}{\deg r}.$$

This asymptotic ρ-value is an improvement over the ρ-values produced by the algorithm of Freeman, Stevenhagen, and Streng, which gives $\rho \approx 2g\widehat{g}$ [9, Theorem 3.4].

To improve the ρ-values further one would try to choose the inputs to Algorithm 3.7 in some clever manner so that the π produced has degree significantly less than $\widehat{g} \deg r$. These choices include the ζ of Step (3), the α_i and β_i of Step (4) (which are chosen from the input Σ), and the input polynomial $r(x)$.

The problem of computing an optimal π has been studied extensively in the case of elliptic curves, where there are only ζ and $r(x)$ to consider. Brezing and Weng [4] and Baretto, Lynn, and Scott [2] both take $r(x)$ to be a cyclotomic polynomial $\Phi_\ell(x)$, where $k \mid \ell$ and $\mathbb{Q}(\zeta_\ell)$ contains the quadratic imaginary field $K = \widehat{K}$, and search through the primitive kth roots of unity $\zeta \in L \cong \mathbb{Q}(\zeta_\ell)$. Other constructions have kept this choice of L but used a different polynomial $r(x)$. In particular, Kachisa, Schaefer, and Scott [12] have systematically searched through the space of $r(x)$ that generate $\mathbb{Q}(\zeta_\ell)$ and found improved ρ-values in several cases.

In higher dimensions we search for a $\pi(x)$ of low degree by following the model of Brezing and Weng. We let $r(x)$ be a cyclotomic polynomial Φ_ℓ such that $k \mid \ell$ and $L \cong \mathbb{Q}(\zeta_\ell)$ contains the specified CM field K. Since L is abelian, in this case the CM field K must also be abelian, and thus equal to the reflex field $\widehat{K}$. We choose the α_i, β_i all to be polynomials that reduce to roots of unity (of any order) in L. Since $r(x)$ is the ℓth cyclotomic polynomial, x is a primitive ℓth root of unity in $\mathbb{Q}[x]/(r_\psi(x))$ for all $\psi \in \Psi$. Thus if we choose α_i, β_i as

$$(\alpha_1, \ldots, \alpha_g) \in \{(x^{a_1}, \ldots, x^{a_g}) : 0 \leq a_i < \ell,\ \textstyle\sum_{i=1}^g a_i = 0\}, \tag{5.1}$$

$$(\beta_1, \ldots, \beta_g) \in \left\{(x^{b_1}, \ldots, x^{b_g}) : 0 \leq b_i < \ell,\ \gcd(\ell, \textstyle\sum_{i=1}^g b_i) = \ell/k\right\}, \tag{5.2}$$

then $\prod \alpha_i = x^{\sum a_i} \equiv 1 \bmod r(x)$, and $\prod \beta_i = x^{\sum b_i}$ is a primitive kth root of unity mod $r(x)$.

For given CM type (K, Φ), embedding degree k, and cyclotomic polynomial $r(x) = \Phi_\ell(x)$, our implementation of Algorithm 3.7 searches through all α_i, β_i satisfying (5.1) and (5.2) and returns the ξ of smallest degree. We illustrate with a detailed example for $g = 2$ that produces ρ-values around 4, thus answering

(in one case) an open problem of Freeman, Stevenhagen, and Streng [9, Open Problem 3.5].

Example 5.2 ($g = 2, k = 5, \rho = 4$)**.** Let $K = \mathbb{Q}(\zeta_5)$, $k = 5$, and

$$r(x) = \Phi_5(x) = x^4 + x^3 + x^2 + x + 1.$$

We choose the CM type $\Phi = \{\phi_1, \phi_2\}$ where ϕ_1 is the identity and $\phi_2 : \zeta_5 \mapsto \zeta_5^3$. Then $\Psi = \{\psi_1, \psi_2\}$, where ψ_1 is the identity and $\psi_2 : \zeta_5 \mapsto \zeta_5^2$. If we use the root $\gamma = \zeta_5$ to factor $r(x)$ in $K[x]$ as in Proposition 3.3, we obtain

$$r(x) = r_1(x)r_2(x)\overline{r_1}(x)\overline{r_2}(x) = (x - \zeta_5)(x - \zeta_5^3)(x - \zeta_5^4)(x - \zeta_5^2).$$

We choose

$$\alpha_1 = x, \quad \alpha_2 = x^3, \quad \beta_1 = x, \quad \beta_2 = x^4$$

and use the Chinese remainder theorem to compute

$$\begin{aligned}\xi(x) = {} & \tfrac{1}{5}(-2\zeta_5^3 - 4\zeta_5^2 - \zeta_5 - 3)x^2 + \tfrac{1}{5}(-\zeta_5^3 - 2\zeta_5^2 + 2\zeta_5 + 1)x \\ & + \tfrac{1}{5}(-2\zeta_5^3 - 4\zeta_5^2 - \zeta_5 - 3).\end{aligned}$$

Taking the type norm $\mathcal{N}_\Phi(\xi)$ gives

$$\begin{aligned}\pi(x) = {} & \tfrac{1}{5}(-\zeta_5^3 + \zeta_5^2 + \zeta_5 - 1)x^4 + \tfrac{1}{5}(\zeta_5^3 + 2\zeta_5 - 3)x^3 + \tfrac{1}{5}(3\zeta_5^2 + 4\zeta_5 - 2)x^2 \\ & + \tfrac{1}{5}(\zeta_5^3 + 2\zeta_5 - 3)x + \tfrac{1}{5}(-\zeta_5^3 + \zeta_5^2 + \zeta_5 - 1),\end{aligned} \tag{5.3}$$

and we compute

$$q(x) = \pi(x)\overline{\pi}(x) = \tfrac{1}{5}\left(x^8 + 2x^7 + 8x^6 + 9x^5 + 15x^4 + 9x^3 + 8x^2 + 2x + 1\right).$$

Since $q(x)$ is irreducible and $q(1) = 11$ and $q(-4) = 11941$ are distinct primes, $q(x)$ represents primes as in Definition 3.5, and thus (π, r) represents a family of abelian surfaces with embedding degree 5.

Let us try to construct an example abelian surface in this family with a prime-order subgrup of at least 224 bits. Since $\deg r = 4$, we input $y_0 = 2^{56}$ to Algorithm 4.1. Using $a = 5$ and $b = 1$ in Step (1), the algorithm outputs $h = 5$ and $x_0 = 360287970189653536$. We then compute

$$\begin{aligned}r(x_0) &= 5 \cdot 336999333339434839819417093366755356243600418613931064245746056605 5021 \\ q(x_0) &= 567842753356117591737134061550119516120362101246772742754568719155575473117806 1 \setminus \\ &\quad 200081110498587388295149385956491111313314236986670485226190 1 \quad (465 \text{ bits}).\end{aligned}$$

Then $r(x_0)$ is 5 times a 231-bit prime r_0. The Frobenius element $\pi(x_0) \in \mathbb{Q}(\zeta_5)$ can be computed from (5.3), and the number of points n is

$$\begin{aligned}N_{K/\mathbb{Q}}(\pi(x_0) - 1) = {} & 182497631597067310044724655183982827340514982783823273505974232371 \setminus \\ & 199356204693993385911772749363583074379038864307843152029282095458 \setminus \\ & 60865115986084608074445691187177358805776435438144493614420 5.\end{aligned}$$

Over any field $\mathbb{F}$ there is a single $\overline{\mathbb{F}}$-isomorphism class of abelian surfaces whose ring of $\overline{\mathbb{F}}$-endomorphisms is isomorphic to $\mathbb{Z}[\zeta_5]$. If $\operatorname{char}\mathbb{F}$ is prime to 10, then this abelian surface is isomorphic (over $\overline{\mathbb{F}}$) to the Jacobian of $C : y^2 = x^5+1$. Over $\mathbb{F}$ we must find the twist of C that is in the correct $\mathbb{F}$-isogeny class; i.e., has a Jacobian with the correct number of $\mathbb{F}$-rational points. By choosing a random point P on each twist and seeing whether $[n]P = O$, we find that the correct curve over $\mathbb{F} = \mathbb{F}_{q(x_0)}$ is

$$C : y^2 = x^5 + 5.$$

The ρ-value of $\mathrm{Jac}(C)$ with respect to the subgroup of order r_0 is 4.02. □

Remark 5.3. The abelian surface $A = \mathrm{Jac}(C)$ computed in Example 5.2 has the property that the bit size of the field $\mathbb{F}_{q^k}$ in which pairings on A take their values is roughly $\rho k/g = 10$ times the bit size of the prime-order subgroup $A[r]$. It follows that A is suitable for applications with security level equivalent to a 112-bit symmetric-key system [8, §1.1]. In addition, since the curve C has a degree-10 twist, we expect that twisting methods such as those developed for elliptic curves [17] can be used to increase the speed of pairing computation on the Jacobian and reduce the size of the input.

We ran Algorithm 3.7 for all degree-4 CM fields K that are primitive (i.e., do not contain a quadratic imaginary subfield) and are contained in a cyclotomic field $\mathbb{Q}(\zeta_\ell)$ with $\varphi(\ell) \le 16$. We let the inputs to the algorithm range over all such K and ℓ and embedding degrees k dividing ℓ. Given an η such that $K = \mathbb{Q}(\eta)$, we let Φ be the CM type that consists of embeddings ϕ_i such that $\phi_i(\eta)$ all have positive imaginary part. We tested all choices of α_i, β_i satisfying (5.1) and (5.2), and computed the ξ of smallest degree that produces a $q(x)$ that represents primes in the sense of Definition 3.5. Some examples appear below.

Example 5.4 $(g = 2, k = 10, \rho = 6)$**.** Let $K = \mathbb{Q}(\zeta_5)$, $k = 10$, $r(x) = \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$. Algorithm 3.7 outputs

$$\begin{aligned}\pi(x) =& \tfrac{1}{25}(\zeta_5^3 - \zeta_5^2 - \zeta_5 + 1)x^6 + \tfrac{1}{25}(-6\zeta_5^3 + 5\zeta_5^2 + 3\zeta_5 - 2)x^5 + \tfrac{1}{5}(2\zeta_5^3 - \zeta_5^2 - 2)x^4 + \tfrac{1}{5}(-2\zeta_5^3 \\ & - \zeta_5 + 4)x^3 + \tfrac{1}{5}(3\zeta_5^3 - 2\zeta_5^2 - 2)x^2 + \tfrac{1}{25}(-4\zeta_5^3 - \zeta_5^2 - \zeta_5 + 11)x + \tfrac{1}{25}(4\zeta_5^3 - 5\zeta_5^2 - 2\zeta_5 - 2).\end{aligned}$$

The ρ-value of this family is 6. On input $y_0 = 2^{40}$, Algorithm 4.1 outputs $h = 5$ and $x_0 = 5497558154509$. We find that A is the Jacobian of the genus 2 curve

$$C : y^2 = x^5 + 15.$$

Then $r(x_0)$ is 5 times a 168-bit prime r_0. The ρ-value of A with respect to r_0 is within 10^{-10} of 6. □

Example 5.5 $(g = 2, k = 16, \rho = 7)$**.** Let $K = \mathbb{Q}(\eta)$, where $\eta = \sqrt{-2+\sqrt{2}}$. Let $k = 16$ and $r(x) = \Phi_{16}(x) = x^8 + 1$. Algorithm 3.7 outputs

$$\begin{aligned}\pi(x) =& \tfrac{1}{64}(-\eta^2 - 2)x^{14} + \tfrac{1}{32}(-\eta^2 - 3\eta - 2)x^{13} + \tfrac{1}{64}(\eta^2 - 4\eta - 16)x^{12} + \tfrac{1}{16}(-2\eta^3 + \eta^2 - 6\eta \\ & + 5)x^{11} + \tfrac{1}{64}(-8\eta^3 + \eta^2 - 28\eta)x^{10} + \tfrac{1}{32}(4\eta^3 - \eta^2 + 7\eta - 2)x^9 + \tfrac{1}{64}(8\eta^3 - \eta^2 + 16\eta \\ & - 34)x^8 + \tfrac{1}{8}(-\eta^3 - 2\eta + 4)x^7 + \tfrac{1}{64}(-8\eta^3 - \eta^2 - 16\eta - 2)x^6 + \tfrac{1}{32}(4\eta^3 - \eta^2 + 13\eta - 2)x^5 \\ & + \tfrac{1}{64}(8\eta^3 + \eta^2 + 28\eta - 16)x^4 + \tfrac{1}{16}(\eta^2 + 2\eta + 5)x^3 + \tfrac{1}{64}(\eta^2 + 4\eta)x^2 + \tfrac{1}{32}(-\eta^2 - \eta - 2)x \\ & + \tfrac{1}{64}(-\eta^2 - 2).\end{aligned}$$

The ρ-value of this family is 7. The single $\overline{\mathbb{Q}}$-isomorphism class of genus 2 curves whose Jacobians have CM by $\mathcal{O}_K$ is given by van Wamelen [22]. On input $y_0 = 2^{18}$, Algorithm 4.1 outputs $h = 2$ and $x_0 = 1083939$. We find A to be the Jacobian of the genus 2 curve

$$C : y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1.$$

Then $r(x_0)$ is 2 times a 160-bit prime r_0. The ρ-value of A with respect to r_0 is 6.91. □

Example 5.6 $(g = 2, k = 13, \rho = 20/3)$**.** Let $K = \mathbb{Q}(\eta)$, where $\eta = \sqrt{-13 + 2\sqrt{13}}$. Let $k = 13$ and let $r(x) = \Phi_{13}(x)$. Algorithm 3.7 outputs

$$\begin{aligned}\pi(x) = &\tfrac{1}{4056}(-19\eta^3 + 183\eta^2 - 377\eta + 2301)x^{20} + \tfrac{1}{338}(-2\eta^3 + 7\eta^2 - 39\eta + 78)x^{19} + \tfrac{1}{4056}(23\eta^3 \\ &+ 177\eta^2 + 481\eta + 2535)x^{18} + \tfrac{1}{1352}(7\eta^3 + 49\eta^2 + 65\eta + 767)x^{17} + \tfrac{1}{2028}(19\eta^3 + 141\eta^2 \\ &+ 221\eta + 1755)x^{16} + \tfrac{1}{1352}(\eta^3 + 97\eta^2 - 65\eta + 1183)x^{15} + \tfrac{1}{2028}(31\eta^3 + 192\eta^2 + 377\eta \\ &+ 2496)x^{14} + \tfrac{1}{1352}(13\eta^3 + 173\eta^2 + 195\eta + 2587)x^{13} + \tfrac{1}{26}(3\eta^2 - 2\eta + 39)x^{12} + \tfrac{1}{52}(\eta^3 + 8\eta^2 \\ &+ 11\eta + 104)x^{11} + \tfrac{1}{312}(5\eta^3 + 33\eta^2 + 55\eta + 507)x^{10} + \tfrac{1}{78}(2\eta^3 + 9\eta^2 + 28\eta + 117)x^9 \\ &+ \tfrac{1}{312}(5\eta^3 + 33\eta^2 + 55\eta + 507)x^8 + \tfrac{1}{4056}(97\eta^3 + 441\eta^2 + 1235\eta + 5811)x^7 + \tfrac{1}{338}(2\eta^3 \\ &+ 32\eta^2 + 13\eta + 429)x^6 + \tfrac{1}{2028}(8\eta^3 + 165\eta^2 + 52\eta + 2535)x^5 + \tfrac{1}{1352}(19\eta^3 + 81\eta^2 + 273\eta \\ &+ 923)x^4 + \tfrac{1}{338}(-\eta^3 + 9\eta^2 - 26\eta + 130)x^3 + \tfrac{1}{4056}(23\eta^3 + 99\eta^2 + 325\eta + 1521)x^2 \\ &+ \tfrac{1}{2028}(8\eta^3 + 3\eta^2 + 130\eta + 39)x + \tfrac{1}{338}(-\eta^2 - 13).\end{aligned}$$

The ρ-value of this family is 20/3. The single $\overline{\mathbb{Q}}$-isomorphism class of genus 2 curves whose Jacobians have CM by $\mathcal{O}_K$ is given by van Wamelen [22]. On input $y_0 = 7 \cdot 2^{15}$, Algorithm 4.1 outputs $h = 13$ and $x_0 = 3127658$. We find A to be the Jacobian of the genus 2 curve

$$C : y^2 = x^5 + 104x^4 + 5408x^3 + 140608x^2 + 1687296x + 7311616.$$

Then $r(x_0)$ is 13 times a 256-bit prime r_0. The ρ-value of A with respect to r_0 is 6.74. □

Some additional families we obtained for $g = 2$ are summarized in Table 1. The $\pi(x)$ produced by Algorithm 3.7 and example varieties of cryptographic size can be found online at `http://math.berkeley.edu/~dfreeman/papers/gen-bw-examples.pdf`.

Table 1. Best ρ-values for families of abelian surfaces.

k	CM field K	$r(x)$	ρ-value	k	CM field K	$r(x)$	ρ-value
6	$\mathbb{Q}(\sqrt{-6+3\sqrt{2}})$	$\Phi_{48}(x)$	7.5	30	$\mathbb{Q}(\zeta_5)$	$\Phi_{60}(x)$	7
8	$\mathbb{Q}(\sqrt{-5+\sqrt{5}})$	$\Phi_{40}(x)$	7.5	32	$\mathbb{Q}(\sqrt{-2+\sqrt{2}})$	$\Phi_{32}(x)$	7.5
15	$\mathbb{Q}(\zeta_5)$	$\Phi_{15}(x)$	7	40	$\mathbb{Q}(\zeta_5)$	$\Phi_{40}(x)$	6.5
20	$\mathbb{Q}(\zeta_5)$	$\Phi_{20}(x)$	6	60	$\mathbb{Q}(\zeta_5)$	$\Phi_{60}(x)$	7

We restrict to $r(x)$ of degree at most 16 because as the degree of $r(x)$ grows it becomes increasingly unlikely that we will find families with ρ-values significantly

less than 8. For the same reason, we expect that non-Galois quartic CM fields K will not provide greatly improved ρ-values, as we must work in a field L that contains the compositum of the Galois closure of K and the cyclotomic field $\mathbb{Q}(\zeta_k)$. In addition, as $\deg r(x)$ and $\deg q(x)$ grow, we expect to find fewer values of x for which both polynomials are primes of a specified size, and eventually we expect not to find any such values of x. (See [8, Proposition 8.1] for a more precise formulation of this idea.)

In dimension $g = 3$, we used the same procedure for the degree-6 Galois CM field $\mathbb{Q}(\zeta_7)$. The family we discovered produces three-dimensional ordinary abelian varieties with ρ-values better than the best previously known examples, which have $\rho \approx 18$ [9].

Example 5.7 ($g = 3, k = 7, \rho = 12$)**.** Let $K = \mathbb{Q}(\zeta_7)$, $k = 7$, and $r(x) = \Phi_7(x)$. Algorithm 3.7 outputs

$$\begin{aligned}\pi(x) =& \tfrac{1}{49}(-2\zeta_7^5 - 2\zeta_7^3 - 2\zeta_7^2 + 6\zeta_7)x^{12} + \tfrac{1}{49}(-7\zeta_7^5 + 4\zeta_7^4 - 4\zeta_7^3 + 2\zeta_7^2 + 13\zeta_7 - 1)x^{11} + \tfrac{1}{49}(-9\zeta_7^5 \\ &+ 10\zeta_7^4 - 2\zeta_7^3 + \zeta_7^2 + 23\zeta_7 + 5)x^{10} + \tfrac{1}{49}(-16\zeta_7^5 + 9\zeta_7^4 - 13\zeta_7^3 - 2\zeta_7^2 + 45\zeta_7 - 2)x^9 \\ &+ \tfrac{1}{49}(-22\zeta_7^5 + 6\zeta_7^4 - 19\zeta_7^3 + 3\zeta_7^2 + 39\zeta_7 - 7)x^8 + \tfrac{1}{49}(-7\zeta_7^5 + 13\zeta_7^4 - 2\zeta_7^3 - 2\zeta_7^2 + 28\zeta_7 \\ &+ 12)x^7 + \tfrac{1}{7}(-2\zeta_7^5 + \zeta_7^4 - 2\zeta_7^3 + \zeta_7^2 + 3\zeta_7 - 1)x^6 + \tfrac{1}{49}(-12\zeta_7^5 - 7\zeta_7^4 - 26\zeta_7^3 - 12\zeta_7^2 + 8\zeta_7)x^5 \\ &+ \tfrac{1}{49}(-7\zeta_7^5 + 3\zeta_7^4 - 10\zeta_7^3 + 5\zeta_7^2 + 8\zeta_7 - 6)x^4 + \tfrac{1}{49}(2\zeta_7^5 + 4\zeta_7^4 + 2\zeta_7^3 - \zeta_7^2 + 5\zeta_7 + 9)x^3 \\ &+ \tfrac{1}{49}(-5\zeta_7^5 - 2\zeta_7^4 - 8\zeta_7^3 + 2\zeta_7^2 - 3\zeta_7 - 5)x^2 + \tfrac{1}{49}(\zeta_7^5 + \zeta_7^4 - 2\zeta_7^3 - 3\zeta_7^2 + 3\zeta_7)x + \tfrac{1}{49}(\zeta_7^4 \\ &+ 2\zeta_7^3 + 2\zeta_7^2 + 2)\end{aligned}$$

The ρ-value of this family is 12. The single $\overline{\mathbb{Q}}$-isomorphism class of genus 3 curves whose Jacobians have CM by $\mathcal{O}_K$ is given by $y^2 = x^7 + 1$. On input $y_0 = 2^{28}$, Algorithm 4.1 outputs $h = 7$ and $x_0 = 1879056152$. We find A to be the Jacobian of the genus 3 curve

$$C : y^2 = x^7 + 16.$$

Then $r(x_0)$ is 7 times a 183-bit prime r_0. The ρ-value of A with respect to r_0 is 12.10. □

We also ran our algorithm for the degree-6 CM field $\mathbb{Q}(\zeta_9)$ and found families with ρ-values of 15 for $k = 9$ and $k = 18$. The $\pi(x)$ output by the algorithm and example varieties of cryptographic size can be found online at `http://math.berkeley.edu/~dfreeman/papers/gen-bw-examples.pdf`.

Abelian varieties with CM by $\mathbb{Q}(\zeta_9)$ are Jacobians of Picard curves of the form $y^3 = x^4 + ax$ [15]. We note that since these curves are not hyperelliptic, for any q-Weil number $\pi \in \mathbb{Z}[\zeta_9]$ there is a curve $C/\mathbb{F}_q$ whose Jacobian has Frobenius element either π or $-\pi$. In the second case the abelian variety over $\mathbb{F}_q$ with Frobenius element π is the quadratic twist of $\mathrm{Jac}(C)$, and is not isomorphic over $\mathbb{F}_q$ to a Jacobian. (See the Appendix of [16] for more details.)

Future Directions

Our construction improves on the best known ρ-values of pairing-friendly ordinary abelian varieties of dimension $g \geq 2$ for many different choices of CM

field K and embedding degree k. However, to make ordinary abelian varieties of dimension $g \geq 2$ competitive with elliptic curves in terms of performance, we must construct varieties with $\rho \leq 2$, with the ultimate goal of producing ρ-values close to 1. Achieving this goal is the most important problem for further work.

Our construction leaves a great deal of room for searching for better parameters. One direction would be to choose various Galois CM fields K and let $L = K(\zeta_k)$. Another approach would be to use the approach of Kachisa, Schaefer, and Scott [12] to search systematically through polynomials $r(x)$ such that $L \cong \mathbb{Q}[x]/(r(x))$. In the case where $g \geq 2$, one could also increase the size of the input Σ, which is the set from which we choose the residues α_i, β_i of ξ modulo factors of $r(x)$ in $\widehat{K}[x]$. In practice we find that when we use elements of Σ with large coefficients, the $q(x)$ computed have coefficients with large denominators and are thus unlikely to take integer values. However, even restricting Σ to contain only polynomials with small coefficients leaves many possible choices for α_i and β_i, and a program that searches systematically through these choices would have a very good chance of finding improved ρ-values.

References

1. R. Balasubramanian and N. Koblitz, "The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm," *Journal of Cryptology* **11** (1998), 141–145.
2. P.S.L.M. Barreto, B. Lynn, and M. Scott, "Constructing elliptic curves with prescribed embedding degrees," in *SCN 2002*, Springer LNCS **2576** (2002), 263–273.
3. P. Bateman and R. Horn, "A heuristic asymptotic formula concerning the distribution of prime numbers," *Math. Comp.* **16** (1962), 363–367.
4. F. Brezing and A. Weng, "Elliptic curves suitable for pairing based cryptography," *Designs, Codes and Cryptography* **37** (2005), 133–141.
5. C. Cocks and R. G. E. Pinch, "Identity-based cryptosystems based on the Weil pairing," Unpublished manuscript, 2001. (While this manuscript is unavailable, the main result appears as [8, Theorem 4.1].)
6. A. Enge, "The complexity of class polynomial computation via floating point approximations," to appear in *Math. Comp.* Preprint available at: `http://fr.arxiv.org/abs/cs.CC/0601104`.
7. D. Freeman, "Constructing pairing-friendly genus 2 curves with ordinary Jacobians," in *Pairings 2007*, Springer LNCS **4575** (2007) 152–176.
8. D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," Cryptology eprint 2006/371, available at `http://eprint.iacr.org`.
9. D. Freeman, P. Stevenhagen, and M. Streng, "Abelian varieties with prescribed embedding degree," to appear in *ANTS-VIII*, Springer LNCS **5011** (2008).
10. S. Galbraith, "Supersingular curves in cryptography," in *ASIACRYPT '01*, Springer LNCS **2248** (2001) 495–513.
11. L. Hitt, "On the minimal embedding field," in *Pairings 2007*, Springer LNCS **4575** (2007), 294–301.
12. E. Kachisa, E. Schaefer, and M. Scott, "Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field," Cryptology eprint 2007/452, available at `http://eprint.iacr.org`.

13. M. Kawazoe and T. Takahashi, "Pairing-friendly hyperelliptic curves of type $y^2 = x^5 + ax$," Cryptology eprint 2008/026, available at `http://eprint.iacr.org`.
14. D. Kohel, "Quartic CM fields database," available at `http://echidna.maths.usyd.edu.au/kohel/dbs/complex_multiplication2.html`.
15. K. Koike and A. Weng, "Construction of CM Picard curves," *Math. Comp.* **74** (2004), 499–518.
16. K. Lauter, with an appendix by J.-P. Serre, "The maximum or minimum number of rational points on genus three curves over nite elds," *Compositio Mathematica* **134** (2002), 87–111.
17. M. Naehrig, P. Barreto, and P. Schwabe, "On compressible pairings and their computation," Cryptology eprint 2007/429, available at `http://eprint.iacr.org`.
18. 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.
19. K. Rubin and A. Silverberg, "Supersingular abelian varieties in cryptology," in *CRYPTO '02*, Springer LNCS **2442**, 2002, 336–353.
20. G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, 1998.
21. J. Tate, "Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)," Séminaire Bourbaki 1968/69, Springer Lect. Notes in Math. **179** (1971) exposé 352, 95–110.
22. P. van Wamelen, "Examples of genus two CM curves defined over the rationals," *Math. Comp.* **68** (1999), 307–320.
23. A. Weng, "Hyperelliptic CM-curves of genus 3," *Journal of the Ramanujan Mathematical Society* **16**:4 (2001), 339–372.