Families of genus 2 curves with small embedding degree

Laura Hitt

Department of Mathematics
The University of Texas at Austin
Austin, TX 78712.
lhitt@math.utexas.edu

Abstract. Hyperelliptic curves of small genus have the advantage of providing a group of comparable size as that of elliptic curves, while working over a field of smaller size. Pairing-friendly hyperelliptic curves are those whose order of the Jacobian is divisible by a large prime, whose embedding degree is small enough for 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 two curves over $\mathbb{F}_q$, for $q = 2^m$, and their corresponding small embedding degrees. We give examples of the parameters for such curves with embedding degree $k < (\log q)^2$, such as $k = 8, 13, 16, 23, 26, 37, 46, 52$.
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 often near 1 and never more than 2.
We also give a sequence of $\mathbb{F}_q$-isogeny classes for a family of Jacobians of genus 2 curves over $\mathbb{F}_q$ whose 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

1 Introduction

The security of elliptic 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 comparable security as in other DL cryptosystems. Formulas for fast arithmetic on Jacobians of hyperelliptic curves over binary fields of genus two are known, as Lange and Stevens give in [10], 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, the Frey-Rück attack (or MOV attack) uses the Tate pairing (or Weil pairing) to map the discrete logarithm problem on the Jacobian of a curve defined over $\mathbb{F}_{q^k}$, for some integer k,

to the discrete logarithm in the multiplicative group of a finite field $\mathbb{F}^*_{q^{k'}}$, for some rational number k', where there are more efficient methods for solving the DLP. (See [8] for an discussion on this rational k'.) So for pairing-based cryptosystems, it is important to find curves with embedding degree k small enough that the pairing is efficiently computable and with k' large enough that the DLP in the finite field is hard. We note that when q is prime, then $k = k'$, so one needs a balance of k being both sufficiently small and sufficiently large.

We know that $k \leq 6$ for supersingular elliptic curves, as first shown by Miyaji, Nakabayashi and Takano in [13]. Galbraith in [5] shows that $k \leq 12$ for supersingular curves of genus two, which is attained in characteristic two. It has also been shown by Galbraith, McKee and Valença in [6] that one can obtain $k = 12$ for ordinary genus two curves in characteristic two. 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 [14] can reduce the DLP to prime-order subgroups. Thus for a curve over $\mathbb{F}_q$ of genus g and embedding degree k with respect to a subgroup of prime order N, one examines the ratio $\rho = \frac{g \log_2 q}{\log_2 N}$. For secure and efficient implementation, the ideal situation is to have $\rho \sim 1$, though currently the best ratio achieved is $\rho \sim 5/4$, as in [3].

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 $\frac{k'}{g}$ should be large enough so that the DLP in $\mathbb{F}^*_{q^{k'}}$ withstands index-calculus attacks.

In this paper, we consider genus two curves over $\mathbb{F}_q$, where $q = 2^m$, and whose associated Jacobian is 2-rank 1, neither supersingular, nor ordinary. Birkner in [2] gives formulas for fast arithmetic on 2-rank 1 curves, so such curves may be worthwhile to consider. We let C be a genus two 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 large integers, $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ for $r \geq 0$ and odd $L \geq 9$, 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 genus two curves over $\mathbb{F}_q$, whose group of $\mathbb{F}_q$-rational points of its Jacobian has order that is divisible by the prime $N_{r,L}$. For example, for each m in the interval $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1) - 1$, we get $\#J_C(\mathbb{F}_q) = 2^x(2^{2^r} + 1)N_{r,L}$, where $x = 2m - 2^r L$. 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 often near 1 and is never

more than 2, which suggests efficient implementation would be possible. We give examples of the parameters for such curves with embedding degree $k = 8, 13, 16, 23, 26, 37, 46, 52$. 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 $\mathrm{ord}_N p$ is the smallest positive x such that $p^x \equiv 1 \bmod N$, then we use $k' = \frac{\mathrm{ord}_{N_{r,L}} 2}{m}$ 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 $q < N < q^g$. A subgroup of $J_C(\mathbb{F}_q)$ with order N is said to have *embedding degree* k if N divides $q^k - 1$, but does not divide $q^i - 1$ for all integers $0 < i < k$. A pairing has been understood to embed the subgroup of order N into the multiplicative group of $\mathbb{F}_{q^k}$, for some integer k. However, it was shown in [8] that when q is not prime, then the minimal embedding field is $\mathbb{F}_{q^{k'}}$, for some rational number k'.

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

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

One can then map $\mathbb{F}^*_{q^k}/\mathbb{F}^{*N}_{q^k}$ 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 a finite field, where there are sub-exponential methods for solving the DLP. Whenever q is not prime, the smallest finite field containing the Nth roots of unity is actually $\mathbb{F}_{q^{k'}}$, where $k' = \frac{\mathrm{ord}_N p}{m}$, 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 $f(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2 \in \mathbb{Z}[t]$ for certain conditions on a_1 and a_2 is shown in [15], but that there exists a Jacobian of a curve defined over $\mathbb{F}_q$ with such a characteristic polynomial is due to [11]. 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 two defined over $\mathbb{F}_q$, with $\#J_C(\mathbb{F}_q) = q^2 + a_1 q + a_2 + a_1 + 1$.

[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.

We use the results of [11] for curves of 2-rank 1 in Theorem 1, letting C be a curve of genus two 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 $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ is a prime[2] for some $r \geq 0$ and odd $L \geq 5$. These primes are of the form $\frac{A^L+1}{A+1}$ where L is prime and A is a positive integer; if the behavior follows that of the primes $\frac{A^L-1}{A-1}$ 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 $L \leq M$ is asymptotic to $\frac{\log\log M}{\log A}$ for fixed A [4]. 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 $N_{r,L}$, and whose (a_1, a_2) have a specific description to be explicitly given later.

3 Family of primes and their 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 1. *Let $L \geq 5$ be odd. $N_{1,L} = \frac{2^{2L}+1}{2^2+1}$ is not a prime.*

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

We now determine the embedding degree for a general prime N 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 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*

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

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.

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

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

Lemma 3. *Let $r \geq 0$ and $L \geq 5$ be odd. If $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ 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. To see this:

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

Thus $x^a + 1 \,|x^A + 1$.

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

Lemma 4. *Let $r \geq 0$ and $L \geq 5$ be odd. If $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ is prime, then $\text{ord}_{N_{r,L}} 2 = 2^{r+1}L$.*

Proof. We have $(2^{2^r} + 1)N_{r,L} = 2^{2^r L} + 1$. So $2^{2^r L} \equiv -1 \bmod N_{r,L}$. This implies $2^{2^{r+1} L} \equiv 1 \bmod N_{r,L}$. So $\text{ord}_{N_{r,L}} 2 \mid 2^{r+1}L$. But by Lemma 3 we know that L is prime, so it must be that either $\text{ord}_{N_{r,L}} 2 = 2^j$ or $\text{ord}_{N_{r,L}} 2 = 2^j L$ for some $0 \leq j \leq r + 1$.

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

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

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

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

We are now able to state the embedding degree k of a group of order $N_{r,L}$, where $q = 2^m$ for a specific range of m. Here we study the traditional embedding degree k. In Section 6, we will revisit this understanding and consider a separate indicator that takes into account the minimal embedding field.

Lemma 5. *Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be prime for some $r \geq 0$ and odd $L \geq 5$, $1 \leq m \leq 2^r(L-1)-1$ and also allow $m = \frac{L+1}{2}$ in the case that $r = 0$, and let k be the embedding degree of the curve C with respect to $N_{r,L}$. Then $k = 2^{r+1-i}$ when $\gcd(\text{ord}_{N_{r,L}} 2, m) = 2^i L$ for $i \in \{0, \ldots, r-1\}$, and $k = 2^{r+1-i}L$ when $\gcd(\text{ord}_{N_{r,L}} 2, m) = 2^i$ for $i \in \{0, \ldots, r + 1\}$.*

Proof. By Lemma 4, we know that $\text{ord}_{N_{r,L}} 2 = 2^{r+1}L$. Suppose $\gcd(\text{ord}_{N_{r,L}} 2, m) = 2^i L$ for $0 \leq i \leq r - 1$. (Note that $i \leq r - 1$ since $\gcd(\text{ord}_{N_{r,L}} 2, m) = 2^i L \leq m \leq 2^r(L - 1) - 1$.) Then by Lemma 2,

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

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

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

(Note that since $\frac{2^{r+1}L}{2^i} \in \mathbb{Z}$ 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 $N_{r,L}$.

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 two [16]. The following theorem is a consequence of [11] and gives the conditions for a curve defined over a field of characteristic two associated with such a Jacobian to exist. (This statement combines Lemma 2.1, Theorem 2.9 part (M) and Corollary 2.17 of [11], as it appears in [12].)

Theorem 1. *Let $q = 2^m$ for a positive integer m. There exists a curve of the form $y^2 + xy = ax^5 + bx^3 + cx^2 + dx$, $a \neq 0, b, c, d$ arbitrary, with 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 [11] show that the conditions on a_1 and a_2 in Theorem 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 [11], but we will not need it for our result. We use this theorem to establish the existence of genus two 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 $N_{r,L}$.

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

Lemma 6. *If a, b, c are integers, with $a, b > 0$, and $2^a(2^b - 1) = c(c+1)$ then $a \leq b$.*

Proof. Suppose c is even. Then $c+1$ is odd. So $2^a \mid c$, and $c = 2^a x$ for some odd integer x such that $|x| \geq 1$, and $x(c+1) = 2^b - 1$. Then $2^b = x(2^a x + 1) + 1$. If $x \geq 1$, then $2^b \geq 2^a + 2$ and so $b > a$. If $x \leq 1$, then $2^b = |x|(2^a|x| - 1) + 1 \geq 2^a$ and so $b \geq a$.

Now suppose $c+1$ is even. Then c is odd. So $2^a \mid c+1$ and $c + 1 = 2^a x$ for some odd integer x such that $|x| \geq 1$ and $xc = 2^b - 1$. Then $2^b = x(2^a x - 1) + 1$. If $x \geq 1$, then $2^b \geq 2^a$, and so $b \geq a$. If $x \leq 1$, then $2^b = |x|(2^a|x| + 1) + 1 \geq 2^a + 2$, and so $b > a$.

Proposition 1. *Let $q = 2^m$, $r \geq 0$ and $L \geq 9$ be prime. When $m = \frac{L+1}{2}$, let $a_1 = 1$ and $a_2 = -2^m$, and when $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1) - 1$, let $a_1 = -1$ and $a_2 = 2^m + 2^{2m-2^rL}$. These a_1 and a_2 satisfy the conditions for the existence of the curves of genus 2 in Theorem 1.*

Proof. We first note that since $L \geq 9$, then $m = \frac{L+1}{2} \geq 5$. Now, clearly a_1 is odd and $|a_1| \leq 4\sqrt{q}$ in both cases of the proposition.

Let us show $2|a_1|\sqrt{q} - 2q \leq a_2 \leq a_1^2/4 + 2q$. The first case (when $a_1 = 1$ and $a_2 = -q$ for $m = \frac{L+1}{2}$), gives $2\sqrt{q} - 2q \leq -q \leq 1/4 + 2q$, which is true for $L \geq 9$. Now consider the second case (when $a_1 = -1$, and $a_2 = 2^m + 2^{2m-2^rL}$):

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

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

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

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:

$$2^{\lceil m/2 \rceil} \mid 2^m + 2^{2m-2^rL}$$

$$\iff 2m - 2^rL \geq \lceil m/2 \rceil$$

$$\iff \lfloor 3m/2 \rfloor \geq 2^rL$$

$$\iff m \geq \lceil 2^{r+1}L/3 \rceil$$

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 6, 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 $m = \frac{L+1}{2}$, since $m \geq 5$ for $L \geq 9$.

The second case yields $\Delta = 2^{2m-2^rL+2}(2^{2^rL-m} - 1) + 1$. For contradiction, suppose $\Delta = 2^{2m-2^rL+2}(2^{2^rL-m} - 1) + 1 = x^2$ for some integer x. 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 $2^{2m-2^rL}(2^{2^rL-m} - 1) = c(c+1)$. We apply Lemma 6, letting $a = 2m - 2^rL$ and $b = 2^rL - m$. We note that $a > 0$ since $m \geq \lceil \frac{2^{r+1}L}{3} \rceil$ implies $\lfloor \frac{3m}{2} \rfloor \geq 2^rL$, and so $2m - 2^rL > 0$. Also $b > 0$ since $m \leq 2^r(L-1) - 1$ implies $m \leq 2^rL$, and so $2^rL - m > 0$. Thus Δ a square implies $2m - 2^rL \leq 2^rL - m$, that is, $m \leq \frac{2^{r+1}L}{3}$. Since L is prime and $L \neq 3$, then $\frac{2^{r+1}L}{3} \notin \mathbb{Z}$, so in fact we have $m \leq \lfloor \frac{2^{r+1}L}{3} \rfloor < \lceil \frac{2^{r+1}L}{3} \rceil$. But we know that $\lceil \frac{2^{r+1}L}{3} \rceil \leq m$, so this will not hold, and hence 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 $\delta = 2^x b$, we must show that either $b \not\equiv 1 \bmod 8$ or $x \equiv 1 \bmod 2$.
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 $m = \frac{L+1}{2}$, since $m \geq 5$ when $L \geq 9$.
Now consider the second case:

$$\delta = (2^m + 2^{2m-2^rL} + 2^{m+1})^2 - 2^{m+2}$$

$$= (2^m + 2^{2m-2^r L})^2 + 2^{m+2}(2^m + 2^{2m-2^r L}) + 2^{2m+2} - 2^{m+2}$$
$$= 2^{2m+3} + 2^{2m} + 2^{3m-2^r L+2} + 2^{3m-2^r L+1} + 2^{4m-2^{r+1}L} - 2^{m+2}$$
$$= 2^{m+2}(2^{m+1} + 2^{m-2} + 2^{2m-2^r L} + 2^{2m-2^r L-1} + 2^{3m-2^r L-2} - 1)$$
$$\Rightarrow b = 2^{m-2}(2^3 + 1) + 2^{2m-2^r L-1}(2 + 1) + 2^{3m-2^{r+1}L-2} - 1.$$

For $m \geq 5$, we have

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

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

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

Clearly $3m-2^{r+1}L-2$ cannot be greater than or equal to 3. Now if $3m-2^{r+1}L-2 = 2$, then we have $4(2^{2^r L-m+1}3+1) \equiv 2 \bmod 8$. But a multiple of 4 cannot be congruent to 2 modulo 8, so this cannot happen. If $3m - 2^{r+1}L - 2 = 1$, then $m = \frac{3+2^{r+1}L}{3}$. But L is prime and $L \neq 3$, so $m \notin \mathbb{Z}$, and this cannot happen as we require an integer m. If $3m-2^{r+1}L-2 = 0$, then we have $2^{2^r L-m+1}3 + 1 \equiv 2 \bmod 8$. But an odd number cannot be congruent to 2 modulo 8, so this cannot happen. Thus $b \not\equiv 1 \bmod 8$, and so δ is not a square in $\mathbb{Z}_2$.

Therefore all the conditions for the existence of genus two 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 2. *Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be a prime for some $r \geq 0$ and odd $L \geq 9$. If $r = 0$, then for $m = \frac{L+1}{2}$ there exists a curve C of genus two over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2 \cdot 3 \cdot N_{0,L}$, and $a_1 = 1, a_2 = -2^m$. If $r \geq 0$, then for each integer m in the interval $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1)-1$, there exists a curve C of genus two over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2^x(2^{2^r}+1)N_{r,L}$, where $x = 2m-2^r L$, and $a_1 = -1, a_2 = 2^m+2^x$.*

Proof. Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be a prime for some $r \geq 0$ and odd $L \geq 9$.

We know by Proposition 1, 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 two over $\mathbb{F}_{2^m}$.

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

$$\#J_C(\mathbb{F}_{2^m}) = 2^{2m} + 2^m - 2^m + 2 = 2^{2m} + 2.$$

$$\#J_C(\mathbb{F}_{2^m}) = 2^{L+1} + 2 = 2(2^L + 1)$$
$$= 2 \cdot 3 \cdot N_{0,L} \text{ since } N_{0,L} = \frac{2^L + 1}{2 + 1}.$$

Now we consider when $r \geq 0$ is an integer not equal to 1, and $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1)-1$. For $a_1 = -1$ and $a_2 = 2^m + 2^x$, where $x = 2m - 2^r L$, we have

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

Thus the theorem is complete.

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

In [9], 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 two. In our case, since $\#J_C(\mathbb{F}_{2^m})$ is divisible by a high power of two, these curves may lend themselves to point compression using methods similar to those in [9].

Table 1 gives some examples of the parameters for curves over $\mathbb{F}_q$ yielding small embedding degrees $k = 8, 13, 16, 23, 26, 37, 46, 52$. 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 1 we have used brute force with MAGMA code to generate some examples of these curves over small $\mathbb{F}_q$.

Example 1. We give examples over small $\mathbb{F}_q$ for $r = 0$. We let g be a primitive element of $\mathbb{F}_q$.

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

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

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

$L = 13,\ m = \frac{L+1}{2} = 7,\ k = 26,\ \rho \sim 7/6,$
$C : y^2 + xy = x^5 + g^{92}x^3 + g^7x^2 + gx,$

$L = 17,\ m = \frac{L+1}{2} = 9,\ k = 34,\ \rho \sim 9/8,$
$C : y^2 + xy = x^5 + g^{103}x^3 + g^5x^2 + gx.$

k	L	r	m	a_1	a_2	ρ
8	37	2	111	-1	$2^{111}+2^{74}$	3/2
8	89	2	267	-1	$2^{267}+2^{178}$	3/2
8	149	2	447	-1	$2^{447}+2^{298}$	3/2
13	13	3	80	-1	$2^{80}+2^{56}$	5/3
16	13	3	91	-1	$2^{91}+2^{78}$	2
23	23	2	64	-1	$2^{64}+2^{36}$	3/2
23	23	2	72	-1	$2^{72}+2^{52}$	5/3
23	23	2	80	-1	$2^{80}+2^{68}$	9/5
26	13	3	72	-1	$2^{72}+2^{40}$	3/2
26	13	3	88	-1	$2^{88}+2^{72}$	9/5
37	37	2	104	-1	$2^{104}+2^{60}$	7/5
37	37	2	112	-1	$2^{112}+2^{76}$	3/2
37	37	2	120	-1	$2^{120}+2^{92}$	5/3
37	37	2	128	-1	$2^{128}+2^{108}$	9/5
37	37	2	136	-1	$2^{136}+2^{124}$	2
46	23	2	68	-1	$2^{68}+2^{44}$	3/2
46	23	2	76	-1	$2^{76}+2^{60}$	7/4
46	23	2	84	-1	$2^{84}+2^{76}$	2
52	13	3	76	-1	$2^{76}+2^{48}$	5/3
52	13	3	88	-1	$2^{88}+2^{64}$	7/4
52	13	3	92	-1	$2^{92}+2^{80}$	2

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

5 Size of the embedding degrees

We examine the size of the embedding degrees of the family of curves from Theorem 2. 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 [7, Section 5.2.1] for discussion of the probability of k in this range.)

Proposition 2. *Let $q = 2^m$, $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be prime for some $r \geq 0$ and odd $L \geq 5$, and k be the embedding degree of the curve C with respect to $N_{r,L}$. If $L \geq 11$, then for each integer m in the interval $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1)-1$, $k < (\log\ q)^2$. If $L \geq 15$, then when $r = 0$ and $m = \frac{L+1}{2}$, $k < (\log\ q)^2$.*

Proof. Let $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1)-1$. By Lemma 5, the largest that k can be is $k = 2^{r+1}L$, so it suffices to consider this case. Given the acceptable range for m, it is enough to show $k < (\log\ q)^2$ for $m = \lceil \frac{2^{r+1}L}{3} \rceil$. Now $k < (\log\ q)^2$ if

$$2^{r+1}L < (\log\ 2^{\frac{2^{r+1}L}{3}})^2$$

$$\iff 2^{r+1}L < \left(\frac{2^{r+1}L}{3}\right)^2 (\log^2 2)$$
$$\iff 9 \cdot 2^{r+1}L < 2^{2r+2}(\log^2 2)L^2$$
$$\iff \frac{9}{2^{r+1}(\log^2 2)} < L.$$

This holds if $L \geq 10$ for $r = 0$. Since we require L to be odd, we can say that $L \geq 11$ for any $r \geq 0$ gives the result.
Now let $m = \frac{L+1}{2}$ and $r = 0$. By Lemma 5, it suffices to consider $k = 2L$. So $k < (\log\ q)^2$ if

$$2L < (\log\ 2^{(L+1)/2})^2$$
$$\iff 2L < \left(\frac{L+1}{2}\right)^2 (\log^2 2)$$
$$\iff 2(L+1) - 2 < \frac{\log^2 2}{4}(L+1)^2$$
$$\iff 0 < \frac{\log^2 2}{4}(L+1)^2 - 2(L+1) + 2.$$

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

6 Minimal embedding field

In [8], 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 $\mathbb{F}^*_{q^k}$. This difference in the size of the groups can be quite large, by as much as a factor of 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 3. *Let $q = 2^m$, and $p \geq 7$ be a prime. If $N = 2^p - 1$ is prime, then for each integer m such that $\lceil \frac{2p}{3} \rceil \leq m \leq p - 1$, there exists a genus two curve C over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2^{2m-p}N$, where $a_1 = -1$ and $a_2 = 2^m - 2^{2m-p}$. The embedding degree is $k = p$ and so the difference in size between the extension degrees of $\mathbb{F}_{q^k}$ and the minimal embedding field $\mathbb{F}_{2^p}$ is m.*

Proof. First let us show that the conditions of Theorem 1 are met for the existence of genus 2 curves C when $a_1 = -1$ and $a_2 = 2^m - 2^{2m-p}$. 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,

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

Clearly the second inequality holds. The first inequality holds if

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

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

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

$$2^{\lceil m/2 \rceil} \mid 2^m - 2^{2m-p} \iff 2m - p \geq \lceil m/2 \rceil$$

$$\iff \lfloor 3m/2 \rfloor \geq p$$

$$\iff m \geq \lceil 2p/3 \rceil.$$

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 $\Delta = 1 - 2^{m+2} + 2^{2m-p+2} + 2^{m+3} = 1 + 2^{2m-p+2} + 2^{m+2} = x^2$ for some integer x. Since Δ is odd, then x is odd, so let $x = 2n + 1$ for some integer n. Then Δ is a square if and only if $2^{2m-p}(2^{p-m} + 1) = n(n+1)$, if and only if $2m - p = p - m$, that is, $m = 2p/3$. But $p \geq 5$ is prime, so m is not an integer, thus 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 $\delta = 2^x b$, we must show that either $b \not\equiv 1 \bmod 8$ or $x \equiv 1 \bmod 2$. Now

$$\delta = (2^m - 2^{2m-p} + 2^{m+1})^2 - 2^{m+2}$$

$$= (2^m - 2^P 2m - p)^2 + 2^{m+2}(2^m - 2^{2m-p}) + 2^{2m+2} - 2^{m+2}$$

$$= 2^{2m+3} + 2^m - 2^{3m-p+2} - 2^{3m-p+1} + 2^{4m-2p} - 2^{m+2}$$

$$2^{m+2}(2^{m+1} + 2^{m-2} - 2^{2m-p} - 2^{2m-p-1} + 2^{3m-2p-2} - 1)$$

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

For $m \geq 5$, we have

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

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

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

$$\Rightarrow 3m - 2p - 2 = 1$$

$$\Rightarrow m = \frac{3 + 2p}{3}.$$

But p is prime, so $m = \frac{3+2p}{3} \notin \mathbb{Z}$. This is a contradiction, so $b \not\equiv 1 \bmod 8$. Thus δ is not a square in $\mathbb{Z}_2$. Therefore the conditions of Theorem 1 are satisfied for the existence of a curve C over $\mathbb{F}_q$.

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

$$\#J_C(\mathbb{F}_{2^m}) = q^2 + a_1 q + a_2 + a_1 + 1 = 2^{2m} - 2^{2m-p}$$

$$\Rightarrow \#J_C(\mathbb{F}_{2^m}) = 2^{2m-p}(2^p - 1) = 2^{2m-p}N.$$

Now we find the embedding degree k with respect to $N = 2^p - 1$. We see that $\mathrm{ord}_N 2 = p$, so $\gcd(\mathrm{ord}_N 2, m) = 1$ since $m \leq p - 1$. Therefore by Lemma 2, $k = p$, and the difference in field exponents is $\frac{m}{\gcd(\mathrm{ord}_N 2, m)} = m$. Thus the proof of the proposition is complete.

In light of [8], 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 $k' = \frac{\mathrm{ord}_{N_{r,L}} 2}{m}$. 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 finite field.

k	L	r	m	a_1	a_2	$\log_2 N_{r,L}$	$k \log_2 q$	$k' \log_2 q$
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
13	13	3	80	-1	$2^{80} + 2^{56}$	95	1040	208
16	13	3	91	-1	$2^{91} + 2^{78}$	95	1456	208
23	23	2	64	-1	$2^{64} + 2^{36}$	87	1472	184
23	23	2	72	-1	$2^{72} + 2^{52}$	87	1656	184
23	23	2	80	-1	$2^{80} + 2^{68}$	87	1840	184
26	13	3	72	-1	$2^{72} + 2^{40}$	95	1872	208
26	13	3	88	-1	$2^{88} + 2^{72}$	95	2288	208
37	37	2	104	-1	$2^{104} + 2^{60}$	143	3848	296
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	68	-1	$2^{68} + 2^{44}$	87	3128	184
46	23	2	76	-1	$2^{76} + 2^{60}$	87	3496	184
46	23	2	84	-1	$2^{84} + 2^{76}$	87	3864	184
52	13	3	76	-1	$2^{76} + 2^{48}$	95	3952	208
52	13	3	88	-1	$2^{88} + 2^{64}$	95	4368	208
52	13	3	92	-1	$2^{92} + 2^{80}$	95	4784	208

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

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 a finite field of around 1024-bits. This means that one needs $\mathbb{F}_{q^{k'}} > 2^{1024}$. 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 finite field is irrelevant. However, for $L \geq 149$, 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 two, 2-rank 1 curves over $\mathbb{F}_q$, for $q = 2^m$, and their corresponding small embedding degrees. In particular, we gave examples of the parameters for such curves with embedding degree $k < (\log q)^2$, such as $k = 8, 13, 16, 23, 26, 37, 46, 52$, so that the computations in $\mathbb{F}_{q^k}$ may be feasible. Our family of curves also yields the ratio ρ often near 1 and never more than 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 for his 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. of Cryptology*, 11(2):141–145, 1998.
2. P. Birkner. Efficient divisor class halving on genus two curves. In *Selected Areas in Cryptography - SAC 2006*, volume 4356 of *Lecture Notes in Computer Science*, pages 317–326. Springer-Verlag, Berlin, 2006.
3. F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptogr.*, 37(1):133–141, 2005.
4. 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.
5. S. D. Galbraith. Supersingular curves in cryptography. In *Advances in Cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Computer Science*, pages 495–513. Springer-Verlag, Berlin, 2001.
6. S. D. Galbraith, J. McKee, and P. Valença. Ordinary abelian varieties having small embedding degree. In R. Cramer and T. Okamoto, editors, *In Proceedings of a workshop on Mathematical Problems and Techniques in Cryptology*, pages 29–45. CRM Barcelona, 2005.
7. S. D. Galbraith and A. J. Menezes. Algebraic curves and cryptography. *Finite Fields Appl.*, 11(3):544–577, 2005.

8. L. Hitt. On the minimal embedding field. In *Pairing-Based Cryptography – Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 294–301. Springer-Verlag, Berlin, 2007.
9. B. King. A point compression method for elliptic curves defined over GF(2^n). In *Public key cryptography—PKC 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 333–345. Springer-Verlag, Berlin, 2004.
10. T. Lange and M. Stevens. Efficient doubling on genus two curves over binary fields. In *Selected Areas in Cryptography - SAC 2004*, volume 3357 of *Lecture Notes in Computer Science*, pages 170–181. Springer-Verlag, Berlin, 2005.
11. D. Maisner and E. Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.
12. G. McGuire and J. F. Voloch. Weights in codes and genus 2 curves. *Proc. Amer. Math. Soc.*, 133(8):2429–2437 (electronic), 2005.
13. A. J. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions Information Theory*, 39(5):1639–1646, 1993.
14. 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*, 24:106–110, 1978.
15. H.-G. Rück. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Math.*, 76(3):351–366, 1990.
16. J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.