Minimal Embedding Field of Supersingular Curves

N.Benger[1] and M.Charlemagne[1⋆]

School of Computing,
Dublin City University,
Ireland.
{nbenger,mcharlemagne}@computing.dcu.ie

Abstract. For any elliptic curve E defined over a finite field $\mathbb{F}_q$, the embedding degree with respect to some prime divisor r of $\#E(\mathbb{F}_q)$ is defined to be the smallest, positive integer k, such that $r|q^k - 1$. For a supersingular curve defined over $\mathbb{F}_q$, where $q = p^m$, $p = 2$ or 3 and m a positive integer, k can be a maximum of 4 over fields of characteristic 2 and 6 over fields of characteristic 3.
It has been shown by L. Hitt in [3] that the minimal embedding field of a curve of genus 1 or 2 defined over a field $\mathbb{F}_q$ is not necessarily $\mathbb{F}_{q^k}$ but in fact $\mathbb{F}_{q^{ord_{rp/m}}} = \mathbb{F}_{p^{ord_{rp}}}$, a potentially much smaller field. This result could drastically reduce the security of pairing based systems, in which the elliptic curve discrete logarithm problem (ECDLP) on a curve defined over some field is mapped to the discrete logarithm problem (DLP) in the the minimal embedding field of said curve.
In this paper it will be shown that the supersingular curves can be chosen in such a way that the minimal embedding field is in fact $\mathbb{F}_{q^k}$ and that Hitt's result does not in fact apply to the optimal supersingular curve case.

1 Introduction

Pairing based cryptography is becoming an important research area, having many useful applications. When constructing a pairing based system, it is important that the elliptic curve discrete logarithm problem (ECDLP) and the discrete logarithm problem (DLP) in the corresponding finite field are equivalently hard. Until recently, it was believed that a pairing maps the ECDLP from a curve over $\mathbb{F}_q$, where $q = p^m$, p a prime and m a positive integer, to the DLP in $\mathbb{F}_{q^k}$ where k is the embedding degree of the curve. It has been shown by Hitt in [3] that the minimal embedding field of a curve is not necessarily $\mathbb{F}_{q^k}$ but in fact $\mathbb{F}_{q^{ord_{rp/m}}} = \mathbb{F}_{p^{ord_{rp}}}$. This has large security implications for pairing based systems as the DLP is more efficiently computed in the smaller field and hence the security of the ECDLP and the DLP in such a case would not be equivalently hard. Hitt's result does not apply to curves over prime fields, but

⋆ These authors acknowledge support from the Science Foundation Ireland under Grant No. 07/RFP/CMSF428

extension fields of fields with small characteristic. The (genus 1) pairing friendly curves over fields of characteristic 2 and 3 are supersingular curves. Other non-supersingular, pairing friendly curves over such fields may exist, however there is currently no known construction for such curves and supersingular curves have the advantage of distortion maps (see [2] for more information). In this paper it will be shown that the minimal embedding field for a supersingular curve with ρ-value $(\log p/\log r)$ 1 is in fact $\mathbb{F}_{q^k}$ and that Hitt's lemma has no effect on the most used curves in pairing based cryptography.

2 Notation

Throughout the paper, the following notation will remain consistent: r will be a prime divisor of N, the number of points on an Elliptic curve. The embedding degree k will be with respect to r. The field characteristic will be denoted p, which will be equal to 2 or 3 throughout this paper and m is a positive integer. As this paper will only be concerned with curves of genus 1, this will no longer be specified.

3 Hitt's Lemma

The following lemma is a result from [3].

Lemma 31 *Let $q = p^m$, for p a prime and m a positive integer. For some prime $r \neq p$ and k the smallest positive integer such that $q^k \equiv 1 \mod r$, k is given by:*

$$k = \frac{ord_r p}{\gcd(ord_r p, m)},$$

where $ord_r p = x > 0 \in \mathbb{Z}$ such that $p^x \equiv 1 \mod r$ and x minimal. It suffices to have $k' \in \mathbb{Q}$, that is, have k' such that $r|q^{k'} - 1$ and $k' = \frac{ord_r p}{m}$. The minimal embedding field given by $\mathbb{F}_{q^{k'}}$.

The result of this lemma is that the minimal embedding field of a curve over $\mathbb{F}_q$ is $\mathbb{F}_{p^{kD}}$, where $D = \gcd(ord_r p, m)$ and not $\mathbb{F}_{p^{km}}$ as previously believed.

4 Effect of Hitt's Lemma

In the case of pairing friendly curves over fields of prime characteristic p for $p \neq 2, 3$ Hitt's lemma has no baring. Over fields of characteristic 2 and 3 however, this is not the case. Pairing friendly elliptic curves are usually chosen to be over prime fields or over fields of characteristic 2 or 3. As Hitt's lemma has no effect on the curves over prime fields, it is therefore only the pairing friendly elliptic curves over fields of characteristic 2 and 3 that are of concern, that is, the supersingular curves. Supersingular curves were the first curves to be recognised as pairing friendly and can achieve embedding degrees $k \in \{1, 2, 3, 4, 6\}$, obtaining maximum embedding degrees of $k = 4$ over $\mathbb{F}_{2^m}$ and $k = 6$ over $\mathbb{F}_{3^m}$.

When assessing the effect of Hitt's lemma, it is easy to see that if $\gcd(ord_r p, m) = D = m$ then $\mathbb{F}_{p^{kD}} = \mathbb{F}_{p^{km}} = \mathbb{F}_{q^k}$, thus $\mathbb{F}_{q^k}$ is the minimal embedding field for a certain curve when $D = m$. In this case Hitt's lemma has no impact on the previously believed size of the minimal embedding field and the security of the pairing based system is not effected.

4.1 Optimal Cases: $p = 2$, $k = 4$ and $p = 3$, $k = 6$.

In order to optimise implementation of a pairing based protocol, when using a supersingular curve, the curve is chosen to have the maximal embedding degree. That is, a supersingular curve over $\mathbb{F}_{2^m}$ with embedding degree $k = 4$ or over $\mathbb{F}_{3^m}$ with embedding degree $k = 6$. For any such supersingular curve, the number of points on the curve is $N = p^m \pm p^{(m+1)/2} + 1$. [2]

Lemma 41 *A supersingular curve over $\mathbb{F}_{p^m}$ with optimal embedding degree (that is, for $p = 2$, $k = 4$ and $p = 3$, $k = 6$) has minimal embedding field $\mathbb{F}_{p^{km}}$.*

Proof. The number of points on such a supersingular curve is $N = p^m \pm p^{(m+1)/2} + 1$. For r a large prime divisor of N: $p^m = \mp p^{(m+1)/2} + 1 \mod r$ and $p^{pm} \equiv -1 \mod r$. Hence $p^{2pm} \equiv 1 \mod r$ thus $ord_r p = 2pm$. Given $ord_r p = 2pm$, $D = \gcd(ord_r p, m) = m$ holds true thus the minimal embedding field is $\mathbb{F}_{p^{km}}$.

For every supersingular curve with optimal embedding degree, Hitt's lemma does not hold. The minimal embedding field is still $\mathbb{F}_{p^{km}}$.

4.2 Other Embedding Degrees

For some implementations, a different embedding degree from the optimal case may be desired.

- If $k = 1$, The number of points on a supersingular curve over $\mathbb{F}_{p^m}$ with embedding degree 1 is given by $N = p^m \pm 2p^{m/2} + 1$. [2] In the case of embedding degree $k = 1$, m is even (which makes the DLP in the field $\mathbb{F}_{p^{km}}$ more vulnerable to other attacks which will not be discussed in this paper and hence less secure).
- If $k = 2$ The case of supersingular curves with embedding degree $k = 2$ is a little more complicated than the cases $k = 1$ and $k = 3$ as the number of points on the curve is not always the same. Three cases will be considered [1]:
  1. $N = p^m + 1$,
  2. if m is odd then $N = p^m \pm p^{\frac{m+1}{2}} + 1$,
  3. if m is even two subcases need to be considered:
     - $N = p^m \pm p^{\frac{m}{2}} + 1$
     - $N = p^m \pm 2p^{\frac{m}{2}} + 1$
- If $k = 3$ From [2], a supersingular curve over $\mathbb{F}_{p^m}$ with prime order and embedding degree $k = 3$ exists $\Leftrightarrow$ m is even and the number of points on the curve is $N = p^m \pm p^{m/2} + 1$.

By inspection, the proof of lemma 41 also covers the case $k = 2$ and m odd, thus for a supersingular curve with embedding degree 2 and odd m, the minimal embedding field is also $\mathbb{F}_{p^{km}}$. The following lemmas distinguish between the other cases.

Lemma 42 *If the number of points on a supersingular curve over $\mathbb{F}_{p^m}$ is given by $N = p^m + 1$ then the minimal embedding field is $\mathbb{F}_{p^{km}}$.*

Proof. As r divides N, $p^m \equiv -1 \mod r$. Hence $ord_r p = 2m$, giving $D = \gcd(ord_r p, m) = m$.

For a supersingular curve with embedding degree 2 and $N = p^m + 1$ points, the minimal embedding field is in fact still $\mathbb{F}_{p^{km}}$.

Lemma 43 *If the number of points on a supersingular curve over $\mathbb{F}_{p^m}$ is given by $N = p^m + 2p^{m/2} + 1$ then the minimal embedding field is $\mathbb{F}_{p^{km}}$.*

Proof. As r divides N, $p^m + 2p^{m/2} + 1 \equiv (p^{m/2} + 1)^2 \equiv 0 \mod r$. Thus $p^{m/2} \equiv -1 \mod r$ and $p^m \equiv 1 \mod r$, hence $D = \gcd(ord_r p, m) = m$ and the minimal embedding field is $\mathbb{F}_{p^{km}}$.

This lemma covers some curves with $k = 1$ and some curves with $k = 2$ and m even. For $k = 1$, or $k = 2$ and even m, and $N = p^m - 2p^{m/2} + 1$, $D = \gcd(ord_r p, m) \leq \frac{m}{2}$ by a similar proof, thus Hitt's lemma holds in this case. Here the minimal embedding field is smaller than previously believed.

Lemma 44 *If the number of points on a supersingular curve over $\mathbb{F}_{p^m}$ is given by $N = p^m - p^{m/2} + 1$ then the minimal embedding field is $\mathbb{F}_{p^{km}}$.*

Proof. As r divides N, $p^m \equiv p^{m/2} - 1 \mod r$. Hence $p^{2m} \equiv p^m - 2p^{m/2} + 1 \equiv -p^{m/2} \mod r$. Thus, $p^{2m-m/2} \equiv -1 \mod r$ and $p^{3m} \equiv 1 \mod r$ giving $ord_r p = 3m$ so $D = \gcd(ord_r p, m) = m$.

This lemma shows that some curves with embedding degree $k = 3$, or $k = 2$ and m even, and $N = p^m - 2p^{m/2} + 1$ have minimal embedding field $\mathbb{F}_{p^{km}}$. Similarly to the above case, for a curve with $N = p^m + p^{m/2} + 1$ points and the given embedding degrees, $D = \gcd(ord_r p, m) \leq \frac{m}{2}$ and so Hitt's lemma also holds.

To sum up the result, the cases which are effected by Hitt's lemma are:

- For $k = 1$ a supersingular curve with $N = p^m - 2p^{m/2} + 1$,
- For $k = 2$ and m even, a supersingular curve with $N = p^m - 2p^{m/2} + 1$ or $N = p^m + p^{m/2} + 1$,
- For $k = 3$ a supersingular curve with $N = p^m + p^{m/2} + 1$.

By observation, it is clear that if a particular curve is effected by Hitt's lemma, then the quadratic twist of the curve is not (if a curve has $N = p^m + t + 1$ points then the quadratic twist of the curve is the curve with $N = p^m - t + 1$ points).

5 conclusion

Hitt showed in [3], that the minimal embedding field of a genus 1 or 2 curve over $\mathbb{F}_{p^m}$ is not necessarily $\mathbb{F}_{p^{mk}}$ as previously believed but $\mathbb{F}_{p^{kD}}$ where $D = \gcd(ord_r p, m)$. As the second field could be significantly smaller than the first, this has large implications for the security of a pairing based system. In this paper it has been shown for the optimal cases for genus 1 pairing friendly curves over fields of characteristic 2 or 3, that is, supersingular curves with embedding degrees $k = 4$ or $k = 6$ respectively, that Hitt's result has no affect and that the minimal embedding field is in fact $\mathbb{F}_{p^{mk}}$. There are some cases in which Hitt's result does have an affect, but those cases can be avoided easily. Should a curve fall under Hitt's lemma, it has been shown that the quadratic twist of the curve does not. It is very easy to check the condition outlined by the cases above, so the cases effected by Hitt's lemma should be easily avoided.

6 Acknowledgments

The authors would like to thank Mike Scott for his encouragement, Laura Hitt and Gary McGuire for their helpful comments.

References

1. Henri Cohen and Gerhard Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC Press, 2005.
2. E. Teske D. Freeman, M. Scott. A taxonomy of pairing friendly elliptic curves. *Cryptology ePrint Archive, Report 2006/372*, 2006. http://eprint.iacr.org.
3. L. Hitt. On the minimal embedding field. *Pairing-Based Cryptography Pairings 2007*, LNCS(4575):294301, 2007.