Generating more Kawazoe-Takahashi Genus 2 Pairing-friendly Hyperelliptic Curves

Ezekiel J Kachisa*

School of Computing
Dublin City University
Ireland
ekachisa@computing.dcu.ie

Abstract. Constructing pairing-friendly hyperelliptic curves with small ρ-values is one of challenges for practicability of pairing-friendly hyperelliptic curves. In this paper, we describe a method that extends the Kawazoe-Takahashi method of generating families of genus 2 ordinary pairing-friendly hyperelliptic curves by parameterizing the parameters as polynomials. With this approach we construct genus 2 ordinary pairing-friendly hyperelliptic curves with $2 < \rho \leq 3$.

Keywords: pairing-friendly curves, hyperelliptic curves.

1 Introduction

Efficient implementation of pairing-based protocols such as one round three way key exchange [16], identity based encryption [3] and digital signatures [4], depends on what are called *pairing-friendly curves*. These are special curves with a large prime order subgroup, so that protocols can resist the known attacks, and small embedding degree for efficient finite field computations.

Even though there are many methods for constructing pairing-friendly elliptic curves [14], there are very few methods that address the problem of constructing ordinary pairing-friendly hyperelliptic curves of higher genus. The first explicit construction of ordinary hyperelliptic curve was shown by David Freeman [11]. Freeman modeled the Cocks-Pinch method [8] to construct ordinary hyperelliptic curves of genus 2. His algorithm produce curves over prime fields with prescribed embedding degree k with ρ-value ≈ 8. Kawazoe and Takahashi [18] constructed pairing-friendly hyperelliptic curves of the form $y^2 = x^5 + ax$ which produced Jacobian varieties with ρ-values between 3 and 4. Recently, Freeman and Satoh [15]

* This author acknowledge support from the Science Foundation Ireland under Grant No. 06/MI/006 through Claude Shannon Institute

proposed algorithms for generating pairing-friendly hyperelliptic curves. In their construction it was shown that if an elliptic curve, E, is defined over a finite field, $\mathbb{F}_p$, and $\mathcal{A}$ is abelian variety isogenous over $\mathbb{F}_{p^d}$ to a product of two isomorphic elliptic curves then the abelian variety, $\mathcal{A}$, is isogenous over $\mathbb{F}_p$ to a primitive subvariety of the Weil restriction of E from $\mathbb{F}_{p^d}$ to $\mathbb{F}_p$. Notably, the Freeman-Satoh algorithm produces hyperelliptic curves with better ρ value than previously reported. The best, for example, achieves a ρ-value of 20/9 for embedding degree $k = 27$. However, the ρ-values of most embedding degrees for ordinary hyperelliptic curves remain too high for an efficient implementation.

For a curve to be suitable for implementation it should possess desirable properties which include efficient implementation of finite field arithmetic and the order of the Jacobian having a large prime factor.

In this paper we generate more Kawazoe-Takahashi genus 2 ordinary pairing-friendly hyperelliptic curves. In particular, we construct curves of embedding degrees $2, 7, 8, 10, 11, 13, 22, 26, 28, 44$ and 52 with ρ-value between 2 and 3.

We proceed as follows: In Section 2 we present mathematical background and facts on constructing pairing-friendly hyperelliptic curves while in Section 3 we discuss the construction of pairing-friendly hyperelliptic curves based on the Kawazoe-Takahashi algorithms and in Section 4 we present the generalization of Kawazoe-Takahashi algorithms for constructing pairing-friendly hyperelliptic curves and we give explicit examples. The paper is concluded in Section 5.

2 Pairing-friendly hyperelliptic curves

2.1 Mathematical background

Let $p > 2$ be a prime, let r be prime distinct from p. We denote a hyperelliptic curve of genus g defined over a finite field $\mathbb{F}_p$ by C. This is a non-singular projective model of the affine curve of the form:

$$y^2 = f(x) \tag{1}$$

where $f(x)$ is a monic polynomial of degree $2g + 1$, has its coefficients in $\mathbb{F}_p[x]$ and has no multiple roots in $\bar{\mathbb{F}_p}$. We denote the Jacobian of C by J_C and a group of the $\mathbb{F}_p$-rational points of the Jacobian of C by $J_C(\mathbb{F}_p)$. This group is isomorphic to degree zero divisor class group of C over $\mathbb{F}_p$.

As in the elliptic curve case the *embedding degree* of Jacobian variety is defined as follows:

Definition 1 ([11]). *Let C be an hyperelliptic curve defined over a prime finite field $\mathbb{F}_p$. Let r be a prime dividing $\#J_C(\mathbb{F}_p)$. The embedding degree of J_C with respect to r is the smallest positive integer k such that $r \mid p^k - 1$ but $r \nmid p^i - 1$ for $0 < i < k$.*

The definition, as in the elliptic curve case, explains that k is the smallest positive integer such that the extension field $\mathbb{F}_{p^k}$, contains a set of rth roots of unity. Hence we refer to a curve C as having embedding degree k with respect to r if and only if a subgroup of order r of its Jacobian J_C does. As such, for an efficient arithmetic implementation curves must have small embedding degree so that arithmetic in $\mathbb{F}_{p^k}$ is feasible. Furthermore, we require that the size of the finite field, $\mathbb{F}_p$, be as small as possible in relation to the the size of the prime order subgroup r. This is measured by a parameter known as the ρ-value. For a g-dimensional abelian variety defined over $\mathbb{F}_p$ this parameter is defined as:

$$\rho = \frac{g \log(\mathrm{p})}{\log(\mathrm{r})}.$$

In the ideal case the abelian varieties of dimension g have a prime number of points in which case $\rho \approx 1$. For pairing-friendly one-dimensional abelian varieties one can reach the ideal case by using the constructions in [19], [6] and [10]. However, this proves not be the case with higher dimensional abelian varieties. Hence the interest has been to construct higher dimensional abelian varieties with low embedding degrees and small ρ-values. And the same time, for security reasons we require r large enough so that discrete logarithm problem (DLP) in the subgroup of prime order r is suitably hard and k sufficiently large enough so that the (DLP) in $\mathbb{F}^*_{p^k}$, withstand the known attacks.

There are two main cryptographic pairings, the Weil and the Tate. In both cases the basic idea is to embed the cryptographic group of order r into a multiplicative group of rth roots of unity, μ_r. A non-degenerate, bilinear map for the Tate pairing, for example, is defined by the following map:

$$t_r : J_C(\mathbb{F}_{p^k})[r] \times J_C(\mathbb{F}_{p^k})/J_C(\mathbb{F}_{p^k}) \longrightarrow (\mathbb{F}^*_{p^k})/(\mathbb{F}^*_{p^k})^r.$$

3 Kawazoe-Takahashi hyperelliptic curves

Kawazoe and Takahashi [18] presented an algorithm which constructed hyperelliptic curves of the form $y^2 = x^5 + ax$ with ordinary Jacobians. Their construction used two approaches, one was based on the Cocks-Pinch method [8] of constructing ordinary pairing-friendly elliptic curves and the other was based on cyclotomic polynomials. This idea was first proposed by Brezing and Weng in [7]. However, both approaches are based on the predefined sizes of the Jacobians as presented in [9]. The order of the Jacobian, $\#J_C$, is closely related to the characteristic polynomial, $\chi(t)$, of the Frobenius endormorphism, π.

Consequently, for genus 2 curves the $\chi(t)$ of the Frobenius is a polynomial known to have the following form:

$$\chi(t) = t^4 - a_1 t^3 + a_2 t^2 - a_1 p t + p^2 \tag{2}$$

within $a_1, a_2 \in \mathbb{F}_p$ and furthermore $\mid a_1 \mid \leq 4p$ and $\mid a_2 \mid \leq 6p$. Hence, $\#J_C$ is determined from Equation 2 by the following relation:

$$\#J_C = \chi(1) = 1 - a_1 + a_2 - a_1 p + p^2. \tag{3}$$

The Hasse-Weil bound describes the interval in which the order of the Jacobian is found as follows:

$$\lceil (\sqrt{p} - 1)^{2g} \rceil \leq \#J_C \leq \lfloor (\sqrt{p} + 1)^{2g} \rfloor \tag{4}$$

Theorem 1 below outlines the characteristic polynomials which defines hyperelliptic curves, C, of the form $y^2 = x^5 + ax$ defined over $\mathbb{F}_p$. The J_C of C for these cases is a simple ordinary Jacobian over $\mathbb{F}_p$.

Theorem 1 ([9],[18]). *Let p be an odd prime, C a hyperelliptic curve defined over $\mathbb{F}_p$ by equation $y^2 = x^5 + ax, Jc$ the Jacobian variety of C and $\chi(t)$ the characteristic polynomial of the pth power Frobenius map of C. Then the following holds: (In the following c, d are integers such that $p = c^2 + 2d^2$ and $c \equiv 1$ (mod 4),$d \in \mathbb{Z}$ (such c and d exists if and only if $p \equiv 1, 3$ (mod 8)).*

1) If $p \equiv 1 \bmod 8$ and $a^{(p-1)/2} \equiv -1 \bmod p$, then $\chi(t) = t^4 - 4dt^3 + 8d^2t^2 - 4dpt + p^2$ and $2(-1)^{(p-1)/8} d \equiv (a^{(p-1)/8} + a^{3(p-1)/8}) c \bmod p$
2) If $p \equiv 1 \bmod 8$ and $a^{(p-1)/4} \equiv -1 \bmod p$, or if $p \equiv 3 \bmod 8$ and $a^{(p-1)/2} \equiv -1 \bmod p$, then $\chi(t) = t^4 + (4c^2 - 2p)t^2 + p^2$

Using the formulae in Theorem 1 Kawazoe and Takahashi developed a Cocks-Pinch-like method to construct genus 2 ordinary pairing-friendly hyperelliptic curves of the form $y^2 = x^5 + ax$. As expected the curves generated by the Cocks-Pinch-like method had their ρ-values close to 4. Furthermore, they also presented cyclotomic families. With this method they managed to construct a $k = 24$ curve with $\rho = 3$. In both cases the ultimate goal is to find integers c and d such that there is a prime

$p = c^2 + 2d^2$ with $c \equiv 1 \pmod 4$ and $\chi(1)$ having a large prime factor. Algorithms 1 and 2 developed from Theorem 1 construct individual genus 2 pairing-friendly hyperelliptic curves with $\rho \approx 4$.

Algorithm 1: Kawazoe-Takahashi Type I pairing-friendly Hyperelliptic curves with $\#J_C = 1 - 4d + 8d^2 - 4dp + p^2$

Input: $k \in \mathbb{Z}$.
Output: a hyperelliptic curve defined by $y^2 = x^5 + ax$ with Jacobian group having a prime subgroup of order r.

1. Choose r a prime such that $lcm(8, k)$ divides $r - 1$.
2. Choose ζ a primitive kth root of unity in $(\mathbb{Z}/r\mathbb{Z})^{\times}, \omega$ a positive integer such that $\omega^2 \equiv -1 \bmod r$ and σ a positive integer such that $\sigma^2 \equiv 2 \bmod r$.
3. Compute integers, c, d such that:
   - $c \equiv (\zeta + \omega)(\sigma(\omega + 1))^{-1} \bmod r$ and $c \equiv 1 \bmod 4$
   - $d \equiv (\zeta\omega + 1)(2(\omega + 1))^{-1} \bmod r$.
4. Compute a prime $p = (c^2 + 2d^2)$ such that $p \equiv 1 \bmod 8$.
5. Find $a \in \mathbb{F}_p$ such that:
   - $a^{(p-1)/2} \equiv -1 \bmod p$ and $2(-1)^{(p-1)/8} d \equiv (a^{(p-1)/8} + a^{3(p-1)/8})c \bmod p$.
6. Define a hyperelliptic curve C by $y^2 = x^5 + ax$.

Algorithm 2: Kawazoe-Takahashi Type II pairing-friendly Hyperelliptic curves with $\#J_C = 1 + (4c^2 - 2p) + p^2$

Input: $k \in \mathbb{Z}$.
Output: a hyperelliptic curve defined by $y^2 = x^5 + ax$ with Jacobian group having a prime subgroup of order r.

1. Choose r a prime such that $lcm(8, k)$ divides $r - 1$.
2. Choose ζ a primitive kth root of unity in $(\mathbb{Z}/r\mathbb{Z})^\times, \omega$ positive integer such that $\omega^2 \equiv -1 \bmod r$ and σ a positive integer such that $\sigma^2 \equiv 2 \bmod r$.
3. Compute integers, c, d such that:
   - $c \equiv 2^{-1}(\zeta - 1)\omega) \bmod r$ and $c \equiv 1 \bmod 4$
   - $d \equiv (\zeta + 1)(2\sigma)^{-1} \bmod r$.
4. Compute a prime $p = (c^2 + 2d^2)$ such that $p \equiv 1, 3 \bmod 8$ and for some integer δ satisfying $\delta^{(p-1)/2} \equiv -1 \bmod p$ and
5. Find $a \in \mathbb{F}_p$ such that:
   - $a = \delta^2$ when $p \equiv 1 \bmod 8$ or $a = \delta$ when $p \equiv 3 \bmod 8$.
6. Define a hyperelliptic curve C by $y^2 = x^5 + ax$.

Remark 1. The key feature in both algorithms is that r is choosen such that $r - 1$ is divisible by 8 so that $\mathbb{Z}/r\mathbb{Z}$ contains both $\sqrt{-1}$ and $\sqrt{2}$ for both c and d to satisfy the conditions in the algorithm.

4 Our generalization

We observe that one can do better if the algorithms are parametrized by polynomials in order to construct curves with specified bit size. We represent *families* of pairing-friendly curves for which parameters c, d, r, p are parametrized as polynomials $c(z), d(z), r(z), p(z)$ in a variable z. In fact this idea of using polynomials was used in other constructions for pairing-friendly curves such as in [19],[2] [21] and [7].

When working with the polynomials we consider polynomials with rational coefficients. The definitions below describes a family of Kawazoe-Takahashi-type of pairing-friendly hyperelliptic curves.

Definition 2 ([14]). *Let $g(z) \in \mathbb{Q}[z]$. We say that $g(z)$ represents primes if the following are satisfied:*

– *$g(z)$ is non constant irreducible polynomial.*

– *$g(z)$ has a positive leading coefficient.*
– *$g(z)$ represents integers i.e for $z_0 \in \mathbb{Z}$, $g(z_0) \in \mathbb{Z}$.*
– *$gcd(\{g(z) : z, g(z) \in \mathbb{Z}\}) = 1$*

Definition 3. *Let $c(z), d(z), r(z)$ and $p(z)$ be non-zero polynomials with rational coefficients. For a given positive integer k the couple $(r(z), p(z))$ parameterizes a family of Kawazoe-Takahashi type of hyperelliptic curves with Jacobian J_C whose embedding degree is k if the following conditions are satisfied:*

(i) *$c(z)$ represents integers such that $c(z) \equiv 1 \bmod 4$;*
(ii) *$d(z)$ represents integers;*
(iii) *$p(z) = c(z)^2 + 2d(z)^2$ represents primes;*
(iv) *$r(z)$ represents primes;*
(v) *$r(z)|1-4d(z)+8d(z)^2-4d(z)p(z)+p(z)^2$ or $r(z)|1+(4c(z)^2-2p(z))+p(z)^2$*
(vi) *$\Phi_k(p(z)) \equiv 0 \bmod r(z)$, where Φ_k is the kth cyclotomic polynomial.*

And we define the ρ-value of this family as $\rho = \frac{2\deg(p(z))}{\deg(r(z))}$.

In [9] they showed that there exists a simple ordinary abelian variety surface with characteristic polynomials of Frobenius $t^4 - 4d + 8d^2 - 4dp + p^2 \in \mathbb{Z}[t]$ or $t^4 + (4c^2 - 2p) + p^2 \in \mathbb{Z}[t]$ with certain conditons on c and d. Hence Definition 3 part (i) and (ii) ensures that the polynomial representation of c and d conforms with the conditions. While condition (v) of Definition 3 ensures that for a given z for which $p(z)$ and $r(z)$ represents prime $r(z)$ divides $\#J_C(z)$. In otherwords, the order of the Jacobian of the constructed curve has a prime order subgroup of size $r(z)$. Finaly, condition (vi) of Definition 3 ensures that the Jacobian of the constructed curve has embedding degree k.

With these definitions we now adapt Algorithms 1 and 2 to the polynomial context. This can be seen in Algorithms 3 and 4 below generalizing Algorithms 1 and 2 respectively. In particular we construct our curves by taking a similar approach as described in [17] for constructing pairing-friendly elliptic curves.

In general this method uses minimal polynomials rather than a cyclotomic polynomial in defining the size of the prime order subgroup. The difficult part is the choosing the right polynomial for representing the size of the cryptographic group.

Algorithm 3: Our generalization for finding pairing-friendly Hyperelliptic curves with $\#J_C(z) = 1 - 4d(z) + 8d(z)^2 - 4d(z)p(z) + p(z)^2$

Input: $k \in \mathbb{Z}, \ell = lcm(8, k), K \cong \mathbb{Q}[z]/\Phi_\ell(z)$
Output: Hyperelliptic curve of genus 2 defined by $y^2 = x^5 + ax$.

1. Choose an irreducible polynomial $r(z) \in \mathbb{Z}[z]$.
2. Choose polynomials $s(z), \omega(z)$ and $\sigma(z)$ in $\mathbb{Q}[z]$ such that $s(z)$ is a primitive kth root of unity, $\omega(z) = \sqrt{-1}$ and $\sigma(z) = \sqrt{2}$ in K.
3. Compute polynomials, $c(z), d(z)$ such that:
   - $c(z) \equiv (s(z) + \omega(z))(\sigma(z)(\omega(z) + 1))^{-1}$ in $\mathbb{Q}[z]/r(z)$.
   - $d(z) \equiv (s(z)\omega(z) + 1)(2(\omega(z) + 1))^{-1}$ in $\mathbb{Q}[z]/r(z)$.
4. Compute a polynomial, $p(z) = c(z)^2 + 2d(z)^2$.
5. For $z_0 \in \mathbb{Z}$ such that:
   – $p(z_0)$ and $r(z_0)$ represents primes and $p(z_0) \equiv 1 \bmod 8$ and
   – $c(z_0), d(z_0)$ represents integers and $c(z_0) \equiv 1 \bmod 4$.
   find $a \in \mathbb{F}_{p(z_0)}$ satisfying:
   - $a^{(p(z_0)-1)/2} \equiv -1 \bmod p(z_0)$ and
   - $2(-1)^{(p(z_0)-1)/8} d(z_0) \equiv (a^{(p(z_0)-1)/8} + a^{3(p(z_0)-1)/8}) c(z_0) \bmod p(z_0)$.
6. Output $(r(z_0), p(z_0), a)$
7. Define a hyperelliptic curve C by $y^2 = x^5 + ax$.

Algorithm 4: Our generalization for finding pairing-friendly Hyperelliptic curves with $\#J_C(z) = 1 + (4c(z)^2 - 2p(z)) + p(z)^2$

Input: $k \in \mathbb{Z}, \ell = lcm(8,k), K \cong \mathbb{Q}[z]/\Phi_\ell(z)$
Output: Hyperelliptic curve of genus 2 defined by $y^2 = x^5 + ax$.

1. Choose an irreducible polynomial $r(z) \in \mathbb{Z}[z]$.
2. Choose polynomials $s(z), \omega(z)$ and $\sigma(z)$ in $\mathbb{Q}[z]$ such that $s(z)$ is a primitive kth root of unity, $\omega(z) = \sqrt{-1}$ and $\sigma(z) = \sqrt{2}$ in K.
3. Compute polynomials, $c(z), d(z)$ such that
   - $c(z) \equiv 2^{-1}(s(z) - 1)\omega(z)) \bmod r(z)$
   - $d(z) \equiv (z(z) + 1)(2\sigma(z))^{-1} \bmod r(z)$
4. Compute an irreducible polynomial $p(z) = (c(z)^2 + 2d(z)^2)$
5. For $z_0 \in \mathbb{Z}$ such that:
   – $p(z_0)$ and $r(z_0)$ represents primes and $p(z_0) \equiv 1, 3 \bmod 8$ and
   – $c(z_0), d(z_0)$ represents integers and $c(z_0) \equiv 1 \bmod 4$.
6. Find $a \in \mathbb{F}_p(z_0)$ such that:
   - $a = \delta^2$ when $p(z_0) \equiv 1 \bmod 8$ or
   - $a = \delta$ when $p(z_0) \equiv 3 \bmod 8$.
7. Output $(r(z_0), p(z_0), a)$.
8. Define a hyperelliptic curve C by $y^2 = x^5 + ax$.

With this approach, apart from reconstructing the Kawazoe-Takahashi genus 2 curves, we discover new families of pairing-friendly hyperelliptic curve of embedding degree $k = 2, 7, 8, 10, 11, 13, 22, 26, 28, 44$ and 52 with $2 < \rho \leq 3$.

The success depends on the the choice of the number field, K. Thus, in the initial step we set K to be isomorphic to a cyclotomic field $\mathbb{Q}(\zeta_\ell)$ for some $\ell = lcm(8,k)$. The condition on ℓ ensures $\mathbb{Q}[z]/r(z)$ contains square roots of -1 and 2. We take the approach as described in [17] for constructing pairing-friendly elliptic curves for defining the irreducible polynomial $r(z)$. Even though this method is time consuming as it involves searching for a right element, it mostly gives a favorable irreducible polynomial $r(z)$, which defines the size of the prime order subgroup . Here we find a minimal polynomial of an element $\gamma \in \mathbb{Q}(\zeta_\ell)$ and call it $r(z)$, where γ is not in any proper subfield of $\mathbb{Q}(\zeta_\ell)$. Since γ is in no proper subfield, then we have $\mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\gamma)$, where the degree of $\mathbb{Q}(\gamma)$ over $\mathbb{Q}$ is $\varphi(\ell)$, where $\varphi(.)$ is *Euler totient function*.

However, with most values of $k > 10$ which are not multiples of 8, the degree of $r(z)$ tends to be large. As observed in [14], for such curves this limits the number of usable primes. The current usable size of r is in the range $[2^{160}, 2^{512}]$.

4.1 The algorithm explained

Step 1: Set up This involves initializing the algorithm by setting $\mathbb{Q}(\zeta_\ell)$ defined as $\mathbb{Q}[z]/\Phi_\ell(z)$. The Choice of this field ensures that it contains ζ_k and $\sqrt{-1}$ and $\sqrt{2}$. The ideal choice, in such a case, is $\mathbb{Q}(\zeta_8, \zeta_k) = \mathbb{Q}(\zeta_{lcm(k,8)})$.

Step 2: Representing $\boldsymbol{\zeta_k}, \boldsymbol{\sqrt{-1}}$ and $\boldsymbol{\sqrt{2}}$ We search for a favorable element, $\gamma \in \mathbb{Q}(\zeta_\ell)$ such that the minimal polynomial of γ has degree $\varphi(\ell)$ and we call this $r(z)$. We redefine our field to $\mathbb{Q}[z]/r(z)$. In this field we find a polynomial that represents $\zeta_k, \sqrt{-1}$ and $\sqrt{2}$.

For ζ_k there are $\varphi(k)$ numbers of primitive kth roots of unity. In fact if $\gcd(\alpha, k) = 1$ then ζ_k^α is also primitive kth root of unity. To find the polynomial representation of $\sqrt{-1}$ and $\sqrt{2}$ in $\mathbb{Q}[z]/r(z)$ we find the solutions of the polynomials $z^2 + 1$ and $z^2 - 2$ in the number field isomorphic to $\mathbb{Q}[z]/r(z)$ respectively.

Steps 3,4,5: Finding the family All computations in the algorithm are done modulo $r(z)$ except when computing $p(z)$. It is likely that polynomials $p(z), c(z)$ and $d(z)$ have rational coefficient. At this point polynomials are tested to determine whether they represent intergers or primes as per Definition 3.

4.2 New curves

We now present a series of new curves constructed using the approach described above. Proving the theorems is simple considering γ has minimal polynomial $r(z)$. We give a proof of Theorem 2. For the other curves the proofs are similar.

We start by constructing a curve of embedding degree, $k = 7$. It is interesting to note that here we get a family with $\rho = 8/3$.

Theorem 2. *Let* $k = 7, \ell = 56$. *Let* $\gamma = \zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ *and define polynomials* $r(z), p(z), c(z), d(z)$ *by the following:*

$r(z) = z^{24} - 24z^{23} + 276z^{22} - 2024z^{21} + 10625z^{20} - 42484z^{19}$

$$
\begin{aligned}
&+ 134406z^{18} - 344964z^{17} + 730627z^{16} - 1292016z^{15} + 1922616z^{14} \\
&- 2419184z^{13} + 2580005z^{12} - 2332540z^{11} + 1784442z^{10} - 1150764z^{9} \\
&+ 621877z^{8} - 279240z^{7} + 102948z^{6} - 30632z^{5} + 7175z^{4} - 1276z^{3} + 162z^{2} - 12z + 1 \\
p(z) &= (z^{32} - 32z^{31} + 494z^{30} - 4900z^{29} + 35091z^{28} - 193284z^{27} + \\
&\quad 851760z^{26} - 3084120z^{25} + 9351225z^{24} - 24075480z^{23} + 53183130z^{22} - \\
&\quad 101594220z^{21} + 168810915z^{20} - 245025900z^{19} + 311572260z^{18} - \\
&\quad 347677200z^{17} + 340656803z^{16} - 292929968z^{15} + 220707810z^{14} - 145300540z^{13} + \\
&\quad 83242705z^{12} - 41279004z^{11} + 17609384z^{10} - 6432920z^{9} + 2023515z^{8} \\
&- 569816z^{7} + 159446z^{6} - 49588z^{5} + 16186z^{4} - 4600z^{3} + 968z^{2} - 128z + 8)/8 \\
c(z) &= (-z^{9} + 9z^{8} - 37z^{7} + 91z^{6} - 147z^{5} + 161z^{4} - 119z^{3} + 57z^{2} - 16z + 2)/2 \\
d(z) &= (z^{16} - 16z^{15} + 119z^{14} - 546z^{13} + 1729z^{12} - 4004z^{11} + 7007z^{10} \\
&- 9438z^{9} + 9867z^{8} - 8008z^{7} + 5005z^{6} - 2366z^{5} + 819z^{4} - 196z^{3} + 28z^{2})/4
\end{aligned}
$$

Then $(r(2z), p(2z))$ constructs a genus 2 hyperelliptic curves. The ρ-value of this family is $8/3$.

Proof. Since $\zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ has minimal polynomial $r(z)$, we apply Algorithm 3 by working in $\mathbb{Q}(\zeta_{56})$ defined as $\mathbb{Q}[z]/r(z)$. We choose $\zeta_7 \mapsto (z-1)^{16}$, $\sqrt{-1} \mapsto (z-1)^{14}$ and $\sqrt{2} \mapsto z(z-1)^7(z-2)(z^6 - 7z^5 + 21z^4 - 35z^3 + 35z^2 - 21z + 7)(z^6 - 5z^5 + 11z^4 - 13z^3 + 9z^2 - 3z + 1)$. Applying Algorithm 3 we find $p(z)$ as stated. Computations with PariGP [23], show that both $r(2z)$ and $p(2z)$ represents primes and $c(2z)$ represents integers such that it is equivalent to 1 modulo 4. Furthermore, by Algorithm 3 the Jacobian of our hypothetical curve has a large prime order subgroup of order $r(z)$ and embedding degree, $k = 7$.

Considering $z_0 = 758$ we now give an example of a 254- bit prime subgroup that is constructed using the parameters in Theorem 2.

Example 1.

$$
\begin{aligned}
r &= 213748555325666652890713665865251428761742681841141544849244\backslash \\
&\quad 05425230130090001 \\
p &= 741504661189142770769829861344257948821797401549707353154351\backslash \\
&\quad 0809548164276504244597566609578179766689 7 \\
c &= -21022477149693687350103984375 \\
d &= 19254930033489381271793153044560509686043701114494 4 \\
a &= 3 \\
\rho &= 2.646.
\end{aligned}
$$

$$C : y^2 = x^5 + 3x$$

The next curve is of embedding degree $k = 8$. According to [25] this family of curves admits higher order twists. This means that it is possible to have both inputs to a pairing defined over a base field. The previous record on this curve was $\rho = 4$. In Theorem 3 below we outline the parameters that defines a family of hyperelliptic curves with $\rho = 3$.

Theorem 3. *Let $k = \ell = 8$. Let $\gamma = \zeta_\ell^3 + \zeta_\ell^2 + \zeta_\ell + 3 \in \mathbb{Q}(\zeta_8)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$
\begin{aligned}
r(z) &= z^4 - 12z^3 + 60z^2 - 144z + 136 \\
p(z) &= (11z^6 - 188z^5 + 1460z^4 - 6464z^3 + 17080z^2 - 25408z + 16448)/64 \\
c(z) &= (3z^3 - 26z^2 + 92z - 120)/8 \\
d(z) &= (-z^3 + 8z^2 - 26z + 32)/8
\end{aligned}
$$

Then $(r(32z)/8, p(32z))$ constructs a genus 2 hyperelliptic curves with embedding degree 8. The ρ-value of this family is 3.

This type of a curve is recommended at the 128 bit security level, see Table 3.1 in [1]. Below we give an example obtained using the above parameters.

Example 2.

$$
\begin{aligned}
r &= 131072000000000989850828800028032436273920352833179209074\backslash \\
&\quad 2477643363528725893137 (257 bits) \\
p &= 184549376000020905654747136986742251766767879474504560418\backslash \\
&\quad 25253266950693364290488511618376615764127711271298317288473 7 \\
c &= 122880000000006959889920000131402093366880826953220034406 25 \\
d &= -409600000000023199641600000438007300106402756513775156991 6 \\
a &= 3 \\
\rho &= 3.012
\end{aligned}
$$

$C : y^2 = x^5 + 3x$

Theorem 4. *Let $k = 10, \ell = 40$. Let $\gamma = \zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$
\begin{aligned}
r(z) = {} & z^{16} - 16z^{15} + 120z^{14} - 560z^{13} + 1819z^{12} - 4356z^{11} + 7942z^{10} - \\
& 11220z^9 + 12376z^8 - 10656z^7 + 7112z^6 - 3632z^5 + 1394z^4 - 392z^3 + 76z^2 - 8z + 1 \\
p(z) = {} & (z^{24} - 24z^{23} + 274z^{22} - 1980z^{21} + 10165z^{20} - 39444z^{19} \\
& +120156z^{18} - 294576z^{17} + 591090z^{16} - 981920z^{15} + 1360476z^{14} -
\end{aligned}
$$

$$
\begin{aligned}
&1578824z^{13} + 1536842z^{12} - 1253336z^{11} + 853248z^{10} - 482384z^{9} + \\
&225861z^{8} - 88872z^{7} + 31522z^{6} - 11676z^{5} + 4802z^{4} - 1848z^{3} + 536z^{2} - 96z + 8)/8 \\
c(z) &= (-z^{7} + 7z^{6} - 22z^{5} + 40z^{4} - 45z^{3} + 31z^{2} - 12z + 2)/2 \\
d(z) &= (z^{12} - 12z^{11} + 65z^{10} - 210z^{9} + 450z^{8} - 672z^{7} + 714z^{6} - 540z^{5} + 285z^{4} - \\
&100z^{3} + 20z^{2})/4
\end{aligned}
$$

Then $(r(4z), p(4z))$ constructs a genus 2 hyperelliptic curve. The ρ-value of this family is 3.

Below is a curve of embedding degree 10 with a prime subgroup of size 249 bits. The ρ-value of its J_C is 3.036.

Example 3.

$$
\begin{aligned}
r &= 4745749105410301406815931235596753944430110861981481094 8\backslash \\
&2797931132143318041 \\
p &= 3392680476835482274427348989075071521908024843148191254 99\backslash \\
&3934108021750448229282701596660539123994672109536233564 17 \\
c &= -118972415903533855079706140671129 5 \\
d &= 4118665121635578103210977882765100527274697866021896847 36 \\
a &= 3 \\
\rho &= 3.036 \\
C &: y^2 = x^5 + 3x
\end{aligned}
$$

Theorem 5. *Let $k = 28, \ell = 56$. Let $\gamma = \zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$
\begin{aligned}
r(z) = {} & z^{24} - 24z^{23} + 276z^{22} - 2024z^{21} + 10625z^{20} - 42484z^{19} + \\
&134406z^{18} - 344964z^{17} + 730627z^{16} - 1292016z^{15} + 1922616z^{14} - \\
&2419184z^{13} + 2580005z^{12} - 2332540z^{11} + 1784442z^{10} - 1150764z^{9} + 621877z^{8} - \\
&279240z^{7} + 102948z^{6} - 30632z^{5} + 7175z^{4} - 1276z^{3} + 162z^{2} - 12z + 1 \\
p(z) = {} & (z^{36} - 36z^{35} + 630z^{34} - 7140z^{33} + 58903z^{32} - 376928z^{31} + \\
&1946800z^{30} - 8337760z^{29} + 30188421z^{28} - 93740556z^{27} + 252374850z^{26} - \\
&594076860z^{25} + 1230661575z^{24} - 2254790280z^{23} + 3667649460z^{22} - \\
&5311037640z^{21} + 6859394535z^{20} - 7909656300z^{19} + 8145387218z^{18} - \\
&7487525484z^{17} + 613613430z^{16} - 4473905808z^{15} + 2893567080z^{14} - 1653553104z^{13} + \\
&830662287z^{12} - 364485108z^{11} + 138635550z^{10} - 45341540z^{9} + 12681910z^{8} - \\
&3054608z^{7} + 660688z^{6} - 141120z^{5} + 32008z^{4} - 7072z^{3} + 1256z^{2} - 144z + 8)/8 \\
c(z) = {} & (-z^{11} + 11z^{10} - 55z^{9} + 165z^{8} - 331z^{7} + 469z^{6} - 483z^{5} + 365z^{4} - 200z^{3} + \\
&76z^{2} - 18z + 2)/2
\end{aligned}
$$

$$\begin{aligned} d(z) = (&z^{18} - 18z^{17} + 153z^{16} - 816z^{15} + 3059z^{14} - 8554z^{13} + 18473z^{12} - 31460z^{11} \\ &+42757z^{10} - 46618z^9 + 40755z^8 - 28392z^7 + 15561z^6 - 6566z^5 + 2058z^4 - \\ &448z^3 + 56z^2)/4 \end{aligned}$$

Then $(r(2z), p(2z))$ constructs a genus 2 hyperelliptic curve. The ρ-value of this family is $\rho \approx 3$.

Here is a curve with a 255 bit prime subgroup constructed from the above parameters:

Example 4.

$$\begin{aligned} r &= 4249196005393859443511221923766676743131100635712211169\backslash \\ &\quad 6903628832285002084 81 \\ p &= 1094889169501305037288247123944801366479653316841535239280\backslash \\ &\quad 568336193026632167195184728514564519636647060505191263121 \\ c &= -66111539648877169993055611952337239 \\ d &= 7398949822445429441933438537752184652533904703318389984 00 \\ a &= 23 \\ \rho &= 2.972 \end{aligned}$$

$C : y^2 = x^5 + 23x$

The following family for $k = 24$ has a similar ρ-value as to a family of $k = 24$ reported in [18]. One can use the following parameters to construct a *Kawazoe-Takahashi Type II* pairing-friendly hyperelliptic curve of embedding degree $k = 24$ with $\rho = 3$.

Theorem 6. *Let $k = \ell = 24$. Let $\gamma = \zeta_{24} + 1 \in \mathbb{Q}(\zeta_{24})$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned} r(z) &= z^8 - 8z^7 + 28z^6 - 56z^5 + 69z^4 - 52z^3 + 22z^2 - 4z + 1 \\ p(z) &= (2z^{12} - 28z^{11} + 179z^{10} - 688z^9 + 1766z^8 - 3188z^7 + \\ &\qquad 4155z^6 - 3948z^5 + 2724z^4 - 1336z^3 + 443z^2 - 88z + 8)/8 \\ c(z) &= (-z^6 + 7z^5 - 20z^4 + 30z^3 - 25z^2 + 11z - 2)/2 \\ d(z) &= (z^5 - 4z^4 + 5z^3 - 2z^2 - z)/4 \end{aligned}$$

Then $(r(8z + 4)/8, p(8z + 4))$ constructs a complete ordinary pairing-friendly genus 2 hyperelliptic curves with embedding degree 24. The ρ-value of this family is 3.

The following family is of embedding degree $k = 2$ with $\rho = 3$. In this case the parameters corresponds to a quadratic twist C' of the curve C whose order of J_C has a large prime of size r.

Theorem 7. *Let $k = 2, \ell = 8$. Let $\gamma = \zeta_8^2 + \zeta_8 + 1 \in \mathbb{Q}(\zeta_8)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
r(z) &= z^4 - 4z^3 + 8z^2 - 4z + 1 \\
p(z) &= (17z^6 - 128z^5 + 480z^4 - 964z^3 + 1089z^2 - 476z + 68)/36 \\
c(z) &= (z^3 - 4z^2 + 7z - 2)/2 \\
d(z) &= (-2z^3 + 7z^2 - 14z + 4)/6
\end{aligned}$$

Then $(r(36z+8)/9, p(36z+8))$ constructs a genus 2 hyperelliptic curve. The ρ-value of this family is 3.

Here is a curve with a 164 bit prime subgroup constructed from the above parameters:

Example 5.

$$\begin{aligned}
r &= 18662407671139230451673881592011637799903138004697 \\
p &= 102792562578915164898226742137468734090998250325265\backslash \\
&\quad 6165164129909459559679217 \\
c &= 23328007191686179030939068128424560723 \\
d &= -15552004794459612687736644908426134338 \\
a &= 10 \\
\rho &= 3.049
\end{aligned}$$

Here our genus 2 hyperelliptic equation is $C' : y^2 = x^5 + 10x$ and hence $C : y^2 = 20(x^5 + 10x)$ is the curve whose $\#J_C$ has a large prime r and its embedding degree is 2 with repect to r.

We now present pairing-friendly hyperelliptic curves of embedding k whose polynomial that defines the prime order subgroup $r(z)$, has its degree greater or equal to 40. The polynomials that defines some of curves can be found in Appendix A. Currently these curves, as already pointed out, are only of theoretical interest. In this table $\ell = lcm(k, 8)$.

Table 1. Families of curves, whose $deg(r(z)) \geq 40$

k	γ	Degree($r(z)$)	Degree($p(z)$)	ρ-value	Modular class
11	ζ_ℓ	40	48	2.400	3 mod 4
13	$\zeta_\ell + 1$	48	64	2.667	4 mod 8
22	$\zeta_\ell + 1$	40	56	2.800	0 mod 4
26	ζ_ℓ	48	56	2.333	3 mod 4
44	$\zeta_\ell + 1$	48	64	2.600	0 mod 4
52	$\zeta_\ell + 1$	48	60	2.500	0 mod 4

5 Conclusion

We have presented an algorithm that produces more Kawazoe-Takahashi type of genus 2 pairing-friendly hyperelliptic curves. In addition we have presented new curves with better ρ-values. A problem with some of the reported curves is that the degree of the polynomial $r(z)$, which defines the prime order subgroup, is too large and hence a very small number, if any, of usable curves could be found. Table 2 summarises the the curves reported in this paper. Curves with $1 \leq \rho \leq 2$ remain elusive.

Table 2. Families of curves, $k < 60$, with $2.000 < \rho \leq 3.000$

k	Degree($r(z)$)	Degree($p(z)$)	ρ-value
2	4	6	3.000
7	24	32	2.667
8	4	6	3.000
10	16	24	3.000
11	40	48	2.400
13	48	64	2.667
22	40	56	2.800
24	8	12	3.000
26	48	56	2.333
28	24	36	3.000
44	48	64	2.600
52	48	60	2.500

References

1. Balakrishnan, J., Belding, J., Chisholm, S., Eisenträger, K., Stange, K. and Teske, E.: Pairings on hyperelliptic curves. Available at `http://www.math.uwaterloo.ca/~eteske/teske/pairings.pdf` (2009).
2. Barreto P.S.L.M., Lynn, B. and Scott, M.: Constructing elliptic curves with prescribed embedding degree. In: Cimato, S., Galdi C., Persiano, G. (eds.) SCN 2002. LNCS, vol. 2576, pp. 263–273, Springer-Verlag (2002).
3. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. SIAM Journal of Computing 32(3), pp. 586-615 (2003).
4. Boneh, D., Lynn, B., and Shacham, H.: Short signatures from the Weil Pairing. In: Boyd, C. (ed.). ASIACRYPT 2001. LNCS, vol. 2248, pp. 514-532. Springer, Verlag (2001).
5. Bosma, W., Cannon, J., and Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. (1997). 24(3-4):235-265.
6. Barreto, P.S.L.M., and Naehrig M.: Pairing-friendly elliptic curves of prime order. Selected Areas in Cryptography – SAC'2005. LNCS, vol. 3897, pp 319–331 Springer (2006).

7. Brezing F. and Weng A.: Elliptic curves suitable for pairing based cryptography, Designs Codes and Cryptography, Vol. 37, No. 1, pp. 133–141 (2005).
8. Cocks, C. and Pinch, R. G. E.: Identity-based cryptosystems based on the Weil pairing. Unpublished manuscript (2001).
9. Furukawa, E., Kawazoe, M., Takahashi, T.: Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields. In: Matsui, M., Zuccherato, R.J. (eds.) SAC 2003. LNCS, vol. 3006, pp. 26-41. Springer, Heidelberg (2004).
10. Freeman, D.: Constructing pairing-friendly elliptic curves with embedding Degree 10. In Algorithmic Number Theory Symposium ANTS-VII,LNCS, vol.4096, pp. 452–465. Springer, Heidelberg (2006).
11. Freeman, D.: A generalized Brezing-Weng method constructing ordinary pairing-friendly abelian varieties. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008, LNCS vol.5209, pp 148–163 Springer, Heidelberg (2008).
12. Freeman, D.: Constructing pairing-friendly genus 2 curves with ordinary Jacobians. In: Takagi, T., Okamoto, T., Okamoto, E.,Okamoto, T. (eds.) Pairing 2007. LNCS, vol.4575, pp. 152-176, Springer, Heidelberg (2007).
13. Freeman, D., Stevenhagen, P. and Streng, M.: Abelian varieties with prescribed embedding degree. In: var der Poorten, A.J., Stein, A. (eds.) ANTS-VIII 2008. LNCS, vol.5011, pp. 60-73. Springer, Heidelberg (2008).
14. Freeman, D., Scott, M. and Teske, E.: A Taxonomy of pairing-friendly elliptic curves. Journal of Cryptology. Volume 23 Issue 2 (2009).
15. Freeman, D., Satoh, T.:Constructing pairing-friendly hyperelliptic curves using Weil restrictions. Cryptography ePrint Archive, Report 2009/103 (2009). Available at `http://eprint.iacr.org`.
16. Joux, A.: A One Round Protocol for Tripartite Diffie-Hellman. In: Bosma, W. (ed.). ANTS 2000. LNCS, vol.1838, pp. 385-394. Springer, Heidelberg (2000).
17. Kachisa, E., Schaeffer, E.F. and Scott M.: Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS vol.5209, pp 126–135 Springer, Heidelberg (2008).
18. Kawazoe, M., Takahashi, T.: Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS vol.5209, pp 164–177 Springer, Heidelberg (2008).
19. Miyaji, A., Nakabayashi, M. and Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fundamentals, E84 pp. 1234 - 1243 (2001).
20. Sakai, R., Ohgishi, K., and Kasahara, M.: (2000). Cryptosystems based on pairing. Symposium on Cryptography and Information Security (SCIS2000), Okinawa, Japan, Jan. 2628, 2000.
21. Scott, M., and Barreto, P. S.: Generating more MNT elliptic curves. Designs, Codes and Cryptography 38, 209-217 (2006).
22. Shamir, A.: Identity-Based cryptosystems and signature schemes. In: Blakery, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47-53. Springer, Heidelberg (1985).
23. PARI-GP, version `2.3.2`, Bordeaux, 2006, `http://pari.math.u-bordeaux.fr/`.
24. Silverman, J. H.: The arithmetic of elliptic curves. Springer-Verlag (1986).
25. Zhang F.: Twisted Ate pairing on hyperelliptic curves and application. Cryptology ePrint Archive Report 2008/274 (2008), `http://eprint.iacr.org/2008/274/`.

Appendix A: More examples

Here we include the polynomials that define curves of some of the embedding degrees in Table 1.

Theorem 8. *Let $k = 11, \ell = 88$. Let $\gamma = \zeta_\ell \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
r(z) &= z^{40} - z^{36} + z^{32} - z^{28} + z^{24} - z^{20} + z^{16} - z^{12} + z^8 - z^4 + 1 \\
p(z) &= 1/8(z^{48} - 2z^{46} + z^{44} + 8z^{24} + z^4 - 2z^2 + 1) \\
c(z) &= -1/2(z^{13} + z^{11}) \\
d(z) &= 1/4(z^{24} - z^{22} - z^2 + 1) \\
\rho &= 12/5
\end{aligned}$$

Family $(r(4z+3)/89, p(4z+3))$

Theorem 9. *Let $k = 13, \ell = 104$. Let $\gamma = \zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
r(z) &= z^{48} - 48z^{47} + 1128z^{46} + ... + 2z^2 - 24z + 1 \\
p(z) &= (z^{64} - 64z^{63} + 2016z^{62} - ... + 4040z^2 - 256z + 8)/8 \\
c(z) &= -(z^{19} - 19z^{18} + 171z^{17} + ... + 249z^2 - 32z + 2)/2 \\
d(z) &= (z^{32} - 32z^{31} + 496z^{30} - ... + 20995z^4 - 2340z^3 + 156z^2)/4 \\
\rho &= 8/3
\end{aligned}$$

Family $(r(8z+4), p(8z+4)$

Theorem 10. *Let $k = 22, \ell = 88$. Let $\gamma = \zeta_\ell \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
r(z) &= z^{40} - z^{36} + z^{32} - z^{28} + z^{24} - z^{20} + z^{16} - z^{12} + z^8 - z^4 + 1 \\
p(z) &= (z^{56} - 2z^{50} + z^{44} + z^{28} + z^{12} - 2z^6 + 1)/8 \\
c(z) &= -(z^{17} + z^{11})/2 \\
d(z) &= (z^{34} - z^{22} + z^{12} + 1)/4 \\
\rho &= 14/5
\end{aligned}$$

Family $(r(4z+3)/89, p(4z+3))$

Theorem 11. *Let $k = 26, \ell = 104$. Let $\gamma = \zeta_\ell \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
r(z) &= z^{48} - z^{44} + z^{40} - z^{36} + z^{32} - z^{28} + z^{24} - z^{20} + z^{16} - z^{12} + z^8 - z^4 + 1 \\
p(z) &= (z^{56} - 2z^{54} + z^{52} + 8z^{28} + z^4 - 2z^2 + 1)/8 \\
c(z) &= -(z^{15} + z^{13})/2 \\
d(z) &= (z^{28} - z^{26} - z^2 + 1)/4 \\
\rho &= 7/3
\end{aligned}$$

Family $(r(4z+3), p(4z+3))$