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

Ezekiel 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 [20], identity based encryption [5] and digital signatures [6], 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 [15], 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 [12]. Freeman modeled the Cocks-Pinch method [9] to construct ordinary hyperelliptic curves of genus 2. His algorithm produced curves over prime fields with prescribed embedding degree k with ρ-value ≈ 8. Kawazoe and Takahashi [22] 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 [16]

* 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 E is defined over $\mathbb{F}_p$, and A is abelian variety isogenous over $\mathbb{F}_{p^d}$ to a product of two isomorphic elliptic curves then the abelian variety 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 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 $7, 8, 10, 11, 13, 22, 26, 28, 44$ 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 and r be prime integers. We denote a hyperelliptic curve of genus g by C and J_C denotes the Jacobian variety of dimension g. This is a quotient group, thus the elements of the Jacobian are not points, they are equivalence classes of divisors of degree zero under relation of linear equivalence. The $\mathbb{F}_p$-rational points are denoted by $J_C(\mathbb{F}_p)$,while $J_C[r]$ represents a prime subgroup of order r. Let $\chi(t)$ denote the characteristic polynomial of the pth power Frobenius Endomorphism of C.

We start by discussing *hyperelliptic curves* in relation to the construction of pairing-friendly curves. The following is the definition of hyperelliptic curves of genus g [10]:

Definition 1. *Let $\mathbb{F}_p$ be a finite field and C be a curve of genus g given by the equation:*

$$C : y^2 + yh(x) = f(x), \tag{1}$$

where $h(x), f(x) \in \mathbb{F}_{p[x]}$ *such that* $deg(f) = 2g + 1$ *and* $deg(h) < g$. *If* f *is monic then* C *is called a hyperelliptic curve of genus* g *defined over* $\mathbb{F}_p$ *if no point over the algebraic closure* $\bar{\mathbb{F}}_p$ *of* $\mathbb{F}_p$ *satisfies both partial derivatives* $2y + h = 0$ *and* $f' - h'y = 0$.

The condition that no point over the algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$ satisfies both partial derivatives $2y + h = 0$ and $f' - h'y = 0$ ensures that the curve is nonsingular.

Points on C, with $g \geq 2$, do not form a group. They form what is known as an involution. The involution of a point $P = (x, y)$ denoted by $\imath$ is defined by $\imath(P) = (x, -y - h(x))$ such that $\imath(\mathcal{O}) = \mathcal{O}$. As such we work with the divisor class group of the curve. The divisor is defined as follows:

Definition 2. *A divisor* D *is a formal sum of points on* C

$$D = \{ \sum_{P \in C(\bar{\mathbb{F}}_p)} n_P P : n_P \in \mathbb{Z} \} \tag{2}$$

where only a finite number of n_p *are non-zero.*

The sum is a formal sum over symbols (P) and addition is carried out coefficient-wise. We define $\deg(D) = \sum_{P \in C(\bar{\mathbb{F}}_p)} n_P \in \mathbb{Z}$ and the *order* of D at P, $ord_P(D) = n_P \in \mathbb{Z}$ and the subgroup of degree 0 divisors is denoted by Div^0_C. The support $supp(D)$ of divisor D is the set of points P with $n_P \neq 0$. The set of all divisors forms additive group under an addition rule:

$$\sum_{P \in C(\bar{\mathbb{F}}_p)} n_P P + \sum_{P \in C(\bar{\mathbb{F}}_p)} m_P P = \sum_{P \in C(\bar{\mathbb{F}}_p)} (n_P + m_P) P \tag{3}$$

As in the elliptic curve case the *embedding degree* is defined as follows for hyperelliptic curves:

Definition 3 ([12]). *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* $J_C[r]$ *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. For practical purposes curves must have small embedding degree so that arithmetic in $\mathbb{F}_{p^k}$ is feasible.

For an efficient arithmetic implementation the size of the finite field, $\mathbb{F}_p$, should be as small as possible relative to the the size of the prime order subgroup r. This is measured by a parameter known as the ρ-value. In the ideal case the Jacobian varieties have a prime number of points in which case $\rho \approx 1$. If p and r are expressed as polynomials then this parameter is defined as $\rho = \frac{g \deg(p(x))}{\deg(\mathrm{r(x)})}$.

Hence the interest has been to construct curves with these attributes: Curves with low embedding degrees and small ρ-values and sufficiently large prime order subgroup.

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

$$w_r : J_C[r] \times J_C[r] \longrightarrow \mu_r$$

while a non degenerate, bilinear map for Tate pairing the map is defined by:

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

When C has genus, $g \leq 1$ and embedding degree k with respect to r, the field $\mathbb{F}_{p^k}$ is generated by coordinates of all r-torsion points. But for higher genus cases Freeman has the following result [13]:

Proposition 1. *Let A be abelian variety over a finite field $\mathbb{F}_p$, $\chi(t)$ the characteristic polynomial of the pth power Frobenius map of A. For a prime number r not dividing p and a positive integer k, suppose the the following hold:*

$$\chi(1) \equiv 0 \pmod{r} \text{ and}$$
$$\Phi_k(p) \equiv 0 \pmod{r}$$

where Φ_k is the kth cyclotomic polynomial. Then A has embedding degree k with respect to r. Furthermore, if $k > 1$ then $A(\mathbb{F}_{p^k})$ contains two linearly independent r-torsion points.

3 Kawazoe-Takahashi hyperelliptic curves

Kawazoe and Takahashi [22] 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 [9] of constructing ordinary pairing-friendly elliptic curves and the other was based on cyclotomic polynomials. Both approaches were based on the predefined sizes of the Jacobians presented in [11]. In general the number of points on a hyperelliptic curve, C, is dependent on the characteristic polynomial, $\chi(t)$. For genus 2 hyperelliptic curves a $\chi(t)$ is given by the following equation:

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

within $a_1, a_2 \in \mathbb{F}_p$ and furthermore $\mid a_1 \mid \leq 4p$ and $\mid a_2 \mid \leq 6p$. It is a well known fact from Equation 4, that the order of hyperelliptic curve of genus g is given by:

$$\#J_C = \chi(1) = 1 - a_1 + a_2 - a_1 p + p^2. \tag{5}$$

The Hess-Weil bound puts the order of the curve in a rather small interval as follows:

$$\left\lceil (\sqrt{p} - 1)^{2g} \right\rceil \leq \#J_C \leq \left\lfloor (\sqrt{p} + 1)^{2g} \right\rfloor \tag{6}$$

Simple ordinary Jacobian on hyperelliptic curves of the form $y^2 = x^5 + ax$ defined over $\mathbb{F}_p$ are given in Theorem 1 below:

Theorem 1 ([11],[22]). *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.

In addition, they also presented cyclotomic families. With this method they managed to construct a $k = 24$ curve with $\rho = 3.000$. 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 $y^2 = x^5 + ax$.

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 $y^2 = x^5 + ax$.

1. Choose r a prime such that $lcm(8, k)$ divides $r - 1$.
2. Choose ζ a primitive kth root of unity in $(\mathbb{Z}/r\mathbb{Z})^\times$, ω 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 -1 and 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 as 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 [21] 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 contentious issue has always been the choice of 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 $\zeta(z), \omega(z)$ and $\sigma(z)$ in $\mathbb{Q}[z]$ such that $\zeta(z)$ 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:
   - $c(z) \equiv (\zeta(z) + \omega(z))(\sigma(z)(\omega(z) + 1))^{-1}$ in $\mathbb{Q}[z]/r(z)$.
   - $d(z) \equiv (\zeta(z)\omega(z) + 1)(2(\omega(z) + 1))^{-1}$ in $\mathbb{Q}[z]/r(z)$.
4. Compute a polynomial, $p(z) = c(z)^2 + 2d(z)^2$.
5. For some $z_0 \in \mathbb{Z}$ 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 $(p(z_0), r(z_0), a)$
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 $\zeta(z), \omega(z)$ and $\sigma(z)$ in $\mathbb{Q}[z]$ such that $\zeta(z)$ 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
   - $c(z) \equiv 2^{-1}(\zeta(z) - 1)\omega(z))$ mod $r(z)$
   - $d(z) \equiv (z(z) + 1)(2\sigma(z))^{-1}$ mod $r(z)$
4. Compute an irreducible polynomial $p(z) = (c(z)^2 + 2d(z)^2)$
5. For some $z_0 \in \mathbb{Z}$ such that:
   - $p(z_0)$ and $r(z_0)$ represents primes and $p(z_0) \equiv 1, 3$ mod 8 and
   - $c(z_0), d(z_0)$ represents integers and $c(z_0) \equiv 1$ mod 4.
6. Find $a \in \mathbb{F}_p(z_0)$ such that:
   - $a = \delta^2$ when $p(z_0) \equiv 1$ mod 8 or
   - $a = \delta$ when $p(z_0) \equiv 3$ mod 8.
7. Output $(p(z_0), r(z_0), a)$.
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 $k = 7, 8, 10, 11, 13, 22, 26, 28, 44$ 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 [21] 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 [15], 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 $\zeta_k, \sqrt{-1}$ and $\sqrt{2}$ 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 $p(z) \in \mathbb{Q}[z]$. But since we need $p(z)$ and $r(z)$ to represent primes, for a favourable set of $r(z), p(z), c(z), d(z)$ we use the following conjecture:

Conjecture 1. Let $f(z) \in \mathbb{Q}[z]$. $f(z)$ represents primes if the following conditions are satisfied:

- $f(z)$ represents integers i.e. for some $z_0 \in \mathbb{Z}$, $f(z_0) \in \mathbb{Z}$.
- $f(z)$ is irreducible polynomial with a positive leading coefficient.
- for some $z_0, z_1 \in \mathbb{Z}$, $gcd(f(z_0), f(z_1)) = 1$.

Hence for a potential set of parameters, we check for a modular class with both $r(z)$ and $p(z)$ represent primes and $p(z) \equiv 1, 3 \bmod 8$ and furthermore $c(z) \equiv 1 \bmod 4$.

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 curve with $\rho = 2.667$.

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:*

$$
\begin{aligned}
r(z) &= z^{24} - 24z^{23} + 276z^{22} - 2024z^{21} + 10625z^{20} - 42484z^{19} \\
&\quad + 134406z^{18} - 344964z^{17} + 730627z^{16} - 1292016z^{15} + 1922616z^{14} \\
&\quad - 2419184z^{13} + 2580005z^{12} - 2332540z^{11} + 1784442z^{10} - 1150764z^{9} \\
&\quad + 621877z^{8} - 279240z^{7} + 102948z^{6} - 30632z^{5} + 7175z^{4} - 1276z^{3} + 162z^{2} - 12z + 1 \\
p(z) &= (z^{32} - 32z^{31} + 494z^{30} - 4900z^{29} + 35091z^{28} - 193284z^{27} + \\
&\quad 851760z^{26} - 3084120z^{25} + 9351225z^{24} - 24075480z^{23} + 53183130z^{22} - \\
&\quad 101594220z^{21} + 168810915z^{20} - 245025900z^{19} + 311572260z^{18} - \\
&\quad 347677200z^{17} + 340656803z^{16} - 292929968z^{15} + 220707810z^{14} - 145300540z^{13} + \\
&\quad 83242705z^{12} - 41279004z^{11} + 17609384z^{10} - 6432920z^{9} + 2023515z^{8} \\
&\quad - 569816z^{7} + 159446z^{6} - 49588z^{5} + 16186z^{4} - 4600z^{3} + 968z^{2} - 128z + 8)/8 \\
c(z) &= (-z^{9} + 9z^{8} - 37z^{7} + 91z^{6} - 147z^{5} + 161z^{4} - 119z^{3} + 57z^{2} - 16z + 2)/2 \\
d(z) &= (z^{16} - 16z^{15} + 119z^{14} - 546z^{13} + 1729z^{12} - 4004z^{11} + 7007z^{10} \\
&\quad - 9438z^{9} + 9867z^{8} - 8008z^{7} + 5005z^{6} - 2366z^{5} + 819z^{4} - 196z^{3} + 28z^{2})/4
\end{aligned}
$$

Then $(r(2z)/8, p(2z))$ constructs a complete ordinary pairing-friendly genus 2 hyperelliptic curves with embedding degree 7. The ρ-value of this family is 2.667.

Proof. Since $\zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ has minimal polynomial $r(z)$. We apply Algorithm 3 by working in $\mathbb{Q}[z]/r(z)$. 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 [31], show that both $r(2z)/8$ 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, $k = 7$. (Kawazoe-Takahashi *Type I* curves have their Jacobian equal to $\#Jc(z) = 1 - 4d(z) + 8d(z)^2 - 4d(z)p(z) + p(z)^2$).

We now give an example of a 254- bit prime subgroup that is constructed using the parameters in Theorem 2 .

Example 1.

$r = 213748555325666652890713665865251428761742681841141544849244\backslash$

$$05425230130090001$$

$$p = 74150466118914277076982986134425794882179740154970735315435108095481642765042445975666095781797666897$$

$$c = -2102247714969368735010398437 5$$

$$d = 19254930033489381271793153044560509686043701114494 4$$

$$a = 3$$

Hence our genus 2 pairing-friendly hyperelliptic equation is $C : y^2 = x^5 + 3x$ whose $\rho = 2.646$ and embedding degree is 7

The next curve is of embedding degree $k = 8$. It is shown in [34] that curves of the form $C : y^5 + ax$ and embedding degree 8 admits higher order twists. In particular a degree 8 twist has a curve of the form $C' : y^5 + a\kappa x$ by $(x, y) \longmapsto (\kappa^{\frac{1}{4}}x, \kappa^{\frac{5}{8}}y)$, where $\kappa \in \mathbb{F}_p$ is not ith power residue in $\mathbb{F}_p$, $i \in \{1, 2, 4, 8\}$ [34].

Hence for this curve 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 $\rho \approx 4.000$. In Theorem 3 below we outline the parameters that defines the hyperelliptic curves of embedding degree 8 with $\rho \approx 3.000$.

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:*

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

Then $(r(32z)/8, p(32z))$ constructs a complete ordinary pairing-friendly genus 2 hyperelliptic curves with embedding degree 8. The ρ-value of this family is 3.000.

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.

$$r = 131072000000009898508288000280324362739203528331792090742477643363528725893137(257bits)$$

$$p = 184549376000020905654747136986742251766767879474504560418252532669506933642904885116183766157641277112712983172884737$$

$$c = 12288000000000695988992000013140209336688082695322003440625$$

$$d = -4096000000000231996416000004380073001064027565137751569916$$

$$a = 3$$

Hence our genus 2 pairing-friendly hyperelliptic equation is $C : y^2 = x^5 + 3x$ with $\rho = 3.012$ of embedding degree 8

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:*

$$\begin{aligned}
r(z) &= z^{16} - 16z^{15} + 120z^{14} - 560z^{13} + 1819z^{12} - 4356z^{11} + 7942z^{10} - \\
&\quad 11220z^9 + 12376z^8 - 10656z^7 + 7112z^6 - 3632z^5 + 1394z^4 - 392z^3 + 76z^2 - 8z + 1 \\
p(z) &= (z^{24} - 24z^{23} + 274z^{22} - 1980z^{21} + 10165z^{20} - 39444z^{19} \\
&\quad +120156z^{18} - 294576z^{17} + 591090z^{16} - 981920z^{15} + 1360476z^{14} - \\
&\quad 1578824z^{13} + 1536842z^{12} - 1253336z^{11} + 853248z^{10} - 482384z^9 + \\
&\quad 225861z^8 - 88872z^7 + 31522z^6 - 11676z^5 + 4802z^4 - 1848z^3 + 536z^2 - 96z + 8)/8 \\
c(z) &= (-z^7 + 7z^6 - 22z^5 + 40z^4 - 45z^3 + 31z^2 - 12z + 2)/2 \\
d(z) &= (z^{12} - 12z^{11} + 65z^{10} - 210z^9 + 450z^8 - 672z^7 + 714z^6 - 540z^5 + 285z^4 - \\
&\quad 100z^3 + 20z^2)/4
\end{aligned}$$

Then $(r(4z), p(4z))$ constructs a complete ordinary pairing-friendly genus 2 hyperelliptic curves with embedding degree 10. The ρ-value of this family is 3.000.

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

Example 3.

$$\begin{aligned}
r &= 4745749105410301406815931235596753944430110861981481094827979311321433 1\backslash \\
&\quad 8041 \\
p &= 3392680476835482274427348989075071521908024843148191254993934108021750 4\backslash \\
&\quad 4822928270159666053912399467210953623356417 \\
c &= -1189724159035338550797061406711295 \\
d &= 4118665121635578103210977882765100527274697866021896847 36 \\
a &= 3
\end{aligned}$$

Hence our genus 2 pairing-friendly hyperelliptic equation is $C : y^2 = x^5 + 3x$ whose embedding degree is 10.

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:*

$$\begin{aligned}
r(z) &= z^{24} - 24z^{23} + 276z^{22} - 2024z^{21} + 10625z^{20} - 42484z^{19} + \\
&\quad 134406z^{18} - 344964z^{17} + 730627z^{16} - 1292016z^{15} + 1922616z^{14} - \\
&\quad 2419184z^{13} + 2580005z^{12} - 2332540z^{11} + 1784442z^{10} - 1150764z^9 + 621877z^8 - \\
&\quad 279240z^7 + 102948z^6 - 30632z^5 + 7175z^4 - 1276z^3 + 162z^2 - 12z + 1 \\
p(z) &= (z^{36} - 36z^{35} + 630z^{34} - 7140z^{33} + 58903z^{32} - 376928z^{31} + \\
&\quad 1946800z^{30} - 8337760z^{29} + 30188421z^{28} - 93740556z^{27} + 252374850z^{26} - \\
&\quad 594076860z^{25} + 1230661575z^{24} - 2254790280z^{23} + 3667649460z^{22} -
\end{aligned}$$

$$5311037640z^{21} + 6859394535z^{20} - 7909656300z^{19} + 8145387218z^{18} - 7487525484z^{17} + 613613430z^{16} - 4473905808z^{15} + 2893567080z^{14} - 1653553104z^{13} + 830662287z^{12} - 364485108z^{11} + 138635550z^{10} - 45341540z^{9} + 12681910z^{8} - 3054608z^{7} + 660688z^{6} - 141120z^{5} + 32008z^{4} - 7072z^{3} + 1256z^{2} - 144z + 8)/8$$

$$c(z) = (-z^{11} + 11z^{10} - 55z^{9} + 165z^{8} - 331z^{7} + 469z^{6} - 483z^{5} + 365z^{4} - 200z^{3} + 76z^{2} - 18z + 2)/2$$

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

Then $(r(2z), p(2z))$ constructs a complete ordinary pairing-friendly genus 2 hyperelliptic curves with embedding degree 28. The ρ-value of this family is $\rho \approx 3.000$.

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

Example 4.

$r = 424919600539385944351122192376667674313110063571221116966903628832285002084 81$

$p = 109488916950130503728824712394480136647965331684153523928056833619302663216719 51 \backslash$
$84728514564519636647060505191263121$

$c = -661115396488771699930556119523372 39$

$d = 739894982244542944193343853775218465253390470331838998400$

$a = 23$

Once again our genus 2 pairing-friendly hyperelliptic equation is $C : y^2 = x^5 + 23x$ whose embedding degree is 28 with $\rho = 2.972$.

The following family is reported in [22]. One can use the following parameters to construct a *Kawazoe-Takahashi Type II* pairing-friendly hyperelliptic curve of embedding degree $k = 24$ with $\rho \approx 3.000$.

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:*

$$r(z) = z^8 - 8z^7 + 28z^6 - 56z^5 + 69z^4 - 52z^3 + 22z^2 - 4z + 1$$

$$p(z) = (2z^{12} - 28z^{11} + 179z^{10} - 688z^9 + 1766z^8 - 3188z^7 + 4155z^6 - 3948z^5 + 2724z^4 - 1336z^3 + 443z^2 - 88z + 8)/8$$

$$c(z) = (-z^6 + 7z^5 - 20z^4 + 30z^3 - 25z^2 + 11z - 2)/2$$

$$d(z) = (z^5 - 4z^4 + 5z^3 - 2z^2 - z)/4$$

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 3.000.

The following curve is of embedding degree $k = 2$ with $\rho = 3.000$. In this case the parameters corresponds to a quadratic twist $C\prime$ of the curve C

which has a large prime of size r. The interesting part of this curve is that one can implementat the curve using the idea of quadratic twists. The use of twists in ordinary pairing friendly curves speed up pairing computation. In this curve for instance, we can choose both inputs from base field.

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:*

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

Then $(r(36z + 8)/9, p(36z + 8))$ constructs a complete ordinary pairing-friendly genus 2 hyperelliptic curves with embedding degree 2. The ρ-value of this family is 3.000.

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

Example 5.

$r = 1866240767113923045167388159201163779990313800469 7$

$p = 10279256257891516489822674213746873409099825032526561651641299094595596792 17$

$c = 233280071916861790309390681284245607 23$

$d = -155520047944596126877366449084261343 38$

$a = 10$

Once again our genus 2 pairing-friendly hyperelliptic equation is $C' : y^2 = x^5 + 10x$ and hence $C : y^2 = 20(x^5 + 10x)$ is the curve whose order has a large prime r and embedding degree is 2 with $\rho = 3.049$.

We now present pairing-friendly hyperelliptic curves of embedding k whose polynomial that defines the the size of the prime subgroup deg $r(z)$ has its degree greater or equal to 40. 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 $deg(r(z)) > 40$

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. (2009) *Pairings on Hyperelliptic Curves*. Available at `http://www.math.uwaterloo.ca/~eteske/teske/pairings.pdf`.
2. Barreto P.S.L.M., Lynn, B. and Scott, M., (2002) *Constructing elliptic curves with prescribed embedding degree.* Security in Communication Networks -SCN 2002, Lecture Notes in Computer Science 2576, pp. 263–273, Springer-Verlag.
3. Barreto P.S.L.M., Lynn, B. and Scott, M., (2003) *On the Selection of Pairing-Friendly Groups.* Symposium on Applied Computing -SAC 2003, Lecture Notes in Computer Science 3006, pp. 17–25, Springer-Verlag.
4. Barreto, P.S.L.M., and Naehrig M., (2006) *Pairing-friendly elliptic curves of prime order*. Selected Areas in Cryptography SAC'2005, Lecture Notes in Computer Science 3897, pp 319–331 Springer-Verlag.
5. Boneh, D., Franklin, M. (2001) *Identity-based encryption from the Weil pairing.* Lecture Notes in Computer Science 2139, pp. 213-229, Springer-Verlag.
6. Boneh, D., Lynn, B., and Shacham, H. (2001). *Short Signatures from the Weil Pairing*. Lecture Notes in Computer Science 2248, pp. 514-532. Springer, Verlag.

7. Bosma, W., Cannon, J., and Playoust, C. (1997). *The Magma algebra system. I. The user language.* J. Symbolic Comput., 24(3-4):235-265.
8. Brezing F. and Weng A., (2005) *Elliptic curves suitable for pairing based cryptography.*, Designs Codes and Cryptography, Vol. 37, No. 1, pp. 133–141.
9. Cocks, C. and Pinch, R. G. E., (2001) *Identity-based cryptosystems based on the Weil pairing.*, Unpublished manuscript.
10. Cohen, H., Frey, G. (2006). *Hanbook of Elliptic and Hyperelliptic Curve Cryptography* Chapman & Hall/CRC.
11. Furukawa, E., Kawazoe, M., Takahashi, T., (2004). *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.
12. Freeman, D., (2006) *A generalized Brezing-Weng method constructing ordinary pairing-friendly abelian varieties.* Cryptography ePrint Archive, Report 2008/155, Available at `http://eprint.iacr.org`.
13. Freeman, D., (2006) *Constructing pairing-friendly elliptic curves with embedding Degree 10.* In Algorithmic Number Theory Symposium ANTS-VII, Lecture Notes in Computer Science 4096, pp. 452–465. Springer-Verlag.
14. Freeman, D., Stevenhagen, P. and Streng, M., (2009) *Abelian varieties with prescribed embedding degree.* Available at `http://theory.stanford.edu/~dfreeman/papers/ants-viii.pdf`
15. Freeman, D., Scott, M. and Teske, E., (2009) *A Taxonomy of pairing-friendly elliptic curves.* Journal of Cryptology. Volume 23 Issue 2.
16. Freeman, D., Satoh, T. (2010) *Constructing pairing-friendly hyperelliptic curves using Weil Restrictions.* Cryptography ePrint Archive.
17. Frey, G., and Rück, H-G., (1994). *A Remark concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves.* Mathematics of Computation, Volume 62, Number 206, pp. 865–874. American Mathematical Society.
18. Galbraith, S.D, McKee, J. and Valenca, P., (2004) *Ordinary Abelian varieties having small embedding degree.* Cryptography ePrint Archive, Report 2004/365, http://eprint.iacr.org/2004/365.
19. Galbraith, S. D., Scott, M. (2008). *Exponentiation in pairing-friendly groups using homomorphisms.* Pairing 2008, Lecture Notes in Computer Science 5209, pp 211–224 Springer-Verlag.
20. Joux, A, (2000). *A One Round Protocol for Tripartite Diffie-Hellman.* Lecture Notes in Computer Science, 1838, pp. 385-394. Springer, Verlag.
21. Kachisa, E., Schaeffer, E.F. and Scott M (2008) *Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field*, Pairing 2008, Lecture Notes in Computer Science 5209, pp 126–135 Springer-Verlag.
22. Kawazoe, M., Takahashi, T., (2008). *Pairing-friendly Hyperelliptic curves with Ordinary Jacobians of type $y^2 = x^5 + ax$.* Cryptography ePrint Archive, Report 2008/026, `http://eprint.iacr.org/`.
23. Kawazoe, M., Sakaeyama, R., Takahashi, T., (2008) *Pairing-friendly Hyperelliptic Curves of type $y^2 = x^5 + ax$.* In: 2008 Symposium on Cryptography and Information Security (SCIS 2008), Miyazaki, Japan.
24. Kang, W., (2007). *Construction of Pairing-friendly elliptic curves by Cocks-Pinch Method.* Cryptography ePrint Archive, Report 2007/110, `http://eprint.iacr.org/`.
25. Miller V.S., (1986) *Short programs for functions on curves.* Unpublished manuscript. Available at `http://crypto.stanford.edu/miller/miller.pdf`.

26. Miyaji, A., Nakabayashi, M. and Takano, S., (2001) *New explicit conditions of elliptic curve traces for FR-reduction*. IEICE Trans. Fundamentals, E84 pp. 1234 - 1243.
27. Menezes, A., Okamoto, T., and Vanstone, S., (1991) *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*. Proceedings of the twenty-third annual ACM symposium on Theory of computing, pp. 80-89. Association for Computing Machinery.
28. Sakai, R., Ohgishi, K., and Kasahara, M. (2000). *Cryptosystems based on pairing*. Symposium on Cryptography and Information Security (SCIS2000), Okinawa, Japan, Jan. 2628, 2000.
29. Scott, M., and Barreto, P. S., (2004). *Generating more MNT elliptic curves*. Cryptology ePrint Archive, Report 2004/058, `http://eprint.iacr.org/`.
30. Shamir, A. (1984). *Identity-Based Cryptosystems and Signature Schemes*. Lecture Notes in Computer Science, 196, pp. 47-53. Springer, Verlag.
31. *PARI-GP*, version `2.3.2`, Bordeaux, 2006, `http://pari.math.u-bordeaux.fr/`.
32. Silverman, J. H. (1986). *The Arithmetic of Elliptic Curves*. Springer-Verlag.
33. Tanaka, S. and Nakamula, K., (2007) *More constructing pairing-friendly elliptic curves for cryptography*. Mathematics arXiv Archive, Report 0711.1942, `http://arxiv.org/abs/0711.1942`.
34. Zhang F., (2008) *Twisted Ate Pairing on Hyperelliptic Curves and Application*. Cryptology ePrint Archive Report 2008/274, `http://eprint.iacr.org/2008/274/`.

Appendix A: Magma Code

Here we include a basic magma code for computing Tate pairing on Hyperelliptic curves[1]. The implementation was done on a pairing-friendly hyperelliptic curve of embedding degree $k = 8$.

Listing 1. Magma code for Tate pairing computation on k=8 curve

```
k:=8;
p:=0x4AF0A9F269200645D6FBDC4F94A975A9F5EDD683B630AF39470343C\\
  6FE7825680D8B8958646620262E34031F8A66C2901;
r:=0x121C81F7DD4528470D24FCE166AD379A5BEDA4C80FF4C2CABAE72AFA\\
   3C23A1011;
c:=122880000000006959889920000131402093366880826953220034406 25;
d:=-40960000000002319964160000043800730010640275651377515699 16;
zk:=819200000000046399232000000876012666912005513009300060158 5;

Z<x> := PolynomialRing(GF(p));
f:= x^5+3*x;
h:=0;
C:=HyperellipticCurve(f);
g:=Genus(C);
Jc := Jacobian(C);
Jc2 := BaseExtend(Jc,8);
```

```
IdJc:=Identity(Jc);
ordJc:=1-4*d+8*d^2-4*d*p+p^2;
cofactor:= ordJc div r;
P:=Random(Jc)*cofactor;
Q:=Random(Jc2);

//Cantor's Algorithm
ReducedDivisor:=function(L,K,M)
u1:=L[1];
v1:=L[2];
u2:=K[1];
v2:=K[2];

d1,e1,e2:=ExtendedGreatestCommonDivisor(u1,u2);
d,c1,c2:=ExtendedGreatestCommonDivisor(d1,v1+v2+h);

h1tilda:= d mod M[1];
h2tilda:= 1;
h3:= 1;


s1:=c1*e1;
s2:=c1*e2;
s3:=c2;
u:=(u1*u2) div d^2;
v:=(((s1*u1*v2) +(s2*u2*v1)+s3*(v1*v2+f))div d) mod u;

repeat;
uprime:=(f-v*h-v^2) div u;
vprime:=(-h-v) mod uprime;

h1tilda:= h1tilda*(M[2]-v) mod M[1];
h2tilda:= h2tilda*uprime mod M[1];

 if Degree(v) gt g then
   h3:=-LeadingCoefficient(v)*h3;
 end if;
  u:=uprime;
  v:=vprime;

until Degree(u) le g;
u:=1/LeadingCoefficient(u)*u;
ReducedD:=[u,v];
dd:=d;
return ReducedD, h1tilda,h2tilda,h3;
end function;

//Miller's Algorithm
HyperTatePairing:= function(D1,D2,r)
D:=D1;
```

```
f1:=1;
f2:=1;
f3:=1;
i:=Floor(Log(2,r))-1;
while i ge 0 do

    f1:=f1^2 mod D2[1];
    f2:=f2^2 mod D2[1];
    f3:=f3^2;
    D,h1,h2,h3:=ReducedDivisor(D,D,D2);
    f1:=f1* h1 mod D2[1];
    f2:=f2*h2 mod D2[1];
    f3:=f3*h3;
    si:=Intseq(r,2);
  if si[i+1] eq 1 then
       D,h1,h2,h3:=ReducedDivisor(D,D1,D2);
       f1:=f1* h1 mod D2[1];
       f2:=f2*h2 mod D2[1];
       f3:=f3*h3;
  end if;
    i:=i-1;
end while;
pairing_value:=Resultant(D2[1],f1) / (f3^(Degree(D2[1]))*Resultant(
    D2[1],f2));
return pairing_value^((p^k-1) div r);
end function;
```