On an Improved Definition of Embedding Degree

Laura Hitt

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

Abstract. We demonstrate a fundamental flaw in the present definition of embedding degree for curves of any genus, and we present examples of elliptic curves and genus 2 curves which highlight the error. We explain how this can yield a dramatic (unbounded) difference between the size of the actual and presumed embedding fields. This observation has serious implications for the security of pairing-based cryptosystems, as curves are no longer as secure as expected. We discuss the appropriate understanding of embedding degree, the bounds that yield sub-exponential attacks, and offer a way of measuring the discrepancy in security.

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

Rubin and Silverberg in [6] 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, and they propose a security parameter that depends on the dimension of the variety, that is, on the genus of the curve.

Our observation explains that there is a fundamental flaw in the conventional *definition* of embedding degree, and this can yield an unbounded difference in the size of the actual and presumed embedding fields. We show that this situation applies to curves of any genus, and whose associated group is not limited to the supersingular case. The observation is only relevant to small characteristic and not to prime fields.

This fact has the serious consequence that curves being used for DL systems may actually be insecure, as the the embedding field can be significantly smaller than the presently assumed field. Because of such a dramatic difference in the size of the embedding fields, the embedding degree k is the wrong parameter to be testing for security.

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 explain the error in the conventional definition of embedding degree, showing that for a curve defined over $\mathbb{F}_q$, the embedding field is not necessarily an extension of $\mathbb{F}_q$, but merely of $\mathbb{F}_p$ (where $q = p^m$). We then measure the discrepancy in the security of the embedding fields, finding that it grows with m. We examine the bounds for attacks to be sub-exponential in the group size of the curve in light of this understanding of the actual embedding field. Finally, in section 4, we give examples of curves that demonstrate when the current definition of k is a poor assessment of security.

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 $\mathbb{F}_q$. 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 $J_C(\mathbb{F}_q)$. 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

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

$\mathbb{F}^*_{q^k}/\mathbb{F}^{*N}_{q^k}$ 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. We know that $k \leq 6$ for supersingular elliptic curves, as first shown in [4], 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 [3], 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 $k \in o((\frac{\log q}{\log\log q})^2)$.[1] We will see in the next section that this parameter k is not the appropriate indicator of the embedding field size, and hence we will need to re-examine the bounds for which an attack can be sub-exponential in the group size of the curve.

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 $\mathbb{F}^*_{q^k}$, the security of a cryptosystem has been assumed to be related to the size of this parameter k.

However, if $q = p^m$, we point out that 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. So there may be curves used in DL systems that are presently regarded as secure against pairing-based attacks, but are in fact insecure, since the embedding field is much smaller than perceived.

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

[1] Thanks to Daniel J. Bernstein for pointing this out.

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

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

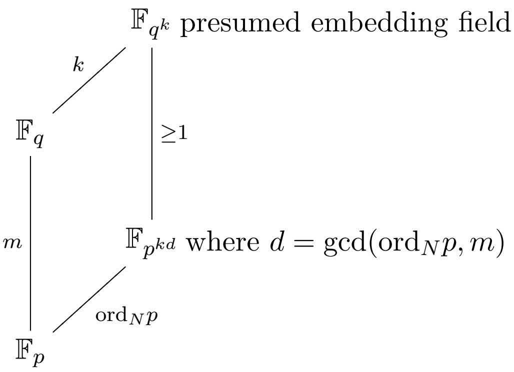
Now let $D = \gcd(\mathrm{ord}_N p, m)$. So we have $k \mid \frac{\mathrm{ord}_N p}{D}$.

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 $\mathbb{F}^*_{p^{\mathrm{ord}_N p}}$, we see 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 embedding fields.



We note that it is possible for this gap to be as large as one dictates, simply by increasing the exponent m prime to $\mathrm{ord}_N p$. Also, whenever q is prime, then there is no difference between presumed and actual embedding field sizes.

To examine the potential difference between the size of the group that actually 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 $\Delta = \frac{m}{\gcd(\mathrm{ord}_N p, m)}$, and let Δ be our additional security parameter, as the size of Δ reveals the relative change in group 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 group size. 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 group size.

Since the actual embedding field is $\mathbb{F}^*_{p^{\mathrm{ord}_N p}} = \mathbb{F}_{p^{kd}}$, where $d = \gcd(\mathrm{ord}_N p, m)$, we see that an attack will now be sub-exponential 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 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 actual embedding field and the field presumed from the conventional definition of embedding degree. Since cryptographic applications 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.

Example 1. Consider the Mersenne prime $N = 2^p - 1$, let $q = 2^{p+1}$. We know from [7] that there exists at least one ordinary elliptic curve over $\mathbb{F}_q$ with $|E(\mathbb{F}_q)| = 2N$. This curve has conventional embedding degree $k = p$, so it has been presumed 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 embedding field grows only linearly in p.

We note that Appendix A of [5], which develops standard specifications for public-key cryptography, states a condition that one needs only to test whether the embedding degree (under the conventional definition) is larger than some small integer B, and the largest B stated is 28. So the curves in Example 1 would be 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, as is desired in practice. These curves have conventional embedding degree $k = p$, so it has been presumed that the embedding field is $\mathbb{F}_{q^k} = \mathbb{F}_{2^{p(p+s)}}$. But in fact, we see that $\gcd(\text{ord}_N 2, p+1) = 1$, so the embedding field is $\mathbb{F}_{2^p}$, and these sizes differ by a factor of $\Delta = p + s$. Again, these curves could be 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. For each $\lceil \frac{2p}{3} \rceil \leq m \leq p-1$, there exists a genus 2 curve[2] 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 conventional embedding degree $k = p$, so the presumed embedding field is $\mathbb{F}_{q^k} = \mathbb{F}_{2^{pm}}$, but in fact the embedding field is $\mathbb{F}_{2^p}$, since $\gcd(\text{ord}_N 2, m) = 1$. 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 flaw in the conventional 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 flawed due to the wrong definition of embedding degree.

Example 4 (Real-World Example). 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, due to our observation of the flawed definition of embedding degree.

As we have mentioned, whenever working over $\mathbb{F}_q$, for q a prime, there is no discrepancy in the notion 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 the flawed definition of embedding degree.

5 Conclusion

We have shown that the embedding degree k is the wrong parameter to be testing for security, and that the currently used definition of embedding degree is incorrect

[2] These results are proven in another paper by the author, currently in preparation.

for curves of any genus. We discuss the accurate understanding of the embedding field, noting that any time $q = p^m$ and $\gcd(\text{ord}_N p, m) \neq m$, then the effect of this flawed definition of embedding degree manifests itself. We show that the size of the actual embedding field, $\mathbb{F}_{p^{\text{ord}_N p}}$, can differ by a factor of m from the presumed field $\mathbb{F}_{q^k}$. So it is possible to make this gap as large as one dictates, simply by increasing the field size q.

This has the serious consequence that curves being used for discrete logarithm systems may actually be insecure, as the DLP would be easier to solve in the actual (significantly smaller) embedding field than in the field gotten from the conventional embedding degree. This paper illuminates the fact that there can be "pairing-friendly" curves that may not be as secure as believed. We presented examples of elliptic curves and genus 2 curves which demonstrate the flawed definition of embedding degree, and we recommend that previously published curves be reviewed to see if their embedding degrees are inaccurate measures of security.

Acknowledgments

I am grateful to Felipe Voloch for his supervision, and to Tanja Lange for her valuable suggestions and encouragement in this work.

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. 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.
4. 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.
5. IEEE P1363. *Standard Specifications for Public Key Cryptography.* IEEE, 2000.
6. 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.
7. 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.