# Generating Pairing-friendly Parameters for the CM Construction of Genus 2 Curves over Prime Fields

Kristin Lauter and Ning Shang

**Abstract.** We present two contributions in this paper. First, we give a quantitative analysis of the scarcity of pairing-friendly genus 2 curves, assuming the Riemann Hypothesis. This result is an improvement relative to prior work which estimated the density of pairing-friendly genus 2 curves heuristically. Second, we present a method for generating pairing-friendly parameters for which $\rho \approx 8$, where $\rho$ is a measure of efficiency in pairing-based cryptography. This method works by solving a system of equations given in terms of coefficients of the Frobenius element. The algorithm is easy to understand and implement.

## 1 Introduction

In order to use the Jacobian variety of a curve over a finite field for discrete logarithm based cryptography, suitable parameters must be chosen, and a curve with those parameters must be found. One such parameter is the underlying finite field $\mathbb{F}_p$ over which the curve is defined. Another important parameter is the cardinality $N$ of the group of $\mathbb{F}_p$-rational points on the Jacobian of the curve. For many implementations of discrete logarithm based cryptographic protocols, $\mathbb{F}_p$ is a prime field, i.e., $p$ is a prime number, and $N$ is prime number or a prime times a small cofactor, to resist the Pohlig-Hellman attack [19] on the discrete logarithm problem. Pairing-based cryptography poses further restrictions on the curves since in addition a small embedding degree is required.

Genus 2 point-counting methods ([13], [11]) choose random curve equations over a finite field and compute the number of points on the Jacobian of the curve until one that is good for discrete logarithm-based cryptography is found. An alternative to point counting is to use the genus 2 Complex Multiplication (CM) algorithm ([25]) to construct curves with a given number of points on its Jacobian. Like the case of the elliptic curve CM method, the genus 2 CM method is very efficient once the class polynomials of the CM field are computed. The hard problem is to find CM fields such that the class polynomials can be computed *and* such that the order of the Jacobian of the curve $N$ and the embedding degree are suitable. For a history of the genus 2 CM method, the reader can refer to [6]. In brief, the algorithm works as follows: Let $K$ be a quartic CM field with primitive CM type.

1. Find a prime $p$ such that there exists $\omega \in K$ with $\omega\bar{\omega} = p$, and an integer $N$ depending on $p$ and $\mathcal{O}_K$ which will be the group order of the Jacobian of the genus 2 curve having CM by $\mathcal{O}_K$. Such $p$ and $N$ can be identified by using a method in [25].
2. Compute the Igusa class polynomials $H_i(x), i = 1, 2, 3$ of $K$. This step can be done using the methods as described in one of [23], [25], [6], [14].
3. Construct a curve $C$ from a set of roots of $H_i(x)$ over $\mathbb{F}_p$ via the Mestre-Cardona-Quer Algorithm [18], [5], and check if the Jacobian of the curve has order $N$.

In practice to use the CM method, the quartic CM field $K$ must have small discriminant. So it is desirable to have algorithms which take as input a given field $K$, and output good cryptographic parameters $p$ and $N$ for a curve $C$ over $\mathbb{F}_p$ with $\#\mathrm{Jac}(C, \mathbb{F}_p) = N$, where $\mathrm{Jac}(C, \mathbb{F}_p)$ denotes the $\mathbb{F}_p$-rational points of the Jacobian of the curve $C$.

The genus 2 CM method is a useful alternative to point counting, since genus 2 point counting methods are still slow, and the low density of pairing-friendly curves among cryptographically strong ones, as we will see in Section 4, makes it extremely hard to find suitable curves for pairing-based cryptography via point counting. This indicates that the CM method is probably the only suitable method for finding pairing-friendly genus 2 curves currently available. In this paper, we

present a method for generating pairing-friendly parameters for the CM construction of genus 2 curves.

The rest of the paper is organized as follows: Section 2 reviews related work. Section 3 gives background on CM fields and pairings. Section 4 shows quantitatively the scarcity of pairing-friendly genus 2 curve among all those that are suitable for discrete-logarithm-based cryptography. Sections 5 and 6 propose two methods, without and with polynomial parameterization, for generating pairing-friendly genus 2 curves. Some sample numerical data can be found in the appendices.

This paper has been published as part of a PhD thesis [22].

## 2 Related work

In 2002, Rubin and Silverberg [20] showed that supersingular Jacobians of genus 2 hyperelliptic curves have small embedding degrees ($\leq 12$). In 2007, Hitt [15] presented, for characteristic 2, the construction of families of genus 2 curves with small embedding degree. Freeman [7] gave a method in 2007 for constructing genus 2 curves with ordinary Jacobians over prime fields, which uses parameterization of the CM fields to obtain conditions that lead to the result, and produces a value $\rho \approx 8$.[1] In 2008, Kawazoe and Takahashi [16] suggested a way to find pairing-friendly parameters to generate curves of the form $y^2 = x^5 + ax$ over $\mathbb{F}_p$ for a prime $p$ written as $p = c^2 + 2d^2$, by exploiting the closed formulas for the order of the Jacobian of such curves. This method produces curves with $\rho \leq 4$, whose Jacobians are however not absolutely simple. In 2008, Freeman, Stevenhagen and Streng [10] and Freeman [8] proposed methods for generating parameters for more general pairing-friendly ordinary abelian varieties. The former constructs a suitable Frobenius element which leads to a pairing-friendly abelian variety by extending a method of Cocks and Pinch [9]. The latter finds suitable polynomials parameterizing key elements and generates good parameters by evaluating such polynomials at many different input values. When applied to the case of genus 2, [10] produces $\rho \approx 8$ and [8] is able to further reduce the value to $\rho < 8$.

Although it is known to some extent (see [12]) that pairing-friendly parameters are very rare, among all the work generating such parameters for genus 2 curves, this is the first paper that analyzes quantitatively how unlikely cryptographically strong pairing-friendly parameters are.

The algorithms presented in this paper, together with those in [7], [10], and [8], are the only known methods that generate pairing-friendly parameters for ordinary genus 2 curves over prime fields, which have absolutely simple Jacobians. Unlike [7], we do not need to parameterize the CM field. Our algorithms are also more concrete and more explicit when compared to [10] and [8]. Therefore, these algorithms are easier to understand and implement.

## 3 Background

### 3.1 The CM field and the Frobenius element

Let $K := \mathbb{Q}(\eta)$, where

$$\eta = \begin{cases} i\sqrt{a + b\sqrt{d}} & \text{if } d \equiv 2, 3 \pmod 4 \\ i\sqrt{a + b\frac{-1+\sqrt{d}}{2}} & \text{if } d \equiv 1 \pmod 4 \end{cases},$$

be a fixed primitive quartic CM field, where $d > 0$ is squarefree and $\mathbb{Q}(\sqrt{d})$ has class number 1. The condition that $K$ is primitive is equivalent to $\Delta > 0$ is not a square, where $\Delta = a^2 - b^2 d$, if $d \equiv 2, 3 \pmod 4$, and $\Delta = a^2 - a \cdot b - b^2\left(\frac{d-1}{4}\right)$, if $d \equiv 1 \pmod 4$. We want to construct a genus 2 hyperelliptic curve $C$ over a finite field $\mathbb{F}_p$ of prime order such that $\text{End}(\text{Jac}(C, \mathbb{F}_p)) \otimes \mathbb{Q} = K$,

---

[1] The definition of $\rho$ can be found later in Section 5. It is a measure of efficiency in pairing-based cryptography. In general, the smaller $\rho$ is, the more efficient the pairing is for cryptography.

and $N := \#\mathrm{Jac}(C, \mathbb{F}_p)$ is "almost prime", meaning that $N$ is a product of a large prime number and a small cofactor.

If such a curve $C$ is found, then there exists an element, called the Frobenius element, $\pi \in \mathrm{End}(\mathrm{Jac}(C, \mathbb{F}_p))$ that satisfies the condition $|\pi| = \sqrt{p}$, where $|\pi|$ is the usual absolute value of the complex number $\pi$.

Assume for simplicity that the Frobenius element $\pi$ is in an order

$$\mathcal{O} := \begin{cases} \mathbb{Z} + \sqrt{d}\mathbb{Z} + \eta\mathbb{Z} + \eta\sqrt{d}\mathbb{Z} & \text{if } d \equiv 2, 3 \pmod 4 \\ \mathbb{Z} + \frac{-1+\sqrt{d}}{2}\mathbb{Z} + \eta\mathbb{Z} + \eta\frac{-1+\sqrt{d}}{2}\mathbb{Z} & \text{if } d \equiv 1 \pmod 4 \end{cases}.$$

We first look at the case $d \equiv 2, 3 \pmod 4$ and write

$$\pi = c_1 + c_2\sqrt{d} + \eta(c_3 + c_4\sqrt{d}), \quad c_i \in \mathbb{Z}.$$

The relationship $\pi\bar{\pi} = p$ gives us

$$(c_1^2 + c_2^2 d + c_3^2 a + c_4^2 ad + 2c_3 c_4 bd) + (2c_1 c_2 + 2c_3 c_4 a + c_3^2 b + c_4^2 bd)\sqrt{d} = p.$$

Since $1$ and $\sqrt{d}$ are linearly independent over $\mathbb{Q}$ we must have

$$c_1^2 + c_2^2 d + c_3^2 a + c_4^2 ad + 2c_3 c_4 bd = p \tag{1}$$
$$2c_1 c_2 + 2c_3 c_4 a + c_3^2 b + c_4^2 bd = 0 \tag{2}$$

Let $\bar{\alpha}$ and $\alpha^\sigma$ denote the imaginary and real embeddings of $K$ into $\overline{K}$. The characteristic polynomial of $\pi$ is

$$h(x) = (x - \pi)(x - \bar{\pi})(x - \pi^\sigma)(x - \bar{\pi}^\sigma)$$
$$= x^4 - 4c_1 x^3 + (2p + 4(c_1^2 - c_2^2 d))x^2 - 4c_1 px + p^2$$

The fact that $\#\mathrm{Jac}_{\mathbb{F}_p}(C) = h(1)$ gives the condition

$$N = (p+1)^2 - 4(p+1)c_1 + 4(c_1^2 - c_2^2 d). \tag{3}$$

We want $N$ to be almost prime, i.e., $N = c \cdot r$ with $r$ prime and $c$ small (say, $c < 2000$).

We have $p \sim N^{\frac{1}{2}}$. Based on the discussions above, Weng ([25]) gives a probabilistic method for searching for parameters for discrete logarithm based cryptography, which produces a prime $p$ and an almost prime $N$.

### 3.2 Weil and Tate-Lichtenbaum pairings

An excellent survey of the best known implementations of pairings on Jacobians of hyperelliptic curves is given in [2]. In this section we give only some basic information that we need about pairings on general abelian varieties.

For an abelian variety $\mathcal{A}$ over a finite field $F$ and an integer $r$ coprime to the characteristic of $F$, the Weil pairing is a nondegenerate, skew-symmetric bilinear map

$$e_r^W : \mathcal{A}(\bar{F})[r] \times \mathcal{A}(\bar{F})[r] \to \mu_r(\bar{F}),$$

where $\bar{F}$ is an algebraic closure of $F$ and $\mu_r(\bar{F})$ is the group of $r^{\text{th}}$ roots of unity in $\bar{F}$; the Tate-Lichtenbaum pairing is a nondegenerate bilinear map

$$e_r^{TL} : \mathcal{A}(F)[r] \times \mathcal{A}(F)/r\mathcal{A}(F) \to F^*/(F^*)^r.$$

$F^*/(F^*)^r$ is isomorphic to $\mu_r(\bar{F})$ if and only if $\mu_r(\bar{F}) \subseteq F$.

**Definition 1 (Embedding degree).** *Let $\mathcal{A}$ be an abelian variety over a finite field $F = \mathbb{F}_p$. Let $r$ be an integer coprime to $p$ which divides $\#\mathcal{A}(F)$. The field $F(\mu_r(\bar{F}))$ is a finite extension $\mathbb{F}_{p^k}$ of $F$. The number $k$ is called the **embedding degree of $\mathcal{A}$ with respect to** $r$, and it is the smallest integer such that $r|(p^k - 1)$.*

We also call the embedding degree of the Jacobian of a nonsingular projective curve $C$ the "embedding degree of the curve $C$." For pairing-based cryptography, we need an abelian variety $\mathcal{A}$ with $\#\mathcal{A}$ almost prime, i.e., $\#\mathcal{A} = h \cdot r$, where $h$ is a small positive integer and $r$ is a prime number, and the embedding degree $k$ of $\mathcal{A}$ with respect to $r$ which is not too large.

**Definition 2 (Pairing-friendly abelian variety).** *Let $H$ and $K$ be positive integers. Let $\mathcal{A}$ be an abelian variety over a finite field $\mathbb{F}_p$. We say $\mathcal{A}$ is **pairing-friendly with respect to parameters** $H$ and $K$ if $\#\mathcal{A} = h \cdot r$ for some positive integer $h \leq H$ and a prime number $r$, and the embedding degree $k$ of $\mathcal{A}$ with respect to $r$ is no larger than $K$.*

By convention, we call an abelian variety "pairing-friendly" if $H$ and $K$ are "small." We also say a nonsingular projective curve $C$ is "pairing-friendly" if $C$ has a pairing-friendly Jacobian. We also call the parameters $(p, \#\mathcal{A})$ "pairing-friendly".

## 4 Pairing-friendly genus 2 curves are rare: a quantitative analysis

In this section, we shall show (assuming the Riemann Hypothesis) quantitatively that there are very few pairing-friendly parameters for genus 2 hyperelliptic curves among all possible almost prime group orders for Jacobians of genus 2 hyperelliptic curves over prime fields. Inspired by [3], in which elliptic curves of prime orders over finite fields are considered, we generalize its result to the genus 2 case to also deal with Jacobians of *almost prime* orders. A heuristic estimation of the density of pairing-friendly genus 2 curves was performed earlier in [12]. Our result shows a more explicit improvement to this prior work. The main result of this section is Theorem 1. Before proving it, we first introduce several lemmas.

Let $p$ be an odd prime number, and let $\log(\cdot)$ denote the natural logarithm.

**Lemma 1.** *Let $M$ and $c$ be positive constants with $c < 4$. For a fixed positive integer $a$, let $\mathcal{S}_{a,c,M}$ denote the set of pairs of primes $(x, y)$ such that $\frac{M}{2} \leq x \leq M$ and $|x^2 - a \cdot y| \leq c \cdot x^{3/2}$. If the Riemann Hypothesis (R.H.) holds, then for large enough $M$, we have*

$$|\mathcal{S}_{a,c,M}| \geq \frac{1}{15} \cdot \frac{c}{a} \cdot \frac{M^{5/2}}{(\log M)^2}.$$

*Proof.* Let $\pi(x)$ be number of primes in the interval $[1, x]$. Let $N = \pi(M) - \pi(\frac{M}{2})$ be the number of primes in $(M/2, M]$. The Prime Number Theorem (P.N.T.) implies $N > \frac{1}{3} \cdot \frac{M}{\log M}$ for $M$ large enough.

Now let $p$ be a prime number in $(M/2, M]$. We look at the number of primes $y$ such that $|p^2 - a \cdot y| \leq c \cdot p^{3/2}$, i.e., $\frac{1}{a}\left(p^2 - c \cdot p^{3/2}\right) \leq y \leq \frac{1}{a}\left(p^2 + c \cdot p^{3/2}\right)$. Denote this number by $N_p$. By a theorem of von Koch (see [1], Theorem 8.3.3), if the R.H. is true,

$$\pi(x) = \text{li}(x) + O(\sqrt{x} \log x),$$

where $\text{li}(x) = \int_2^x dt / \log t$. Moreover, by a result of L. Schoenfeld (see [21], Corollary 1), if R.H. is true, there exists an effectively computable positive constant $c_1$ such that $|\pi(x) - \text{li}(x)| <$

$c_1 \cdot \sqrt{x} \log x$, when $x \geq 2657$. According to this result, when $p$ is large, we have

$$
\begin{aligned}
N_p &\geq \pi\left(\frac{1}{a}\left(p^2 + c \cdot p^{3/2}\right)\right) - \pi\left(\frac{1}{a}\left(p^2 - c \cdot p^{3/2}\right)\right) \\
&> \mathrm{li}\left(\frac{1}{a}\left(p^2 + c \cdot p^{3/2}\right)\right) - \mathrm{li}\left(\frac{1}{a}\left(p^2 - c \cdot p^{3/2}\right)\right) \\
&\quad - \frac{1}{a} \cdot c_1 (p^2 + c \cdot p^{3/2})^{1/2} \log\left(p^2 + c \cdot p^{3/2}\right) \\
&\quad - \frac{1}{a} \cdot c_1 \left(p^2 - c \cdot p^{3/2}\right)^{1/2} \log\left(p^2 - c \cdot p^{3/2}\right) \\
&> \int_{\frac{1}{a}\left(p^2 - c \cdot p^{3/2}\right)}^{\frac{1}{a}\left(p^2 + c \cdot p^{3/2}\right)} \frac{\mathrm{d}t}{\log t} - \frac{1}{a} \cdot 2c_1 \left(p^2 + c \cdot p^{3/2}\right)^{1/2} \log\left(p^2 + c \cdot p^{3/2}\right) \\
&> \frac{1}{\log\left(\frac{1}{a} \cdot \left(M^2 + c \cdot M^{3/2}\right)\right)} \cdot \frac{1}{a}\left(2c\left(\frac{M}{2}\right)^{3/2}\right) - \frac{1}{a} \cdot 2c_1 \left(2M^2\right)^{1/2} \log\left(2M^2\right) \\
&> \frac{1}{\log\left(2M^2\right) - \log a} \cdot \frac{c}{a\sqrt{2}} M^{3/2} - \frac{1}{a} \cdot 8c_1 M \log M \\
&> \frac{1}{a}\left(\frac{cM^{3/2}}{4\log M} - 8c_1(M\log M)\right) \\
&> \frac{1}{5} \cdot \frac{c}{a} \cdot \frac{M^{3/2}}{\log M}.
\end{aligned}
$$

The last inequality holds if $\frac{1}{20} \cdot cM^{3/2}/\log M > 8 \cdot c_1 M \log M$, i.e., $M^{1/2}/(\log M)^2 > 160 \cdot c_1/c$.

Note that the vaule $p$ does not appear in the resulting inequality above. Summing over all suitable primes $p$, we obtain

$$
|\mathcal{S}_{a,c,M}| = \sum_{\substack{\frac{M}{2} \leq p \leq M \\ p \text{ prime}}} N_p \geq \frac{1}{5} \cdot \frac{c}{a} \cdot \frac{M^{3/2}}{\log M} \cdot \frac{1}{3} \cdot \frac{M}{\log M} = \frac{1}{15} \cdot \frac{c}{a} \cdot \frac{M^{\frac{5}{2}}}{(\log M)^2}
$$

for large enough $M$. $\qquad\square$

*Remark 1.* Note that in the proof above, the constant $c/15$ depends only on $M$ (and constant $c_1$), but not on $a$.

*Remark 2.* If we take $a = 1$, the result of Lemma 1 is comparable to the heuristic result in [12] (estimate of the volume of $S$ in Section 4.2 of [12]).

**Lemma 2.** *Let $M$ and $K$ be positive constants. For a fixed positive integer $a$, let $\mathcal{T}_{a,M,K}$ denote the set of pairs of primes $(x,y)$ such that $\frac{M}{2} \leq x \leq M$, $|x^2 - a \cdot y| \leq 5x^{3/2}$ and $y|(x^k - 1)$ for some $k \leq K$. Then $|\mathcal{T}_{a,M,K}| < \frac{45}{8}M^{3/2}(K+1)^2 \log(5^{3/2}M)$.*

*Proof.* For every nonzero integer $h$ with $|h| \leq 5M^{3/2}$, let $\mathcal{B}_h^{(e)}$ be the set of primes $y$ such that $y|h^{k/2} - 1$ for some even integer $k$ with $0 < k \leq K$. Since $h^{k/2} - 1$ has fewer than $\log(|h|^{k/2})$ distinct prime divisors, we have

$$
\begin{aligned}
|\mathcal{B}_h^{(e)}| &< \sum_{\substack{k=2 \\ k \text{ even}}}^{K} \frac{k}{2} \log|h| \leq \frac{1}{2}\left(\frac{K}{2}\right)\left(\frac{K}{2} + 1\right) \log|h| \\
&\leq \frac{1}{2}\left(\frac{K}{2}\right)\left(\frac{K}{2} + 1\right)(3/2)\log(5^{3/2}M) \\
&\leq \frac{3}{16}K(K+2)\log(5^{3/2}M).
\end{aligned}
$$

Now for the same $h$, let $\mathcal{B}_h^{(o)}$ denote the set of primes $y$ such that $y|h^k - 1$ for some odd integer $k$ with $0 < k \leq K$. Since $h^k - 1$ has fewer than $\log(|h|^k)$ distinct prime divisors,

$$\begin{aligned}
|\mathcal{B}_h^{(o)}| &< \sum_{\substack{k=1 \\ k \text{ odd}}}^{K} k \log|h| \leq \frac{\lceil \frac{K}{2} \rceil (K+1)}{2} \log|h| \\
&\leq \frac{1}{4}(K+1)^2 \, (3/2) \log\left(5^{3/2}M\right) \\
&= \frac{3}{8}(K+1)^2 \log\left(5^{3/2}M\right).
\end{aligned}$$

Let $\mathcal{B}_h$ be the set of pairs of primes $(x, y)$ such that $x^2 - a \cdot y = h$. When $k$ is even, we have

$$h^{k/2} = \left(x^2 - a \cdot y\right)^{k/2} = x^k + y \cdot (\text{polynomial in } x \text{ and } y);$$

thus $y|h^{k/2} - 1$ is equivalent to $y|x^k - 1$. Similarly, when $k$ is odd, $y|x^k - 1$ implies $y|x^{2k} - 1$, which again implies $y|h^k - 1$. Therefore, we must have

$$\begin{aligned}
|\mathcal{B}_h| &\leq |\mathcal{B}_h^{(e)}| + |\mathcal{B}_h^{(o)}| \\
&\leq \frac{3}{16}K(K+2)\log\left(5^{3/2}M\right) + \frac{3}{8}(K+1)^2 \log\left(5^{3/2}M\right) \\
&< \frac{9}{16}(K+1)^2 \log(5^{3/2}M).
\end{aligned}$$

Summing over all such integer $h$ and note that $\frac{M}{2} \leq x \leq M$, we have

$$|\mathcal{T}_{a,M,K}| \leq \sum_{0 < |h| \leq 5M^{3/2}} |\mathcal{B}_h| < \frac{45}{8}M^{3/2}(K+1)^2 \log(5^{3/2}M).$$

$\square$

*Remark 3.* It is worth noting that the result in Lemma 2 does not require $M$ to be large.

*Remark 4.* It is possible that the result of Lemma 2 may be further refined to be closer to the heuristic result in [12] (the estimate of the volume of $S'$ in Section 4.2 of [12]). However, such a refinement would likely require techniques different from those used in the proof of Lemma 2.

**Lemma 3.** *Let $\widetilde{\mathcal{S}}_{H,c,M}$ denote the set of pairs of primes $(x, y)$ such that $\frac{M}{2} \leq x \leq M$ and $\left|x^2 - a \cdot y\right| \leq c \cdot x^{3/2}$ for some $a \in \mathbb{Z}$, $1 \leq a \leq H$. Let $\widetilde{\mathcal{T}}_{H,M,K}$ denote the set of pairs of primes $(x, y)$ such that $\frac{M}{2} \leq x \leq M$, $\left|x^2 - a \cdot y\right| \leq 5x^{3/2}$ for some $a \in \mathbb{Z}$, $1 \leq a \leq H$, and $y|(x^k - 1)$ for some $k \leq K$. If the R.H. holds, then for large $M$,*

$$\frac{\widetilde{\mathcal{T}}_{H,M,K}}{\widetilde{\mathcal{S}}_{H,c,M}} < c' \frac{H \cdot (K+1)^2 (\log M)^3}{c \cdot M}$$

*for an effectively computable positive constant $c'$. A possible choice of such a constant is $c' = 90$ .*

*Proof.* Let $a$ be an integer such that $1 \leq a \leq H$. By Lemma 1 and Lemma 2, we have

$$\begin{aligned}
\frac{\mathcal{T}_{a,M,K}}{\mathcal{S}_{a,c,M}} &< \frac{\frac{45}{8}M^{3/2}(K+1)^2 \log(5^{3/2}M)}{\frac{1}{15} \cdot \frac{c}{a} \cdot \frac{M^{\frac{5}{2}}}{(\log M)^2}} \\
&< 90 \cdot \frac{a \cdot (K+1)^2 (\log M)^3}{c \cdot M} \\
&< 90 \cdot \frac{H \cdot (K+1)^2 (\log M)^3}{c \cdot M}
\end{aligned}$$

for $M$ large enough. Note that $\widetilde{\mathcal{T}}_{H,M,K} = \sum\limits_{1 \le a \le H} \mathcal{T}_{a,M,K}$ and $\widetilde{\mathcal{S}}_{H,c,M} = \sum\limits_{1 \le a \le H} \mathcal{S}_{a,c,M}$, and consider Remark 1 following Lemma 1. Hence we have

$$\frac{\widetilde{\mathcal{T}}_{H,M,K}}{\widetilde{\mathcal{S}}_{H,c,M}} < 90 \cdot \frac{H \cdot (K+1)^2 (\log M)^3}{c \cdot M}$$

for large $M$. □

**Theorem 1.** *Assume the Riemann Hypothesis. Let $H$ and $K$ be positive constants. Let $(p, N)$ be a randomly (w.r.t. uniform distribution) chosen pair in which $p$ is a prime in the interval $[\frac{M}{2}, M]$ and $N$ is the group order of the Jacobian of a genus 2 curve $C$ defined over $\mathbb{F}_p$ with $N = \#\mathrm{Jac}(C, \mathbb{F}_p) = h \cdot r$, with $1 \le h \le H$ and $r$ prime. For $M$ large enough, the probability that $(p, N)$ is pairing-friendly with respect to parameters $H$ and $K$ is less than*

$$c'' \frac{H \cdot (K+1)^2 (\log M)^3}{M}$$

*for an effectively computable positive constant $c''$.*

*Proof.* The Riemann Hypothesis for abelian varieties over finite fields, proved by Weil in [24], implies the Hasse-Weil bound for genus 2 curves, i.e.,

$$\#\mathrm{Jac}(C, \mathbb{F}_p) \in \left[ (\sqrt{p} - 1)^4, (\sqrt{p} + 1)^4 \right].$$

For $p$ large enough, we have $\#\mathrm{Jac}(C, \mathbb{F}_p) \in \left[ p^2 - 5p^{3/2}, p^2 + 5p^{3/2} \right]$. Let $c = 1/9$. By Proposition 2.4 of [17], almost all integers $z \in \left[ p^2 - cp^{3/2}, p^2 + cp^{3/2} \right]$ can be assumed to be the cardinality of the Jacobian of a genus 2 hyperelliptic curve (given by a quintic or sextic polynomial) over $\mathbb{F}_p$. In Lemma 3, let $c = 1/9$, $x = p$, $y = r$ and $a = h$. The conclusion then follows, observing that $c = 1/9$ is small enough so that the total number of pairs $(p, N)$ in the statement of Theorem 1 is strictly larger than $\widetilde{\mathcal{S}}_{H,c,M}$. Note that we can choose $c'' = 10c'$, where $c'$ is the constant from Lemma 3. □

Theorem 1 says there are very few pairing-friendly parameters for genus 2 hyperelliptic curves when $H$ and $K$ are much smaller than $p$.

## 5 Algorithms for generating pairing-friendly genus 2 curves over prime fields

Let $k$ be a desired embedding degree. Let $C$ be a genus 2 hyperelliptic curve defined over a finite field $\mathbb{F}_p$ whose Jacobian over $\mathbb{F}_p$ has a subgroup of order $r$ such that $\mathrm{Jac}(C, \mathbb{F}_p)$ has embedding degree $k$ with respect to $r$. The ratio of the bit length of $\#\mathrm{Jac}(C, \mathbb{F}_p)$ to the bit length of $r$ is a good measure of efficiency in pairing-based cryptography. Define

$$\rho = 2\log(p)/\log(r).$$

In many pairing-based cryptographic applications, we prefer this value to be close to 1.

In [7], a method to generate genus 2 curves with ordinary Jacobians over prime fields with low embedding degrees is proposed. An important part of this method is a parameterization of the CM field. The method generates curves with value $\rho \approx 8$. We propose another way of generating good parameters, without parameterizing the CM field, which gives a similar $\rho$ value.

Let $K := \mathbb{Q}(\eta)$ be a fixed quartic CM field. We want to construct a genus 2 hyperelliptic curve $C$ over a prime field $\mathbb{F}_p$ such that $\mathrm{Jac}(C, \mathbb{F}_p)$ has CM by $K$, and such that $\mathrm{Jac}(C, \mathbb{F}_p)$ has a subgroup of prime order $r$, and $\mathrm{Jac}(C, \mathbb{F}_p)$ has a prescribed embedding degree $k$ with respect to $r$. For cryptographic applications, we need $p$ and $r$ to be large. We will present the algorithm for the

case $d \equiv 2, 3 \pmod 4$ in this paper, where $d$ is as defined in Section 3.1. The case $d \equiv 1 \pmod 4$ can be treated similarly.

In the case $d \equiv 2, 3 \pmod 4$, such a curve can be constructed if we can find a simultaneous integral solution $(c_1, c_2, c_3, c_4, p, r)$, in which $p$ and $r$ are large prime numbers, to the following system of equations:

$$c_1^2 + c_2^2 d + c_3^2 a + c_4^2 ad + 2c_3 c_4 bd = p \tag{4}$$

$$2c_1 c_2 + 2c_3 c_4 a + c_3^2 b + c_4^2 bd = 0 \tag{5}$$

$$(p+1)^2 - 4c_1(p+1) + 4(c_1^2 - dc_2^2) \equiv 0 \pmod r \tag{6}$$

$$\Phi_k(p) \equiv 0 \pmod r. \tag{7}$$

Here $a, b, d$ and $k$ are fixed, and $\Phi_k(x)$ is the $k^{\text{th}}$ cyclotomic polynomial. Equations (4) and (5) mean that the prime $p$ corresponds to a good Weil number, as discussed in Section 3.1. Equation (6) ensures that the Jacobian has a subgroup of prime order $r$. Equation (7) guarantees that the Jacobian of the curve the embedding degree with respect to $r$ is at most $k$. Note that Equation 7 implies $p^k \equiv 1 \pmod r$. Given that $p^{r-1} \equiv 1 \pmod r$, we must have $k|(r-1)$, i.e., $r \equiv 1 \pmod k$.

---

**Algorithm 1** Generating pairing parameters for $K = \mathbb{Q}(\eta)$, $d \equiv 2, 3 \pmod 4$

---

**Require:** Integers $a, b, d$ with $d > 0$ squarefree, $d \equiv 2, 3 \pmod 4$, $a^2 - b^2 d > 0$ not a square; a prescribed embedding degree $k$; a bit size $n$ of the desired subgroup order; maximum numbers of trials, $M_1$ and $M_2$.

**Ensure:** Integers $c_1, c_2, c_3, c_4$, prime numbers $p$ and $r$, where $r$ has $n$ bits, satisfying Equations (4), (5), (6), (7); or "Not found."

1: Let $c_1 = \pm 1$.
2: **repeat**
3:     Choose a prime number $r$ of $n$ bits such that $r \equiv 1 \pmod k$.
4:     With $c_1$ fixed as above, try to solve the system of equations given by (4), (5), (6), (7) over the finite field $\mathbb{F}_r$ for a simultaneous solution $(\bar{c}_2, \bar{c}_3, \bar{c}_4, \bar{p})$.
5:     **if** such a solution exists **then**
6:       **repeat**
7:         Choose lifts $c_3$ and $c_4$ of $\bar{c}_3$ and $\bar{c}_4$ to $\mathbb{Z}$ such that $f := bc_3^2 + 2ac_3 c_4 + bdc_4^2$ is even. Set $c_2 = -c_1 f/2$.
8:         Let $p = ac_3^2 + 2bdc_3 c_4 + 2adc_4^2 + 1 + dc_2^2$.
9:         **if** $p$ is prime **then**
10:           Return $(c_1, c_2, c_3, c_4, p, r)$.
11:         **end if**
12:       **until** Lines 7 through 11 have been tried $M_2$ times.
13:     **end if**
14: **until** $M_1$ primes $r$ have been tried.
15: Return "Not found."

---

**Theorem 2.** *If $(c_1, c_2, c_3, c_4, p, r)$ is returned by Algorithm 1, then it provides a solution to the system of equations (4), (5), (6), (7).*

*Proof.* It is clear that if $(c_1, c_2, c_3, c_4, p, r)$ is returned, then Equations (6) and (7) are automatically satisfied. Equations (4) and (5) are satisfied by the constructions in Step 7 and 8. Step 9 ensures that $p$ is prime. □

Depending on $p$ and $\mathcal{O}_K$, there are 2 or 4 possibilities for the group order $\#\mathrm{Jac}(C, \mathbb{F}_q)$ [25] [6]. However, for a demonstration purpose, in the algorithm above we are only interested in curves $C$ whose Jacobian has exact group order given by

$$N = (p+1)^2 - 4c_1(p+1) + 4(c_1^2 - dc_2^2).$$

Algorithm 1 looks difficult to analyze because we do not know how likely it is that a solution is found in Step 4. However, experimental results show that the algorithm returns valid parameters quickly and with high probability.

**Example 3.** Using Algorithm 1 in the case of $a = 2, b = -1, d = 2$, some suitable pairing parameters are found in Appendix A, where $r$ are 160, 256, 512 and 1024 bits, respectively. The computations were performed by the computer algebra system MAGMA [4]. Note that $K = \mathbb{Q}(i\sqrt{2 - \sqrt{2}}) \neq \mathbb{Q}(\zeta_5)$ is Galois, so there are only two possibilities for the group order $\#\mathrm{Jac}(C, \mathbb{F}_p)$ [25], namely,

$$N_1 = (p + 1)^2 - 4c_1(p + 1) + 4(c_1^2 - dc_2^2),$$

or the group order for a quadratic twist of the curve:

$$N_2 = 2(p + 1)^2 + 8(c_1^2 - c_2^2 d) - N_1.$$

## 6 Generating parameters with polynomial parameterization of coefficients $c_i$

The parameter $c_1$ produced by Algorithm 1 is always $\pm 1$ and the size of $c_2$ dominates that of $c_1, c_3$ and $c_4$. In fact, this is not necessary. We can modify the search method using the idea of polynomial parameterization and produce pairing parameters with $c_1, c_2, c_3$ and $c_4$ roughly of the same size. The algorithm is stated as Algorithm 2.

---

**Algorithm 2** Generating pairing parameters for $K = \mathbb{Q}(\eta)$, $d \equiv 2, 3 \pmod 4$ with polynomial parameterization

---

**Require:** Integers $a, b, d$ with $d > 0$ squarefree, $d \equiv 2, 3 \pmod 4$, $a^2 - b^2 d > 0$ not a square; a prescribed embedding degree $k$; a bit size $n$ of the desired subgroup order; maximum numbers of trials, $M_1$ and $M_2$.

**Ensure:** Integers $c_1, c_2, c_3, c_4$, prime numbers $p$ and $r$, where $r$ has $n$ bits, satisfying Equations (4), (5), (6), (7); or "Not found."

1: Choose degree 2 bivariate polynomials $C_3(x, y)$ and $C_4(x, y) \in \mathbb{Z}[x, y]$ such that there is a factorization in $\mathbb{Z}[x, y]$
$$bC_3^2 + 2aC_3C_4 + bdC_4^2 = U \cdot V,$$
where $U$ and $V$ are bivariate polynomials of degree 2. Let $C_1(x, y) = U(x, y)$ and $C_2(x, y) = -\frac{1}{2}V(x, y)$.

2: **repeat**

3:     Choose a prime number $r$ of $n$ bits such that $r \equiv 1 \pmod k$.

4:     Try to solve the system of equations given by (5), (6), (7), with $c_i$ replaced by $C_i(x, y), i = 1, 2, 3, 4$, over the finite field $\mathbb{F}_r$ for a simultaneous solution $(\bar{x}, \bar{y}, \bar{p})$.

5:     **if** Such a solution exists **then**

6:         **repeat**

7:             Choose lifts $x$ and $y$ of $\bar{x}$ and $\bar{y}$ to $\mathbb{Z}$ such that $c_i := C_i(x, y), i = 1, 2, 3, 4$ are all integers. Let $p = ac_3^2 + 2bdc_3c_4 + 2adc_4^2 + c_1^2 + dc_2^2$.

8:             **if** $p$ is prime **then**

9:                 Return $(c_1, c_2, c_3, c_4, p, r)$.

10:             **end if**

11:         **until** Lines 7 through 10 have been tried $M_2$ times.

12:     **end if**

13: **until** $M_1$ primes $r$ have been tried.

14: Return "Not found."

---

Similarly to Theorem 2, we have

**Theorem 3.** *If $(c_1, c_2, c_3, c_4, p, r)$ is returned by Algorithm 2, then it provides a solution to the system of equations (4), (5), (6), (7).*

In Algorithm 2, it is clear that we need $\gcd(C_1, C_2, C_3, C_4) = 1 \in \mathbb{Z}[x, y]$ so that a prime $p$ can be found.

**Example 3.** Let $C_3(x, y) = C_4(x, y) = xy$, $C_1(x, y) = x^2$ and $C_2(x, y) = -(a + b(1 + d)/2)y^2$. Then they satisfy $bC_3^2 + 2aC_3C_4 + bdC_4^2 + 2C_1C_2 = 0$. Using these polynomials in the above algorithm, we have found for $K = \mathbb{Q}(i\sqrt{2 - \sqrt{2}})$ (i.e., $a = 2, b = -1, d = 2$) parameters in which $r$ are 160, 256, 512 and 1024 bits, respectively. Some of these parameters are presented in Appendix B.

Since $x$ and $y$ are roughly the same size as $r$, the value of $p$ obtained by this method is $\approx r^4$. It is thus a natural thought that if we parameterize the polynomials $C_i(x, y)$ with degree 1 polynomials in $\mathbb{Z}[x, y]$, then the size of $p$ may be reduced to $\approx r^2$. Unfortunately, the following Proposition 1 shows that such parameterizations will not succeed in achieving this goal.

**Proposition 1.** *Let $a, b, d$ be integers such that $d$ is squarefree and $a^2 - b^2d > 0$ is not a square. Let $f(X, Y) = bX^2 + 2aXY + bdY^2$ be a bivariate polynomial in $\mathbb{Q}[X, Y]$. Let $F, G$ be polynomials of total degree 1 in $\mathbb{Q}[X_1, X_2, \ldots, X_n]$ such that $F$ and $G$ are not associated with one another. Then $f(F, G)$ is irreducible in $\mathbb{Q}[X_1, X_2, \ldots, X_n]$.*

*Proof.* First we note that $b \neq 0$, as indicated by the condition that $a^2 - b^2d > 0$ is not a square. Let $D = a^2 - b^2d$. Let $\alpha = -a/b + \sqrt{D}/b$ and $\beta = -a/b - \sqrt{D}/b$. Then $f(X, Y)$ can be factored over $\bar{\mathbb{Q}}$ as

$$f(X, Y) = bX^2 + 2aXY + bdY^2 = b(X - \alpha Y)(X - \beta Y),$$

where $\bar{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.

Let $F$ and $G$ be polynomials of total degree 1 in $\mathbb{Q}[X_1, X_2, \ldots, X_n]$. Write

$$F(X_1, X_2, \ldots, X_n) = \sum_{i=1}^{n} f_i X_i + f_0,$$

$$G(X_1, X_2, \ldots, X_n) = \sum_{i=1}^{n} g_i X_i + g_0,$$

where $f_i, g_i \in \mathbb{Q}$. Suppose $f(F, G)$ is reducible in $\mathbb{Q}[X_1, X_2, \ldots, X_n]$. Then we can write

$$f(F, G) = bH_1 \cdot H_2,$$

where $H_j = \sum_{i=1}^{n} h_i^{(j)} X_i + h_0^{(j)} \in \mathbb{Q}[X_1, X_2, \ldots, X_n]$, $j = 1, 2$, both of total degree 1.

Now we have

$$b(F - \alpha G)(F - \beta G) = f(F, G) = bH_1 \cdot H_2.$$

Note that $\mathbb{Q}(\sqrt{D})[X_1, X_2, \ldots, X_n]$ is a unique factorization domain. Because $F - \alpha G$, $F - \beta G$, $H_1$ and $H_2$ are of degree 1, they are irreducible. without of loss of generality, we may assume

$$F - \alpha G = \gamma H_1, \tag{8}$$

for some $\gamma \in \mathbb{Q}(\sqrt{D})^\times$. We can write $\gamma = s + t\sqrt{D}$ with $s, t \in \mathbb{Q}$ and $t \neq 0$. Here we require $t \neq 0$ as the polynomial on the left hand side of Equation (8) is in $\mathbb{Q}(\sqrt{D})[X_1, X_2, \ldots, X_n] \backslash \mathbb{Q}[X_1, X_2, \ldots, X_n]$.

Equation (8) gives

$$F - (-a/b + \sqrt{D}/b)G = (s + t\sqrt{D})H_1.$$

Equating the coefficients of $X_i$ and the constant terms on both sides of the above equation, we obtain

$$f_i + (a/b)g_i + (g_i/b)\sqrt{D} = s \cdot h_i^{(1)} + t \cdot h_i^{(1)}\sqrt{D}, \quad 0 \leq i \leq n.$$

This in turn gives

$$f_i + (a/b)g_i = s \cdot h_i^{(1)}, \tag{9}$$

$$g_i/b = t \cdot h_i^{(1)}. \tag{10}$$

If $g_i = 0$ for some $i$, we must have $h_i^{(1)} = 0$ by (10), which again implies $f_i = 0$ by (9). Otherwise, if $g_i \neq 0$, we can divide both sides of (9) and (10) to obtain

$$b(f_i/g_i) = s/t,$$

thus

$$f_i/g_i = s/(b \cdot t).$$

Therefore, for all $0 \leq i \leq n$, we have $f_i = c \cdot g_i$, where the constant $c = s/(b \cdot t) \in \mathbb{Q}$. Hence $F = c \cdot G$, i.e., $F$ and $G$ are associated. $\qquad\square$

An alternative way to do polynomial parameterization in Step 1 of Algorithm 2 is to use degree 1 and degree 2 polynomials for $C_3(x, y)$ and $C_4(x, y)$. This will produce different kinds of $c_i$'s, but the resulting $\rho$ value is still approximately 8 in general. On-going research is aiming at reducing further the value of $\rho$.

# References

1. E. Bach and J. Shallit. *Algorithmic Number Theory, Volume I: Efficient Algorithms.* The MIT Press, August 1996.
2. J. Balakrishnan, J. Belding, S. Chisholm, K. Eisenträger, K. Stange, and E. Teske. Pairings on hyperelliptic curves. http://arxiv.org/PS_cache/arxiv/pdf/0908/0908.3731v2.pdf.
3. 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(2):141–145, 1998.
4. W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system I: the user language. *J. Symb. Comput.*, 24(3-4):235–265, 1997.
5. G. Cardona and J. Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, volume 13, pages 71–83, 2005.
6. K. Eisenträger and K. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. In *Arithmetic, Geometry and Coding Theory (AGCT), Séminaires et Congrés 21 (2009)*, pages 161–176, 2005.
7. D. Freeman. Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians. In *Proceedings of Pairing-Based Cryptography (Pairing 2007)*, volume 4575 of *LNCS*, pages 152–176. Springer, 2007.
8. D. Freeman. A Generalized Brezing-Weng Algorithm for Constructing Pairing-Friendly Ordinary Abelian Varieties. In Steven Galbraith and Kenneth Paterson, editors, *Pairing-Based Cryptography - Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 146–163. Springer Berlin / Heidelberg, 2008.
9. D. Freeman, M. Scott, and E. Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology*, 23:224–280, 2010.
10. D. Freeman, P. Stevenhagen, and M. Streng. Abelian varieties with prescribed embedding degree. In *Algorithmic Number Theory VIII*, pages 60–73, 2008.
11. E. Furukawa, M. Kawazoe, and T. Takahashi. Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields. In Mitsuru Matsui and Robert Zuccherato, editors, *Selected Areas in Cryptography*, volume 3006 of *Lecture Notes in Computer Science*, pages 26–41. Springer Berlin / Heidelberg, 2004.
12. S.D. Galbraith, J.F. McKee, and P.C. Valenca. Ordinary abelian varieties having small embedding degree. *Finite Fields and Their Applications*, 13(4):800–814, 2007.
13. P. Gaudry and R. Harley. Counting points on hyperelliptic curves over finite fields. In Wieb Bosma, editor, *Algorithmic Number Theory*, volume 1838 of *Lecture Notes in Computer Science*, pages 313–332. Springer Berlin / Heidelberg, 2000.

14. P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 114–129. Springer Berlin / Heidelberg, 2006.

15. L. Hitt. Families of genus 2 curves with small embedding degree. Cryptology ePrint Archive, Report 2007/001, 2007.

16. M. Kawazoe and T. Takahashi. Pairing-friendly hyperelliptic curves of type $y^2 = x^5 + ax$. In *Symposium on Cryptography and Information Security (SCIS)*, 2008.

17. H.W. Lenstra, Jr, J. Pila, and C. Pomerance. A hyperelliptic smoothness test, II. *Proc. London Math. Soc.*, 84(1):105–146, 2002.

18. J-F Mestre. Construction de courbes de genre 2 à partir de leurs modules. (Construction of genus 2 curves starting from their moduli). Effective methods in algebraic geometry, Proc. Symp., Castiglioncello/Italy 1990, Prog. Math. 94, 313-334 (1991)., 1991.

19. S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Trans. Information Theory*, 24:106–110, 1978.

20. K. Rubin and A. Silverberg. Supersingular abelian varieties in cryptology. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 336–353. Springer Berlin / Heidelberg, 2002.

21. L. Schoenfeld. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. *Mathematics of Computation*, 30(134):337–360, April 1976.

22. N. Shang. *Low genus algebraic curves in cryptography*. PhD thesis, Purdue University, West Lafayette, USA, January 2009. Available at `https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2009-07.pdf`.

23. P. Van Wamelen. Examples of genus two CM curves defined over the rationals. *Mathematics of Computation*, 68(225):307–320, 1999.

24. A. Weil. Variétés Abéliennes et Courbes Algébriques. *Paris, Hermann*, 1948.

25. A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Mathematics of Computation*, 72(241):435–458, 2002.

# Pairing-friendly Genus 2 Curves: Numerical Data

## A  Parameters produced by Algorithm 1

Here are some parameters found by Algorithm 1 for the CM field $K = \mathbb{Q}\left(i\sqrt{2-\sqrt{2}}\right)$ and embedding degree $k = 5$. Corresponding to this CM field there is a genus 2 curve defined over the rationals [23].

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

The curves over prime fields corresponding to these parameters are either $C$ reduced modulo $p$, or its quadratic twist $C'$.

On average, a MAGMA script found one set of parameters with $r = 160, 256, 512$ and $1024$ bits in 0.0918, 0.3486, 2.9938, and 46.5615 seconds, respectively. The computations were performed on an AMD Quad-Core Opteron(TM) 2.4GHz computer running Linux kernel release 2.6.9-34.0.1.ELsmp; only one processor was used for computation.

$\underline{r : 160 \text{ bits. } k = 5.}$

$p = 252823257935282285362732638695054084330470208363294037922085422639242974021428617016685256858478396063171049776321146642543762678397966294736679271737114219377482492730434694368080216503567747137$

$r = 1461501637330902918203684832716283019655932544881$

$N = 639195997530102770743719375835116542403184563967996666440138384615623110413594200676694946117805225330312612310827044910981825287799285223669398540557821913799656773145627033786990082785436750266486800684006923590556954728131135395897277972576354640367835735384699586219721088378014250469051652054375345643144789566661934242933804835085555547551176509593355362651103369722888755552378947584$

$c_1 = 1$

$c_2 = 11243292621276079848206331730630023731174251699959569954973786210137165821520551831056883188430192$

$c_3 = -64248144848395594424557829122788871673183688623832$

$c_4 = -10980201790932738122979450154259988889529711346380$

$\rho \approx 8.072$

The equation of the curve over $\mathbb{F}_p$ is $y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$.

$\underline{r : 256 \text{ bits. } k = 5.}$

$p = 704881071480907162078296670102869074389758456316878620976045254499487753057018612511712201735014180524772377962473016939310167112744621549084701281800977311922475243532026678663444416777984086642261820360878053209107260269920646366156330351242218700528276622717003991911130319025660067745840160149952389932917329$

$r = 115792089237316195423570985008687907853269984665640564039457584007913129642241$

$N = 496857324932071752145912838893889169489835622033784989598880614229969960057380528145341182621544436360674179722969415484955886684347872770026411053244140018566049974700076815541374371031592611720892555014703585816910913734818476522890003367060634939104658599174570132609823174216276573137866957202831985326892972974643475849712058075634522614506805458611699021204439299923123514578344182885280717576928922896637801778010790956345539296480701514721219823943376856364544844490404257431312550838391605233331165$

209132474804644712415449375768349765769814512250344721171550541443831388350786300229054528190120614531020814267875552

$c_1 = 1$

$c_2 = -593667024299357207475224021693404867559353586749362364291192910163117377314091174679730494164377377555124836261959845126549114759751896733965375133869149502$

$c_3 = -3548809313566683873624287099133190257445712680595264225876058829990309058529874$

$c_4 = -5936979480813871848895779658124341164096655715011808647348987318596163181064168$

$\rho \approx 8.093$

The equation of the curve over $\mathbb{F}_p$ is $y^2 = 3(-x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1)$.

## B    Parameters produced by Algorithm 2

Below are some examples of the parameters found by Algorithm 2 for $K = \mathbb{Q}(i\sqrt{2 - \sqrt{2}})$ and embedding degree $k = 3$. Here, we choose $C_3(x, y) = C_4(x, y) = xy$, $C_1(x, y) = x^2$ and $C_2(x, y) = -(a + b(1 + d)/2)y^2$ in Step 1 of Algorithm 2.

On average, our MAGMA implementation found one set of parameters with $r = 160, 256, 512$ and $1024$ bits in $0.1092, 0.4468, 4.1718$, and $50.0140$ seconds, respectively. The computations were performed on an AMD Quad-Core Opteron(TM) 2.4GHz computer running Linux kernel release 2.6.9-34.0.1.ELsmp; only one processor was used for computation.

$r : 160$ bits. $k = 3$.

$p = 2760322067827918576043085019199885911367408859313438987402563848662416467553702979623124723634053832810065253894017495098779682257468497626596054621968600128109029276968729859800558964868162387810481$

$r = 1461501637330902918203684832716283019655932543447$

$N = 7619377918137796319947339411066337081547390363031357462014146126836813740229511268625176061099440881442259428060861564412453929893287845956340341615473801381877788622808833784218658203120398140352297108203162864445083452431605957965377710200274713729091231956302784852535130492706506152564351364423861208959016750122994621253699118662098804381727358336213778156291342604171682918546278978314937568$

$c_1 = 853413751674246325960655910542033278192644078137851807206531855460335897482560901762777003565546321$

$c_2 = -467312771754171603865894820458465529298297100229438686497717835334951148694691783854304471959958498$

$c_3 = c_4 = -893097022442711268703148300906455700266481456199004270995167374051672546438742749426798352836518846$

$\rho \approx 8.2401$

The equation of the curve over $\mathbb{F}_p$ is $y^2 = 3(-x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1)$.

$r : 256$ bits. $k = 3$.

$p = 822920761971611209794051125149779261868007917105814333422807428702492483230083267137722107007539895222282160142127021544643255654790661296929370353893229675700191477216018550151093614656582383928029105989773078845819669931262786638243789783462295242237448794562285423898483720827257224421582887155754347373346337$

$r = 115792089237316195423570985008687907853269984665640564039457584007913129640743$

$N = 6771985804839371942637307533597848073765705721625192468898693422808253032215444487859365278749079347589549730845666733117453777198238279219494$

528067898898802444337872521971715298664355377109626744303642701670738909572492483970382806444921112182297078703529019972656022670120081903677992042490892895555013596712575651692176016210908268738361775620639618631060792503322957268647411120627219341692712631035265600931543321649702304993088353733186022177113837635426687931704695261041122831639155388140714003673423775883028281057290061738442630720051414075948315034087299281022702814170148521555266833233821764657269729790825740482
$c_1 = 89956738739147921738147694727435158471278087464983900240906088404369117034478629557785770257234423972877031276763948663931761267676699233257997$
$62748414274889$
$c_2 = -37991623628115110376463338097314310242107491290686099464180935183342377361666157361851641781338965280295434753862169111244409012722954687$
$785372266393538$
$c_3 = c_4 = 82675299346181868737297716142467627782679598234083431484114422288087906493405752740627824201485645210824879536505195273507388849360615838$
$257032702979376742$
$\rho = 8.0950$
The equation of the curve over $\mathbb{F}_p$ is $y^2 = -x^5 + 3x^4 + 2x^3 - 6x^2 - 3x + 1$.