On the security of pairing-friendly abelian varieties over non-prime fields

Naomi Benger[1], Manuel Charlemagne[1], and David Mandell Freeman[2]

[1] School of Computing, Dublin City University, Ireland
{nbenger,mcharlemagne}@computing.dcu.ie*
[2] CWI and Universiteit Leiden, Netherlands
freeman@cwi.nl**

Abstract. Let A be an abelian variety defined over a non-prime finite field $\mathbb{F}_q$ that has embedding degree k with respect to a subgroup of prime order r. In this paper we give explicit conditions on q, k, and r that imply that the minimal embedding field of A with respect to r is $\mathbb{F}_{q^k}$. When these conditions hold, the embedding degree k is a good measure of the security level of a pairing-based cryptosystem that uses A.
We apply our theorem to supersingular elliptic curves and to supersingular genus 2 curves, in each case computing a maximum ρ-value for which the minimal embedding field must be $\mathbb{F}_{q^k}$. Our results are in most cases stronger (i.e., give larger allowable ρ-values) than previously known results for supersingular varieties, and our theorem holds for general abelian varieties, not only supersingular ones.

1 Introduction

Suppose we wish to implement a pairing-based cryptosystem using the Weil or Tate pairing on an abelian variety A defined over a finite field $\mathbb{F}_q$ of q elements. For our implementation to be both efficient and secure, we need (1) the group $A(\mathbb{F}_q)$ to contain a subgroup of large prime order r, and (2) the group of rth roots of unity $\mu_r \subset \overline{\mathbb{F}}_q$ to be contained in an extension field $\mathbb{F}_{q^k}$ that is both large enough for the discrete logarithm problem in $\mathbb{F}_{q^k}^*$ to be computationally infeasible and small enough for the pairing to be computed efficiently. The degree k of this extension is known as the *embedding degree* of A (with respect to r).

The embedding degree of A is commonly used as a measure of the security level of our pairing-based cryptosystem. However, Hitt [7] observed that when the field size q is not prime, the rth roots of unity may be contained in a proper subfield $F \subset \mathbb{F}_{q^k}$. It follows that the security level is determined not by k but rather by the rational number $k' \leq k$ for which the smallest such field F has cardinality $q^{k'}$. Thus when given an abelian variety $A/\mathbb{F}_q$ with embedding degree

* Supported by Science Foundation Ireland under Grant No. 07/RFP/CMSF428
** Supported by a National Science Foundation International Research Fellowship, with additional support from the Office of Multidisciplinary Activities in the NSF Directorate for Mathematical and Physical Sciences.

k and q not prime, to determine the security level of cryptosystems using A one must check whether the smallest $F \subset \mathbb{F}_{q^k}$ containing μ_r — known as the *minimal embedding field* of A (with respect to r) — is in fact $\mathbb{F}_{q^k}$.

The purpose of this paper is to answer the following question: given an abelian variety $A/\mathbb{F}_q$ that has embedding degree k with respect to r, how can we guarantee that the minimal embedding field of A with respect to r is $\mathbb{F}_{q^k}$?

Rubin and Silverberg [13, 14] have given an answer to this question in the case where A is supersingular by demonstrating a lower bound on r that guarantees that the minimal embedding field is $\mathbb{F}_{q^k}$. Their bound depends on q and on the dimension g of the supersingular abelian variety, but does not depend on k.

The main result of this paper is to give explicit conditions on q, r, and k that guarantee that the minimal embedding field of an abelian variety $A/\mathbb{F}_q$ — supersingular or not — that has embedding degree k with respect to r is in fact $\mathbb{F}_{q^k}$. The conditions lead to a lower bound on r that depends on q and k, but not on the dimension g. When A is a supersingular elliptic curve or abelian surface, our bound improves on the result of Rubin and Silverberg in most of the cases relevant to cryptography. Our result thus guarantees more abelian varieties are suitable for use in pairing-based cryptography than any previous result had done.

Our main theorem appears in Section 2. In Section 3 we apply our main theorem to the case of supersingular elliptic curves, which are known to have embedding degree $k \in \{1, 2, 3, 4, 6\}$. We conclude that when k is even and either the group order r is sufficiently large or the extension degree m is prime, then the minimal embedding field is $\mathbb{F}_{q^k}$. In particular, we deduce that Hitt's observation has no effect in cryptographic contexts for supersingular elliptic curves in characteristic 2 or 3. When k is odd and r is sufficiently large then the minimal embedding field is either $\mathbb{F}_{q^k}$ or $\mathbb{F}_{q^{k/2}}$, depending on the sign of the trace of Frobenius.

Section 4 gives analogous results for some supersingular abelian varieties of dimension $g \geq 2$. Finally, in Section 5 we present some open problems related to this work.

2 A framework for analyzing the minimal embedding field

In this section we set up the framework for our analysis of the minimal embedding field of abelian varieties. After giving formal definitions, we discuss the results of Hitt [7] and Rubin and Silverberg [13], and then state our main theorem.

We first recall some standard terminology and notation. If K is a field then $\overline{K}$ denotes an algebraic closure of K. If q is a prime power then $\mathbb{F}_q$ denotes a field of q elements. An *abelian variety* is a smooth, projective, geometrically integral group variety. If A is an abelian variety defined over a field K, we denote by $A(K)$ the group of K-rational points of A. An *elliptic curve* is a one-dimensional abelian variety. An elliptic curve E over a field K of characteristic p is *supersingular* if $E(\overline{K})$ has no p-torsion points. A general abelian variety is supersingular if it

is isogenous (over $\overline{K}$) to a product of supersingular elliptic curves. An abelian variety A defined over K is *simple* if it is not isogenous over K to a product of lower-dimensional abelian varieties.

Definition 2.1. Let A be an abelian variety defined over $\mathbb{F}_q$, where $q = p^m$ for some prime p and integer m. Let $r \neq p$ be a prime dividing $\#A(\mathbb{F}_q)$. The *embedding degree of A with respect to r* is the smallest integer k such that r divides $q^k - 1$.

Definition 2.2. Let A, q, and r be as above. The *minimal embedding field of A with respect to r* is the smallest extension of $\mathbb{F}_p$ containing the rth roots of unity $\mu_r \subset \overline{\mathbb{F}}_p$.

If $A/\mathbb{F}_q$ has embedding degree k with respect to r, then $\mathbb{F}_{q^k}$ is the smallest extension of $\mathbb{F}_q$ containing the rth roots of unity. In particular, the r-Weil pairing ([15, §III.8] and [11, §16]) and the r-Tate pairing [2] take values in a subgroup and a quotient group of $\mathbb{F}_{q^k}^*$, respectively. The key observation made by Hitt [7] is that these pairings actually take values in the minimal embedding field and that this field may be a proper subfield of $\mathbb{F}_{q^k}$. Specifically, her main lemma is as follows:

Lemma 2.3 ([7, Lemma 1]). *Let $q = p^m$ for some prime p and positive integer m, let $r \neq p$ be a prime, and let k be the smallest integer such that r divides $q^k - 1$. Then*

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

where $\mathrm{ord}_r(p)$ is the order of p in $(\mathbb{Z}/r\mathbb{Z})^*$.

A result of this lemma is that the minimal embedding field of an abelian variety $A/\mathbb{F}_q$ is $\mathbb{F}_{q^{k'}}$, where $k' = \mathrm{ord}_r(p)/m \in \mathbb{Q}$, and not $\mathbb{F}_{q^k}$. Since the security of a pairing-based cryptosystem using A is determined by k', Hitt's result implies that such a cryptosystem could be significantly less secure than previously believed. Indeed, Hitt gives examples of abelian varieties where $k/k' = m$, which is the largest possible ratio for these parameters [7, §4]. It is important to note that when the abelian variety is defined over a prime field (i.e., when $m = 1$) Hitt's lemma has no effect, as the minimal embedding field is always $\mathbb{F}_{q^k}$.

A natural question following from Hitt's observation is in what cases the embedding degree k is an accurate indicator of security. More precisely, we have:

Question 2.4. Let A be an abelian variety over $\mathbb{F}_q$ that has embedding degree k with respect to r. Is the minimal embedding field of A with respect to r equal to $\mathbb{F}_{q^k}$?

Our goal is to give explicit conditions on q, r, and k such that the answer to Question 2.4 is yes.

In the case where $A/\mathbb{F}_q$ is supersingular and elementary (i.e., isogenous over $\mathbb{F}_q$ to a power of a simple abelian variety), Rubin and Silverberg have given conditions on q, r, and k that imply an affirmative answer to Question 2.4.

Their theorem is phrased in terms of the "cryptographic exponent" c_A, which is defined only for supersingular varieties. When A has embedding degree k with respect to a prime r and $r \nmid 2k$, the cryptographic exponent is the smallest half-integer c_A such that r divides $q^{c_A} - 1$. Thus c_A is equal to either k or $k/2$; the latter can only occur when q is a square and k is odd [14, Definition 4.1 and Theorem 6.1].

Theorem 2.5 ([13, Theorem 7] and [14, Theorem 6.3]). *Suppose A is an elementary supersingular abelian variety of dimension g over $\mathbb{F}_q$, $q = p^m$, $r \neq p$ is a prime divisor of $\#A(\mathbb{F}_q)$, and s is the multiplicative order of p mod r. Let $F_A(x) \in \mathbb{Z}[x]$ be the characteristic polynomial of Frobenius for A, and let f be the unique integer such that $F_A(x)^{1/f}$ is irreducible in $\mathbb{Z}[x]$. If q is a square, assume $r > (1+p)^{mg/2f}$. If q is not a square, assume $r > (1+\sqrt{p})^{2mg/3f}$ and $r > 7$. Then $p^s = q^{c_{A,q}}$, so $\mathbb{F}_{q^{c_{A,q}}}$ is the smallest extension of $\mathbb{F}_p$ whose multiplicative group has a subgroup of order r.*

We now turn our attention to proving our own bounds, which will apply to all abelian varieties, not just supersingular ones, and will improve on the bounds in Theorem 2.5 in many cases.

Our theorem depends crucially on some results about cyclotomic polynomials. For $k \in \mathbb{N}$, the *kth cyclotomic polynomial* $\Phi_k \in \mathbb{Z}[x]$ is the minimal polynomial of a primitive kth root of unity in $\overline{\mathbb{Q}}$. The following lemma demonstrates the relevance of these polynomials to our problem.

Lemma 2.6. *Let $q = p^m$ be a prime power, and $A/\mathbb{F}_q$ be an abelian variety. Let $r \neq p$ be a prime dividing $\#A(\mathbb{F}_q)$, and let k, s be integers not divisible by r. Then*

1. *A has embedding degree k with respect to r if and only if $r \mid \Phi_k(q)$.*
2. *The minimal embedding field of A with respect to r is $\mathbb{F}_{p^s}$ if and only if $r \mid \Phi_s(p)$.*

Proof. The first statement appears as [3, Proposition 2.4]; we observe that the same proof applies to the second statement. □

Lemma 2.6 allows us to rephrase Question 2.4 as follows: given that r divides $\Phi_k(p^m)$, does r divide $\Phi_{km}(p)$? To answer the question in this form we will use the following properties of cyclotomic polynomials, which appear in or can be easily derived from the discussion of [9, §VI.3].

Fact 2.7. Let $\Phi_k(x)$ denote the kth cyclotomic polynomial. Then

1. $x^k - 1 = \prod_{d \mid k} \Phi_d(x)$.
2. The degree of $\Phi_k(x)$ is $\varphi(k) := \#\{e \in \mathbb{Z} : 1 \leq e \leq k \text{ and } \gcd(e,k) = 1\}$.
3. If ℓ is a prime not dividing k, then $\Phi_k(x^\ell) = \Phi_{k\ell}(x)\Phi_k(x)$.
4. If ℓ is a prime dividing k, then $\Phi_k(x^\ell) = \Phi_{k\ell}(x)$.

We will also use the following lemma, an alternative proof of which can be found in [14, Lemma 5.2].

Lemma 2.8. *If k and m are coprime, then*

$$\Phi_k(x^m) = \prod_{d|m} \Phi_{kd}(x). \tag{2.1}$$

Proof. We first compare the degrees of the polynomials on each side of (2.1). Clearly the left hand side has degree $m\varphi(k)$. Now for any coprime numbers x and y we have $\varphi(xy) = \varphi(x)\varphi(y)$. Since $(k, m) = 1$ by assumption it is also true that $(k, d) = 1$ for all $d \mid m$. It follows that the degree of the right hand side of (2.1) is $\varphi(k) \sum_{d|m} \varphi(d)$, which by Fact 2.7 (1) and (2) is equal to $m\varphi(k)$.

We next compare the roots of the two polynomials. Suppose ζ is a root of $\Phi_{kd}(x)$ for some $d \mid m$. Since ζ is a primitive kdth root of unity, ζ^d is a primitive kth root of unity. Write $m = de$. Since $\gcd(k, e) = 1$, it follows that $(\zeta^d)^e = \zeta^m$ is also a primitive kth root of unity, so ζ is also a root of $\Phi_k(x^m)$.

Since the two polynomials in (2.1) are both monic and have the same degree, and furthermore all roots of the right hand side are also roots of the left hand side, we conclude that the two polynomials are equal. □

We are now prepared to give our main theorem, which we state as a fact about cyclotomic polynomials only, without reference to abelian varieties.

Theorem 2.9. *Let k be a positive integer, p^m a prime power, and r a prime. Write $m = \alpha\beta$, where every prime dividing α also divides k and $\gcd(k, \beta) = 1$. (This factorization is unique.) Denote by e the smallest prime factor of β. Suppose $r \mid \Phi_k(p^m)$ and that one of the following holds:*

1. *$m = \alpha$ (and $\beta = 1$);*
2. *β is prime and $r > \Phi_{k\alpha}(p)$;*
3. *$r > p^{km/e}$; or*
4. *$4 \mid m$ or $2 \mid k$ and $r > p^{km/2e} + 1$.*

Then $r \mid \Phi_{km}(p)$.

Proof. We first note that Fact 2.7 (4) implies

$$\Phi_k(p^m) = \Phi_{k\alpha}(p^\beta). \tag{2.2}$$

Since $k\alpha$ and β are coprime, Lemma 2.8 implies that $\Phi_k(p^m)$ has $\Phi_{km}(p)$ as a factor. Our strategy in each case is to show that the remaining factors of $\Phi_k(p^m)$ are all smaller than r. Since r is prime, it then follows that if r divides $\Phi_k(p^m)$ then r divides $\Phi_{km}(p)$.

We now consider each case separately:

1. Since $m = \alpha$ it follows immediately that $\Phi_k(p^m) = \Phi_{km}(p)$.
2. Since β is a prime not dividing $k\alpha$, equation (2.2) and Fact 2.7 (3) imply that
$$\Phi_k(p^m) = \Phi_{k\alpha\beta}(p)\Phi_{k\alpha}(p) = \Phi_{km}(p)\Phi_{k\alpha}(p).$$
Since $r > \Phi_{k\alpha}(p)$, it follows that $r \mid \Phi_{km}(p)$.

3. By equation (2.2) and Lemma 2.8 we have

$$\Phi_k(p^m) = \prod_{d|\beta} \Phi_{kd\alpha}(p) = \prod_{d|\beta} \Phi_{km/d}(p). \tag{2.3}$$

   By assumption we have $r > p^{km/d}$ for all $d \mid \beta$ except for $d = 1$, and by Fact 2.7 (1) we have $p^{km/d} > \Phi_{km/d}(p)$. It follows that $r \mid \Phi_{km}(p)$.
4. Given the factorization of $\Phi_k(p^m)$ as in (2.3), the same analysis as in Case 3 shows that $r > \Phi_{km/d}(p)$ for all $d \mid \beta$ with $d \geq 2e$. Since e is the smallest prime dividing β, if $d \mid \beta$ and $1 < d < 2e$ then d is prime, so it suffices to show that $r > \Phi_{km/d}(p)$ for all primes d dividing β. Let d be such a prime. The assumption $4 \mid m$ or $2 \mid k$ then implies that km/d is even. In this case we have $x^{km/d} - 1 = (x^{km/2d} + 1)(x^{km/2d} - 1)$, and by Fact 2.7 (1) $\Phi_{km/d}(x)$ must divide the first factor. Since $d \geq e$, if $r > p^{km/2e} + 1$ then $r > \Phi_{km/d}(p)$. □

Using Lemma 2.6 to interpret Theorem 2.9 in the context of abelian varieties, we obtain the following corollary:

Corollary 2.10. *Let A be an abelian variety over $\mathbb{F}_q$, where $q = p^m$ with p prime. Let $r \neq p$ be a prime dividing $\#A(\mathbb{F}_q)$, and suppose A has embedding degree k with respect to r. Assume that $r \nmid km$. If q, k, and r satisfy any of the conditions (1)–(4) of Theorem 2.9, then the minimal embedding field of A with respect to r is $\mathbb{F}_{p^{km}}$.*

We note that the case where m is prime, which is usually recommended for cryptographic applications in order to prevent Weil descent attacks (e.g., [6, 5]), falls into case (2) of Theorem 2.9. If p is small ($p = 2$ and $p = 3$ are common choices) and $k < m$ with m prime, then the bound on r given by the theorem is very weak; i.e., A will have minimal embedding field $\mathbb{F}_{p^{km}}$ with respect to any r that is even remotely close to cryptographic size.

Remark 2.11. If k is odd and m is even then $\Phi_k(x^m) = \Phi_k(x^{m/2})\Phi_{2k}(x^{m/2})$. Since $\varphi(k) = \varphi(2k)$ for odd k, these two factors have the same degree and we cannot use the above techniques to show that r divides $\Phi_{km}(p)$ and does not divide $\Phi_{km/2}(p)$. Applying Theorem 2.9 recursively to each factor allows us to determine conditions on q, k, and r guaranteeing that r divides one of the two expressions $\Phi_{km}(p)$ and $\Phi_{km/2}(p)$, but additional information is needed to determine which one. In the context of pairing-friendly curves, this situation rarely occurs as even embedding degrees are preferred as are prime values for m. However, see Propositions 3.6 and 3.8 below for some specific cases where it does occur.

3 Supersingular elliptic curves over non-prime fields

In this section we focus on supersingular elliptic curves, which are the most well known pairing-friendly abelian varieties defined over non-prime fields. If E is

an elliptic curve defined over the finite field $\mathbb{F}_q$, then the number of $\mathbb{F}_q$-rational points is given by $\#E(\mathbb{F}_q) = q + 1 - t$, where t is the trace of the q-power Frobenius endomorphism. A theorem of Hasse (the "Hasse-Weil bound") says that $|t| \leq 2\sqrt{q}$ [15, Theorem V.1.1]. An elliptic curve E is supersingular if and only if $\gcd(t, q) > 1$ [15, Ex. 5.10].

Menezes, Okamoto and Vanstone [10] gave a complete classification of supersingular elliptic curves over finite fields $\mathbb{F}_q$, with $q = p^m$. They showed that five possible embedding degrees k can occur, corresponding to five possible absolute values of the trace of Frobenius t:

k	t	$\#E(\mathbb{F}_q)$	p, m
1	$\pm 2\sqrt{q}$	$q \mp 2\sqrt{q} + 1$	any p, m even
2	0	$q + 1$	any p, any m
3	$\pm\sqrt{q}$	$q \mp \sqrt{q} + 1$	$p \equiv 2 \bmod 3$, m even
4	$\pm\sqrt{2q}$	$q \mp \sqrt{2q} + 1$	$p = 2$, m odd
6	$\pm\sqrt{3q}$	$q \mp \sqrt{3q} + 1$	$p = 3$, m odd

When comparing the sizes of r and q as in Theorem 2.5, it is useful to introduce a parameter ρ, which roughly approximates the ratio of the bit size of the entire group $A(\mathbb{F}_q)$ to the bit size of r.

Definition 3.1. Let A be a g-dimensional abelian variety over $\mathbb{F}_q$, and suppose r divides $\#A(\mathbb{F}_q)$. The *ρ-value* of A (with respect to r), denoted $\rho(A)$, is $\frac{g \log q}{\log r}$.

Since the speed of computations on $A(\mathbb{F}_q)$ is determined by $\#A(\mathbb{F}_q) \approx q^g$ but security is determined by the size of r, for fast implementations one usually wishes to choose an A with r as close to $\#A(\mathbb{F}_q)$ as possible; that is, with ρ-value as close to 1 as possible.

We first consider the families of supersingular elliptic curves with embedding degrees 4 and 6, in characteristic 2 and 3 respectively. These families are often proposed for use in pairing-based cryptography as their embedding degrees are the maximum possible for supersingular elliptic curves, it is easy to generate curves of near-prime order, and there has been some research into optimizing curve arithmetic in small characteristic (e.g., [12]). We conclude in both cases that if either m is prime or r is sufficiently large (though not necessarily close to q), then the minimal embedding field is $\mathbb{F}_{q^k}$. In cryptographic contexts at least one of these conditions always holds, so we deduce that Hitt's observation (Lemma 2.3) has no effect in practice.

Proposition 3.2 ($k = 4$). *Let $q = 2^m$ with m odd, and let E be a supersingular elliptic curve over $\mathbb{F}_q$ that has embedding degree 4 with respect to a prime $r \nmid 2m$. If either*

- $\rho < \frac{3}{2}\left(1 - \frac{1}{\log_2 r}\right)$, *or*
- *m is prime and $r > 5$,*

then E has minimal embedding field $\mathbb{F}_{q^4}$.

Proof. If we write $m = \alpha\beta$ as in Theorem 2.9, then the smallest prime dividing β must be at least 3. Thus if $r > q^{2/3} + 1$ then condition (4) of Theorem 2.9 is satisfied. If m is prime and $r > 5$ then condition (2) of Theorem 2.9 is satisfied. In both cases, by Corollary 2.10 E has minimal embedding field $\mathbb{F}_{q^4}$. An easy calculation shows that if $\rho < \frac{3}{2}(1 - \frac{1}{\log_2 r})$ then $r > q^{2/3} + 1$. □

Proposition 3.3 ($k = 6$)**.** *Let $q = 3^m$ with m odd, and let E be a supersingular elliptic curve over $\mathbb{F}_q$ that has embedding degree 6 with respect to a prime $r \nmid 6m$. If either*

- $\rho < \frac{5}{3}\left(1 - \frac{1}{\log_2 r}\right)$, *or*
- *m is prime and $r > 7$,*

then E has minimal embedding field $\mathbb{F}_{q^6}$.

Proof. The proof is entirely analogous to that of Proposition 3.2. □

Remark 3.4. In both of the above cases the cryptographic exponent $c_{A,q}$ defined by Rubin and Silverberg is equal to k. Rubin and Silverberg's result (Theorem 2.5) thus implies that when $k = 4$, the conclusion of Proposition 3.2 holds whenever $\rho < \frac{3\log 2}{2\log(1+\sqrt{2})} \approx 1.18$, and that when $k = 6$, the conclusion of Proposition 3.3 holds whenever $\rho < \frac{3\log 3}{2\log(1+\sqrt{3})} \approx 1.64$. Thus in both cases our result is stronger (i.e., requires a weaker upper bound on ρ) for sufficiently large r. In particular, since $\rho \approx 3/2$ is recommended for $k = 4$ curves to achieve a security level equivalent to an 80-bit symmetric-key system [3, Table 1.1], our result shows that supersingular $k = 4$ curves are appropriate for this security level for any extension degree m.

For some implementations one may wish to use supersingular elliptic curves with very small embedding degrees. We thus continue our analysis by investigating the cases $1 \le k \le 3$. The case $k = 2$ is the most straightforward.

Proposition 3.5 ($k = 2$)**.** *Let $q = p^m$, and let E be a supersingular elliptic curve over $\mathbb{F}_q$ that has embedding degree 2 with respect to a prime $r \nmid 2m$. If either*

- $\rho < 3\left(1 - \frac{1}{\log_2 r}\right)$, *or*
- *m is prime and $r > p + 1$,*

then E has minimal embedding field $\mathbb{F}_{q^2}$.

Proof. The proof is entirely analogous to that of Proposition 3.2. □

Rubin and Silverberg's result (Theorem 2.5) says that the conclusion of Proposition 3.5 holds whenever $\rho < 2 - \epsilon$ when m is even and whenever $\rho < 3 - \epsilon$ when m is odd, with $\epsilon \to 0$ as $p \to \infty$. Thus our result is stronger when m is even.

The cases $k = 1$ and $k = 3$ are more subtle, as it is impossible to avoid the possibility that the minimal embedding field is $\mathbb{F}_{p^{k/2}}$ even when r is very large. However, if we know the sign of the trace we can apply Theorem 2.9 to determine when the minimal embedding field is $\mathbb{F}_{p^k}$ or $\mathbb{F}_{p^{k/2}}$.

Proposition 3.6 ($k = 1$). *Let $q = p^m$ with m even, and let E be a supersingular elliptic curve over $\mathbb{F}_q$ that has embedding degree 1 with respect to a prime $r \nmid m$. If E has trace $-2p^{m/2}$ and $\rho < 6(1 - \frac{1}{\log_2 r})$, then E has minimal embedding field $\mathbb{F}_q$. If E has trace $2p^{m/2}$ and $\rho < 4$, then E has minimal embedding field $\mathbb{F}_{q^{1/2}}$.*

Proof. Let $m' = m/2$. Suppose E has trace $-2p^{m'}$. Then $\#E(\mathbb{F}_q) = (p^{m'} + 1)^2$, so r divides $\Phi_2(p^{m'})$. We now apply Theorem 2.9 with $k = 2$ and $m = m'$. If we write $m' = \alpha\beta$ as in the theorem, then the smallest prime dividing the β of Theorem 2.9 must be at least 3. Thus if $r > p^{m'/3} + 1 = q^{1/6} + 1$ then condition (4) of the theorem is satisfied, so by Corollary 2.10 E has minimal embedding field $\mathbb{F}_{p^{2m'}} = \mathbb{F}_q$. An easy calculation shows that if $\rho < 6(1 - \frac{1}{\log_2 r})$ then $r > q^{1/6} + 1$.

Now suppose E has trace $2p^{m'}$. Then $\#E(\mathbb{F}_q) = (p^{m'} - 1)^2$, so r divides $\Phi_1(p^{m'})$. We now apply Theorem 2.9 with $k = 1$ and $m = m'$. If $r > p^{m'/2} = q^{1/4}$ (or equivalently, if $\rho < 4$) then condition (3) of the theorem is satisfied, so by Corollary 2.10 E has minimal embedding field $\mathbb{F}_{p^{m'}} = \mathbb{F}_{q^{1/2}}$. □

When $k = 1$, Rubin and Silverberg's cryptographic exponent c_A is equal to 1 when E has negative trace and 1/2 when E has positive trace; in both cases the integer f of Theorem 2.5 is equal to 2. Thus Theorem 2.5 says that the conclusion of Proposition 3.6 holds whenever $\rho < 4 - \epsilon$, with $\epsilon \to 0$ as $p \to \infty$. Our result is stronger for the first case as well as for small p.

Remark 3.7. Proposition 3.6 demonstrates the somewhat surprising fact that the minimal embedding field of an elliptic curve E can be *smaller* than the field of definition of E. In fact such a curve is easy to construct. Let $p > 3$ be prime, and let $E/\mathbb{F}_p$ be a supersingular elliptic curve over $\mathbb{F}_p$. Let $E'/\mathbb{F}_{p^2}$ be a quadratic twist of E over $\mathbb{F}_{p^2}$; that is, a curve equipped with an isomorphism $E' \to E$ given by $(x, y) \mapsto (ux, u^{3/2}y)$ for some non-square[3] $u \in \mathbb{F}_{p^2}^*$. Then $\#E'(\mathbb{F}_{p^2}) = (p-1)^2$, and the minimal embedding field of E' with respect to any $r \mid p - 1$ is $\mathbb{F}_p$.

Finally, we consider the case of embedding degree $k = 3$. As with $k = 1$, the minimal embedding field can be determined from the sign of the trace.

Proposition 3.8 ($k = 3$). *Let $q = p^m$ with m even, and let E be a supersingular elliptic curve over $\mathbb{F}_q$ that has embedding degree 3 with respect to a prime $r \nmid 3m$. If E has trace $p^{m/2}$ and $\rho < \frac{10}{3}(1 - \frac{1}{\log_2 r})$, then E has minimal embedding field $\mathbb{F}_{q^3}$. If E has trace $-p^{m/2}$ and $\rho < 4/3$, then E has minimal embedding field $\mathbb{F}_{q^{3/2}}$.*

[3] If $j(E) = 0$ then u must also be a cube; if $j(E) = 1728$ then u must be a square but not a fourth power.

Proof. The proof is entirely analogous to that of Proposition 3.6. □

When $k = 3$, Rubin and Silverberg's cryptographic exponent c_A is equal to 3 when E has positive trace and $3/2$ when E has negative trace. Thus Theorem 2.5 says that the conclusion of Proposition 3.8 holds whenever $\rho < 2 - \epsilon$, with $\epsilon \to 0$ as $p \to \infty$. Our result is stronger for the first case.

4 Higher-dimensional supersingular abelian varieties

In this section we briefly sketch the application of our main result to supersingular abelian varieties of dimension $g \geq 2$ defined over non-prime fields. Such varieties have been proposed for use in pairing-based cryptography as they have the potential to be more efficient than supersingular elliptic curves.

We first consider simple supersingular abelian varieties of dimension $g = 2$. Such varieties, known as *abelian surfaces*, can be described as Jacobians of genus 2 curves. Cardona and Nart [1] give a detailed description of the possible group orders and embedding degrees for simple supersingular abelian surfaces, analogous to the Menezes-Okamoto-Vanstone classification for elliptic curves.

Table 1 lists each isogeny class of simple supersingular abelian surfaces over $\mathbb{F}_q$ (with $q = p^m$) and its embedding degree k, as calculated by Cardona and Nart. The isogeny classes are described by a pair of integers (s, t), which correspond to the coefficients of the characteristic polynomial of Frobenius $x^4 + sx^3 + tx^2 + sqx + q^2$. An asterisk next to the embedding degree indicates that the minimal embedding field is $\mathbb{F}_{q^{k/2}}$, not $\mathbb{F}_{q^k}$.

When the extension degree m is prime, as is most often the case in cryptography, Corollary 2.10 tells us that if $r > \Phi_k(p)$ then the minimal embedding field of a supersingular abelian surface with respect to r is $\mathbb{F}_{p^k}$. For the cases of small characteristic most often proposed for cryptography, we have the following:

Proposition 4.1. *Let A be a simple supersingular abelian surface over $\mathbb{F}_q$, where $q = p^m$, $p \in \{2, 3, 5\}$, and m is prime. Suppose A has embedding degree k with respect to a prime $r > m$. If $r > 781$ then the minimal embedding field of A with respect to r is $\mathbb{F}_{q^k}$.*

For more general situations, Table 1 gives two parameters for each isogeny class that are related to the minimal embedding field. A value of α in the column "Cor. 2.10 max ρ" indicates that whenever $r \nmid km$ is prime and $\rho < \alpha$, Corollary 2.10 implies that an abelian variety in the isogeny class has minimal embedding field $\mathbb{F}_{q^k}$ with respect to r (or $\mathbb{F}_{q^{k/2}}$ in the asterisked cases). When the value is $\alpha - \epsilon$ one can take $\epsilon = \alpha / \log_2 r$.

A value of β in the column "RS max ρ" indicates that whenever r is prime and $\rho < \beta$, Rubin and Silverberg's result (Theorem 2.5) implies that an abelian variety in the isogeny class has minimal embedding field $\mathbb{F}_{q^k}$ with respect to r (or $\mathbb{F}_{q^{k/2}}$ in the asterisked cases). When p is not fixed, the values β are limits as $p \to \infty$.

Table 1. Maximal ρ-values guaranteeing a simple supersingular abelian surface over $\mathbb{F}_q$ ($q = p^m$) with embedding degree k has minimal embedding field $\mathbb{F}_{q^k}$ ($\mathbb{F}_{q^{k/2}}$ in the cases marked with a *).

(s,t)	conditions on p and m	k	Cor. 2.10 max ρ	RS max ρ
$(0,-2q)$	m odd	1	6	6
$(0,2q)$	m even, $p \equiv 1 \pmod 4$	2	$6-\epsilon$	4
$(2\sqrt{q},3q)$	m even, $p \equiv 1 \pmod 3$	3*	8/3	4
$(-2\sqrt{q},3q)$	m even, $p \equiv 1 \pmod 3$	3	$20/3-\epsilon$	4
$(0,0)$	m odd, $p \neq 2$	4	$3-\epsilon$	3
$(0,0)$	m even, $p \not\equiv 1 \pmod 8$	4	$3-\epsilon$	2
$(0,q)$	m odd	3	10/3	3
$(0,-q)$	m odd, $p \neq 3$	6	$10/3-\epsilon$	3
$(0,-q)$	m even, $p \not\equiv 1 \pmod{12}$	6	$10/3-\epsilon$	2
$(\sqrt{q},q)$	m even, $p \not\equiv 1 \pmod 5$	5*	8/5	2
$(-\sqrt{q},q)$	m even, $p \not\equiv 1 \pmod 5$	5	$12/5-\epsilon$	2
$(\pm\sqrt{5q},3q)$	m odd, $p = 5$	5	6/5	2.06
$(\pm\sqrt{2q},q)$	m odd, $p = 2$	12	$5/3-\epsilon$	1.18

We conclude our analysis by applying our main result to a particularly interesting case of a supersingular abelian variety in dimension $g = 4$. Rubin and Silverberg [13, §5.1] show that if $q = 3^m$ and E is a supersingular elliptic curve over $\mathbb{F}_q$ with embedding degree 6, then there is a simple 4-dimensional abelian variety $A/\mathbb{F}_q$ with embedding degree $k = 30$. This A can be constructed as a subvariety of the restriction of scalars $\mathrm{Res}_{\mathbb{F}_{q^5}/\mathbb{F}_q} E$. The ratio $k/g = 7.5$ is the largest known for a supersingular abelian variety, which makes the variety appealing for practical use as it allows for higher security levels using fewer bits than a $k = 6$ elliptic curve or a $k = 12$ abelian surface.

Proposition 4.2. *Let $q = 3^m$ with m odd, and let A be a simple supersingular 4-dimensional abelian variety over $\mathbb{F}_q$ that has embedding degree 30 with respect to a prime $r \nmid 30m$. If either*

- $\rho < \dfrac{28}{15}\left(1 - \dfrac{1}{\log_2 r}\right)$, *or*
- *m is prime and $r > 8400$,*

then A has minimal embedding field $\mathbb{F}_{q^{30}}$.

Proof. The proof is entirely analogous to that of Proposition 3.2. □

We note that if A is an abelian variety as in Proposition 4.2, Rubin and Silverberg's result (Theorem 2.5) shows that the result holds whenever $r > (1+\sqrt{3})^{8m/3}$, or $\rho \lessapprox 1.64$. Thus our result ($\rho \lessapprox 1.87$) is stronger.

5 Conclusion

Given an abelian variety A defined over a finite field $\mathbb{F}_q$ such that A has embedding degree k with respect to a subgroup of prime order r, we consider the

question of whether the minimal embedding field of A with respect to r is $\mathbb{F}_{q^k}$. A positive answer to this question implies that the embedding degree k is a good measure of the security level of a pairing-based cryptosystem that uses A.

Our main results, Theorem 2.9 and Corollary 2.10, give explicit conditions on the field size q, the embedding degree k, and the subgroup order r that imply an affirmative answer to our question. We have applied our theorem to supersingular elliptic curves (Section 3) and to supersingular genus 2 curves (Section 4), in each case computing a maximum ρ-value for which the minimal embedding field must be $\mathbb{F}_{q^k}$. Our results are in most cases stronger (i.e., give larger allowable ρ-values) than the corresponding result of Rubin and Silverberg (Theorem 2.5). Our result thus guarantees more abelian varieties are suitable for use in pairing-based cryptography than any previous result had done.

Our theorem holds for general abelian varieties, not only supersingular ones. However, at present there exists only a single explicit construction of non-supersingular abelian varieties over non-prime fields with small embedding degree. This construction, due to Hitt O'Connor et al. [8, Algorithm 3], produces abelian surfaces over $\mathbb{F}_{p^2}$ with p-rank 1 (i.e., neither ordinary nor supersingular) and $\rho \approx 16$. These ρ-values are far too large both for practical use and for Corollary 2.10 to provide a useful result.

It is thus an open problem to construct non-supersingular abelian varieties — including elliptic curves — over non-prime fields with small embedding degree and $\rho < 16$. Such a construction would not only expand our library of pairing-friendly abelian varieties but could potentially lead to improvement in the performance of pairing-based protocols, in the same way that elliptic curves over non-prime fields can lead to performance improvements for standard elliptic curve cryptography [4]. Once such varieties are constructed, our results can be used to determine whether the embedding degree also describes the minimal embedding field of these varieties.

References

1. Gabriel Cardona and Enric Nart. Zeta function and cryptographic exponent of supersingular curves of genus 2. In *Pairing-Based Cryptography — Pairing 2007*, volume 4575 of *Springer LNCS*, pages 132–151, 2007.
2. Sylvain Duquesne and Gerhard Frey. Background on pairings. In *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, pages 115–124. Chapman & Hall/CRC, Boca Raton, FL, 2006.
3. David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372, 2006.
4. Steven D. Galbraith, Xibin Lin, and Michael Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. To appear in *Advances in Cryptology — EUROCRYPT 2009*, 2009.
5. P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15(1):19–46, 2002.
6. Pierrick Gaudry. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. To appear in *J. Symbolic Computation*.

7. L. Hitt. On the minimal embedding field. In *Pairing-Based Cryptography — Pairing 2007*, volume 4575 of *Springer LNCS*, pages 294–301, 2007.
8. Laura Hitt O'Connor, Gary McGuire, Michael Naehrig, and Marco Streng. CM construction of genus 2 curves with p-rank 1. Cryptology ePrint Archive, Report 2008/491, 2008.
9. Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, revised third edition, 2002.
10. A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39:1639–1646, 1993.
11. J. S. Milne. Abelian varieties. In G. Gornell and J. Silverman, editors, *Arithmetic Geometry*, pages 103–150, New York, 1986. Springer.
12. Volker Müller. Fast multiplication on elliptic curves over small fields of characteristic two. In *Journal of Cryptology*, volume 11 of *Springer LNCS*, pages 219–234, 1998.
13. Karl Rubin and Alice Silverberg. Supersingular abelian varieties in cryptology. In *Advances in Cryptology — CRYPTO 2002*, volume 2442 of *Springer LNCS*, pages 336–353, 2002.
14. Karl Rubin and Alice Silverberg. Using abelian varieties to improve pairing-based cryptography. To appear in *Journal of Cryptology*, 2009.
15. Joseph Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.