On the Minimal Embedding Field

Laura Hitt

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

Abstract. We discuss the underlying mathematics that causes the embedding degree of a curve of any genus to not necessarily correspond to the minimal embedding field, and hence why it may fail to capture the security of a pairing-based cryptosystem. Let C be a curve of genus g defined over a finite field $\mathbb{F}_q$, where $q = p^m$ for a prime p. The Jacobian of the curve is an abelian variety, $J_C(\mathbb{F}_q)$, of dimension g defined over $\mathbb{F}_q$. For some prime N, coprime to p, the embedding degree of $J_C(\mathbb{F}_q)[N]$ is defined to be the smallest positive integer k such that N divides $q^k - 1$. Hence, $\mathbb{F}^*_{q^k}$ contains a subgroup of order N. To determine the security level of a pairing-based cryptosystem, it is important to know the minimal field containing the Nth roots of unity, since the discrete logarithm problem can be transported from the curve to this field, where one can perform index calculus. We show that it is possible to have a dramatic (unbounded) difference between the size of the field given by the embedding degree, $\mathbb{F}_{p^{mk}}$, and the minimal embedding field that contains the Nth roots of unity, $\mathbb{F}_{p^d}$, where $d \mid mk$.
The embedding degree has utility as it indicates the field one must work over to compute the pairing, while a security parameter should indicate the minimal field containing the embedding. We discuss a way of measuring the difference between the size of the two fields and we advocate the use of two separate parameters. We offer a possible security parameter, $k' = \frac{\mathrm{ord}_N p}{g}$, and we present examples of elliptic curves and genus 2 curves which highlight the difference between them. While our observation provides a proper theoretical understanding of minimal embedding fields in pairing-based cryptography, it is unlikely to affect curves used in practice, as a discrepancy may only occur when q is non-prime. Nevertheless, it is an important point to keep in mind and a motivation to recognize two separate parameters when describing a pairing-based cryptosystem.

Keywords: pairing-based cryptosystems, embedding degree, discrete logarithm, elliptic curve cryptography, security.

1 Introduction

The use of elliptic curves over finite fields in public-key cryptography provides greater security and more efficient performance than first generation public key techniques, such as RSA and Diffie-Hellman. Hyperelliptic curves of small genus (that is, the associated Jacobian abelian varieties with low dimension) are also believed to 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 (DLP) 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.

Galbraith in [2] notes that for a genus g curve, k/g is a more accurate indicator of the security, as it reflects the applicability of sub-exponential algorithms for solving the DLP in the finite field. Rubin and Silverberg in [7] also recognize that there may be a difference between the size of the field $\mathbb{F}_{q^k}$ and the actual embedding field for supersingular abelian varieties. They show that for supersingular abelian varieties, the difference in the size of the exponent can be at most a factor of two.

Our observation is not limited to the supersingular case and explains that the difference in the fields is related to the order of the characteristic modulo the prime N, not merely on the dimension of the variety. We see that for curves of any genus, the difference in the size of the exponent can be unbounded. Our observation only impacts non-prime fields of small characteristic.

The possible dramatic difference in the size of the fields has the implication in theory that there could be curves used in DL systems that are presently regarded as secure against pairing-based attacks, but are in fact insecure. That is, there could be "pairing-friendly" curves that may not be as secure as previously believed. However, although the literature is lacking a proper discussion of this minimal embedding field issue, it seems that in practice these curves in low characteristic are already avoided or work is done over prime fields.

In section 2, we give a preliminary framework and examine the bounds on k for pairing-based attacks to be sub-exponential in q. In section 3, we discuss the underlying mathematics that causes the embedding degree of a curve to not necessarily correspond to the minimal embedding field, and hence why it may fail to capture the security of a pairing-based cryptosystem. We show that for a curve of any genus defined over $\mathbb{F}_q$, the pairing in a group of order N embeds in a field that is not necessarily an extension of $\mathbb{F}_q$, but merely of $\mathbb{F}_p$ (where $q = p^m$). In particular, the embedding field is $\mathbb{F}_{p^{\mathrm{ord}_N p}}$. We measure the difference in size of the field exponents, finding that it grows with m. We advocate the use of two separate parameters: an embedding degree to indicate the field one must work over to compute the pairing, and a security parameter, such as $k' = \frac{\mathrm{ord}_N p}{g}$, to indicate the field containing the embedding. We then examine the bounds for attacks to be sub-exponential in the group size of the curve in light of this understanding of the minimal embedding field. Finally, in section 4, we give examples of curves that demonstrate when the embedding degree k does not correspond to the minimal embedding field and hence is a poor assessment of security. Although these curves have not been chosen for practical implementation, we hope that, for mathematical completeness, subsequent literature will acknowledge the possible difference between the field suggested by embedding degree and the actual minimal embedding field.

2 Preliminaries

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ for some prime p and positive integer m, and let C be a curve over $\mathbb{F}_q$. The Jacobian of the curve is an abelian variety, J_C, of dimension g defined over $\mathbb{F}_q$. Assume there exists a prime N dividing the order of $J_C(\mathbb{F}_q)$. 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

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

$\mathbb{F}_{q^k}^*/\mathbb{F}_{q^k}^{*N}$ 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. We know that $k \leq 6$ for supersingular elliptic curves, as first shown in [5], and [2] gives an upper bound of 12 on k for supersingular genus 2 curves. However, for most non-supersingular curves, k is enormous.

We should note the bound on the size of the embedding field for the attack to be sub-exponential. The latest results, in [4], 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 $k \in o((\frac{\log\ q}{\log\log q})^2)$. Galbraith in [2] noted that the size of the group $J_C(\mathbb{F}_q)$ is approximately q^g, so to determine the applicability of the sub-exponential algorithms for solving the DLP in finite fields, one should actually consider k/g.

3 An Examination of the Embedding Degree

Given a subgroup of order N of a curve over $\mathbb{F}_q$, the standard definition of the embedding degree k is that k is the smallest integer such that $N \mid q^k - 1$. Since the MOV attack first used pairings to transport the discrete log problem on the curve to the discrete log problem in $\mathbb{F}^*_{q^k}$, where one can perform index calculus, the security of a cryptosystem has been assumed to be related to the size of this parameter k.

However, we point out that to properly determine the security level of a pairing-based cryptosystem, it is important to know the minimal field containing the Nth roots of unity and to incorporate this exponent as a security parameter. If $q = p^m$, then the pairings embed into μ_N which lies in $\mathbb{F}^*_{p^{\mathrm{ord}_N p}}$, not merely in $\mathbb{F}^*_{q^k}$. That is, the embedding is into the multiplicative group of an extension of $\mathbb{F}_p$, which is not necessarily an extension of $\mathbb{F}_q$. This difference in the size of the groups can be quite large, by as much as a factor of m.

Let us examine the present definition embedding degree with respect to a general prime N over $\mathbb{F}_q$. We let $\mathrm{ord}_N p$ be the smallest x such that $p^x \equiv 1 \bmod N$.

Lemma 1. *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*

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

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

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

Now let $D = \gcd(\mathrm{ord}_N p, m)$. So 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.

□

Since μ_N lies in $\mathbb{F}^*_{p^{\mathrm{ord}_N p}}$, it is apparent that the embedding field is not $\mathbb{F}_{q^k} = \mathbb{F}_{p^{km}}$, but $\mathbb{F}_{p^{\mathrm{ord}_N p}} = \mathbb{F}_{p^{kD}}$, where $D = \gcd(\mathrm{ord}_N p, m)$. So it is possible for the size of the actual and presumed embedding fields to differ by a factor of m.

The following field diagram helps to illustrate the difference in these fields of discussion.

$$\begin{tikzcd}
 & \mathbb{F}_{q^k} \text{ presumed embedding field} \\
\mathbb{F}_q \arrow[ur, dash, "k"] \arrow[dd, dash, "m"'] & \\
 & \mathbb{F}_{p^{kD}} \text{ minimal embedding field, } D = \gcd(\mathrm{ord}_N p, m) \arrow[uu, dash, "\geq 1"'] \\
\mathbb{F}_p \arrow[ur, dash, "\mathrm{ord}_N p"'] &
\end{tikzcd}$$

We note that it is possible for this gap to be as large as one dictates, simply by increasing the exponent m prime to $\mathrm{ord}_N p$.

We see that the term "embedding degree" is a bit of a misnomer, as the minimal embedding field is not necessarily the one indicated by the embedding degree. We suggest a separate parameter be used to indicate security against solving the DLP in the finite field, such as $k' = \frac{\mathrm{ord}_N p}{g}$. Whenever q is prime, then there is no difference between presumed and actual minimal embedding field sizes, so in that case we have $k = g \cdot k'$.

To examine the potential difference between the size of the minimal field that contains the embedding and the one under the conventional notion of embedding degree, let $q = p^m$ with $m \neq 1$, and let us consider $[\mathbb{F}_{q^k} : \mathbb{F}_{p^{\mathrm{ord}_N p}}]$. That is, set $\Delta = \frac{m}{\gcd(\mathrm{ord}_N p, m)}$, so the size of Δ reveals the relative change in field size. We see that $\Delta = 1$ if and only if $\gcd(\mathrm{ord}_N p, m) = m$, which corresponds to k being an accurate indicator of the minimal embedding field. However, it is not unusual to have $\gcd(\mathrm{ord}_N p, m) = 1$, hence $\Delta = m$, showing k to be the least accurate indicator of the minimal embedding field.

Since the minimal embedding field is $\mathbb{F}_{p^{\mathrm{ord}_N p}} = \mathbb{F}_{p^{kD}}$, where $D = \gcd(\mathrm{ord}_N p, m)$, we see that an attack will now be sub-exponential in q if $k \in o(\frac{m(\log q)^2}{D(\log\log p^{\mathrm{ord}_N p})^2})$; that is, if $k \in o(\Delta \frac{(\log q)^2}{(\log\log p^{\mathrm{ord}_N p})^2})$. So clearly more curves will be susceptible to pairing attacks than previously anticipated.

4 Examples

Let us look at some examples of genus 1 and genus 2 curves that clearly emphasize this difference between the size of the minimal embedding field and the field suggested by the conventional notion of embedding degree. Since cryptographic applications usually focus on prime fields and binary fields, and this difference in the embedding field is only visible in the extension field case, we will give examples in characteristic 2. Although these curves have not been chosen for practical implementation, we hope subsequent literature will acknowledge the possibility of having a smaller embedding field in certain situations.

Example 1. Consider the Mersenne prime $N = 2^p - 1$, let $q = 2^{p+1}$. We know from [8] that there exists at least one ordinary elliptic curve over $\mathbb{F}_q$ with $|E(\mathbb{F}_q)| = 2N$. This curve has embedding degree $k = p$, so this would suggest that the embedding field is $\mathbb{F}_{q^k} = \mathbb{F}_{2^{p(p+1)}}$. But in fact, we see that $\gcd(\mathrm{ord}_N 2, p+1) = 1$, so the embedding field is $\mathbb{F}_{2^p}$, and these sizes differ by a factor of $\Delta = p + 1$. We note that in this case the "presumed" embedding field grows quadratically in p, but the actual minimal embedding field grows only linearly in p.

We note that Appendix A of [6], which develops standard specifications for public-key cryptography, states a condition that one needs only to test whether the embedding degree is larger than some small integer B, and the largest B stated is 28. So the curves in Example 1 could have been considered as secure for DL systems. However, in light of this paper's observations, we see that the resulting embedding field size is smaller than q, with embedding degree 1, so the DLP is easy to break.

Curves in Example 1 might be discarded since the field exponent is not prime and thus Weil descent attacks might apply. We now show how this example can be generalized and also works with more general exponents.

Example 2. Let $N = 2^p - 1$, and $q = 2^{p+s}$, for $1 \leq s \leq p+1,\ s \neq p$. Then for each s, there exists at least one non-supersingular elliptic curve over $\mathbb{F}_q$ with $|E(\mathbb{F}_q)| = 2^s N$. We emphasize that this allows for the extension degree to be prime. These curves have embedding degree $k = p$, which suggests that the embedding field is $\mathbb{F}_{q^k} = \mathbb{F}_{2^{p(p+s)}}$. But in fact, we see that $\gcd(\mathrm{ord}_N 2, p+1) = 1$, so the embedding field is $\mathbb{F}_{2^p}$, and these sizes differ by a factor of $\Delta = p + s$. Again, these curves could have been considered as secure for DL systems, but in light of this paper's observations, we see that the resulting field size is smaller than q, with embedding degree 1, so the DLP is easy to break.

Example 3. We can consider the Mersenne prime $N = 2^p - 1$ for genus 2 curves as well, as in [3]. We note that these examples have an absolutely simple Jacobian, so these curves are not merely the product of an elliptic curve from Example 2 and another elliptic curve. For each $\lceil \frac{2p}{3} \rceil \leq m \leq p-1$, there exists a genus 2 curve over $\mathbb{F}_{2^m}$ with $\#J_C(\mathbb{F}_{2^m}) = 2^{2m-p}N$. Each curve is given by the Weil polynomial with coefficients $(a_1, a_2) = (-1, 2^m - 2^{2m-p})$. These curves have embedding degree $k = p$, which suggests that the embedding field is $\mathbb{F}_{q^k} = \mathbb{F}_{2^{pm}}$, but in fact the embedding field is $\mathbb{F}_{2^p}$, since $\gcd(\mathrm{ord}_N 2, m) = 1$. One might previously have considered these curves as secure for DL systems, but we now see the DLP is easy to break.

This observation of the misleading notion of embedding degree has motivated us to check the accuracy of k as a security parameter in curve examples in the published literature. The following is an actually proposed system in [1] which is insecure due to the observations we have mentioned above.

Example 4 (from published literature). For embedding degree $k = 5$, the results of [1], give the family of genus 2 curves with ordinary Jacobian, where $q = l^2$, $a_1 = l-1$, and $a_2 = 2l^2 + 1$ for some integer l such that $q = p^m$. We see that for many choices of l, $\Delta = m$, which signals a most inaccurate embedding degree measure. So this is a "real-world" case in which the curve might have looked suitable for pairing-based systems but is not, revealing that the embedding degree is not always an accurate indicator of cryptographic security.

As we have mentioned, whenever working over $\mathbb{F}_q$, for q a prime, there is no discrepancy between the mathematical and cryptographic notions of embedding degree, but when q is a prime power there may be a significant difference. The techniques given in [1] are presented in general for prime powers q, although most of the curves examples they list are over a prime field, and hence escape the discrepancy. One should be cautious when using these techniques to generate curves, as certain parameters may yield a prime power q, and hence the curves could be insecure in light of our observation.

We now give two numerical examples taken from [3]. Though these curves are not used in practice, they serve to illustrate our observation.

Example 5. Consider the genus 2 curve over $\mathbb{F}_{2^{267}}$ given by the Weil polynomial with coefficients $(a_1, a_2) = (-1, 2^{267} + 2^{178})$. Then $\#J_C(\mathbb{F}_{2^{267}}) = 2^{178} \cdot 17 \cdot N$, where $N = \frac{2^{4(89)}+1}{17}$ is prime, and the embedding degree is $k = 8$. So we have a 351-bit DLP on the curve, and a 2136-bit DLP in $\mathbb{F}_{q^k}^*$, which is considered hard. However, in the minimal embedding field, we have only a 712-bit DLP, which is considered easy.

Example 6. Consider the genus 2 curve over $\mathbb{F}_{2^{136}}$ given by the Weil polynomial with coefficients $(a_1, a_2) = (-1, 2^{136} + 2^{124})$. Then $\#J_C(\mathbb{F}_{2^{136}}) = 2^{124} \cdot 17 \cdot N$, where $N = \frac{2^{4(37)}+1}{17}$ is prime, and the embedding degree is $k = 37$. So we have a 5032-bit DLP in $\mathbb{F}_{q^k}^*$, which is considered hard. However, in the minimal embedding field, we have only a 296-bit DLP, which is considered easy.

5 Conclusion

We have shown the underlying mathematics that causes the embedding degree of a curve of any genus to not necessarily correspond to the minimal embedding field, and hence why it may fail to capture the security of a pairing-based cryptosystem. The minimal embedding field is not $\mathbb{F}_{q^k} = \mathbb{F}_{p^{km}}$, but $\mathbb{F}_{p^{\mathrm{ord}_N p}} = \mathbb{F}_{p^{kD}}$, where $D = \gcd(\mathrm{ord}_N p, m)$. So it is possible for the size of the actual and presumed embedding fields to differ by a factor of m. Thus one can make this gap as large as one dictates, simply by increasing the field size q. The effect of our observation can be seen any time $q = p^m$ and $\gcd(\mathrm{ord}_N p, m) \neq m$.

We advocate the use of two separate parameters: the traditional embedding degree[1] k to indicate the field one must work over to compute the pairing, and a security parameter, $k' = \frac{\mathrm{ord}_N p}{g}$, to indicate the difficulty of solving the DLP in the finite field containing the embedding. In the case of prime fields, $k = g \cdot k'$, so the observation of this paper is not relevant to such cases.

The possible substantial difference in the size of the fields has the implication in theory that there could be curves used in DL systems that are presently regarded as secure against pairing-based attacks but are in fact insecure. That is, there could be "pairing-friendly" curves that may not be as secure as previously believed. However, although the literature is lacking a proper discussion of this minimal embedding field issue, it seems that in practice these curves in low characteristic are already avoided or work is done over prime fields. So while our observation provides a proper theoretical understanding, it is unlikely to affect curves used in practice. Nevertheless, it is an important point to keep in mind and a motivation to recognize two separate parameters when describing a pairing-based cryptosystem.

References

1. 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.
2. 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.
3. Laura Hitt. Families of genus 2 curves with small embedding degree. Cryptology ePrint Archive, Report 2007/001, 2007. http://eprint.iacr.org/.
4. 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.

[1] Although this can be a misleading name, we do not attempt to change it in order to avoid causing unnecessary confusion simply for the sake of theoretical accuracy.

5. 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.
6. IEEE P1363. *Standard Specifications for Public Key Cryptography.* IEEE, 2000.
7. Karl Rubin and Alice Silverberg. Supersingular abelian varieties in cryptology. In *Advances in cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Comput. Sci.*, pages 336–353. Springer, Berlin, 2002.
8. W. C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 53–64. Amer. Math. Soc., Providence, R.I., 1971.