© de Gruyter 2009
J. Math. Crypt. **3** (2009), 19–36 DOI 10.1515 / JMC.2009.002

Families of genus 2 curves with small embedding degree

Laura Hitt

Communicated by Alfred Menezes

Abstract. In cryptographic applications, hyperelliptic curves of small genus have the advantage of providing a group of comparable size to that of elliptic curves, while working over a field of smaller size. Pairing-friendly hyperelliptic curves are those for which the order of the Jacobian is divisible by a large prime, whose embedding degree is small enough for pairing computations to be feasible, and whose minimal embedding field is large enough for the discrete logarithm problem in it to be difficult. We give a sequence of $\mathbb{F}_q$-isogeny classes for a family of Jacobians of genus 2 curves over $\mathbb{F}_q$, for $q = 2^m$, and the corresponding small embedding degrees. We give examples of the parameters for such curves with embedding degree $k < (\log q)^2$, such as $k = 8, 13, 16, 23, 26$.

For secure and efficient implementation of pairing-based cryptography on genus g curves over $\mathbb{F}_q$, it is desirable that the ratio $\rho = \frac{g \log_2 q}{\log_2 N}$ be approximately 1, where N is the order of the subgroup with embedding degree k. We show that for our family of curves, ρ is between 1 and 2.

We also give a sequence of $\mathbb{F}_q$-isogeny classes for a family of Jacobians of genus 2 curves over $\mathbb{F}_q$ for which the minimal embedding field is much smaller than the finite field indicated by the embedding degree k. That is, the extension degrees in this example differ by a factor of m, where $q = 2^m$, demonstrating that the embedding degree can be a far from accurate measure of security. As a result, we use an indicator $k' = \frac{\mathrm{ord}_N 2}{m}$ to examine the cryptographic security of our family of curves.

Keywords. embedding degree, genus 2, hyperelliptic curves, binary curves, pairing-based cryptography.

AMS classification. 94A60,11T71,14G50.

1 Introduction

The security of elliptic and hyperelliptic curve cryptosystems is based on the computational difficulty of solving the discrete logarithm problem (DLP). There is currently no sub-exponential algorithm for solving the discrete logarithm problem on the Jacobians of properly chosen curves. With hyperelliptic curves of small genus, it is possible to work over a smaller field while achieving security comparable to that of other discrete-log-based cryptosystems. Formulas for fast arithmetic on Jacobians of hyperelliptic curves over binary fields of genus 2 are known, as Lange and Stevens give in [16], which garners more support for their use in cryptosystems.

Pairings on groups have been used for constructive purposes such as identity-based encryption, one-round three-party key agreement and short digital signatures. On the other hand, pairings have been used destructively to attack cryptographic security. For example, informally, the Frey–Rück attack and MOV attack use the Tate pairing and Weil pairing, respectively, to map the discrete logarithm problem on the curve's Jacobian defined over $\mathbb{F}_q$ to the discrete logarithm in the multiplicative group of the extension field $\mathbb{F}_{q^k}$, for some integer k, where there are more efficient methods for solving the DLP. This extension degree k is known as the *embedding degree*. We will say a curve C has embedding degree k with respect to an integer N if and only if a subgroup of order N of its Jacobian J_C does. So for pairing-based cryptosystems, it is important to find curves with embedding degree k small enough that the pairing is efficiently computable yet large enough that the DLP in the multiplicative group of the finite field is hard.

We know that $k \leq 6$ for supersingular elliptic curves, as first shown by Miyaji, Nakabayashi and Takano in [19]. Galbraith in [10] shows that $k \leq 12$ for supersingular curves of genus 2, which is attained in characteristic 2. Freeman in [8] shows one can obtain arbitrary k for ordinary genus 2 curves. In general, one expects k to be roughly the size of the prime-order subgroup, and for cryptographic applications such a k would be much too large for the computation of pairings to be feasible.

It is also desirable for the number of $\mathbb{F}_q$-rational points of the Jacobian of C to be prime or near-prime, since the attack of [20] can reduce the DLP to prime-order subgroups. Thus for a curve over $\mathbb{F}_q$ of genus g whose Jacobian has a subgroup of prime order N with embedding degree k, one examines the ratio $\rho = \frac{g \log_2 q}{\log_2 N}$. For secure and efficient implementation, the ideal situation is to have $\rho \sim 1$. For elliptic curves of prime order, one can get $\rho \sim 1$ for prescribed embedding degree k, as done by Miyaji–Nakabayashi–Takano in [19] for $k = 3, 4, 6$, Barreto–Naehrig in [2] for $k = 12$ and Freeman in [7] for $k = 10$. Freeman's construction in [8] gives ordinary hyperelliptic curves of genus 2 with $\rho \sim 8$.

This leads to the understanding of a *pairing-friendly* hyperelliptic curve over $\mathbb{F}_q$ as one that satisfies the following conditions: (1) The number of $\mathbb{F}_q$-rational points of the Jacobian of C, denoted $\#J_C(\mathbb{F}_q)$, should be divisible by a sufficiently large prime N so that the DLP in the order-N subgroup of $J_C(\mathbb{F}_q)$ is suitably hard, (2) the embedding degree k should be sufficiently small so that the arithmetic in $\mathbb{F}_{q^k}$ can be efficiently implemented, and (3) the security indicator k' should be large enough so that the DLP in $\mathbb{F}^*_{q^{k'}}$ withstands index-calculus attacks.

In this paper, we consider genus 2 curves over $\mathbb{F}_q$, where $q = 2^m$, and whose associated Jacobian has 2-rank 1, i.e. is neither supersingular, nor ordinary. Birkner in [3] gives formulas for fast arithmetic on 2-rank 1 curves, so such curves may be worthwhile to consider. We let C be a genus 2 curve over $\mathbb{F}_q$ of the form

$$y^2 + xy = ax^5 + bx^3 + cx^2 + dx$$

where $a \in \mathbb{F}_q^*$, $b, c, d \in \mathbb{F}_q$, and with characteristic polynomial of Frobenius $f(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2 \in \mathbb{Z}[t]$. Our approach is as follows. In Section 3, we give a parametrization of a family of integers, $N_{r,\ell} = \frac{2^{2^r \ell}+1}{2^{2^r}+1}$ for $r \geq 0$ and odd $\ell \geq 9$, and we determine the embedding degrees for subgroups of Jacobians of curves over $\mathbb{F}_q$ having these orders when they are prime. In Section 4, we associate with each of these primes a sequence of fields $\mathbb{F}_q$ and genus 2 curves C over $\mathbb{F}_q$, such that the Jacobian of each curve has an $\mathbb{F}_q$-rational subgroup of order $N_{r,\ell}$. For example, for each m in the interval $\lceil \frac{2^{r+1}\ell}{3} \rceil \leq m \leq 2^r(\ell - 1) - 1$, if $q = 2^m$ we get $\#J_C(\mathbb{F}_q) = 2^x(2^{2^r} + 1)N_{r,\ell}$, where $x = 2m - 2^r \ell$. We describe the curves by the $\mathbb{F}_q$-isogeny class of their Jacobians, such as having $a_1 = -1$, and $a_2 = 2^m + 2^x$ in the case mentioned above (where a_1 and a_2 are the coefficients of the characteristic polynomial of Frobenius). We show that for our family of curves the ratio ρ is between 1 and 2, which suggests efficient implementation could be possible if the curves can be explicitly constructed. We give examples of the parameters for such curves with embedding degree $k = 8, 13, 16, 23, 26$. In Section 5, we show that the embedding degree k is always "small" for the curves presented in this paper, that is, $k < (\log q)^2$, so that computations in $\mathbb{F}_{q^k}$ may be feasible.

In Section 6, we give an example of another family of curves, whose minimal embedding field and the field indicated by the embedding degree k have extension degrees that differ by a factor of m. This demonstrates that the embedding degree may be an inaccurate indicator of security. If $\text{ord}_N p$ is the smallest positive x such that $p^x \equiv 1 \bmod N$, then we use $k' = \frac{\text{ord}_N 2}{m}$ to examine the cryptographic security of our family of 2-rank 1 curves.

2 Preliminaries

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ for some prime p and positive integer m,[1] and let C be a smooth projective curve over $\mathbb{F}_q$ with genus $g \geq 1$. There exists an abelian variety, called the *Jacobian of* C, denoted J_C, of dimension g such that $J_C(\mathbb{F}_q)$ is isomorphic to the degree zero divisor class group of C over $\mathbb{F}_q$. Assume there exists a prime N dividing the order of $J_C(\mathbb{F}_q)$, with N relatively prime to q. A subgroup of $J_C(\mathbb{F}_q)$ with order N is said to have *embedding degree k with respect to* N if N divides $q^k - 1$, but does not divide $q^i - 1$ for all integers $1 \leq i < k$.

The Tate pairing is a (bilinear, non-degenerate) function

$$J_C(\mathbb{F}_{q^k})[N] \times J_C(\mathbb{F}_{q^k})/NJ_C(\mathbb{F}_{q^k}) \longrightarrow \mathbb{F}_{q^k}^*/\mathbb{F}_{q^k}^{*N}.$$

One can then map $\mathbb{F}_{q^k}^*/\mathbb{F}_{q^k}^{*N}$ isomorphically into the set of Nth roots of unity, μ_N, by raising the image to the power $\frac{q^k-1}{N}$.

Pairing-based attacks transport the discrete logarithm problem in $J_C(\mathbb{F}_q)$ to the discrete logarithm in the multiplicative group of a finite field, where there are subexponential methods for solving the DLP. As shown in [12], whenever q is not prime, the smallest finite field containing the Nth roots of unity is actually $\mathbb{F}_{q^{k'}}$, where $k' = \frac{\text{ord}_N p}{m}$, and this field may be much smaller than $\mathbb{F}_{q^k}$. So for pairing-based cryptosystems, one would like to find curves with k' large enough for the DLP in the minimal embedding field to be difficult, but with embedding degree k small enough for computations to be feasible. For most non-supersingular curves, the embedding degree is enormous. We will give a sequence of (non-supersingular, non-ordinary) 2-rank 1 curves with small embedding degree.

The fact that there exist simple abelian surfaces with characteristic polynomial of Frobenius $f(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2 \in \mathbb{Z}[t]$ for certain conditions on a_1 and a_2 is shown in [21]. Howe in [13] showed which characteristic polynomials of Frobenius

[1] We view $\mathbb{F}_q$ as a general field extension, though for practical cryptographic applications, one usually restricts to prime degree field extensions in order to avoid Weil descent attacks [9].

correspond to isogeny classes of abelian surfaces that contain ordinary Jacobians of genus 2 hyperelliptic curves, and the non-ordinary case is a consequence of [14] and [17]. So we have that (a_1, a_2) determines the $\mathbb{F}_q$-isogeny class of the Jacobian of a smooth projective curve C of genus 2 defined over $\mathbb{F}_q$, with $\#J_C(\mathbb{F}_q) = q^2 + a_1 q + a_2 + a_1 + 1$.

In Theorem 4.1, we use the results of [17, 14, 6] for curves whose non-ordinary Jacobian has 2-rank 1, letting C be a curve of genus 2 over $\mathbb{F}_q$ of the form $y^2 + xy = ax^5 + bx^3 + cx^2 + dx$, where $a \in \mathbb{F}_q^*$ and $b, c, d \in \mathbb{F}_q$. We consider when $N_{r,\ell} = \frac{2^{2^r \ell}+1}{2^{2^r}+1}$ is a prime[2] for some $r \geq 0$ and odd $\ell \geq 5$. These primes are of the form $\frac{A^\ell+1}{A+1}$ where ℓ is prime and A is a positive integer; if the behavior follows that of the primes $\frac{A^\ell-1}{A-1}$ and there is no algebraic factorization, then we would expect there to be infinitely many such primes, and that the number of such primes with $\ell \leq M$ is asymptotic to $\frac{\log \log M}{\log A}$ for fixed A [5]. Experimental evidence seems to confirm this for $r = 0, 2, 3$.

Our families of curves will be those whose Jacobian is such that its group of $\mathbb{F}_q$-rational points has order divisible by $N_{r,\ell}$, and whose (a_1, a_2) have a specific description to be explicitly given later.

3 Family of primes and the associated embedding degrees

We must first prove several lemmas that will enable us to achieve our main result. We begin by noting that $r = 1$ never yields a prime.

Lemma 3.1. *Let $\ell \geq 5$ be odd. $N_{1,\ell} = \frac{2^{2\ell}+1}{2^2+1}$ is not a prime.*

Proof. Let $P = \frac{2^\ell+1}{2+1} = N_{0,\ell}$. We see that $9P^2 = 2^{2\ell} + 2^{\ell+1} + 1$. So $N_{1,\ell} = \frac{9P^2 - 2^{\ell+1}}{2^2+1}$. Now ℓ is odd, so $\ell + 1$ is even. So $N_{1,\ell} = \frac{(3P - 2^{\frac{\ell+1}{2}})(3P + 2^{\frac{\ell+1}{2}})}{2^2+1}$, and for $\ell > 1$, each factor is greater than 1. Now $N_{1,\ell} \in \mathbb{Z}$ and $2^2 + 1$ is prime, so $(\frac{3P - 2^{\frac{\ell+1}{2}}}{2^2+1}) \in \mathbb{Z}$ or $(\frac{3P + 2^{\frac{\ell+1}{2}}}{2^2+1}) \in \mathbb{Z}$. Since $3P + 2^{\frac{\ell+1}{2}} = 2^\ell + 1 + 2^{\frac{\ell+1}{2}}$ equals 5 only if $\ell = 1$ and $3P - 2^{\frac{\ell+1}{2}} = 2^\ell + 1 - 2^{\frac{\ell+1}{2}}$ equals 5 only if $\ell = 3$, then this is a nontrivial factorization when $\ell \geq 5$. Thus, $N_{1,\ell}$ is not prime for $\ell \geq 5$. □

We now determine the embedding degree with respect to a general prime N, for a (sub)group of order N defined over $\mathbb{F}_q$. We let $\mathrm{ord}_N p$ be the smallest positive integer x such that $p^x \equiv 1 \bmod N$.

Lemma 3.2. *Let $q = p^m$ for some prime p and positive integer m, N be a prime not equal to p, and k be the smallest positive integer such that $q^k \equiv 1 \bmod N$. Then*

$$k = \frac{\mathrm{ord}_N p}{\gcd(\mathrm{ord}_N p, m)}.$$

[2] $N_{r,\ell} = 2^{2^r(\ell-1)} - 2^{2^r(\ell-2)} + 2^{2^r(\ell-3)} - 2^{2^r(\ell-4)} + \cdots - 2^{2^r} + 1$, so clearly $N_{r,\ell} \in \mathbb{Z}$ for $r \geq 0$ and odd $\ell \geq 5$.

Proof. Let $D = \gcd(\mathrm{ord}_N p, m)$. We observe that

$$1 \equiv p^{\mathrm{ord}_N p} \equiv (p^{\mathrm{ord}_N p})^{m/D} \equiv (p^m)^{\mathrm{ord}_N p/D} \bmod N,$$

so since $q = p^m$ and k is the smallest integer such that $q^k \equiv 1 \bmod N$, then we have $k \mid \frac{\mathrm{ord}_N p}{D}$.

We also know that $\mathrm{ord}_N p \mid mk$, and this implies $\frac{\mathrm{ord}_N p}{D} \mid \frac{m}{D}k$. But $\gcd(\frac{\mathrm{ord}_N p}{D}, \frac{m}{D}) = 1$, therefore it must be that $\frac{\mathrm{ord}_N p}{D} \mid k$. Thus we have $k = \frac{\mathrm{ord}_N p}{D}$ and the proof is complete. □

Motivated by this understanding of k, we determine $\mathrm{ord}_{N_{r,\ell}} 2$ via the following lemmas.

Lemma 3.3. *Suppose $r \geq 0$, $\ell \geq 5$, and ℓ is odd. If $N_{r,\ell} = \frac{2^{2^r \ell}+1}{2^{2^r}+1}$ is prime, then ℓ is prime.*

Proof. We first note that if $A = ab$ for positive integers a, b where b is odd, then $x^a + 1 \mid x^A + 1$ for any integer x, since

$$x^A + 1 = x^{ab} + 1 = (x^a + 1)(x^{a(b-1)} - x^{a(b-2)} + x^{a(b-3)} - \cdots + 1).$$

Now, if our odd ℓ is not prime, then $\ell = ab$ for odd $a, b > 1$. By the above argument, $2^{2^r} + 1 \mid 2^{2^r a} + 1$ and $2^{2^r a} + 1 \mid 2^{2^r \ell} + 1$, and thus $\frac{2^{2^r a}+1}{2^{2^r}+1} \mid \frac{2^{2^r \ell}+1}{2^{2^r}+1}$. But if $\frac{2^{2^r \ell}+1}{2^{2^r}+1}$ is prime, then it must be that $a = \ell$, and hence ℓ is prime. □

Lemma 3.4. *Suppose $r \geq 0$, $\ell \geq 5$, and ℓ is odd. If $N_{r,\ell} = \frac{2^{2^r \ell}+1}{2^{2^r}+1}$ is prime, then $\mathrm{ord}_{N_{r,\ell}} 2 = 2^{r+1}\ell$.*

Proof. We have $(2^{2^r} + 1)N_{r,\ell} = 2^{2^r \ell} + 1$. So $2^{2^r \ell} \equiv -1 \bmod N_{r,\ell}$. This implies $2^{2^{r+1}\ell} \equiv 1 \bmod N_{r,\ell}$. So $\mathrm{ord}_{N_{r,\ell}} 2 \mid 2^{r+1}\ell$. But by Lemma 3.3 we know that ℓ is prime, so it must be that either $\mathrm{ord}_{N_{r,\ell}} 2 = 2^j$ or $\mathrm{ord}_{N_{r,\ell}} 2 = 2^j \ell$ for some $0 \leq j \leq r+1$.

We know that $N_{r,\ell} > 2^{2^r(\ell-2)} \geq 2^{2^r 3} > 2^{2^{r+1}} - 1$ for $\ell \geq 5$, therefore, $\mathrm{ord}_{N_{r,\ell}} 2 \neq 2^j$ for $0 \leq j \leq r+1$.

Now suppose $\mathrm{ord}_{N_{r,\ell}} 2 = 2^j \ell$ for some $0 \leq j \leq r$. Then

$$\begin{aligned} 2^{2^j \ell} \equiv 1 \bmod N_{r,\ell} \quad &\Rightarrow \quad (2^{2^j \ell})^{2^{r-j}} \equiv 1 \bmod N_{r,\ell}, \\ &\Rightarrow \quad 2^{2^r \ell} \equiv 1 \bmod N_{r,\ell}. \end{aligned}$$

But we know that $2^{2^r \ell} \equiv -1 \bmod N_{r,\ell}$. Thus it must be that $j = r + 1$ and so $\mathrm{ord}_{N_{r,\ell}} 2 = 2^{r+1}\ell$. □

We are now able to state the embedding degree k with respect to $N_{r,\ell}$ of a (sub)group of order $N_{r,\ell}$ defined over $\mathbb{F}_q$, where $q = 2^m$ for a specific range of m. Here we study the traditional embedding degree k. In Section 6, we will consider a different indicator that takes into account the minimal embedding field.

Lemma 3.5. *Let $N_{r,\ell} = \frac{2^{2^r \ell}+1}{2^{2^r}+1}$ be prime for some $r \geq 0$ and odd $\ell \geq 5$, and let $1 \leq m \leq 2^r(\ell-1)-1$. Suppose there is a genus 2 curve C defined over $\mathbb{F}_q$, where $q = 2^m$, such that $N_{r,\ell}$ divides $\#J_C(\mathbb{F}_q)$. Let k be the embedding degree of C with respect to $N_{r,\ell}$. Then $k = 2^{r+1-i}$ when $\gcd(\mathrm{ord}_{N_{r,\ell}}2, m) = 2^i\ell$ for $i \in \{0,\ldots,r-1\}$, and $k = 2^{r+1-i}\ell$ when $\gcd(\mathrm{ord}_{N_{r,\ell}}2, m) = 2^i$ for $i \in \{0,\ldots,r+1\}$.*

Proof. By Lemma 3.4, we know that $\mathrm{ord}_{N_{r,\ell}}2 = 2^{r+1}\ell$. Suppose $\gcd(\mathrm{ord}_{N_{r,\ell}}2, m) = 2^i\ell$ for $0 \leq i \leq r-1$. (Note that $i \leq r-1$ since $\gcd(\mathrm{ord}_{N_{r,\ell}}2, m) = 2^i\ell \leq m \leq 2^r(\ell-1)-1$.) Then by Lemma 3.2,

$$k = \frac{\mathrm{ord}_{N_{r,\ell}}2}{\gcd(\mathrm{ord}_{N_{r,\ell}}2, m)} = \frac{2^{r+1}\ell}{2^i\ell} = 2^{r+1-i}.$$

Now suppose $\gcd(\mathrm{ord}_{N_{r,\ell}}2, m) = 2^i$ for $0 \leq i \leq r+1$. Then

$$k = \frac{\mathrm{ord}_{N_{r,\ell}}2}{\gcd(\mathrm{ord}_{N_{r,\ell}}2, m)} = \frac{2^{r+1}\ell}{2^i} = 2^{r+1-i}\ell.$$

(Note that since $\frac{2^{r+1}\ell}{2^i} \in \mathbb{Z}$ and ℓ is odd, then $i \leq r+1$.) □

We note that the embedding degree k is unbounded as ℓ is unbounded. We now seek to find curves over $\mathbb{F}_q$ associated with Jacobians whose group of $\mathbb{F}_q$-rational points has order divisible by $N_{r,\ell}$.

4 Genus 2 curves for a given $\mathbb{F}_q$-isogeny class of Jacobians

We know that the (a_1, a_2) determines the $\mathbb{F}_q$-isogeny class of the Jacobian of a curve of genus 2 [22]. The following theorem is a consequence of [17, 14, 6] and gives the conditions for a curve defined over a field of characteristic 2 associated with a Jacobian that has 2-rank 1 to exist. Cardona–Pujolas–Nart in [6] showed that such a 2-rank 1 curve will be of the form given in Theorem 4.1. (Our statement combines Lemma 2.1, Theorem 2.9 part (M) and Corollary 2.17 of [17], as it appears in [18].)

Theorem 4.1. *Let $q = 2^m$ for a positive integer m. There exists a curve of the form $y^2 + xy = ax^5 + bx^3 + cx^2 + dx$, $a \in \mathbb{F}_q^*$, $b, c, d \in \mathbb{F}_q$, whose Jacobian has characteristic polynomial $f(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2$ if the following conditions hold:*

1. *a_1 is odd,*
2. *$|a_1| \leq 4\sqrt{q}$,*
3. *(a) $2|a_1|\sqrt{q} - 2q \leq a_2 \leq a_1^2/4 + 2q$,*
   (b) a_2 is divisible by $2^{\lceil m/2 \rceil}$,
   (c) $\Delta = a_1^2 - 4a_2 + 8q$ is not a square in $\mathbb{Z}$,
   (d) $\delta = (a_2 + 2q)^2 - 4qa_1^2$ is not a square in $\mathbb{Z}_2$ (the 2-adic integers).

The authors of [17] show that the conditions on a_1 and a_2 in Theorem 4.1 guarantee that the Jacobian of the given curve has 2-rank 1, in other words is neither ordinary nor supersingular. A converse is also proven in [17], but we will not need it for our result. We use Theorem 4.1 to establish the existence of genus 2 curves with specific conditions on (a_1, a_2). We then show these are the conditions needed so that the order of $J_C(\mathbb{F}_q)$ is divisible by $N_{r,\ell}$.

We first give a lemma that will be used in the proof of the next proposition.

Lemma 4.2. *Let a, b, c be integers, with $a, b > 0$.*

i) If $2^a(2^b-1) = c(c+1)$ then $a \le b$.

ii) If $2^a(2^b+1) = c(c+1)$ then $a \le b$ or $(a,b) = (2,1)$.

Proof. Without loss of generality, we may choose the sign of c and $c+1$ so that c is even. Then $c+1$ is odd. We consider case $i)$ first. Since c is even, then $2^a \mid c$, $c = 2^a x$ for some odd integer x, and $x(c+1) = 2^b - 1$. Then $2^b = x(2^a x+1)+1$. If $x > 0$, then $2^b \ge 2^a + 2$ and so $b > a$. If $x < 0$, then $2^b = |x|(2^a|x|-1)+1 \ge 2^a$ and so $b \ge a$.

Now we consider case $ii)$. Since c is even, then $2^a \mid c$, $c = 2^a x$ for some odd integer x, and $x(c+1) = 2^b + 1$. Then $2^b = x(2^a x+1)-1$. If $x > 0$, then $2^b \ge 2^a$ and so $b \ge a$. If $x < 0$, then $2^b = |x|(2^a|x|-1)-1 \ge 2^a - 2$. Thus $b \ge a$ unless $(a,b) = (2,1)$. □

Proposition 4.3. *Let $q = 2^m$, $r \ge 0$ and $\ell \ge 11$ be prime. When $m = \frac{\ell+1}{2}$, let $a_1 = 1$ and $a_2 = -2^m$, and when $\lceil \frac{2^{r+1}\ell}{3} \rceil \le m \le 2^r(\ell-1)-1$, let $a_1 = -1$ and $a_2 = 2^m + 2^{2m-2^r\ell}$. These a_1 and a_2 satisfy the conditions for the existence of the curves of genus 2 in Theorem 4.1.*

Proof. We first note that since $\ell \ge 9$, then $m \ge 6$ and $q \ge 64$. Now, clearly a_1 is odd and $|a_1| \le 4\sqrt{q}$ in both cases of the proposition.

Let us show $2|a_1|\sqrt{q} - 2q \le a_2 \le a_1^2/4 + 2q$. The first case (when $a_1 = 1$ and $a_2 = -q$ for $m = \frac{\ell+1}{2}$), gives $2\sqrt{q} - 2q \le -q \le 1/4 + 2q$, which is true for $q \ge 64$. Now consider the second case (when $a_1 = -1$, and $a_2 = 2^m + 2^{2m-2^r\ell}$):

$$2\sqrt{q} - 2q \le a_2 \le 1/4 + 2q$$

$$\iff 2^{m/2+1} - 2^{m+1} \le 2^m + 2^{2m-2^r\ell} \le 1/4 + 2^{m+1}.$$

Clearly the first inequality holds. The second inequality holds if $2^{2m-2^r\ell} \le 2^m$, which holds if $m \le 2^r\ell$. This is true since $m \le 2^r(\ell-1)-1$.

Let us show $2^{\lceil m/2 \rceil} \mid a_2$. Clearly the first case is true: $2^{\lceil m/2 \rceil} \mid -2^m$. Now consider the second case:

$$\begin{aligned} 2^{\lceil m/2 \rceil} \mid 2^m + 2^{2m-2^r\ell} &\iff 2m - 2^r\ell \ge \lceil m/2 \rceil \\ &\iff \lfloor 3m/2 \rfloor \ge 2^r\ell \\ &\iff m \ge \lceil 2^{r+1}\ell/3 \rceil \end{aligned}$$

Thus the condition holds.

Now we show $\Delta = a_1^2 - 4a_2 + 8q$ is not a square in $\mathbb{Z}$. The first case yields $\Delta = 1 + 3 \cdot 2^{m+2}$. Suppose $\Delta = 1 + 3 \cdot 2^{m+2} = x^2$ for some integer x. Since $1 + 3 \cdot 2^{m+2}$ is odd, then x is odd, so let $x = 2c + 1$ for some integer c. Then Δ is a square if and only if $3 \cdot 2^m = 2^m(2^2 - 1) = c(c+1)$. We apply Lemma 4.2, letting $a = m$ and $b = 2$. Then Δ is a square implies $m \leq 2$. Thus Δ is not a square in $\mathbb{Z}$ for $m = \frac{\ell+1}{2}$, since $m \geq 6$ for $\ell \geq 9$.

The second case yields $\Delta = 2^{2m-2^r\ell+2}(2^{2^r\ell-m} - 1) + 1$. For contradiction, suppose $\Delta = x^2$ for some integer x. We claim that $2m - 2^r\ell + 2 > 0$, and thus Δ is odd. To see this is true, we note that since ℓ is prime, $m \geq \lceil \frac{2^{r+1}\ell}{3} \rceil$ implies $2m - 2^r\ell \geq 2^r\ell - m + 1$. Also $m \leq 2^r(\ell - 1) - 1$ implies $2^r\ell - m \geq 2^r + 1$, thus putting the two together, we see our claim is true. Now since Δ is odd, then x is odd, so let $x = 2c + 1$ for some integer c. Then Δ is a square if and only if $2^{2m-2^r\ell}(2^{2^r\ell-m} - 1) = c(c+1)$. We apply Lemma 4.2, letting $a = 2m - 2^r\ell$ and $b = 2^r\ell - m$. We note that $a > 0$ and $b > 0$ by the same argument as above. By the lemma, if Δ is a square then $2m - 2^r\ell \leq 2^r\ell - m$, that is, $m \leq \lfloor \frac{2^{r+1}\ell}{3} \rfloor$. But we require that $m \geq \lceil \frac{2^{r+1}\ell}{3} \rceil$, and since $\ell \geq 9$ is prime, then $\lfloor \frac{2^{r+1}\ell}{3} \rfloor \neq \lceil \frac{2^{r+1}\ell}{3} \rceil$, so this cannot happen. Therefore Δ is not a square.

Now we show $\delta = (a_2 + 2q)^2 - 4qa_1^2$ is not a square in the 2-adic integers, $\mathbb{Z}_2$. That is, for $\delta = 2^t b$, it is sufficient to prove that $b \not\equiv 1 \bmod 8$ or $t \equiv 1 \bmod 2$.
The first case yields $\delta = q^2 - 4q = 2^{m+2}(2^{m-2} - 1)$. So $b = 2^{m-2} - 1 \equiv -1 \bmod 8$ for $m \geq 5$. Therefore δ is not a square in $\mathbb{Z}_2$ for $m = \frac{\ell+1}{2}$, since $m \geq 6$ when $\ell \geq 9$.
Now consider the second case:

$$\begin{aligned}
\delta &= (2^m + 2^{2m-2^r\ell} + 2^{m+1})^2 - 2^{m+2} \\
&= (2^m + 2^{2m-2^r\ell})^2 + 2^{m+2}(2^m + 2^{2m-2^r\ell}) + 2^{2m+2} - 2^{m+2} \\
&= 2^{2m+3} + 2^{2m} + 2^{3m-2^r\ell+2} + 2^{3m-2^r\ell+1} + 2^{4m-2^{r+1}\ell} - 2^{m+2} \\
&= 2^{m+2}(2^{m+1} + 2^{m-2} + 2^{2m-2^r\ell} + 2^{2m-2^r\ell-1} + 2^{3m-2^{r+1}\ell-2} - 1).
\end{aligned}$$

We will consider two cases. First, let us suppose $3m - 2^{r+1}\ell - 2 > 0$, and hence all these powers of 2 are positive. Then

$$b = 2^{m-2}(2^3 + 1) + 2^{2m-2^r\ell-1}(2 + 1) + 2^{3m-2^{r+1}\ell-2} - 1.$$

For $m \geq 5$, we have

$$\begin{aligned}
b &\equiv 2^{2m-2^r\ell-1}(3) + 2^{3m-2^{r+1}\ell-2} - 1 \bmod 8 \\
&\equiv 2^{3m-2^{r+1}\ell-2}(2^{2^r\ell-m+1}3 + 1) - 1 \bmod 8.
\end{aligned}$$

Now, suppose $b \equiv 1 \bmod 8$. Then

$$b + 1 \equiv 2^{3m-2^{r+1}\ell-2}(2^{2^r\ell-m+1}3 + 1) \equiv 2 \bmod 8.$$

For this to be true, we must have $3m - 2^{r+1}\ell - 2 \leq 1$. If $3m - 2^{r+1}\ell - 2 = 1$, then $m = \frac{3+2^{r+1}\ell}{3}$. But ℓ is prime and $\ell \neq 3$, so $m \notin \mathbb{Z}$, and this cannot happen as we require an integer m. We are already under the assumption that $3m - 2^{r+1}\ell - 2 \neq 0$, thus by contradiction we see that $b \not\equiv 1 \bmod 8$. Therefore, for $3m - 2^{r+1}\ell - 2 > 0$, δ is not a square in $\mathbb{Z}_2$.

Now suppose that $3m - 2^{r+1}\ell - 2 = 0$ (it cannot be negative, due to our bounds on m). Then

$$\begin{aligned}\delta &= 2^{2m+3} + 2^{2m} + 2^{3m-2^r\ell+2} + 2^{3m-2^r\ell+1}\\ &= 2^{2m+3} + 2^{2m} + 2^{2^r\ell+3}(2+1)\\ &= 2^{2^r\ell+3}(2^{2m-2^r\ell} + 2^{2m-2^r\ell-3} + 3).\end{aligned}$$

The hypotheses that $3m - 2^{r+1}\ell - 2 = 0$ and $\ell \geq 11$ imply $2m - 2^r\ell - 3 > 0$, so $2^{2^r\ell+3}$ is the largest even factor of δ. If $r > 0$, then $2^r\ell + 3 \equiv 1 \bmod 2$, so δ is not a square in $\mathbb{Z}_2$. If $r = 0$, then consider $b = 2^{2m-2^r\ell} + 2^{2m-2^r\ell-3} + 3$. For $\ell \geq 11$, we have $2m - 2^r\ell - 3 = 2^r\ell - 5/3 \geq 9$, which implies that $b \not\equiv 1 \bmod 8$. Thus δ is not a square in $\mathbb{Z}_2$.

Therefore all the conditions for the existence of genus 2 curves C over $\mathbb{F}_q$ are satisfied for the given (a_1, a_2) described in the proposition. □

We are now able to state our main result in the following theorem.

Theorem 4.4. *Let $N_{r,\ell} = \frac{2^{2^r\ell}+1}{2^{2^r}+1}$ be a prime for some $r \geq 0$ and prime $\ell \geq 11$. If $r = 0$, then for $m = \frac{\ell+1}{2}$ there exists a curve C of genus 2 over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2 \cdot 3 \cdot N_{0,\ell}$, and $a_1 = 1, a_2 = -2^m$. If $r \geq 0$, then for each integer m in the interval $\lceil \frac{2^{r+1}\ell}{3} \rceil \leq m \leq 2^r(\ell - 1) - 1$, there exists a curve C of genus 2 over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2^x(2^{2^r} + 1)N_{r,\ell}$, where $x = 2m - 2^r\ell$, and $a_1 = -1, a_2 = 2^m + 2^x$.*

Proof. Let $N_{r,\ell} = \frac{2^{2^r\ell}+1}{2^{2^r}+1}$ be a prime for some $r \geq 0$ and prime $\ell \geq 11$.

We know by Proposition 4.3 that the (a_1, a_2) stated in the theorem, with m in the specified range, satisfy the conditions for the existence of a curve C of genus 2 over $\mathbb{F}_{2^m}$.

First we consider when $r = 0$ and $m = \frac{\ell+1}{2}$. For $a_1 = 1$ and $a_2 = -2^m$, we have

$$\begin{aligned}\#J_C(\mathbb{F}_{2^m}) &= 2^{2m} + 2^m - 2^m + 2\\ &= 2^{\ell+1} + 2\\ &= 2(2^\ell + 1)\\ &= 2 \cdot 3 \cdot N_{0,\ell} \text{ since } N_{0,\ell} = \frac{2^\ell + 1}{2+1}.\end{aligned}$$

Now we consider when $r \geq 0$ is an integer not equal to 1, and $\lceil \frac{2^{r+1}\ell}{3} \rceil \leq m \leq$

$2^r(\ell-1)-1$. For $a_1=-1$ and $a_2=2^m+2^x$, where $x=2m-2^r\ell$, we have

$$\begin{aligned}\#J_C(\mathbb{F}_{2^m}) &= 2^{2m}-2^m+2^m+2^x\\ &= 2^{2m}+2^x\\ &= 2^x(2^{2^r\ell}+1)\\ &= 2^x(2^{2^r}+1)N_{r,\ell} \text{ since } N_{r,\ell}=\frac{2^{2^r\ell}+1}{2^{2^r}+1}.\end{aligned}$$

Thus the theorem is complete. □

Now let $\#J_C(\mathbb{F}_q)=hN_{r,\ell}$. For the most efficient implementation of a pairing-based cryptosystem, we would like the cofactor h to be small, that is, for the ratio $\rho=\frac{2\log_2 q}{\log_2 N_{r,\ell}}$ to be approximately 1. For our family of curves, we see that $\rho\sim\frac{m}{2^{r-1}(\ell-1)}$, which is between 1 and 2. In particular, when $m=\frac{\ell+1}{2}$, we get $\rho\sim\frac{\ell+1}{\ell-1}$. When $\lceil\frac{2^{r+1}\ell}{3}\rceil\leq m\leq 2^r(\ell-1)-1$, the ratio can be as small as $\rho\sim\frac{4\ell}{3(\ell-1)}$ and at most $\rho\sim 2-\frac{2}{2^r(\ell-1)}$.

In [15], an algorithm for point compression is proposed when the order of an elliptic curve over $\mathbb{F}_{2^m}$ is divisible by a power of 2. In our case, since $\#J_C(\mathbb{F}_{2^m})$ is divisible by a high power of 2, these curves may lend themselves to point compression using methods similar to those in [15].

Table 1 gives some examples of the parameters for curves over $\mathbb{F}_q$ yielding small embedding degrees $k=8,13,16,23,26$. Our parameter space was $11\leq\ell\leq 500$ and $0\leq r\leq 5$, and we have displayed only a small selection of the output.

An efficient method of determining the explicit coefficients of a curve when given the (a_1,a_2) parameters that distinguish the $\mathbb{F}_q$-isogeny class of its Jacobian is not yet established. As such, in Example 4.5 we have used brute force with MAGMA [4] code to generate some examples of these curves over small $\mathbb{F}_q$.

Example 4.5. We give examples of curves over small $\mathbb{F}_q$ for $r=0$, along with the approximation of ρ. We let g be a generator of $\mathbb{F}_q^*$.

$\ell=11,\ m=\frac{\ell+1}{2}=6,\ k=11,\ \rho=1.27,$
$C: y^2+xy=x^5+g^8x^3+g^3x^2+gx,$

$\ell=11,\ m=\lceil\frac{2^{r+1}\ell}{3}\rceil=8,\ k=11,\ \rho=1.70,$
$C: y^2+xy=x^5+g^7x^3+g^7x,$

$\ell=11,\ m=2^r(\ell-1)-1=9,\ k=22,\ \rho=1.91,$
$C: y^2+xy=x^5+g^8x^3+g^3x,$

$\ell=13,\ m=\frac{\ell+1}{2}=7,\ k=26,\ \rho=1.23,$
$C: y^2+xy=x^5+g^{92}x^3+g^7x^2+gx,$

$\ell=17,\ m=\frac{\ell+1}{2}=9,\ k=34,\ \rho=1.17,$
$C: y^2+xy=x^5+g^{103}x^3+g^5x^2+gx.$

k	ℓ	r	m	a_1	a_2	ρ
8	37	2	111	-1	$2^{111} + 2^{74}$	1.54
8	89	2	267	-1	$2^{267} + 2^{178}$	1.52
8	149	2	447	-1	$2^{447} + 2^{298}$	1.51
8	173	2	519	-1	$2^{519} + 2^{346}$	1.51
8	239	4	2868	-1	$2^{2868} + 2^{1912}$	1.51
8	251	2	753	-1	$2^{753} + 2^{502}$	1.51
8	307	2	921	-1	$2^{921} + 2^{614}$	1.51
8	317	2	951	-1	$2^{951} + 2^{634}$	1.50
13	13	3	80	-1	$2^{80} + 2^{56}$	1.67
16	13	3	91	-1	$2^{91} + 2^{78}$	1.90
16	239	4	3346	-1	$2^{3346} + 2^{2868}$	1.76
23	23	2	64	-1	$2^{64} + 2^{36}$	1.46
23	23	2	72	-1	$2^{72} + 2^{52}$	1.64
23	23	2	80	-1	$2^{80} + 2^{68}$	1.82
26	13	3	72	-1	$2^{72} + 2^{40}$	1.50
26	13	3	88	-1	$2^{88} + 2^{72}$	1.83
32	239	4	2629	-1	$2^{2629} + 2^{1434}$	1.38
32	239	4	3107	-1	$2^{3107} + 2^{2390}$	1.63
32	239	4	3585	-1	$2^{3585} + 2^{3346}$	1.88
37	37	2	104	-1	$2^{104} + 2^{60}$	1.45
37	37	2	112	-1	$2^{112} + 2^{76}$	1.56
37	37	2	120	-1	$2^{120} + 2^{92}$	1.67
37	37	2	128	-1	$2^{128} + 2^{108}$	1.78
37	37	2	136	-1	$2^{136} + 2^{124}$	1.89
46	23	2	68	-1	$2^{68} + 2^{44}$	1.55
46	23	2	76	-1	$2^{76} + 2^{60}$	1.73
46	23	2	84	-1	$2^{84} + 2^{76}$	1.91
52	13	3	76	-1	$2^{76} + 2^{48}$	1.58
52	13	3	84	-1	$2^{84} + 2^{64}$	1.75
52	13	3	92	-1	$2^{92} + 2^{80}$	1.92
167	167	0	84	1	-2^{84}	1.02
191	191	0	96	1	-2^{96}	1.01
199	199	0	100	1	-2^{100}	1.01

Table 1. Examples of parameters for families of genus 2 curves over $\mathbb{F}_{2^m}$ with small embedding degree k and their approximate ρ values.

5 Size of the embedding degrees

We examine the size of the embedding degrees of the family of curves from Theorem 4.4. We find that for cryptographic sizes, these curves always yield embedding degrees such that $k < (\log\ q)^2$, which suggests that the embedding degree may be small enough so that computations are feasible. (See [1] and [11, Section 5.2.1] for discussion of the probability of k in this range.)

Proposition 5.1. *Let $\ell \geq 11$ be odd, $r \geq 0$ and $N_{r,\ell} = \frac{2^{2^r\ell}+1}{2^{2^r}+1}$ be prime. For each integer m in the interval $\lceil \frac{2^{r+1}\ell}{3} \rceil \leq m \leq 2^r(\ell-1)-1$, let C be a genus 2 curve defined over $\mathbb{F}_q$, where $q = 2^m$, such that $N_{r,\ell}$ divides $\#J_C(\mathbb{F}_q)$. Then the embedding degree k of C with respect to $N_{r,\ell}$ is such that $k < (\log\ q)^2$. If $\ell \geq 15$ and $r = 0$, then also for $m = \frac{\ell+1}{2}$, the embedding degree of C with respect to $N_{r,\ell}$ is such that $k < (\log\ q)^2$.*

Proof. Let $\lceil \frac{2^{r+1}\ell}{3} \rceil \leq m \leq 2^r(\ell-1)-1$. By Lemma 3.5, the largest that k can be is $k = 2^{r+1}\ell$, so it suffices to consider this case. Given the acceptable range for m, it is enough to show $k < (\log\ q)^2$ for $m = \lceil \frac{2^{r+1}\ell}{3} \rceil$. Now $k < (\log\ q)^2$ if

$$\begin{aligned} 2^{r+1}\ell < (\log\ 2^{\frac{2^{r+1}\ell}{3}})^2 &\iff 2^{r+1}\ell < \left(\frac{2^{r+1}\ell}{3}\right)^2 (\log^2 2) \\ &\iff 9 \cdot 2^{r+1}\ell < 2^{2r+2}(\log^2 2)\ell^2 \\ &\iff \frac{9}{2^{r+1}(\log^2 2)} < \ell. \end{aligned}$$

This holds if $\ell \geq 10$ for $r = 0$. Since we require ℓ to be odd, we can say that $\ell \geq 11$ for any $r \geq 0$ gives the result.
Now let $m = \frac{\ell+1}{2}$ and $r = 0$. By Lemma 3.5, it suffices to consider $k = 2\ell$. So $k < (\log\ q)^2$ if

$$\begin{aligned} 2\ell < (\log\ 2^{(\ell+1)/2})^2 &\iff 2\ell < \left(\frac{\ell+1}{2}\right)^2 (\log^2 2) \\ &\iff 2(\ell+1) - 2 < \frac{\log^2 2}{4}(\ell+1)^2 \\ &\iff 0 < \frac{\log^2 2}{4}(\ell+1)^2 - 2(\ell+1) + 2. \end{aligned}$$

This holds if $\ell + 1 > \frac{2+\sqrt{4-2(\log^2 2)}}{\frac{\log^2 2}{2}}$, that is, if $\ell \geq 15$. □

6 Minimal embedding field

In [12], we constructed examples to show that the embedding degree k is not always the appropriate indicator of cryptographic security, as the actual minimal embedding field (where solving the DLP would take place) can be much smaller than suggested by k. In particular, if $q = p^m$, then the pairings embed into μ_N which lies in $(\mathbb{F}_{p^{\mathrm{ord}_N p}})^*$, not merely in $\mathbb{F}_{q^k}^*$. The ratio of the extension degrees $[\mathbb{F}_{q^k} : \mathbb{F}_p]$ and $\mathrm{ord}_N p$ can be as large as m.

To illustrate the discrepancy, we now give a family of curves with a difference of a factor of m between the extension degrees of the minimal embedding field and the field indicated by the embedding degree k. This family of curves is such that $\#J_C(\mathbb{F}_q)$ is divisible by a Mersenne prime N.

Theorem 6.1. *Let $\ell \geq 7$ be a prime. If $N = 2^\ell - 1$ is prime, then for each integer m such that $\lceil \frac{2\ell}{3} \rceil \leq m \leq \ell - 1$, there exists a genus 2 curve C over $\mathbb{F}_q$, where $q = 2^m$, with the property that $\#J_C(\mathbb{F}_{2^m}) = 2^{2m-\ell}N$, where $a_1 = -1$ and $a_2 = 2^m - 2^{2m-\ell}$. The embedding degree of C with respect to N is ℓ, and the minimal embedding field is $\mathbb{F}_{2^\ell}$. Thus the ratio of the extension degrees $[\mathbb{F}_{q^k} : \mathbb{F}_2]$ and $[\mathbb{F}_{2^\ell} : \mathbb{F}_2]$ is m.*

Proof. First let us show that the conditions of Theorem 4.1 are met for the existence of genus 2 curves C when $a_1 = -1$ and $a_2 = 2^m - 2^{2m-\ell}$. We note that since $\ell \geq 7$, then $m \geq 5$. Clearly a_1 is odd, and $|a_1| \leq 4\sqrt{q}$. Let us show $2\sqrt{q} - 2q \leq a_2 \leq 1/4 + 2q$, that is,

$$2^{m/2+1} - 2^{m+1} \leq 2^m - 2^{2m-\ell} \leq 1/4 + 2^{m+1}.$$

Clearly the second inequality holds. The first inequality holds if

$$2^{m/2+1} + 2^{2m-\ell} = 2^m(2^{1-m/2} + 2^{m-\ell}) \leq 2^m 3.$$

This holds if $m - \ell \leq 1$. But our restriction that $\lceil \frac{2\ell}{3} \rceil \leq m \leq \ell - 1$ implies $m - \ell \leq -1$, so we see this condition holds.

Now let us show that $2^{\lceil m/2 \rceil}$ divides a_2.

$$\begin{aligned} 2^{\lceil m/2 \rceil} \mid 2^m - 2^{2m-\ell} &\iff 2m - \ell \geq \lceil m/2 \rceil \\ &\iff \lfloor 3m/2 \rfloor \geq \ell \\ &\iff m \geq \lceil 2\ell/3 \rceil. \end{aligned}$$

Thus the condition holds.

Now let us show $\Delta = a_1^2 - 4a_2 + 8q$ is not a square in $\mathbb{Z}$.
For contradiction, suppose $\Delta = 1 - 2^{m+2} + 2^{2m-\ell+2} + 2^{m+3} = 1 + 2^{2m-\ell+2} + 2^{m+2} = x^2$ for some integer x. We claim that $2m - \ell + 2 > 0$, and thus Δ is odd. To see this, we note that $\lceil \frac{2\ell}{3} \rceil \leq m$ implies $2m - \ell \geq \ell - m + 1$. Also, $m \leq \ell - 1$ implies $\ell - m \geq 1$, thus putting the two together, we see our claim is true. Now since Δ is odd, then x is odd, so let $x = 2c + 1$ for some integer c. Then Δ is a square if and only if $2^{2m-\ell}(2^{\ell-m} + 1) = c(c+1)$. We apply Lemma 4.2, letting $a = 2m - \ell$ and $b = \ell - m$. Clearly $a > 0$ and $b > 0$ by the above argument. The lemma implies $2m - \ell \leq \ell - m$, or $2m - \ell = 2$ and $\ell - m = 1$. If the latter case, then $2m - (1 + m) - 2 = 0$, which implies $m = 3$. But we know that $m \geq 5$, so this cannot happen. If the former case, then $2m - \ell \leq \ell - m$ implies $m \leq \lfloor 2\ell/3 \rfloor$. But we require that $m \geq \lceil 2\ell/3 \rceil$, and since $\ell \geq 7$ is prime, then $\lfloor 2\ell/3 \rfloor \neq \lceil 2\ell/3 \rceil$, so this cannot happen. Therefore Δ is not a square in $\mathbb{Z}$.

Now let us show $\delta = (a_2+2q)^2 - 4qa_1^2$ is not a square in $\mathbb{Z}_2$. That is, for $\delta = 2^t b$, it is sufficient to prove that $b \not\equiv 1 \bmod 8$ or $t \equiv 1 \bmod 2$. Now

$$\begin{aligned}\delta &= (2^m - 2^{2m-\ell} + 2^{m+1})^2 - 2^{m+2}\\ &= (2^m - 2^{2m-\ell})^2 + 2^{m+2}(2^m - 2^{2m-\ell}) + 2^{2m+2} - 2^{m+2}\\ &= 2^{2m+3} + 2^{2m} - 2^{3m-\ell+2} - 2^{3m-\ell+1} + 2^{4m-2\ell} - 2^{m+2}\\ &= 2^{m+2}(2^{m+1} + 2^{m-2} - 2^{2m-\ell} - 2^{2m-\ell-1} + 2^{3m-2\ell-2} - 1).\end{aligned}$$

We will consider two cases. First, let us suppose $3m - 2\ell - 2 > 0$, and hence all these powers of 2 are positive. Then

$$b = 2^{m-2}(2^3+1) - 2^{2m-\ell-1}(2+1) + 2^{3m-2\ell-2} - 1.$$

For $m \geq 5$, we have

$$b \equiv -2^{2m-\ell-1}3 + 2^{3m-2\ell-2} - 1 \equiv 2^{3m-2\ell-2}(1 - 2^{\ell-m+1}3) - 1 \bmod 8.$$

Now, suppose $b \equiv 1 \bmod 8$. Then

$$b + 1 \equiv 2^{3m-2\ell-2}(1 - 2^{\ell-m+1}3) \equiv 2 \bmod 8.$$

For this to be true, we must have $3m - 2\ell - 2 \leq 1$. If $3m - 2\ell - 2 = 1$, then $m = \frac{3+2\ell}{3}$. But ℓ is a prime not equal to 3, so $m \notin \mathbb{Z}$, and this cannot happen as we require an integer m. We are already under the assumption that $3m - 2\ell - 2 \neq 0$, thus by contradiction we see that $b \not\equiv 1 \bmod 8$. Therefore, for $3m - 2\ell - 2 > 0$, δ is not a square in $\mathbb{Z}_2$.

Now suppose that $3m - 2\ell - 2 = 0$ (it cannot be negative, due to our bounds on m). Then

$$\begin{aligned}\delta &= 2^{2m+3} + 2^{2m} - 2^{3m-\ell+2} - 2^{3m-\ell+1}\\ &= 2^{2m+3} + 2^{2m} - 2^{3m-\ell+1}(2+1)\\ &= 2^{\ell+3}(2^{2m-\ell} + 2^{2m-\ell-3} - 3).\end{aligned}$$

The hypotheses that $3m - 2\ell - 2 = 0$ and $\ell \geq 7$ imply that $2m - \ell - 3 > 0$, so $2^{\ell+3}$ is the largest even factor of δ. Since $\ell + 3 \equiv 0 \bmod 2$, we must show that $2^{2m-\ell} + 2^{2m-\ell-3} - 3 \not\equiv 1 \bmod 8$. The case that $\ell = 7$ cannot occur because this implies $m = 16/3 \notin \mathbb{Z}$. When $\ell = 11$, N is not prime, so we do not consider this case. For $\ell \geq 13$, we have $2m - \ell - 3 > 2$, which implies $2^{2m-\ell} + 2^{2m-\ell-3} - 3 \equiv 5 \bmod 8$. Thus δ is not a square in $\mathbb{Z}_2$.

Therefore the conditions of Theorem 4.1 are satisfied for the existence of a curve C over $\mathbb{F}_q$.

Now let us show that $\#J_C(\mathbb{F}_{2^m}) = 2^{2m-\ell}N$ whenever $a_1 = -1$ and $a_2 = 2^m - 2^{2m-\ell}$. Recall that $\#J_C(\mathbb{F}_q) = q^2 + a_1 q + a_2 + a_1 + 1$. So

$$\begin{aligned}\#J_C(\mathbb{F}_{2^m}) &= 2^{2m} - 2^{2m-\ell}\\ &= 2^{2m-\ell}(2^\ell - 1)\\ &= 2^{2m-\ell}N.\end{aligned}$$

Now we find the embedding degree k with respect to $N = 2^{\ell} - 1$. We see that $\mathrm{ord}_N 2 = \ell$, so $\gcd(\mathrm{ord}_N 2, m) = 1$ since $m \leq \ell - 1$. Therefore the embedding degree is $k = \ell$ by Lemma 3.2, and the minimal embedding field is $\mathbb{F}_{2^{\ell}}$. Thus the ratio of the extension degrees $[\mathbb{F}_{q^k} : \mathbb{F}_2]$ and $[\mathbb{F}_{2^{\ell}} : \mathbb{F}_2]$ is m. □

k	ℓ	r	m	a_1	a_2	$\log_2 N_{r,\ell}$	$k \log_2 q$	$k' \log_2 q$
8	37	2	111	-1	$2^{111} + 2^{74}$	143	888	296
8	89	2	267	-1	$2^{267} + 2^{178}$	351	2136	712
8	149	2	447	-1	$2^{447} + 2^{298}$	591	3576	1192
8	173	2	519	-1	$2^{519} + 2^{346}$	687	4152	1384
8	239	4	2868	-1	$2^{2868} + 2^{1912}$	3807	22944	7648
8	251	2	753	-1	$2^{753} + 2^{502}$	999	6024	2008
8	307	2	921	-1	$2^{921} + 2^{614}$	1223	7368	2456
8	317	2	951	-1	$2^{951} + 2^{634}$	1263	7608	2536
13	13	3	80	-1	$2^{80} + 2^{56}$	95	1040	208
16	239	4	3346	-1	$2^{3346} + 2^{2868}$	3807	53536	7648
23	23	2	80	-1	$2^{80} + 2^{68}$	87	1840	184
26	13	3	88	-1	$2^{88} + 2^{72}$	95	2288	208
32	239	4	2629	-1	$2^{2629} + 2^{1434}$	3807	84128	7648
32	239	4	3107	-1	$2^{3107} + 2^{2390}$	3807	99424	7648
32	239	4	3585	-1	$2^{3585} + 2^{3346}$	3807	114720	7648
37	37	2	112	-1	$2^{112} + 2^{76}$	143	4144	296
37	37	2	120	-1	$2^{120} + 2^{92}$	143	4440	296
37	37	2	128	-1	$2^{128} + 2^{108}$	143	4736	296
37	37	2	136	-1	$2^{136} + 2^{124}$	143	5032	296
46	23	2	84	-1	$2^{84} + 2^{76}$	87	3864	184
52	13	3	92	-1	$2^{92} + 2^{80}$	95	4784	208
149	149	2	400	-1	$2^{400} + 2^{204}$	591	59600	1192
149	149	2	584	-1	$2^{584} + 2^{572}$	591	87016	1192
173	173	2	464	-1	$2^{464} + 2^{236}$	687	80272	1384
173	173	2	680	-1	$2^{680} + 2^{668}$	687	117640	1384

Table 2. Examples of families of genus 2 curves over $\mathbb{F}_{2^m}$ with appropriate parameters for comparison of security.

In light of [12], we revisit the family of curves presented in Section 4, and now we not only consider the embedding degree k, but also the minimal embedding field, indicated by $k' = \frac{\mathrm{ord}_{N_{r,\ell}} 2}{m}$. Table 2 gives the examples of our curves with the sizes (in bits) of the fields $\mathbb{F}_{q^k}$, $\mathbb{F}_{q^{k'}}$ and the prime-order subgroup, thus providing a more accurate security comparison between the DLP on the Jacobian of the curve and in the multiplicative group of the finite field. Our parameter space was $11 \leq \ell \leq 500$, $0 \leq r \leq 5$, though we have only displayed a small selection of the output. We emphasize that for each ℓ, r there exists a curve over $\mathbb{F}_{2^m}$ for each m in the interval $\lceil \frac{2^{r+1}\ell}{3} \rceil \leq m \leq 2^r(\ell - 1) - 1$, with the same security parameters $\log_2 N$ and $k' \log_2 q$.

We recall that the difficulty of solving the DLP in a subgroup of prime 160-bit order of the Jacobian of a hyperelliptic curve is roughly equivalent to solving the DLP in the multiplicative group of a finite field of around 1024-bits. This means that one needs $q^{k'} > 2^{1024}$. We present the numerical data in Table 2, recognizing that for some of these examples, the DLP on the Jacobian of the curve is easy, so the difficulty of the DLP in the multiplicative group of the finite field is irrelevant. However, for $\ell \geq 149$, one expects the DLP to be suitably hard in both places.

7 Concluding remarks

Hyperelliptic curves are receiving increased attention for use in cryptosystems, which motivates the search for pairing-friendly curves. We have produced a sequence of $\mathbb{F}_q$-isogeny classes for a family of Jacobians of genus 2, 2-rank 1 curves over $\mathbb{F}_q$, for $q = 2^m$, and the corresponding small embedding degrees. In particular, we gave examples of the parameters for such curves with embedding degree $k < (\log q)^2$, such as $k = 8, 13, 16, 23, 26, 32, 37, 46, 52$, so that the computations in $\mathbb{F}_{q^k}$ may be feasible. Our family of curves also yields the ratio ρ between 1 and 2.

We have also given another family of curves over $\mathbb{F}_q$, whose minimal embedding field is much smaller than the one indicated by the embedding degree k. That is, the field exponents differ by a factor of m, which demonstrates that the embedding degree may be an inaccurate indicator of security. As a result, we used an indicator $k' = \frac{\mathrm{ord}_N 2}{m}$ to better examine the cryptographic security of our family of curves.

An efficient and systematic way of determining the explicit coefficients of a curve when given the (a_1, a_2) parameters that distinguish the isogeny class of its Jacobian is not yet established. This is an area to be explored in future research, so that one can construct such curves of cryptographic size.

Acknowledgments. I am grateful to Felipe Voloch for his supervision, and to Tanja Lange for her valuable suggestions on an earlier draft of this paper. I would also like to thank Steven Galbraith and the referees for their valuable comments.

References

[1] R. Balasubramanian and N. Koblitz, *The Improbability that an Elliptic Curve has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm*, J. Cryptology 11 (1998), pp. 141–145.

[2] P. S. L. M. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, Selected areas in cryptography, Lecture Notes in Comput. Sci. 3897, Springer-Verlag, Berlin, 2006, pp. 319–331.

[3] P. Birkner, *Efficient Divisor Class Halving on Genus Two Curves*, Selected Areas in Cryptography - SAC 2006, Lecture Notes in Computer Science 4356, Springer-Verlag, Berlin, 2006, pp. 317–326.

[4] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24(3-4) (1997), pp. 235–265.

[5] C. K. Caldwell, *Heuristics: Deriving the Wagstaff Mersenne Conjecture*, The prime pages: prime number research, records, and resources, 2006, Available at http://primes.utm.edu/mersenne/heuristic.html.

[6] G. Cardona, J. Pujolas, and E. Nart, *Curves of genus two over fields of even characteristic*, Math. Z. 250 (2005), pp. 177–201.

[7] D. Freeman, *Constructing pairing-friendly elliptic curves with embedding degree 10*, Algorithmic number theory, Lecture Notes in Comput. Sci. 4076, Springer-Verlag, Berlin, 2006, pp. 452–465.

[8] ______, *Constructing pairing-friendly genus 2 curves over prime fields with ordinary Jacobians*, Pairing-Based Cryptography – Pairing 2007, Lecture Notes in Computer Science 4575, Springer-Verlag, Berlin, 2007, pp. 152– 176.

[9] G. Frey, *Applications of arithmetical geometry to cryptographic constructions*. Proceedings of the Fifth International Conference on Finite Fields and Applications, pp. 128–161. Springer-Verlag, 1999.

[10] S. D. Galbraith, *Supersingular Curves in Cryptography*, Advances in Cryptology—ASIACRYPT 2001 (Gold Coast), Lecture Notes in Computer Science 2248, Springer-Verlag, Berlin, 2001, pp. 495–513.

[11] S. D. Galbraith and A. J. Menezes, *Algebraic Curves and Cryptography*, Finite Fields Appl. 11 (2005), pp. 544–577.

[12] L. Hitt, *On the Minimal Embedding Field*, Pairing-Based Cryptography – Pairing 2007, Lecture Notes in Computer Science 4575, Springer-Verlag, Berlin, 2007, pp. 294–301.

[13] E. W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. 347 (1995), pp. 2361–2401.

[14] ______, *Kernels of polarizations of abelian varieties over finite fields*, J. Algebraic Geom. 5 (1996), pp. 583–608.

[15] B. King, *A Point Compression Method for Elliptic Curves Defined over* $\mathrm{GF}(2^n)$, Public Key Cryptography—PKC 2004, Lecture Notes in Computer Science 2947, Springer-Verlag, Berlin, 2004, pp. 333–345.

[16] T. Lange and M. Stevens, *Efficient Doubling on Genus Two Curves over Binary Fields*, Selected Areas in Cryptography - SAC 2004, Lecture Notes in Computer Science 3357, Springer-Verlag, Berlin, 2005, pp. 170–181.

[17] D. Maisner and E. Nart, *Abelian Surfaces over Finite Fields as Jacobians*, Experiment. Math. 11 (2002), pp. 321–337. With an appendix by Everett W. Howe.

[18] G. McGuire and J. F. Voloch, *Weights in Codes and Genus 2 Curves*, Proc. Amer. Math. Soc. 133 (2005), pp. 2429–2437 (electronic).

[19] A. Miyaji, M. Nakabayashi, and S. Takano, *New Explicit Conditions of Elliptic Curve Traces for FR-Reduction*, IEICE Transactions on Fundamentals E84-A (2001), pp. 1234–1243.

[20] S. C. Pohlig and M. E. Hellman, *An Improved Algorithm for Computing Logarithms over $GF(p)$ and its Cryptographic Significance*, IEEE Transactions on Information Theory 24 (1978), pp. 106–110.

[21] H.-G. Rück, *Abelian Surfaces and Jacobian Varieties over Finite Fields*, Compos. Math. 76 (1990), pp. 351–366.

[22] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), pp. 134–144.

Received 27 February, 2007; revised 14 December, 2008

Author information

Laura Hitt, 321 Abbey Drive, Austin, TX 78737, USA.
Email: hitt36@gmail.com