Families of Genus 2 Curves with Small Embedding Degree

Laura Hitt

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

Abstract. Hyperelliptic curves of small genus have the advantage of achieving the same security in the group while working over a smaller field than with elliptic curves. Pairing-friendly curves are those whose Jacobian is divisible by a large prime and whose embedding degree is small enough for computations to be feasible, but large enough that the curves are not susceptible to sub-exponential attacks. 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 their corresponding small embedding degrees. We give examples of the parameters for such curves with embedding degree $k < (\frac{\log\ q}{\log\log q})^2$, such as $k = 8, 13, 16, 23, 26, 37, 46$, and for curves with $(\frac{\log\ q}{\log\log q})^2 < k < (\log q)^2$. 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 embedding field is much smaller than the presumed embedding field indicated by the embedding degree k. That is, the field exponent differs by a factor of m, thus illustrating the weakness in the conventional definition of embedding degree.

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

1 Introduction

The computational intractability of the elliptic curve discrete logarithm problem is the mathematical basis for security of elliptic curve cryptosystems. Elliptic (and hyperelliptic) curves are especially attractive for cryptography as there is currently no sub-exponential algorithm for solving the discrete logarithm problem (DLP) on properly chosen curves. Thus they provide greater security and more efficient performance than first generation public key techniques, such as RSA and Diffie-Hellman. The result is faster implementations, bandwidth and storage savings, and reduced energy consumption. The performance of such cryptosystems depends essentially on efficient arithmetic in the underlying finite field, and applications usually focus on prime fields or binary fields. Binary finite fields, $\mathbb{F}_{2^m}$, have the advantage of "carry-free" addition and are more interesting for hardware implementation. [7] gives formulas for fast arithmetic on hyperelliptic curves, garnering more support for their use in cryptosystems. With hyperelliptic curves of small genus (that is, whose associated Jacobian abelian variety is of low dimension), it is possible to work over a smaller field while achieving the same security in the group. Thus hyperelliptic curves can offer the benefits of having comparable levels of security with smaller key sizes than other finite abelian groups.

Pairings on groups have been used constructively to design cryptographic protocols and to solve problems that have been open for many years, such as identity-based encryption, one-round three-party key agreement, and short 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 to the discrete logarithm in the finite field $\mathbb{F}_{q^k}^*$, where there are more efficient methods for solving the DLP. So for pairing-based cryptosystems, it is important to find curves where the embedding degree k is small enough that the pairing is efficiently computable, but large enough that the DLP in $\mathbb{F}_{q^k}^*$ is hard.

This leads to the understanding of a *pairing-friendly* curve over $\mathbb{F}_q$ as one that satisfies the following two conditions: (1) $\#J_C(\mathbb{F}_q)$ 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 resistant to Pollard's rho attack (and other known attacks), and (2) The embedding degree k should be sufficiently large so that the DLP in $\mathbb{F}_{q^k}^*$ withstands index-calculus attacks, but small enough that the arithmetic in $\mathbb{F}_{q^k}$ can be efficiently implemented. It is important to note that while k must be small enough to enable pairings in the group, if it is too small, then the embedding field $\mathbb{F}_{q^k}$ is small enough to warrant the curve insecure for DL systems.

We know that $k \leq 6$ for supersingular elliptic curves, as first shown in [9]. [3] gives an upper bound of 12 on k for supersingular genus 2 curves, which is attained in characteristic two. It has also been shown in [2] that one can obtain $k = 12$ for ordinary genus 2 curves in characteristic two. However, for most non-supersingular curves, the embedding degree is enormous.

In this paper, we consider genus 2 curves over $\mathbb{F}_q$, where $q = 2^m$, whose associated Jacobian is neither supersingular (2-rank 0), nor ordinary (2-rank 2), but rather has 2-rank 1. [1] gives formulas for fast arithmetic on 2-rank 1 curves, so such curves are interesting to consider. We let C be a genus 2 curve over $\mathbb{F}_q$ of the form

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

where $b, c, d \in \mathbb{F}_q^*$. In section 3, we give a parametrization of a family of large primes, $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1}$ for $r \geq 0$ and odd $L > 7$, and we determine the embedding degrees for subgroups having these prime orders. In section 4, we associate with each of these primes a sequence of genus 2 curves over $\mathbb{F}_{2^m}$, whose Jacobian order is divisible by the prime N_r. For example, for each m in the interval $\lceil \frac{2^{r+1}(L+2)}{3} \rceil \leq m \leq 2^r(L+1)-1$, we get $\#J_C(\mathbb{F}_{2^m}) = 2^x(2^{2^r}+1)N_r$, where $x = 2m - 2^r(L+2)$. We describe the curves by the $\mathbb{F}_q$-isogeny class of their Jacobians, for example, having $a_1 = -1$, and $a_2 = 2^m + 2^x$ in the case mentioned above. We give examples of the parameters for such curves with embedding degree $k = 8, 13, 16, 23, 26, 37, 46$. In section 5, we show that the embedding degree k is always small, that is, $k < (\log q)^2$, so that computations in $\mathbb{F}_{q^k}$ are feasible. Then we examine which curves have $k > (\frac{\log\ q}{\log\log q})^2$, so that the DLP in $\mathbb{F}^*_{q^k}$ is considered hard and the curves are not susceptible to sub-exponential attacks. Finally, in section 6, we note the difference between the embedding field presumed by the conventional definition of embedding degree k and the actual embedding field. We give an example of another family of curves for which this difference is maximal (the field exponent differs by a factor of m), and then we consider the extent to which this discrepancy applies to our family of 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 curve over $\mathbb{F}_q$. Let $J_C(\mathbb{F}_q)$ be the Jacobian of C over $\mathbb{F}_q$ and assume there exists a prime N dividing the order of $J_C(\mathbb{F}_q)$, with $q < N < q^2$. 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 $0 < i < k$.

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

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

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

Pairing-based attacks can transport the discrete logarithm problem in $J_C(\mathbb{F}_q)$ to the discrete logarithm in the finite field $\mathbb{F}^*_{q^k}$, where there are sub-exponential methods for solving the DLP. So for pairing-based cryptosystems, one would like to find curves where the embedding degree k is small enough for computations to be feasible, but large enough for the DLP in the embedding field to be difficult. For most non-supersingular curves, the embedding degree is enormous. We will give a sequence of 2-rank 1 curves with small embedding degree.

The fact that there exist simple abelian surfaces with characteristic polynomial $f(t) = t^4 + a_1t^3 + a_2t^2 + qa_1t + q^2 \in \mathbb{Z}[t]$ is shown in [10], but that there exists a Jacobian of a genus 2 curve with such a characteristic polynomial is due to [8]. So

[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 have that (a_1, a_2) determines the $\mathbb{F}_q$-isogeny class of the Jacobian of a smooth projective curve C defined over $\mathbb{F}_q$, with $\#J_C(\mathbb{F}_q) = q^2 + a_1 q + a_2 + a_1 + 1$.

We let C be a genus 2 curve over $\mathbb{F}_q$ of the form $y^2 + xy = x^5 + bx^3 + cx^2 + dx$, where $b, c, d \in \mathbb{F}_q^*$. We consider when $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1}$ is a prime[2] for some $r \geq 0$ and odd $L > 1$. We have seen experimentally that for $r \leq 3$, N_r is very often prime, though it appears that primality does not occur for $r \geq 4$. Our families of curves will be those whose Jacobian order is divisible by N_r, 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 $L > 1$ be odd. $N_1 = \frac{2^{2(L+2)}+1}{2^2+1}$ is not a prime.*

Proof. We first note that $N_1 = 2^{2(L+1)} - 2^{2(L)} + 2^{2(L-1)} - 2^{2(L-2)} + \cdots - 2 + 1$, so $N_1 \in \mathbb{Z}$. Let $P = \frac{2^{L+2}+1}{2+1} = N_0$. We see that $9P^2 = 2^{2(L+2)} + 2^{L+3} + 1$. So $N_1 = \frac{9P^2 - 2^{L+3}}{2^2+1}$. Now L is odd, so $L+3$ is even. So $N_1 = \frac{(3P - 2^{\frac{L+3}{2}})(3P + 2^{\frac{L+3}{2}})}{2^2+1}$. Now $N_1 \in \mathbb{Z}$ and $2^2 + 1$ is prime, so either $(\frac{3P - 2^{\frac{L+3}{2}}}{2^2+1}) \in \mathbb{Z}$ and $(3P + 2^{\frac{L+3}{2}}) \in \mathbb{Z}$, or $(3P - 2^{\frac{L+3}{2}}) \in \mathbb{Z}$ and $(\frac{3P + 2^{\frac{L+3}{2}}}{2^2+1}) \in \mathbb{Z}$. Either way, N_1 is not prime.

□

We now determine the embedding degree for a general prime N over $\mathbb{F}_q$. We let $\text{ord}_N p$ be the smallest 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 prime, and k be the smallest integer such that $q^k \equiv 1 \bmod N$. Then*

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

Proof. Clearly $k \mid \frac{\text{ord}_N p}{\gcd(\text{ord}_N p, m)}$, since

$$1 \equiv p^{\text{ord}_N p} \equiv (p^{\text{ord}_N p})^{m/\gcd(\text{ord}_N p, m)} \equiv (p^m)^{\text{ord}_N p/\gcd(\text{ord}_N p, m)} \bmod N.$$

Now let $D = \gcd(\text{ord}_N p, m)$. So we have $k \mid \frac{\text{ord}_N p}{D}$.

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

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 $\mathrm{ord}_{N_r} 2$ via the following lemmas.

Lemma 3. *Let L be odd. If $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1}$ is prime for some $r \geq 0$, then $L+2$ is prime.*

Proof. $L+2$ is odd, so if $L+2$ is not prime, then $L+2 = ab$, where a, b are odd. If $a \geq 3$ and $a \mid L+2$, then $2^a + 1 \mid 2^{2^r(L+2)} + 1$. This implies that $2^a + 1 \mid (2^{2^r} + 1)N_r$. But $\gcd(2^{2^r} + 1, N_r) = 1$. Now $2^a + 1 \nmid 2^{2^r} + 1$ for a odd and $2^a + 1 \nmid N_r$, since N_r is prime. Therefore $a = 1$, and hence $L+2$ is prime.

□

Lemma 4. *Let L be odd. If $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1}$ is prime for some $r \geq 0$, then* $\mathrm{ord}_{N_r} 2 = 2^{r+1}(L+2)$.

Proof. We have $(2^{2^r} + 1)N_r = 2^{2^r(L+2)} + 1$. So $2^{2^r(L+2)} \equiv -1 \bmod N_r$. This implies $2^{2^{r+1}(L+2)} \equiv 1 \bmod N_r$. So $\mathrm{ord}_{N_r} 2 \mid 2^{r+1}(L+2)$. But by Lemma 3 we know that $L+2$ is prime, so it must be that either $\mathrm{ord}_{N_r} 2 \mid 2^{r+1}$ or $\mathrm{ord}_{N_r} 2 \mid 2^{r+1}(L+2)$. The former cannot happen since $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1} > 2^{2^{r+1}}$. It follows that $\mathrm{ord}_{N_r} 2 = 2^{r+1}(L+2)$.

□

We are now able to state the embedding degree k of a group of order N_r over $\mathbb{F}_q$, where $q = 2^m$ for a specific range of m. (The upper bound is required so that $q < N_r$, and the choice for lower bound will be evident in Proposition 1).

Lemma 5. *Let L be odd, and let $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1}$ be prime for some $r \geq 0$, and let k be the embedding degree of curve C with respect to N_r. Let $\lceil \frac{2^{r+1}(L+2)}{3} \rceil \leq m \leq 2^r(L+1) - 1$, and also allow $m = \frac{L+1}{2} + 1$ in the case that $r = 0$. Then $k = 2^{r+1-i}$ when* $\gcd(\mathrm{ord}_N 2, m) = 2^i(L+2)$ *for $i \in \{0, \ldots, r-2\}$, and $k = 2^{r+1-i}(L+2)$ when* $\gcd(\mathrm{ord}_N 2, m) = 2^i$ *for $i \in \{0, \ldots, r+1\}$.*

Proof. By Lemma 2, we know $k = \frac{\mathrm{ord}_N 2}{\gcd(\mathrm{ord}_N 2, m)}$. By Lemma 4, we know that $\mathrm{ord}_{N_r} 2 = 2^{r+1}(L+2)$. The results follow immediately, with the possible i's determined by the size restriction on m.

□

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 order is divisible by N_r.

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, and the following theorem found in [8] gives the conditions for a genus 2 curve associated with such a Jacobian to exist.

Theorem 1. *There exists a curve of the form $y^2 + xy = x^5 + bx^3 + cx^2 + dx$, $b, c, d \in \mathbb{F}_q^*$, with $N = q + 1 + a_1$ points over $\mathbb{F}_q = \mathbb{F}_{2^m}$ and having simple Jacobian if and only if*

1. a_1 is odd

2. $|a_1| \leq 4\sqrt{q}$

3. there exists an integer a_2 such that

(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).

We use this theorem 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 $\#J_C(\mathbb{F}_q)$ is divisible by N_r.

Proposition 1. *Let $q = 2^m$, $L > 1$ be odd, and $r \geq 0$. When $m = \frac{L+1}{2} + 1 \geq 5$, let $a_1 = 1$ and $a_2 = -2^m$, and when $\lceil \frac{2^{r+1}(L+2)}{3} \rceil \leq m \leq 2^r(L + 1) - 1$, let $a_1 = -1$ and $a_2 = 2^m + 2^{2m - 2^r(L+2)}$. For $L \geq 7$, these a_1 and a_2 satisfy the conditions for the existence of the genus 2 curves in Theorem 1.*

We give the proof in the appendix.

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

Theorem 2. *Let $L \geq 7$ be odd, and $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1}$ be a prime for some $r \geq 0$. If $r = 0$, then for $m = \frac{L+1}{2} + 1$ there exists a genus 2 curve over F_{2^m} with the property that $\#J_C(\mathbb{F}_{2^m}) = 2 \cdot 3 \cdot N_0$, and $a_1 = 1, a_2 = -2^m$. If $r \geq 0$, then for each integer m in the interval $\lceil \frac{2^{r+1}(L+2)}{3} \rceil \leq m \leq 2^r(L + 1) - 1$, there exists a genus 2 curve over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2^x(2^{2^r} + 1)N_r$, where $x = 2m - 2^r(L + 2)$, and $a_1 = -1, a_2 = 2^m + 2^x$.*

Proof. Let $L \geq 7$ be odd. Let $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1}$ be a prime for some $r \geq 0$.

Let us first consider when $m = \frac{L+1}{2} + 1$ and $r = 0$. We will find a_1, a_2 so that $\#J_C(\mathbb{F}_{2^m}) = 2 \cdot 3 \cdot N_0$. Suppose $a_1 = 1$. Then we need an a_2 such that $\#J_C(\mathbb{F}_{2^m}) = 2^{2m} + 2^m + a_2 + 2 = 2 \cdot 3 \cdot N_0$. That is, such that $2^{2m} + 2^m + a_2 + 2 = 2^{L+3} + 2$. Since

$m = \frac{L+1}{2} + 1$, then $L = 2m - 3$, so we have $2^{2m} + 2^m + a_2 = 2^{2m}$. Thus $a_2 = -2^m$. So we see that $a_1 = 1$ and $a_2 = -2^m$ satisfy $\#J_C(\mathbb{F}_{2^m}) = 2 \cdot 3 \cdot N_0$.

Now let $r \geq 0$ be any integer not equal to 1, and let us consider when $\lceil \frac{2^{r+1}(L+2)}{3} \rceil \leq m \leq 2^r(L+1) - 1$. We will find a_1, a_2 so that $\#J_C(\mathbb{F}_{2^m}) = 2^{2m} + a_1 2^m + a_1 + a_2 + 1 = 2^x(2^{2^r} + 1)N_r$ for some integer x. Suppose $a_1 = -1$. Then we need an a_2 such that $2^{2m} - 2^m + a_2 = 2^{2^r(L+2)+x} + 2^x$. Suppose $2^{2m} = 2^{2^r(L+2)+x}$, and so $-2^m + a_2 = 2^x$. Then $x = 2m - 2^r(L+2)$, and $a_2 = 2^m + 2^x$. Thus we have found an (a_1, a_2) that satisfy $\#J_C(\mathbb{F}_{2^m}) = 2^x(2^{2^r} + 1)N_r$. Now, by Proposition 1, these (a_1, a_2) above, with m in the specified range, satisfy the conditions for the existence of a genus 2 curve over $\mathbb{F}_{2^m}$. Thus the theorem is complete.

□

In [6], 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 [6].

A 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. As such, we have used brute force with MAGMA code to generate some examples of these curves over small $\mathbb{F}_q$ in the families described above.

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

$$L = 9,\ m = \frac{L+1}{2} + 1 = 6,\ C : y^2 + xy = x^5 + g^8x^3 + g^3x^2 + gx$$

$$L = 9,\ m = \lceil \frac{2^{r+1}(L+2)}{3} \rceil = 8,\ C : y^2 + xy = x^5 + g^7x^3 + g^7x$$

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

$$L = 11,\ m = \frac{L+1}{2} + 1 = 7,\ C : y^2 + xy = x^5 + g^{92}x^3 + g^7x^2 + gx$$

$$L = 15,\ m = \frac{L+1}{2} + 1 = 9,\ C : y^2 + xy = x^5 + g^{103}x^3 + g^5x^2 + gx$$

5 Size of the Embedding Degrees

The latest results, in [5], give an algorithm for computing discrete logarithms in finite fields $\mathbb{F}_{q^k}$ with heuristic complexity $L_{q^k}(1/3) = \exp(o(\log q^k)^{1/3}(\log\log q^k)^{2/3})$. So in order for an attack to be sub-exponential in q, one needs $k \in o((\frac{\log\ q}{\log\log q})^2)$.

We examine the size of the embedding degrees of the family of curves in Theorem 2. We find that these curves always yield embedding degrees such that $k < (\log\ q)^2$, but only sometimes yield embedding degrees such that $k < (\frac{\log\ q}{\log\log q})^2$. This means the embedding degree is always "small," so computations are feasible, and for some curves it is still large enough for the discrete log problem to be hard. The following theorems establish these results.

Proposition 2. *Let $q = 2^m$, $L > 1$ be odd, $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1}$ be prime for some $r \geq 0$, and k be the embedding degree of curve C with respect to N_r. If $L \geq 9$, then for each integer m in the interval $\lceil\frac{2^{r+1}(L+2)}{3}\rceil \leq m \leq 2^r(L+1)-1$, $k < (\log\ q)^2$. If $L \geq 13$, then when $r = 0$ and $m = \frac{L+1}{2}+1$, $k < (\log\ q)^2$.*

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

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

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

$$\Leftrightarrow 9 \cdot 2^{r+1}(L+2) < 2^{2r+2}(\log^2 2)(L+2)^2$$

$$\Leftrightarrow 0 < 2^{r+1}(\log^2 2)(L+2) - 9.$$

This holds if $L > \frac{9}{2^{r+1}(\log^2 2)} - 2$, that is, if $L \geq 8$ for $r = 0$, and $L \geq 1$ for $r \geq 2$. Since we require L to be odd, we can say that $L \geq 9$ for any $r \geq 0$ gives the result. Now let $m = \frac{L+1}{2}+1$ and $r = 0$. By Lemma 5, it suffices to consider $k = 2(L+2)$.

$$k < (\log\ q)^2 \Leftrightarrow 2(L+2) < (\log\ 2^{(L+1)/2+1})^2 = ((L+1)/2+1)^2(\log^2 2)$$

$$\Leftrightarrow 2(L+1)+2 < \frac{\log^2 2}{4}(L+1)^2 + (\log^2 2)(L+1) + \log^2 2$$

$$\Leftrightarrow 0 < \frac{\log^2 2}{4}(L+1)^2 + ((\log^2 2 - 2))(L+1) + (\log^2 2 - 2).$$

This holds if $L+1 > \frac{-(\log^2 2-2)+\sqrt{(\log^2 2-2)^2-(\log^2 2)(\log^2 2-2)}}{\frac{\log^2 2}{2}}$, that is, if $L \geq 13$.

□

Now we determine when the embedding degree is small enough that the curve may be susceptible to attacks that are sub-exponential in q.

Proposition 3. *Let $q = 2^m$, $L > 1$ be odd, $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1}$ be prime for some $r \geq 0$, and k be the embedding degree of curve C with respect to N_r. Then in the following cases we have $k < (\frac{\log\ q}{\log\log q})^2$:*
(i) for $r = 0$ and $m = \frac{L+3}{2}$, if m is odd and $m \geq 205$ (that is, $L \geq 405$), or if m is even and $m \geq 56$ (that is, $L \geq 107$).
(ii) for $r = 2, 3$ and m in the interval $\lceil \frac{2^{r+1}(L+2)}{3} \rceil \leq m \leq 2^r(L+1)-1$, if $(L+2) \mid m$ and $L \geq 11$.

We give the proof in the appendix.

k	L	r	m	a_1	a_2	$\log_2 N_r$
8	11	3	78	-1	$2^{78} + 2^{52}$	95
8	21	2	69	-1	$2^{69} + 2^{46}$	87
8	35	2	111	-1	$2^{111} + 2^{74}$	143
8	87	2	267	-1	$2^{267} + 2^{178}$	351
8	147	2	447	-1	$2^{447} + 2^{298}$	591
13	11	3	80	-1	$2^{80} + 2^{56}$	95
16	11	3	91	-1	$2^{91} + 2^{78}$	95
23	21	2	64	-1	$2^{64} + 2^{36}$	87
23	21	2	72	-1	$2^{72} + 2^{52}$	87
23	21	2	80	-1	$2^{80} + 2^{68}$	87
26	11	3	72	-1	$2^{72} + 2^{40}$	95
26	11	3	88	-1	$2^{88} + 2^{72}$	95
37	35	2	104	-1	$2^{104} + 2^{60}$	143
37	35	2	112	-1	$2^{112} + 2^{76}$	143
37	35	2	120	-1	$2^{120} + 2^{92}$	143
37	35	2	128	-1	$2^{128} + 2^{108}$	143
37	35	2	136	-1	$2^{136} + 2^{124}$	143
46	21	2	68	-1	$2^{68} + 2^{44}$	87
46	21	2	76	-1	$2^{76} + 2^{60}$	87
46	21	2	84	-1	$2^{84} + 2^{76}$	87

Table 1. Examples of parameters for families of curves over $\mathbb{F}_{2^m}$ with embedding degree $k < (\frac{\log\ q}{\log\log q})^2$.

For the cases not addressed in Proposition 3, that is, when $(L+2) \nmid m$, then whether or not $k < (\frac{\log\ q}{\log\log q})^2$ depends on precisely which m in the interval $\lceil \frac{2^{r+1}(L+2)}{3} \rceil \leq m \leq 2^r(L+1)-1$ is chosen and on $\gcd(2^{r+1}(L+2), m)$. More precisely, if $\gcd(2^{r+1}(L+2), m) = 2^i$, then $k < (\frac{\log\ q}{\log\log q})^2$ holds if and only if

$$2^{r+1-i} < \frac{m^2(\log 2)^2}{(\log m + \log(\log 2))^2}.$$

k	L	r	m	a_1	a_2	$\log_2 N_r$
184	21	2	73	-1	$2^{73} + 2^{54}$	87
184	21	2	75	-1	$2^{75} + 2^{58}$	87
184	21	2	77	-1	$2^{77} + 2^{62}$	87
202	99	0	75	-1	$2^{75} + 2^{49}$	99
202	99	0	77	-1	$2^{7} + 2^{53}$	99
202	99	0	79	-1	$2^{79} + 2^{57}$	99
202	99	0	81	-1	$2^{81} + 2^{61}$	99
202	99	0	83	-1	$2^{83} + 2^{65}$	99
208	11	3	77	-1	$2^{77} + 2^{50}$	95
208	11	3	79	-1	$2^{79} + 2^{54}$	95
208	11	3	81	-1	$2^{81} + 2^{58}$	95
208	11	3	83	-1	$2^{83} + 2^{62}$	95
254	125	0	85	-1	$2^{85} + 2^{43}$	125
254	125	0	87	-1	$2^{87} + 2^{47}$	125
254	125	0	89	-1	$2^{89} + 2^{51}$	125
254	125	0	91	-1	$2^{91} + 2^{55}$	125
254	125	0	93	-1	$2^{93} + 2^{59}$	125
254	125	0	95	-1	$2^{95} + 2^{63}$	125
296	35	2	99	-1	$2^{99} + 2^{50}$	143
296	35	2	101	-1	$2^{101} + 2^{54}$	143
296	35	2	103	-1	$2^{103} + 2^{58}$	143
296	35	2	105	-1	$2^{105} + 2^{62}$	143

Table 2. Examples of parameters for families of curves over $\mathbb{F}_{2^m}$ with embedding degree $(\frac{\log\ q}{\log\log q})^2 < k < (\log q)^2$.

The curves whose embedding degree is $k < (\frac{\log\ q}{\log\log q})^2$ are susceptible to sub-exponential attacks should not be used in strict cryptographic applications such as Diffie-Hellman key exchange or El-Gamal encryption. However, they may still be considered for a pairing-based cryptographic protocols such as identity-based encryption, if we allow for less efficiency by increasing the size of q. Table 1 gives some examples of the parameters for various such curves over $\mathbb{F}_q$ yielding small embedding degrees $k = 8, 13, 16, 23, 26, 37, 46$. The family of curves presented in this paper also contains curves whose embedding degree is small enough for computations to be feasible, but large enough that the curves are not susceptible to sub-exponential attacks. Table 2 gives examples of such pairing-friendly curves.

6 New Embedding Degree

In [4], the author noted that the conventional embedding degree k is not the appropriate indicator of the embedding field size, as the actual size can be much smaller than presumed. 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. If $\Delta = \frac{m}{\gcd(\mathrm{ord}_N p, m)}$, then $\Delta = 1$ corresponds to k being an accurate indicator of group size, and $\Delta = m$ corresponds to k being the least accurate indicator of the group size. Since the actual embedding field is $\mathbb{F}^*_{p^{\mathrm{ord}_N p}} = \mathbb{F}_{p^{kd}}$, where $d = \gcd(\mathrm{ord}_N p, m)$, then an attack will now be subexponential in q if $k < \frac{m(\log q)^2}{d(\log\log p^{\mathrm{ord}_N p})^2}$, that is, if $k < \Delta\frac{(\log q)^2}{(\log\log p^{\mathrm{ord}_N p})^2}$. So clearly more curves will be susceptible to sub-exponential attacks than previously anticipated.

Let us give a family of curves whose parameter $\Delta = m$. This family of curves is such that $\#J_C(\mathbb{F}_q)$ is divisible by a Mersenne prime N.

Proposition 4. *Let $q = 2^m$, and $p \geq 5$ 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 2 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 k is $k = p$ and the additional parameter is $\Delta = m$.*

We give the proof in the appendix. This family of curves demonstrates a case when the conventional embedding degree k is an inaccurate assessment of security, in fact, the most inaccurate possible. That is, pairings on this group embed into $\mathbb{F}^*_{2^p}$, not merely into $\mathbb{F}^*_{q^k} = \mathbb{F}^*_{2^{mp}}$.

So now we examine the additional security parameter Δ for the families of genus 2 curves corresponding to the prime N_r's given in Theorem 2. As we mentioned, it is desirable for Δ to be near 1, and far from m. We find Δ is often close to 1, and is at most $m/4$ for the curves with $k < (\frac{\log q}{\log\log q})^2$ in Table 1, so there is minimal discrepancy. However, for the curves in Table 2, we find that $\Delta = m$, so there is a difference in field exponent by a factor of m.

7 Concluding Remarks

Hyperelliptic curves are receiving increased attention for use in cryptosystems, which involves searching for pairing-friendly curves. We have given 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 their corresponding small embedding degrees. In particular we gave examples of the parameters for such curves with (conventional) embedding degree $k < (\frac{\log q}{\log\log q})^2$, such as $k = 8, 13, 16, 23, 26, 37, 46$, and for curves with $(\frac{\log q}{\log\log q})^2 < k < (\log q)^2$. A 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.

The curves whose embedding degree is $k < (\frac{\log q}{\log\log q})^2$ are susceptible to subexponential attacks should not be used in strict cryptographic applications such as Diffie-Hellman key exchange or El-Gamal encryption. However, they may still be considered for a pairing-based cryptographic protocols such as identity-based encryption, if we allow for less efficiency by increasing the size of q. The family of curves presented in this paper also contains curves whose embedding degree is small enough for computations to be feasible, but large enough that the curves are not susceptible to known sub-exponential attacks.

We noted the occurrences when the actual embedding field is smaller than the embedding field presumed by the conventional definition of embedding degree k. We gave an example of a family of curves for which this difference is maximal, that is, when the field exponent differs by a factor of m, demonstrating the weakness in the current definition of embedding degree.

Acknowledgments

I am grateful to Felipe Voloch for his supervision, and to Tanja Lange for her valuable suggestions and encouragement in this work. I would also like to thank Michael Naehrig and Peter Birkner for their comments.

References

1. Peter Birkner. Efficient divisor class halving on genus two curves. Cryptology ePrint Archive, Report 2006/257, 2006. http://eprint.iacr.org/.
2. S. Galbraith, J. McKee, and P. Valença. Ordinary abelian varieties having small embedding degree. Cryptology ePrint Archive, Report 2004/365, 2004. Available from http://eprint.iacr.org/2004/365.
3. Steven D. Galbraith. Supersingular curves in cryptography. In *Advances in cryptology—ASIACRYPT 2001 (Gold Coast)*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 495–513. Springer, Berlin, 2001.
4. Laura Hitt. On an improved definition of embedding degree. Cryptology ePrint Archive, Report 2006/415, 2006. http://eprint.iacr.org/.
5. A. Joux, R. Lercier, N. Smart, and F. Vercauteren. The Number Field Sieve in the Medium Prime Case. In C. Dwork, editor, *Advances in Cryptology - CRYPTO 2006. 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*, pages 326–344. Springer Berlin / Heidelberg, August 2006.
6. Brian 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 Comput. Sci.*, pages 333–345. Springer, Berlin, 2004.
7. Tanja Lange and Marc Stevens. Efficient doubling on genus two curves over binary fields. In *Selected areas in cryptography*, volume 3357 of *Lecture Notes in Comput. Sci.*, pages 170–181. Springer, Berlin, 2005.
8. Daniel Maisner and Enric Nart. Abelian surfaces over finite fields as Jacobians. *Experiment. Math.*, 11(3):321–337, 2002. With an appendix by Everett W. Howe.
9. Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

10. Hans-Georg Rück. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Math.*, 76(3):351–366, 1990.

A Proof of Proposition 1

We give the proof of Proposition 1, which establishes the existence of genus 2 curves with specific conditions on (a_1, a_2). Theorem 2 showed that the Jacobian of each of these curves is divisible by the prime $N_r = \frac{2^{2^r(L+2)}+1}{2^{2^r}+1}$, for odd $L > 1$ and $r \geq 0$.

Proof. Clearly a_1 is odd and $|a_1| \leq 4\sqrt{q}$.

Let us show $2|a_1|\sqrt{q} - 2q \leq a_2 \leq a_1^2/4 + 2q$. Clearly the first case (when $a_1 = 1$ and $a_2 = -q$ for $m = \frac{L+1}{2} + 1 \geq 5$) giving $2\sqrt{q} - 2q \leq -q \leq 1/4 + 2q$ is true. Now consider the second case (when $a_1 = -1$, and $a_2 = 2^m + 2^{2m-2^r(L+2)}$):

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

$$\iff 2^{m/2+1} - 2^{m+1} \leq 2^m + 2^{2m-2^r(L+2)} \leq 1/4 + 2^{m+1}.$$

Clearly the first inequality holds. The second inequality holds if and only if $2^{2m-2^r(L+2)} \leq 2^m$, which holds if and only if $m \leq 2^r(L+2)$. 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:

$$2^{\lceil m/2 \rceil} \mid 2^m + 2^{2m-2^r(L+2)}$$

$$\iff 2m - 2^r(L+2) \geq \lceil m/2 \rceil$$

$$\iff \lfloor 3m/2 \rfloor \geq 2^r(L+2)$$

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

Thus the condition holds.

Now we show $\varDelta = a_1^2 - 4a_2 + 8q$ is not a square in $\mathbb{Z}$. The first case yields $\varDelta = 1 + 3 \cdot 2^{m+2}$. Suppose $\varDelta = 1 + 3 \cdot 2^{m+2} = x^2$ for some integer x. Since $1 + 3 \cdot 2^{m+2}$ is odd, then x is odd, so let $x = 2k+1$ for some integer k. Then $\varDelta$ is a square if and only if $3 \cdot 2^m = k(k+1)$. Now, either k or $k+1$ is odd. If $k = 3$, then $k+1 = 4 = 2^m$, so $m = 2$. If $k+1 = 3$, then $k = 2 = 2^m$, so $m = 1$. Thus $\varDelta$ is not a square in $\mathbb{Z}$ for $m \geq 3$. The second case yields $\varDelta = 2^{2(m+1-2^{r-1}(L+2))}(2^{2^r(L+2)-m} - 1) + 1$. For contradiction, suppose $\varDelta = 2^{2(m+1-2^{r-1}(L+2))}(2^{2^r(L+2)-m} - 1) + 1 = x^2$ for some integer x. Since $\varDelta$ is odd, then x is odd, so let $x = 2k+1$ for some integer k. Then $\varDelta$ is a square if and only if $2^{2m-2^r(L+2)}(2^{2^r(L+2)-m} - 1) = k(k+1)$. That is, if and only if $2^{2m-2^r(L+2)}$ and $(2^{2^r(L+2)-m} - 1)$ differ by one. But such powers of two can never be this close, so $\varDelta$ 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 $m \geq 5$.
Now consider the second case:

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

$$= (2^m + 2^{2m-2^r(L+2)})^2 + 2^{m+2}(2^m + 2^{2m-2^r(L+2)}) + 2^{2m+2} - 2^{m+2}$$

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

$$= 2^{m+2}(2^{m+1} + 2^{m-2} + 2^{2m-2^r(L+2)} + 2^{2m-2^r(L+2)-1} + 2^{3m-2^r(L+2)-2} - 1)$$

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

For $m \geq 5$, we have

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

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

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

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

$$\Rightarrow m = \frac{3 + 2^{r+1}(L+2)}{3}$$

But $L+2$ is prime, so $m = \frac{3+2^{r+1}(L+2)}{3} \notin \mathbb{Z}$. This is a contradiction, so $b \not\equiv 1 \bmod 8$. Thus δ is not a square in $\mathbb{Z}_2$.

Therefore the 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.

□

B Proof of Proposition 3

We give the proof of Proposition 3, which determines which curves have embedding degree small enough that the curve may be susceptible to attacks that are subexponential in q.

Proof. First let $r = 0$ and $m = \frac{L+3}{2}$. Then by Lemma 5, $k = 2^{1-i}(L+2)$, where $\gcd(2(L+2), m) = 2^i$, $i = 0, 1$. Suppose $i = 0$, that is, m is odd. Then

$$k < (\frac{\log\ q}{\log\log q})^2 \Leftrightarrow 2(L+2) < \frac{m^2(\log 2)^2}{(\log m + \log(\log 2))^2}$$

$$\Leftrightarrow (L+2) < \frac{(L+3)^2(\log 2)^2}{8(\log(L+3) - \log 2 + \log(\log 2))^2}.$$

This holds true for $L \geq 405$, that is, for $m \geq 205$.
Now suppose $i = 1$, that is, m is even. Then

$$k < (\frac{\log\ q}{\log\log q})^2 \Leftrightarrow 2(L+2) < \frac{m^2(\log 2)^2}{(\log m + \log(\log 2))^2}$$

$$\Leftrightarrow (L+2) < \frac{(L+3)^2(\log 2)^2}{4(\log(L+3) - \log 2 + \log(\log 2))^2}.$$

This holds true for $L \geq 107$, that is, for $m \geq 56$.
Now let $r \geq 0$ and $\lceil \frac{2^{r+1}(L+2)}{3} \rceil \leq m \leq 2^r(L+1) - 1$ and suppose $(L+2)|m$. We see that if $(L+2)|m$ then $r \neq 0$ for m in this interval. Suppose $r \geq 2$. By Lemma 5, $k = 2^{r+1-i}$, where $\gcd(2^{r+1}(L+2), m) = 2^i(L+2)$ for $i \in \{0, 1, \ldots, r-2\}$. It suffices to show $k < (\frac{\log\ q}{\log\log q})^2$ for the smallest m in this interval, so we suppose $m = (L+2)$.

$$k < (\frac{\log\ q}{\log\log q})^2 \Leftrightarrow 2^{r+1} < \frac{(L+2)^2(\log 2)^2}{(\log(L+2) + \log(\log 2))^2}.$$

For $r = 2$, this holds for $L \geq 5$, for $r = 3$, this holds for $L \geq 11$.

□

C Proof of Proposition 4

We give a proof of Proposition 4, which establishes the existence of a family of curves whose Jacobian is divisible by a Mersenne prime. The proposition also determines the embedding degree and measures the discrepancy between the size of the actual and presumed embedding fields.

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.

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

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

$$\iff m \geq \lceil \frac{2p}{3} \rceil$$

Thus the condition holds.

Now let us show $\mathit{\Delta} = a_1^2 - 4a_2 + 8q$ is not a square in $\mathbb{Z}$.
For contradiction, suppose $\mathit{\Delta} = 1-2^{m+2}+2^{2m-p+2}+2^{m+3} = 1+2^{2m-p+2}+2^{m+2} = x^2$ for some integer x. Since $\mathit{\Delta}$ is odd, then x is odd, so let $x = 2n+1$ for some integer n. Then $\mathit{\Delta}$ 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 $\mathit{\Delta}$ 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 additional security parameter is $d = \frac{m}{\gcd(\mathrm{ord}_N 2, m)} = m$. Thus the proof of the proposition is complete.

□