SUPERSINGULAR CURVES IN CRYPTOGRAPHY

STEVEN D. GALBRAITH

Abstract. Frey and Rück gave a method to transform the discrete logarithm problem in the divisor class group of a curve over $\mathbb{F}_q$ into a discrete logarithm problem in some finite field extension $\mathbb{F}_{q^k}$. The discrete logarithm problem in the divisor class group can therefore be solved using index calculus algorithms as long as k is small.

In the elliptic curve case it was shown by Menezes, Okamoto and Vanstone that for supersingular curves one has $k \leq 6$. In this paper curves of higher genus are studied. Bounds on the possible values for k in the case of supersingular curves are given. Ways to ensure that a curve is not supersingular are also discussed.

A constructive application of supersingular curves to cryptography is given, by generalising an identity-based cryptosystem due to Boneh and Franklin.

1. Introduction

Frey and Rück [13] described how the Tate pairing can be used to map the discrete logarithm problem on the divisor class group of a curve C over a finite field $\mathbb{F}_q$ into the multiplicative group $\mathbb{F}_{q^k}^*$ of some extension of the base field. This has significant implications for cryptography as there are well-known subexponential algorithms for solving the discrete logarithm problem in a finite field. Therefore, there is a method for solving the discrete logarithm problem in the divisor class group in those cases where the extension degree k is small.

The extension degree required is the smallest integer k such that the exponent of the divisor class group $\mathrm{Pic}_C^0(\mathbb{F}_q)$ divides $q^k - 1$. In general, the value of k depends on both the curve and the finite field and it is usually very large (i.e., $\log(k) \approx \log(q)$).

Menezes, Okamoto and Vanstone [27] showed that for supersingular elliptic curves the value k above is always less than or equal to 6. This is an important result as it provides a good upper bound on the complexity of the attack in the supersingular case. The conclusion which has traditionally been drawn is that supersingular elliptic curves should be considered to be weaker than the general case for cryptography.

When generalising cryptography to divisor class groups of higher genus curves [20] it is important know what values of k can arise. In Section 9 we will show that for supersingular curves there is an upper bound, which depends only on the genus, on the values of the extension degree k. This bound is sufficiently small that supersingular curves must be considered a weak case for cryptography.

Date: January 7, 2010.

This research was supported by the Centre for Applied Cryptographic Research at the University of Waterloo, the NRW-Initiative für Wissenschaft und Wirtschaft "Innovationscluster für Neue Medien", cv cryptovision gmbh (Gelsenkirchen), and Hewlett-Packard laboratories Bristol.

It is important to be able to detect these weak cases in advance, especially when, as is often the case, one is considering curves defined over small fields and using the zeta function to compute the group order over extension fields. The authors of [35] were unable to find any secure hyperelliptic curves of genus two over $\mathbb{F}_2$. In Section 12 we explain how to avoid equations for supersingular curves in characteristic two, and we give some examples of secure genus two curves over $\mathbb{F}_2$, thereby solving the problems of [35].

Recently the Weil pairing has found positive applications in cryptography. In Section 3 we generalise an identity-based cryptosystem due to Boneh and Franklin [4]. Our scheme provides the same functionality as the scheme of Boneh and Franklin but with a significant improvement in bandwidth.

2. The Tate pairing

Let C be a non-singular, irreducible curve of genus g over a finite field $\mathbb{F}_q$ where q is a power of a prime p. The Jacobian of the curve C is an abelian variety $\mathrm{Jac}(C)$ of dimension g defined over $\mathbb{F}_q$. Since all curves over finite fields have a rational degree one divisor the Jacobian represents the divisor class group of the curve Pic^0_C (for details see [7], [20], [42]).

Those readers only interested in elliptic curves can take C to be an elliptic curve and can think of $\mathrm{Jac}(C)(\mathbb{F}_q) = \mathrm{Pic}^0_C(\mathbb{F}_q) = C(\mathbb{F}_q)$.

2.1. **Definition of the Tate pairing.** The Tate pairing is defined in full generality as a pairing between abelian varieties over local fields. We follow the definitions of Frey and Rück [13] (who themselves follow the formulation of Lichtenbaum) and therefore consider the pairing on the prime-to-p part of the divisor class group of a curve C over a finite field $\mathbb{F}_q$. (We do not consider the p-part, although see Rück [34].)

Let l be a positive integer which is coprime to q. In most applications l is a prime and $l | \#\mathrm{Pic}^0_C(\mathbb{F}_q)$. Let k be a positive integer such that the field $\mathbb{F}_{q^k}$ contains the lth roots of unity (in other words, $l|(q^k-1)$). Let $G = \mathrm{Pic}^0_C(\mathbb{F}_{q^k})$ and write $G[l]$ for the subgroup of divisors of order l and G/lG for the quotient group (which is also a group of exponent l). Then the Tate pairing is a mapping

$$\langle \cdot, \cdot \rangle : G[l] \times G/lG \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^l. \tag{1}$$

The Tate pairing satisfies the following properties [13]:

1. (Well-defined) $\langle 0, Q \rangle \in (\mathbb{F}^*_{q^k})^l$ for all $Q \in G$ and $\langle P, Q \rangle \in (\mathbb{F}^*_{q^k})^l$ for all $P \in G[l]$ and all $Q \in lG$.
2. (Non-degeneracy) For each divisor class $P \in G[l] - \{0\}$ there is some divisor class $Q \in G$ such that $\langle P, Q \rangle \notin (\mathbb{F}^*_{q^k})^l$.
3. (Bilinearity) For any integer n, $\langle nP, Q \rangle \equiv \langle P, nQ \rangle \equiv \langle P, Q \rangle^n$ modulo lth powers.

There are more properties, but these are the ones which will be used in the rest of the paper. We will think of the left hand parameter of the pairing as the 'interesting' divisor and the right hand one as 'auxiliary'.

In general there is no relationship between the Tate pairing and the Weil pairing, as they are defined on different sets. However, when E is an elliptic curve such that $l^2 \| \#E(\mathbb{F}_{q^k})$ and P, Q are independent points in $E(\mathbb{F}_{q^k})[l]$ then we have $e_l(P,Q) = \langle P, Q \rangle / \langle Q, P \rangle$. A consequence of this is that the Tate pairing is not symmetric.

The Weil pairing requires working over the field $\mathbb{F}_q(E[l])$ generated by the coordinates of all the l-division points. In general, one would expect the Weil pairing to require a larger field than that used for the Tate pairing. One observation is that for elliptic curves these fields are usually the same.

Theorem 1. *(Koblitz) Let E be an elliptic curve over $\mathbb{F}_q$ and let l be a prime dividing $\#E(\mathbb{F}_q)$. Suppose that $l \not| (q-1)$. The $E[l] \subset E(\mathbb{F}_{q^k})$ if and only if $l|(q^k-1)$.*

Proof. The proof was given by Koblitz at ECC 1997 but we give a sketch here. Let $E[l]$ be generated by $\{P, Q\}$ where P is defined over $\mathbb{F}_q$. The Frobenius automorphism of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ corresponds to $\sigma = \left(\begin{smallmatrix} 1 & 0 \\ a & q \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$. under the representation on $E[l]$. It is clear that $\sigma^k = \left(\begin{smallmatrix} 1 & 0 \\ (1+q+\cdots+q^{k-1})a & q^k \end{smallmatrix}\right)$. When $q \not\equiv 1 \pmod{l}$ it follows that $\sigma^k = 1$ if and only if $q^k \equiv 1 \pmod{l}$. □

It is an interesting question to study generalisations of this property to the higher genus setting.

2.2. **Computing the Tate pairing.** The Tate pairing may be computed using the following process: Since $lP = 0$ there is some function f on the curve C such that the divisor of the function f, which is denoted (f), is equal to $l(P) - l(\infty)$. Then $\langle P, Q\rangle = f(Q')$ where Q' is a divisor in the same class as Q such that the support of Q' is disjoint with the support of (f). This computation is easily implemented in practice by using the double and add algorithm and evaluating all the intermediate functions at Q' (see [13], [14] for details).

The value $f(Q')$ lies in $\mathbb{F}_{q^k}$ and is only determined up to a multiple of an lth power. By raising it to the power $(q^k - 1)/l$ we obtain a precise lth root of unity.

One subtlety when implementing the Tate pairing is finding a divisor class Q' with support disjoint from the partial terms in the addition chain for lP. In the elliptic curve case this is done by taking $Q' = (Q + S) - (S)$ where Q is the target point and where S is an arbitrary point (not necessarily of order l). In the higher genus case general Riemann-Roch algorithms can give an analogous solution. In practice, it is often easier not to choose the class Q first but to just choose two 'random' effective divisors E_1 and E_2 of degree g and set $Q' = E_1 - E_2$. If E_1 and E_2 are chosen randomly over $\mathbb{F}_{q^k}$ then with high probability we expect $\langle P, Q'\rangle^{(q^k-1)/l} \neq 1$.

2.3. **The Frey-Rück attack.** We now recall how the Tate pairing is used to attack the discrete logarithm problem in the divisor class group of a curve (this approach is often called the Frey-Rück attack, after [13]). Let $D_1, D_2 \in \mathrm{Pic}^0_C(\mathbb{F}_q)$ be divisors of order l for which we want to solve the discrete logarithm problem $D_2 = \lambda D_1$. Let k be the smallest integer such that $l|(q^k - 1)$. The method proceeds as follows:

(1) Choose random divisors $Q \in \mathrm{Pic}^0_C(\mathbb{F}_{q^k})$ until $\langle D_1, Q\rangle \notin (\mathbb{F}^*_{q^k})^l$.
(2) Compute $\zeta_i = \langle D_i, Q\rangle \in \mathbb{F}^*_{q^k}$.
(3) Map the ζ_i to lth roots of unity (by raising to the power $(q^k - 1)/l$). This step is actually optional since the linear algebra in the index calculus method should be performed modulo l.
(4) Solve the discrete logarithm problem $\zeta_2 = \zeta_1^\lambda$ in the subgroup of order l of the finite field $\mathbb{F}^*_{q^k}$ using an index calculus method.

This strategy is practical when k is small. This leads to the following important question for cryptography:

Main Question: Are there certain weak cases of curves for which k is always small?

One of the goals of this paper is to show that, as in the case of elliptic curves, supersingular curves always have small k.

Of course, there are lots of non-supersingular elliptic curves for which the Frey-Rück attack applies (for instance, elliptic curves E over $\mathbb{F}_p$ with $p-1$ points). In general an elliptic curve $E/\mathbb{F}_q$ may be vulnerable to the attack when considered as a group over some extension $\mathbb{F}_{q^m}$ but not when considered as a group over some other extension $\mathbb{F}_{q^{m'}}$. However, if E is supersingular over $\mathbb{F}_q$, then the bound k is small for all groups $E(\mathbb{F}_{q^n})$ regardless of the value of n.

2.4. **Non-degeneracy of the Tate pairing.** We now discuss the non-degeneracy property a little more closely. Let $P \in G[l]$. We consider the possibilities for $\langle P, P\rangle$.

To compute $\langle P, P\rangle$ it is necessary to compute a divisor Q in the same class as P but which has support disjoint from all the intermediate terms in the computation of lP. One can then compute $\langle P, Q\rangle$ to obtain the value of the pairing. If $P \in lG$ then $\langle P, P\rangle \in (\mathbb{F}_{q^k}^*)^l$. If $P \in \mathrm{Pic}_C^0(\mathbb{F}_q)$ then $\langle P, P\rangle \in \mathbb{F}_q$, and if l does not divide $(q-1)$ then every element of $\mathbb{F}_{q^k}^*)^l$ is an lth power and thus the pairing is trivial. Hence to have $\langle P, P\rangle \notin (\mathbb{F}_{q^k}^*)^l$ it is necessary (but not sufficient) that $l|(q-1)$ and so $k = 1$.

For elliptic curves the following result holds.

Lemma 1. *Let $P \in E(\mathbb{F}_q)$ be a point of prime order l. Let $\mathbb{F}_{q^k}$ be the extension over which all points of order l are defined, and write $G = E(\mathbb{F}_{q^k})$. Suppose that $l^2 \| \#G$ (i.e., that $G[l] \cong G/lG$). Then for every point $R \in G[l]$ such that $R \notin \mathrm{Pic}_C^0(\mathbb{F}_q)$ one has $\langle P, R\rangle \notin (\mathbb{F}_{q^k}^*)^l$.*

Proof. There is some point $Q \in G$ of order l such that $\langle P, Q\rangle \neq 1$ and so $Q \notin \mathrm{Pic}_C^0(\mathbb{F}_q)$. Therefore $\{P, Q\}$ form a basis for $G[l]$. Every $R \in G[l]$ is of the form $R = aP + bQ$ and if $R \notin \mathrm{Pic}_C^0(\mathbb{F}_q)$ then $b \neq 0$ and so $\langle P, R\rangle \equiv \langle P, Q\rangle^b \not\equiv 1$ modulo $(\mathbb{F}_{q^k}^*)^l$. □

Since an endomorphism maps an element of order l to another, we obtain the following Corollary.

Corollary 1. *In the situation of the above lemma, let ψ be an endomorphism of $\mathrm{Jac}(C)$ which is not defined over $\mathbb{F}_q$. If $\psi(P) \notin \mathrm{Pic}_C^0(\mathbb{F}_q)$ then $\langle P, \psi(P)\rangle \neq 1$.*

The above corollary gives a very useful technique for finding points where the pairing is non-degenerate. We refer to the maps ψ as 'non-$\mathbb{F}_q$-rational endomorphisms' (Verheul [46] calls them 'distortion maps'). These endomorphisms always exist for supersingular elliptic curves, but they do not exist for non-supersingular curves (see Verheul [46] Theorem 4.1). In many (but not all) cases it is possible to choose ψ to be an automorphism of the curve.

In the higher genus case there are usually many 'independent' choices for ψ. One question for further study is whether there are always enough non-$\mathbb{F}_q$-rational

endomorphisms which arise from non-$\mathbb{F}_q$-rational mappings from the curve C to itself.

Non-$\mathbb{F}_q$-rational endomorphisms can be used to solve the decision Diffie-Hellman problem on supersingular curves (see Joux and Nguyen [19]).

In all cases, to compute the pairing, there is still the task of finding an auxiliary divisor $Q = E_1 - E_2$. If P is defined over a subfield of $\mathbb{F}_{q^k}$ then pair of divisors E_1, E_2 must be truly defined over the large field $\mathbb{F}_{q^k}$. The probability of randomly chosen E_1, E_2 which are not defined over a subfield yielding a non-degenerate pairing should be approximately $1 - 1/l$.

3. Identity-based cryptosystems using the Tate pairing

Identity based cryptography was proposed by Shamir [37] as a response to the problem of managing public keys. The basic principle is that it should be possible to derive a user's public data only from their identity. It is therefore necessary to have a trusted dealer who can provide a user with the secret key corresponding to the public key which is derived from their identity. It has turned out to be rather difficult to construct efficient and secure identity-based cryptosystems.

Recently, Boneh and Franklin [4] developed a new identity-based cryptosystem using the Weil pairing on a specific supersingular elliptic curve. In this section we describe a generalised version of their scheme which applies to elliptic curves and higher genus curves and which has some efficiency improvements over the original scheme. Note that we only discuss the basic scheme of [4]; the extension to a scheme secure against a chosen ciphertext attack is straightforward.

Note that Cocks [8] has recently proposed an identity-based encryption scheme which is quite different from the approach of Boneh and Franklin.

3.1. Dealer's system parameters.

The dealer sets up the scheme by choosing a finite field $\mathbb{F}_q$ and a curve C over $\mathbb{F}_q$ of genus g such that:

(1) There is a large prime l dividing the order of the group $\mathrm{Pic}^0_C(\mathbb{F}_q)$.
(2) The degree k needed for the Tate pairing embedding of the subgroup of order l (i.e., the smallest k such that $l|(q^k - 1)$) is relatively small.

One approach is to take C to be a supersingular curve.

The dealer then chooses a divisor $P \in \mathrm{Pic}^0_C(\mathbb{F}_q)$ of order l and a secret integer $1 < s < l$ and computes $P' = sP$. The dealer publishes q, C, l, k, P and P' and keeps the integer s secret. The public data for the scheme also includes two hash functions H_1 and H_2 (these are called G and H in [4]). The function H_1 is used to map identities to bitstrings which are then used to represent divisors in $\mathrm{Pic}^0_C(\mathbb{F}_{q^k})$. The function H_2 maps elements of the subgroup of order l of $\mathbb{F}^*_{q^k}$ to bitstrings of a certain length N. Both hash functions are required to be cryptographically strong and are modelled in the security proofs as random oracles.

Assuming the difficulty of the discrete logarithm problem in $\mathrm{Pic}^0_C(\mathbb{F}_q)$ it is not possible for anyone to know the value of s except the dealer.

3.2. User's public key.

We now discuss how a user's identity gives rise to a public key. Write $G = \mathrm{Pic}^0_C(\mathbb{F}_{q^k})$. Each user A in the system has an identity (such as their name or email address). We must specify a deterministic procedure for converting an identity to a divisor $Q_A \in G = \mathrm{Pic}^0_C(\mathbb{F}_{q^k})$. This procedure must satisfy the following properties:

(1) Q_A must be such that $\langle P, Q_A\rangle \notin (\mathbb{F}_{q^k}^*)^l$.
(2) The process should be one-way, in the sense that it be infeasible to find an identity which gives rise to a given point Q_A.
(3) The points Q_A should be distributed uniformly in an appropriate set.

In [4] this process (which Boneh and Franklin call 'MapToPoint') is solved using a cryptographically strong hash function H_1 and a non-$\mathbb{F}_q$-rational endomorphism ψ.

This method can be generalised as follows. The identity bitstring is concatenated with a padding string and then passed through the hash function H_1 (which is constructed to yield a full domain output). This process is repeated using a deterministic sequence of padding strings until the output is the x-coordinate (or $a(x)$-term in the higher genus case) of an element Q of $\mathrm{Pic}_C^0(\mathbb{F}_q)$. It is then easy to find the rest of the representation of Q. One then sets $Q_A = \psi(mQ) \in G$, for a suitable choice of non-$\mathbb{F}_q$-rational endomorphism from the available possibilities, where m is the cofactor $\#\mathrm{Pic}_C^0(\mathbb{F}_q)/l^a$. For elliptic curves, by Corollary 1, we have $\langle P, Q_A\rangle^{(q^k-1)/l} \neq 1$.

Another approach (which does not require non-$\mathbb{F}_q$-rational endomorphisms) is to use the hash of the bitstring to obtain a divisor E_1. One can then extend to a divisor class $Q_A = E_1 - E_2$ by using a fixed choice for E_2. One should then check that $\langle P, Q_A\rangle \neq 1$ (note that checking this non-degeneracy requires some computational effort). If this check fails then a new divisor Q_A must be chosen (e.g., by continuing the process to get the next candidate divisor). The probability that $\langle P, Q_A\rangle \in (\mathbb{F}_{q^k}^*)^l$ for randomly chosen Q_A is approximately $1/l$, so this case is almost guaranteed to never occur. Of course, one can check that l divides the order of Q_A by multiplying by the cofactor (which is known) but this calculation is not required. The fact that Q_A should represent an element of G/lG rather than $G[l]$ is no problem in practice, since we usually expect to have $G[l^\infty] = G[l]$.

To summarise, every user A has a public key consisting of the divisor Q_A and everyone can obtain this public key just knowing the identity of the user.

3.3. **Extraction of a user's secret key.** Each user asks the dealer for a private key $Q'_A = sQ_A$. This must be transmitted to the user using a secure channel.

3.4. **Encryption.** Let the message M be a bitstring of length N and suppose we want to send this to user A with a given identity. The first step is to derive their public key Q_A from their identity. We must also obtain the public keys P and P' of the dealer. The remaining steps are

(1) Choose a random integer $1 \leq r \leq l$.
(2) Compute $R = rP$.
(3) Compute $S = M \oplus H_2(\langle P', Q_A\rangle^{r(q^k-1)/l})$. (Here $\langle P', Q_A\rangle$ is an element of $\mathbb{F}_{q^k}^*$ which is then raised to the appropriate power.)
(4) Send (R, S).

Note that, when using the Tate pairing (instead of the Weil pairing), it is necessary to raise the value to some cofactor as the value of the Tate pairing is not uniquely determined. This has been presented in the case where $l \| (q^k - 1)$ but it works more generally too.

A more versatile encryption process is obtained by using $H_2(\langle P', Q_A\rangle^r)$ as the key for a fixed symmetric encryption function and encrypting M in the usual way.

3.5. **Decryption.** To decrypt, user A simply uses their private key Q'_A to compute $\langle R, Q'_A\rangle$. Since $\langle rP, sQ_A\rangle \equiv \langle P, Q_A\rangle^{rs} \equiv \langle P', Q_A\rangle^r$ modulo lth powers the message is recovered from

$$M = S \oplus H_2(\langle R, Q'_A\rangle^{(q^k-1)/l}).$$

3.6. **Security.** The security of this system relies on the following variation of the Diffie-Hellman problem:

Definition 1. *The* **Tate-Diffie-Hellman problem (TDH)** *is the following: Given $P, P' = sP, R = rP$ in $\mathrm{Pic}^0_C(\mathbb{F}_q)$ of order l and $Q_A \in G$ such that $\langle P, Q_A\rangle \notin (\mathbb{F}^*_{q^k})^l$ compute $\zeta = \langle P, Q_A\rangle^{rs(q^k-1)/l}$.*

Let $P \in \mathrm{Pic}^0_C(\mathbb{F}_q)$ be any divisor of large prime order. We make the assumption that the Tate-Diffie-Hellman problem is hard over random divisors P', R, Q_A with respect to either of the two methods we have given for generating points Q_A corresponding to users' identities.

Certainly, if one can solve the elliptic curve Diffie-Hellman problem then one can compute rsP and thus $\langle rsP, Q_A\rangle$. It is not clear whether the converse holds. Similarly, if one can solve the Diffie-Hellman problem in $\mathbb{F}^*_{q^k}$ then one can solve TDH.

We point out that TDH is obviously at least as hard as the Decision Diffie-Hellman problem (DDH) in $\mathrm{Pic}^0_C(\mathbb{F}_q)$, but this is not very interesting since DDH is easy for supersingular curves which have a non-$\mathbb{F}_q$-rational endomorphism (see [19], [46]).

To produce a cryptosystem with strong security properties (indistinguishability of encryptions under a chosen ciphertext attack) one uses a method of Fujisaki and Okamoto which is discussed thoroughly in [4]. First it is necessary to establish that the basic scheme has the 'one-way encryption' (ID-OWE) security property (see Section 2 of [4]).

The proof that the scheme has the ID-OWE property depends on the public key generation process. If non-$\mathbb{F}_q$-rational endomorphisms are used then the argument is analogous to the one used in Theorem 4.1 of [4]. The security result holds under the assumptions that the hash functions H_1 and H_2 are random oracles and that the computational TDH problem is hard. The reader is referred to [4] for the details.

If non-$\mathbb{F}_q$-rational endomorphisms are not used in the public key derivation process then the arguments of [4] do not apply. I have heuristic arguments for the security of the scheme but it is an open problem to provide a rigorous reductionist proof of security.

3.7. **Parameter sizes.** To resist algorithms for solving the Diffie-Hellman problem in $\mathrm{Pic}^0_C(\mathbb{F}_q)$ it is necessary that $q^g \geq 2^{160}$. To resist algorithms for solving the Diffie-Hellman problem in $\mathbb{F}^*_{q^k}$ it is necessary that $q^k \geq 2^{1024}$.

Boneh and Franklin [4] use $g = 1$ and $k = 2$ and so they must take q to be of size at least 512 bits (actually they take q to have at least 1024 bits, but 512 bits would have been sufficient). The whole point of our generalisation is the observation that if k can be taken to be larger than 2 then q may be taken to be smaller. In the next subsection we discuss the advantages which can be obtained from using larger values of k. In 3.9 we give the details for a curve with $k = 6$.

3.8. **Performance.** We briefly list some advantages and disadvantages of the generalised scheme compared with the scheme of [4].

- The bandwidth (number of bits) of an encryption (R, S) is roughly $qg + N$, while the security depends on the size of q^k. Typically N might be 160 bits. For the scheme of Boneh and Franklin q must be at least 512 bits, which is rather large. The bandwidth requirements can be easily reduced by using curves with larger values of k (see the example in 3.9 below).
- For the same reason, the dealer's public keys also require less storage and communication bandwidth with the new scheme.
- The dominant cost in encryption and decryption is the evaluation of the Tate pairing. This involves computations in the large field $\mathbb{F}_{q^k}$ so the cost of encryption and decryption depends only the number of bits in the large prime l. Hence the computation cost for both schemes is comparable when they are equally optimised (see [4]), although there are some time savings when working in characteristic two.
- If non-$\mathbb{F}_q$-rational endomorphisms are not used then the process of finding a user's public key from their identity is slightly more complicated for our scheme and more memory is required for this process. Hence both the dealer and the encryptor require higher computational overhead. However, this data is never transmitted.

3.9. **Characteristic three example.** With elliptic curves one can realise an improvement of k from 2 to 6 by taking the elliptic curves

$$E_1 : y^2 = x^3 - x + 1 \qquad \text{and} \qquad E_2 : y^2 = x^3 - x - 1$$

over $\mathbb{F}_{3^l}$, which have characteristic polynomial of Frobenius $P_{E_1}(X) = X^2 + 3X + 3$ and $P_{E_2}(X) = X^2 - 3X + 3$ respectively. These curves are thoroughly discussed by Koblitz in [22].

We first list some values for m where the group order of $E_i(\mathbb{F}_{3^m})$ is equal to a small cofactor times a large prime l.

m	i	# bits in l	c
79	2	125	1
97	1	151	7
149	1	220	$7 \cdot 15199$
163	1	256	7
163	2	259	1
167	1	262	7
167	2	237	$8017 \cdot 44089$
173	2	241	16420688749
193	2	306	1
239	2	379	1

A convenient non-$\mathbb{F}_3$-rational endomorphism for E_1 is

$$\psi : (x, y) \longmapsto (\alpha - x, iy)$$

where $i \in \mathbb{F}_{3^2}$ satisfies $i^2 = -1$ and $\alpha \in \mathbb{F}_{3^3}$ satisfies $\alpha^3 - \alpha + 2 = 0$. Similarly, a convenient non-$\mathbb{F}_3$-rational endomorphism for E_1 is

$$\psi : (x, y) \longmapsto (\beta - x, iy)$$

where $\beta^3 - \beta + 1 = 0$. Using these maps one can implement a method analogous to that of [4] for computing a point Q_A corresponding to a users identity. In this case the proof of security is almost exactly the same as that in [4].

Consider, say, the case $l = 163$ which is a 259 bit field. Since $k = 6$ the size of the field $\mathbb{F}_{q^k}$ is 1551 bits. If messages are of length $N = 160$ bits then an encryption requires $160 + 260 = 420$ bits (259 bits for the x-coordinate of the point and one bit to specify the y-coordinate). For equivalent security using the Boneh-Franklin scheme with $k = 2$ one must take p to be $\lceil 1551/2 \rceil = 776$ bits and so an encryption will require $160 + 776 = 936$ bits (we have 776 as the Boneh-Franklin scheme only requires sending the y-coordinate). Hence our scheme requires less than half the bandwidth of the Boneh-Franklin scheme for the same security level.

On the other hand, it seems to be non-trivial to obtain a fast implementation of finite field arithmetic in characteristic three (this is a subtlety which also has some impact on the results of [22]).

3.10. **Characteristic two example.** In characteristic two there are curves available which attain the Frey-Rück embedding degree $k = 4$. In these cases the bandwidth improvement is not as significant as that seen with the characteristic three example above. However, it is easy to get an improvement in performance over the scheme in [4].

Consider the elliptic curves

$$E_1 : y^2 + y = x^3 + x \qquad \text{and} \qquad E_2 : y^2 + y = x^3 + x + 1$$

over $\mathbb{F}_2$. One can easily see that $\#E_1(\mathbb{F}_2) = 5$ and $\#E_2(\mathbb{F}_2) = 1$. Then E_1 has characteristic polynomial of Frobenius $P_{E_1}(X) = X^2 + 2X + 2$ while E_2 is the quadratic twist of E_1 and has $P_{E_2}(X) = X^2 - 2X + 2$.

Some suitable field extensions giving large prime factors are as follows. Given m and i we have $\#E_i(\mathbb{F}_{2^m}) = cl$ where l is a large prime and where c is a cofactor.

m	i	# bits in l	c
233	1	210	$5 \cdot 3108221$
239	2	239	1
241	2	241	1
271	1	252	$5 \cdot 97561$
283	1	281	5
283	2	283	1
353	2	353	1
367	2	367	1
397	2	397	1
457	2	457	1

A convenient non-$\mathbb{F}_2$-rational endomorphism for both these curves is given by

$$\psi : (x, y) \mapsto (u^2 x + s^2, y + u^2 s x + s)$$

where $u \in \mathbb{F}_{2^2}$ satisfies $u^2 + u + 1 = 0$ and $s \in \mathbb{F}_{2^4}$ satisfies $s^2 + (u + 1)s + 1 = 0$.

We implemented the Tate pairing in Magma using only the built-in finite field routines. We give a comparison between characteristic 2 and large characteristic p for equivalent sized finite fields. We give the average time (in seconds) for the computation of the Tate pairing and the finite field exponentiation. We also give a comparison of the communication bandwidth (number of bits) for the basic scheme (assuming a 160 bit hash function H).

The first case is with 965 bit finite field security (i.e., using E_2 over $\mathbb{F}_{2^{241}}$, which has a prime number of points).

Characteristic	Time	Bandwidth
2	2.4	402
p	4.3	642

Now for 1132 bit finite field security. This time using $E_1(\mathbb{F}_{2^{283}})$ whose number of points is 5 times a prime.

Characteristic	Time	Bandwidth
2	3.4	444
p	6.1	726

Clearly, the elliptic curves used by Boneh and Franklin lead to a scheme which requires about twice the computation time and over one and a half times the bandwidth compared with using curves in characteristic two.

3.11. **Examples in characteristic greater than three.** The curves used by Boneh and Franklin applied in the case of large characteristic and had $k = 2$. This is optimal when working over $\mathbb{F}_p$.

However, by working over $\mathbb{F}_{p^2}$ one can obtain curves with $k = 3$. For example let p be a prime such that $p \equiv 2 \mod 3$ and let $\alpha \in \mathbb{F}_{p^2}$ be a non-cube. Then

$$E : y^2 = x^3 + \alpha$$

has $P(T) = T^2 \pm pT + p^2$ and the embedding degree is $k = 3$. Of course, the ECDLP on curves with $p^2 + p + 1$ points can be reduced to $\mathbb{F}^*_{p^3}$, and so we truly have $k = 6$ only for curves with $p^2 - p + 1$ points.

3.12. **Open questions.** We have seen that larger values of k help to make a more efficient identity-based cryptosystem. The problem is therefore to find curves C which have suitable large values of k (without being too large). This is very closely related to the Main Question of section 2.3

For supersingular curves we will show in Section 9 that there is an upper bound $k(g)$ (depending only on the genus g) for the values of k. The values of $k(g)$ are large enough to give good performance for the identity-based cryptosystem. However, it does not seem to be possible to find suitable curves to realise this performance improvement. Therefore it does not seem to be worthwhile to use curves of genus greater than one for the identity based cryptosystem (or any of the other new applications of the Weil and Tate pairings in cryptography).

It is not necessary to insist on supersingular curves for the identity-based cryptosystem. There exist other curves of genus g over fields $\mathbb{F}_q$ for which k is of the size we desire. However, if E is a non-supersingular elliptic curve over $\mathbb{F}_q$ with small k then it is usually the case that the order of $E(\mathbb{F}_q)$ is not divisible by a large prime. (One exception is the case $l = (p-1)/2$, but these only have $k = 1$.) This phenomena is indicated by the results of Balasubramanian and Koblitz [2] and is confirmed by computer experiments. It would be interesting to have a construction for suitable non-supersingular curves (for instance, using the CM method). It is an open problem to provide an efficient construction (if one exists).

In conclusion, it seems that the supersingular elliptic curves with $k = 4$ and $k = 6$ (see Subsections 3.10 and 3.9) are the optimal choice for the identity-based cryptosystem.

4. Background on curves over finite fields

Let C be a non-singular, irreducible curve over a finite field $\mathbb{F}_q$. The Frobenius endomorphism π on the Jacobian is induced by the endomorphism $\pi : x \mapsto x^q$ of the field $\mathbb{F}_q$. As an endomorphism of $\mathrm{Jac}(C)$, π satisfies a characteristic polynomial $P(X)$ of degree $2g$ with integer coefficients. We have $P(X) = X^{2g}L(1/X)$ where $L(t)$ is the polynomial arising in the numerator of the zeta function of the curve (called the L-polynomial in Stichtenoth [42] V.1.14 and called $P_1(T)$ in Theorem V.2.2 of [38]). We can factor $P(X)$ over the complex numbers as $P(X) = \prod_{i=1}^{2g}(X - \alpha_i)$. It turns out that the algebraic integers α_i have certain remarkable properties. The following result (see Stichtenoth [42] Theorem V.1.15) combining results due to Weil and others gives some of these facts.

Theorem 2. *Let C be a curve of genus g over $\mathbb{F}_q$ and let $P(X) = \prod_{i=1}^{2g}(X - \alpha_i)$ be the characteristic polynomial of the Frobenius endomorphism on $\mathrm{Jac}(C)$. Then*

1. *The algebraic integers α_i satisfy $|\alpha_i| = \sqrt{q}$.*
2. *The algebraic integers α_i come in (complex) conjugate pairs and can be ordered so that $\alpha_i\alpha_{i+g} = q$. In particular, if some $\alpha_i = \pm\sqrt{q}$ then so does α_{i+g}.*
3. *$P(X)$ has the following form*

$$X^{2g} + a_1X^{2g-1} + a_2X^{2g-2} + \cdots + a_gX^g + qa_{g-1}X^{g-1} + \cdots + q^{g-1}a_1X + q^g$$

where $a_1, \ldots, a_g \in \mathbb{Z}$ are, up to sign, the elementary symmetric polynomials in the α_i.

4. *For any integer $r \geq 1$ we have*

$$\#C(\mathbb{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r.$$

5. *For any integer $r \geq 1$ we have*

$$\#\mathrm{Jac}(C)(\mathbb{F}_{q^r}) = \prod_{i=1}^{2g}(1 - \alpha_i^r).$$

6. $|\#C(\mathbb{F}_{q^r}) - (q^r + 1)| \leq 2gq^{r/2}$.
7. $(\sqrt{q} - 1)^{2g} \leq \#\mathrm{Jac}(C)(\mathbb{F}_{q^r}) \leq (\sqrt{q} + 1)^{2g}$.

Note that statements 3, 6 and 7 follow easily from the others. We also remark that the bound given in item 6 of the above theorem has been improved by Serre to $|\#C(\mathbb{F}_{q^r}) - (q^r + 1)| \leq g\lfloor 2q^{r/2} \rfloor$ (see Stichtenoth [42] Theorem V.3.1).

The formula of property 5 for $\#\mathrm{Jac}(C)(\mathbb{F}_{q^r})$ is extremely useful. It gives an efficient method for computing the number of points in the divisor class group of a curve over a large-degree extension of the field $\mathbb{F}_q$ once one has computed $P(X)$ (see the next section for details about computing $P(X)$).

For cryptography one wants a curve such that $\#\mathrm{Jac}(C)(\mathbb{F}_{q^r})$ is divisible by a large prime l. The strategy is to try values of r until one is found for which the prime l is sufficiently large for the required security of the application. Note that composite r are likely to give highly composite group orders due to subgroups, and so one invariably uses prime values of r. To be sure that the group resists the known attacks ([13], [34]) on the discrete logarithm problem one should check that $\gcd(l, q) = 1$ and that $q^{kr} \not\equiv 1 \pmod{l}$ for 'small' k. If the original curve is

supersingular then, as we will show, it is futile to try many different values for r since the Frey-Rück attack will always work. Hence, it is important to know that such curves should be discarded right from the start.

5. Computing $P(X)$

From a theoretical point of view, the problem of computing $P(X)$ for any curve has a polynomial time solution (asymptotically as the field size increases and the genus remains fixed) due to Pila [31], however this algorithm does not seem to be suited for practical computation.

Recently there have been some breakthroughs in algorithms for counting points on higher genus curves, particularly in the case of small characteristic. Nevertheless there is still interest in using subfield curves. In this section we focus on some elementary methods which can be used in cases where q is fairly small.

Given a curve $C/\mathbb{F}_q$ of genus $g > 1$ compute $\#C(\mathbb{F}_{q^r})$ for $1 \leq r \leq g$ by exhaustive search. If the curve is given as a non-singular plane curve $f(x, y) = 0$ with a known number of rational points at infinity then the exhaustive search involves trying all values $x_0 \in \mathbb{F}_{q^r}$ and then calculating the number of roots of $f(x_0, y)$ in $\mathbb{F}_{q^r}$. From the values $t_r = q^r + 1 - \#C(\mathbb{F}_{q^r}) = \sum_{i=1}^{2g} \alpha_i^r$ one can obtain the coefficients of $P(X)$ using Newton's identities $a_m = \frac{1}{m}(-t_m - \sum_{i=1}^{m-1} a_i t_{m-i})$ (see Cohen [9] Proposition 4.3.3). This naive algorithm takes time $O(q^g (\log q^g)^c)$ for some constant c, which can also be written as $O(q^{g+\epsilon})$.

One method to speed this up is to compute $\#C(\mathbb{F}_{q^r})$ for $r = 1, \ldots, g-1$ and then to try all values of $\#C(\mathbb{F}_{q^g}) - (q^g + 1)$ (i.e., all integers in the interval $[-2gq^{g/2}, 2gq^{g/2}]$) and test the correctness of the group order probabilistically by computations on $\mathrm{Jac}(C)$ over $\mathbb{F}_q$ or over some extension $\mathbb{F}_{q^m}$. This produces a method of complexity $O(q^{g-1+\epsilon})$.

A variation on the above strategy is to use the method of Stein and Teske [40] which computes $\#\mathrm{Jac}(C)(\mathbb{F}_q)$ in time proportional to q^d where $d \in \mathbb{Z}$ is a suitable rounding of $(2g-1)/5$. One computes $\#C(\mathbb{F}_{q^r})$ for $r = 1, \ldots, g-1$ and then computes $\#\mathrm{Jac}(C)(\mathbb{F}_q)$ from which it is possible to deduce $P(X)$. This method also has complexity $O(q^{g-1+\epsilon})$.

Similarly, one can compute $\#C(\mathbb{F}_{q^r})$ only up to $r = g-2$ and then compute $\#\mathrm{Jac}(C)(\mathbb{F}_q)$ and $\#\mathrm{Jac}(C)(\mathbb{F}_{q^2})$ using [40]. This method has the superior complexity $O(q^{g-2+\epsilon})$ when $g = 4$ or $g \geq 6$. This trick cannot be extended.

6. Supersingular Elliptic Curves

We now recall some facts (see Silverman [38] Theorem V.3.1) about supersingular elliptic curves.

Theorem 3. *Let $q = p^n$ and let E be an elliptic curve over $\mathbb{F}_q$. Suppose the characteristic polynomial of the Frobenius endomorphism is $P(X) = X^2 - tX + q$ so that $\#E(\mathbb{F}_q) = q + 1 - t$. The following conditions are equivalent (in which case, the elliptic curve is said to be 'supersingular').*

1. *The endomorphism ring of E (over the algebraic closure of $\mathbb{F}_q$) is non-commutative (it is an order in a quaternion algebra).*
2. *E has no points of order p, i.e., $E(\overline{\mathbb{F}}_q)[p] = \{0\}$.*
3. *$p | t$.*
4. *There is some integer k such that $\pi^k = \pm q^{k/2}$.*

If none of these conditions hold then the elliptic curve is said to be 'ordinary'.

We now explain why supersingular elliptic curves are always susceptible to the Frey-Rück attack.

Corollary 2. *([27]) Suppose E is a supersingular elliptic curve over $\mathbb{F}_q$. Then statement 4 of Theorem 3 is satisfied for some $k \leq 6$. Furthermore, for that k we have, for every r, that the exponent of the group $E(\mathbb{F}_{q^r})$ divides $q^{rk}-1$.*

Proof. The usual proof that $k \leq 6$ uses results of Waterhouse [47]. We will give an alternative argument in Section 9. Note that k is always such that $q^{k/2} \in \mathbb{Z}$.

For all points $P \in E(\mathbb{F}_{q^r})$ we have $P = \pi^{rk}(P) = \pm[q^{rk/2}]P$. In other words, $[q^{rk}-1]P = 0$ which proves the second assertion. □

This result means that, as discussed in Section 2.3, it is possible to map the discrete logarithm problem on a supersingular elliptic curve $E(\mathbb{F}_{q^r})$ into a discrete logarithm problem in the multiplicative group of the finite field $\mathbb{F}_{q^{kr}}$ with $k \leq 6$. The discrete logarithm problem may then be solved using a subexponential algorithm.

Of course, for any elliptic curve and for any r, if N is the prime-to-p part of $\#E(\mathbb{F}_{q^r})$ then there is some integer k such that $N|(q^{rk}-1)$ (namely, the order of q^r in the group $(\mathbb{Z}/N\mathbb{Z})^*$). The importance of Corollary 2 is that k does not depend on r and that it is universally bounded over all supersingular curves. If the degree could be arbitrarily large then supersingular elliptic curves would not necessarily be weak for cryptography.

Condition 3 of Theorem 3 (that E is supersingular if and only if $p|t$) is often used in practice as a test for whether an elliptic curve is supersingular or not. In Section 8 we will give an analogue of this test in the higher dimensional situation.

7. Generalisation of the notion of Supersingularity

To understand the effect of the Frey-Rück attack on divisor class groups of curves we need a suitable analogue of the notion of supersingularity. We will see that the following definition is the one which is appropriate for our application.

Definition 2. *(Oort [28]) An abelian variety A over $\mathbb{F}_q$ is called* **supersingular** *if A is isogenous (over $\overline{\mathbb{F}}_q$) to a product of supersingular elliptic curves. A curve C over $\mathbb{F}_q$ is called* **supersingular** *if $\mathrm{Jac}(C)$ is supersingular.*

In fact, as can be deduced from Oort [28], the isogeny is defined over some finite extension of $\mathbb{F}_q$. Furthermore, since all supersingular elliptic curves are isogenous over some finite extension one can assume that A is isogenous to E^g.

It is clear that a supersingular abelian variety can have no points of order p. An abelian variety A over $\mathbb{F}_q$ such that $A(\overline{\mathbb{F}}_p)[p] = \{0\}$ is called 'very special' [24]. In dimensions one and two it happens that every very special abelian variety is supersingular, but for dimension three or more this is no longer necessarily the case (see Li and Oort [24] p. 9).

We note, for completeness, that an abelian variety A of dimension g over a finite field $\mathbb{F}_q$ is said to be 'ordinary' if and only if $\#A(\overline{\mathbb{F}}_q)[p] = p^g$. Therefore, when the dimension is two or more then there are abelian varieties which are between the cases of ordinary and very special (e.g., the product $E_1^i \times E_2^{g-i}$ where E_1 is a supersingular elliptic curve and E_2 is an ordinary elliptic curve). The amount of p-torsion can be determined by considering $P_A(T)$ modulo p (see [26], [41]).

An equivalent definition of supersingularity for abelian varieties is that the endomorphism ring $\mathrm{End}_{\overline{\mathbb{F}}_q}(A)$ has rank $4g^2$ over $\mathbb{Z}$. Supersingular abelian varieties have non-commutative endomorphism rings but the converse is not in general true (e.g., the example $E_1^i \times E_2^{g-i}$ above).

An important tool in the study of abelian varieties over finite fields is the following powerful theorem due to Tate [44].

Theorem 4. *Let A and B be abelian varieties over $\mathbb{F}_q$ and let $P_A(X)$ and $P_B(X)$ be the respective characteristic polynomials of Frobenius. Then B is isogenous over $\mathbb{F}_q$ to an abelian subvariety of A if and only if $P_B(X)|P_A(X)$.*

The following result follows from the work of Manin and Oort and the theorems quoted above.

Theorem 5. *The following conditions on an abelian variety A over $\mathbb{F}_q$ of dimension g are equivalent.*

1. *A is isogenous (over some finite extension of $\mathbb{F}_q$) to E^g for some supersingular elliptic curve E (i.e., A is supersingular).*
2. *There is some integer k such that the characteristic polynomial of Frobenius on A over $\mathbb{F}_{q^k}$ is $P(X) = (X \pm q^{k/2})^{2g}$.*
3. *There is some integer k such that $\pi^k = \pm q^{k/2}$.*
4. *For some positive integer k we have $\#A(\mathbb{F}_{q^k}) = (q^{k/2} \pm 1)^{2g}$.*

The third property is the one which is most important for our application (due to an analogue of Corollary 2). However, it is not yet clear what values for k might arise for such curves.

There is a wealth of literature within coding theory about supersingular curves as, over certain extensions, they have the maximal number of points. There is also a wealth of literature in algebraic geometry about supersingular abelian varieties, due to their importance to the study of certain moduli problems (see [24]).

8. A criterion for supersingularity

The following result is a restatement of Proposition 1 of [43]. It gives a simple test for whether or not an abelian variety is supersingular, once $P(X)$ has been computed. Due to its importance in this paper we provide a proof.

Theorem 6. *Suppose $q = p^n$ and suppose A is an abelian variety of dimension g over $\mathbb{F}_q$. Suppose*

$$P(X) = X^{2g} + a_1 X^{2g-1} + a_2 X^{2g-2} + \cdots + a_g X^g + \cdots + q^{g-1} a_1 X + q^g$$

is the characteristic polynomial of the Frobenius endomorphism on A. Then A is supersingular if and only if, for all $1 \leq r \leq g$,

$$p^{\lceil rn/2 \rceil} \mid a_r.$$

Proof. The roots α_i are algebraic integers in some number field K. For each prime $\wp$ of $\mathcal{O}_K$ above p there is an extension ν of the p-adic valuation, so choose one of these arbitrarily and normalise so that $\nu(q) = 1$.

Results of Manin and Oort (see [28] p. 116) show that A is supersingular if and only if $\nu(\alpha_i) = 1/2$ for all i (this is essentially the content of Property 3 of Theorem 5). The statement then follows easily from the fact that the $a_r \in \mathbb{Z}$ are symmetric polynomials of degree r in the α_i.

Conversely, if A is not supersingular then there must be some $\nu(\alpha_i) < 1/2$. From $\alpha_i\alpha_{g+i} = q$ we see that there are at most $r \leq g$ values with $\nu(\alpha_i) < 1/2$ and for all other values we have $\nu(\alpha_i) \geq 1/2$. Now consider the coefficient a_r which is the rth symmetric polynomial in the α_i. This coefficient therefore has one term with valuation strictly less than all other terms (and strictly less than $r/2$). Therefore, the numerical condition in the theorem cannot be satisfied for a_r. □

9. The bound on the extension degree

The number k in Theorem 5 is related to the degree of the isogeny $\mathrm{Jac}(C) \sim E^g$. There are several interesting open problems relating to the degrees of isogenies in the splitting of Jacobians. The case of supersingular curves is the easiest case for these problems.

The values of k which arise depend on properties of cyclotomic polynomials (i.e., irreducible factors over $\mathbb{Z}$ of $X^m - 1$ for some m). Hence we make the following definitions.

Definition 3. *For each positive integer g let $\mathcal{P}_g = \{p(X) \in \mathbb{Z}[X] : \deg p(X) = 2g, p(X)$ irreducible over $\mathbb{Z}, p(X)|(X^m - 1)$ for some $m\}$. For each $p(X) \in \mathcal{P}_g$ define $m(p(X)) = \min\{m : p(X)|(X^m - 1)\}$. Define $k'(g)$ to be $\max\{m(p(X)) : p(X) \in \mathcal{P}_g\}$. Define $k(g)$ to be*

$$\max\Big\{\mathrm{lcm}\big(m(p_1(X)), \ldots, m(p_n(X))\big) : g = \sum_{i=1}^{n} g_i,\ p_i(X) \in \mathcal{P}_{g_i}\Big\}.$$

Theorem 7. *Let A be a supersingular abelian variety of dimension g over a field $\mathbb{F}_q$, then there exists an integer $k \leq k(g)$ such that, for all integers $r \geq 1$, the exponent of $A(\mathbb{F}_{q^r})$ divides $q^{kr} - 1$.*

We emphasise that the bound $k(g)$ depends only on the genus and not on the abelian variety A.

Proof. First, take a quadratic extension so that q^r is a square, i.e., consider $q_0 = q^{2r}$. Let $P(X)$ be the characteristic polynomial of the Frobenius endomorphism on A over $\mathbb{F}_{q_0}$ and write α_i for the roots (they are the squares of the values of the roots corresponding to A over $\mathbb{F}_q$).

We follow the proof of Theorem 4.2 of Oort [28] and consider

$$P'(X) = P(\sqrt{q_0}X)/q_0^g = X^{2g} + (a_1/\sqrt{q_0})X^{2g-1} + \cdots + 1$$

which has roots $\alpha_i/\sqrt{q_0}$. By Theorem 6 the coefficients of $P'(X)$ are integers.

The numbers $\alpha_i/\sqrt{q_0}$ are algebraic integers which are units but, by Theorem 4.1 of Manin [25], it follows that they are actually roots of unity. Therefore $P'(X)$ is a product of cyclotomic polynomials.

By definition of $k(g)$ there is some $k \leq k(g)$ such that $(\alpha_i/\sqrt{q_0})^k = 1$ for all i. In other words, $\alpha_i^k = q_0^{k/2}$ for all i and so $\pi^k = q_0^{k/2}$. It follows by the argument of Corollary 2 that the exponent of $A(\mathbb{F}_{q_0^k})$ divides $q_0^{k/2} - 1$ (also see Stichtenoth and Xing [43] Proposition 2). Since $q_0^{k/2} - 1 = q^{rk} - 1$ and the exponent of $A(\mathbb{F}_{q^r})$ divides the exponent of $A(\mathbb{F}_{q_0})$ the result is proven. □

We now consider the values of $k(g)$. Cyclotomic polynomials $X^m - 1$ factor into products of polynomials $\Phi_n(X)$ for each $n|m$ (see Lang [23] VI.3). The polynomials $\Phi_n(X)$ have degree $\varphi(n)$ (this is the Euler φ-function) so the values of $k'(g)$ are

g	$k'(g)$	$k(g)$	$k(g)/g$
1	6	6	6
2	12	12	6
3	18	$30 = \mathrm{lcm}(6, 10)$	10
4	30	$60 = \mathrm{lcm}(10, 12)$	15
5	22	$120 = \mathrm{lcm}(8, 10, 6)$	24
6	42	$210 = \mathrm{lcm}(6,10,14)$	35
7	$\star$	$420 = \mathrm{lcm}(5,7,12)$	60
8	60	$840 = \mathrm{lcm}(3,5,7,8)$	105

TABLE 1. Values of $k(g)$. The symbol $\star$ indicates the fact that there are no irreducible cyclotomic polynomials of degree 14 (since there are no integers N with $\varphi(N) = 14$).

related to the problem of finding the largest value of n for which $\varphi(n) = 2g$. The extremal case is when n is the product of the first k primes and so $\varphi(n) = n\frac{1}{2}\frac{2}{3}\cdots\frac{p_k-1}{p_k}$ (e.g., $\varphi(6) = 2, \varphi(30) = 8, \varphi(210) = 48$ etc). The values of $k(g)$ relate to the ways of taking least common multiples of the $m(p(X))$. Table 1 lists the values of $k'(g)$ and $k(g)$ for small values of g.

The notation in the $k(g)$ column of Table 1 indicates how the maximum value is attained. For example the case $k(3) = 30$ comes from the cyclotomic polynomials $\Phi_6(X) = X^2 - X + 1$ and $\Phi_{10}(X) = X^4 - X^3 + X^2 - X + 1$. It follows that the smallest degree m such that $\Phi_6(X)\Phi_{10}(X)|(X^m - 1)$ is $m = \mathrm{lcm}(6, 10) = 30$. Hence an abelian variety with $P(X) = q^3\Phi_6(X/\sqrt{q})\Phi_{10}(X/\sqrt{q})$ (which must exist by the Honda-Tate theorem [45]) would have embedding degree 30.

We observe that the above result gives the exact bound $k = 6$ in the elliptic curve case $g = 1$. We only go as far as $g = 8$ since there are subexponential algorithms for solving the discrete logarithm problem on high-genus curves. Indeed, experimental results (e.g., Gaudry [16]) suggest that curves of genus greater than 5 are unlikely to be used for cryptography, as the field size would have to be rather larger than had previously been thought (thus reducing any other advantage which they may have had).

The bound $k(g)$ is sharp, in the sense that there exists an abelian variety over some finite field $\mathbb{F}_q$ for which the bound $k(g)$ is attained. However, we are more interested in Jacobian varieties of curves than in general abelian varieties. When the dimension is sufficiently large none of the abelian varieties for which large values of k are obtained are isogenous to Jacobians of curves. We return to this problem in Section 11.

What do these results tell us about the security of the discrete logarithm problem in the divisor class group of a curve? Recall that the advantage of the divisor class group of a curve of genus g over $\mathbb{F}_q$ is that, over a field $\mathbb{F}_q$ the group has size approximately q^g. Hence, to determine the applicability of the subexponential algorithms for solving the discrete logarithm problem in finite fields, we really should consider $k(g)/g$ which is seen in Table 1 to grow rather slowly. This supports the notion that supersingular curves should be considered weaker than the general case for cryptography.

10. The Curves of Interest in Cryptography

In cryptography the curves under consideration are those for which there are efficient methods for computing in the divisor class group. The main example is of course elliptic curves. One can also use hyperelliptic curves (quadratic function fields) [7], [20]. Recently algorithms have been given for cubic function fields (see [36], [3]) and, more generally, superelliptic curves [15] and curves which have a totally ramified point [1].

For curves of genus 2 or more it has often been the case that curves are defined over small fields such as $\mathbb{F}_2$ or $\mathbb{F}_{2^2}$ to facilitate easy point counting as discussed in Sections 4 and 5.

For now we recall a couple of facts. A hyperelliptic curve of genus g has a non-singular affine equation of the form

$$y^2 + h(x)y = f(x)$$

where $\deg h(x) \leq g+1$ and $\deg f(x) \leq 2g+2$. In characteristic not equal to two we can take $h(x) = 0$ and the curve has one point at infinity if $\deg f(x) = 2g+1$ and two points at infinity (possibly defined over a quadratic extension) if $\deg f(x) = 2g+2$. In characteristic two the curve has two points at infinity if and only if $\deg(h(x)) = g+1$ (and if $h(x)$ has a root then one may transform to an equation with only one point at infinity). The case of hyperelliptic curves with one point at infinity is favoured for simplicity but the other case is more general. See [29], [30] for more details.

A superelliptic curve (see [15]) has an affine equation of the form $y^n = f(x)$ over $\mathbb{F}_q$ where $\gcd(n, q) = 1$, $\gcd(n, \deg f(x)) = 1$ and $\gcd(f(x), f'(x)) = 1$. Such curves have only one point at infinity and they have genus $\frac{1}{2}(n-1)(\deg f(x) - 1)$.

When working with a new family of curves it is important to know that they give examples not already found in the earlier families. The following result shows that there exist superelliptic curves which are not hyperelliptic.

Theorem 8. *Consider the superelliptic curve $C : y^m = f(x)$ over a field k where $m \geq 3$ is odd and coprime to the characteristic of the field k. Suppose that $\deg(f(x)) = d$, $\gcd(m, d) = 1$, $\gcd(f(x), f'(x)) = 1$, and that $(3m-1)/(m-1) \leq d$. Then C is not hyperelliptic.*

Proof. Suppose instead that C is hyperelliptic with function field F. Then there exists a function w such that $[F : k(w)] = 2$. From the equation for the curve we have $[F : k(x)] = m$.

The condition $(3m-1)/(m-1) \leq d$ implies that $m \leq g$ and so, by Proposition VI.2.4 (a) of [42] we have $k(x) \subset k(w)$.

It follows that $m = [F : k(x)] = [F : k(w)][k(w) : k(x)]$ which is a contradiction since m is odd. □

11. Are large values of k attained for curves?

In Section 9 we have given an upper bound on the value of k which can arise. This bound is sharp, in the sense that it is attained for some supersingular abelian variety of dimension g. However, when the genus is three or more, not every abelian variety is isogenous to the Jacobian of a curve. Hence it makes sense to ask what the maximum values of k are for supersingular curves of genus g.

In this section some examples of curves with relatively large values for k are given. When $g > 2$ it is seen that the values are much lower than the upper bounds given above. To actually prove sharp bounds in this case is an interesting open problem and we do not have any theoretical results in this direction.

Note that the maximum value for k is attained in the case of genus one and two curves. This fact is not surprising since every elliptic curve is a Jacobian, and every isogeny class of abelian varieties of dimension two contains a representative which is either a product of elliptic curves or the Jacobian of a hyperelliptic curve (possibly this process requires an extension of the ground field). However, in the case of dimension four or more we would not necessarily expect the bounds to be attained.

The case of dimension three is particularly interesting, since every isogeny class of absolutely simple abelian varieties of dimension three should contain a Jacobian of a genus three curve (not necessarily hyperelliptic) over some extension field. However, we have not found any supersingular curves giving values of k near the bound. One further surprising fact is that we have not found any supersingular hyperelliptic curves of genus three in characteristic two.

Field	Curve C	$P(X)$	# points	k
$\mathbb{F}_p$ (1)	$y^2 = x^3 + a$	$X^2 + p$	$p+1$	2
$\mathbb{F}_3$	$y^2 = x^3 + 2x \pm 1$	$X^2 \pm 3X + 3$	7,1	6
$\mathbb{F}_2$	$y^2 + y = x^5 + x^3$	$X^4 + 2X^3 + 2X^2 + 4X + 4$	13	12
$\mathbb{F}_3$	$y^2 = x^6 + x + 2$	$X^4 + 3X^2 + 9$	13	3
$\mathbb{F}_5$	$y^2 = x^5 + 2x^4 + x^3 + x + 3$	$X^4 - 5X^3 + 15X^2 - 25X + 25$	11	5
$\mathbb{F}_{2^2} = \mathbb{F}_2(\theta)$	$x^4 + \theta x y^3 + y z^3$ (2)	$X^6 - 8X^3 + 2^6$	57	9
$\mathbb{F}_3$	$y^2 = x^7 + 1$	$X^6 + 3^3$	28	6
$\mathbb{F}_5$	$y^2 = x^8 + 2x^4 + 3x^2 + 2$	$X^6 - 5X^5 + 20X^4 - 50X^3$ $+100X^2 - 125X + 125$	66	10
$\mathbb{F}_7$	$y^2 = x^8 + x^4 + 5x^3$ $+6x^2 + x + 2$	$X^6 + 7X^5 + 21X^4 + 49X^3 + 147X^2$ $+7^3X + 7^3$	911	14
$\mathbb{F}_2$	$y^2 + y = x^9 + x^4 + 1$	$X^8 - 2X^7 + 2X^6 - 4X^5$ $+8X^4 - 8X^3 + \cdots + 2^4$	5	12

Notes: (1) In the first row p must be an odd prime congruent to 2 modulo 3.

(2) This genus 3 curve is a plane quartic and is not hyperelliptic. It can be written as the affine superelliptic curve $z^3 = x^4 + \theta x^2$.

It should be possible to generate supersingular curves of genus two and three using the CM method. This is an avenue for further research.

It may strike the reader as strange that we mainly list curves over small fields such as $\mathbb{F}_2$ or $\mathbb{F}_3$. Remember that one can consider the group $\mathrm{Pic}^0_C(\mathbb{F}_{q^l})$ for some large prime number l and the value k for this case will be exactly the same. More importantly, it is known that for elliptic curves one can only obtain $k > 3$ in characteristic two or three, and we expect analogous results in the higher genus case (this is another avenue for further research). Hence it makes sense to search for large values of k only when the characteristic of the field is small.

12. Equations of supersingular curves

For applications, especially when using subfield curves, it is very important to know in advance which equations are likely to give rise to supersingular curves. For instance, Sakai, Sakurai and Ishizuka [35] suggested some hyperelliptic curves for use in cryptography. On page 172 they mention that they were unable to find any secure genus 2 curves over $\mathbb{F}_2$. The reason for this is that they restricted their attention to equations of the form $C : y^2 + y = f(x)$ for some monic polynomial $f(x) \in \mathbb{F}_2[x]$ of degree 5. We will show that all genus two curves of this form over $\mathbb{F}_{2^n}$ are supersingular.

The first observation is that any hyperelliptic curve in characteristic two of the form $y^2 + h(x)y = f(x)$ with $1 \leq \deg(h(x)) \leq g + 1$ cannot be supersingular. To see this note that any root x_0 of $h(x)$ gives rise to a point (x_0, y_0) (possibly over a quadratic extension) of order 2, and recall that a supersingular curve in characteristic p has no points (even over algebraic extensions) of order p.

Therefore, curves of the form $y^2 + y = f(x)$ are certainly a poor choice in characteristic two if one wants to avoid supersingular cases. However, the argument sketched above does not imply that all such curves are necessarily supersingular. Our main result in this section is that this is true in the case of genus two curves. The first result concerns the polynomial $P(X)$ for curves of this form.

Lemma 2. *Let C be a genus 2 curve over $\mathbb{F}_{2^n}$ of the form $y^2 + cy = f(x)$ where $f(x)$ is monic of degree 5 and $c \in \mathbb{F}_{2^n}^*$. Then the coefficients a_1 and a_2 in the polynomial $P(X)$ are both even.*

Proof. For equations of this form the number of points on the curve over all extensions $\mathbb{F}_{2^{nm}}$ is odd, since apart from the point at infinity, points come in pairs (x_0, y_0) and $(x_0, y_0 + c)$. The fact that $\#C(\mathbb{F}_{2^n}) = 2^n + 1 - a_1$ is odd implies that a_1 is even.

On $C(\mathbb{F}_{2^{2n}})$ there are two points for each possible $x_0 \in \mathbb{F}_{2^n}$ (the corresponding y-coordinates may be in $\mathbb{F}_{2^n}$ or $\mathbb{F}_{2^{2n}}$). For any point with $x_0 \notin \mathbb{F}_{2^n}$ there are the four distinct 'conjugates' $(x_0, y_0), (x_0, y_0 + c), (\pi(x_0), \pi(y_0)), (\pi(x_0), \pi(y_0) + c)$ where π is the Frobenius automorphism of $\mathbb{F}_{2^{2n}}/\mathbb{F}_{2^n}$. It follows that $\#C(\mathbb{F}_{2^{2n}}) \equiv 1 \pmod{2^{n+1}}$. Write $t_2 = 2^{2n} + 1 - \#C(\mathbb{F}_{2^{2n}})$. Then t_2 is divisible by 4 and from $a_1^2 = t_2 + 2a_2$ it follows that a_2 is even. □

If the curve C is actually defined over $\mathbb{F}_2$ then Theorem 6 implies that the curve is supersingular. In the general case we need a further argument.

Theorem 9. *Let C be a genus 2 curve over $\mathbb{F}_{2^n}$ of the form $y^2 + cy = f(x)$ where $f(x)$ is monic of degree 5 and $c \in \mathbb{F}_{2^n}^*$. Then C is supersingular.*

Proof. Using Lemma 2 we see that $P(X) \equiv X^4 \pmod 2$. By a result of Manin [26] (also see Stichtenoth [41] Satz 1) it follows that $\mathrm{Jac}(C)(\overline{\mathbb{F}}_{2^n})$ has no points of order 2. In the case of dimension 2, this condition is known (see Li and Oort [24] p. 9) to be equivalent to supersingularity. □

An alternative proof of the above result can be given by using the theory of the Newton polygon and some class field theory. One shows that, in genus 2, the only polynomials $P(X)$ which satisfy the condition of Lemma 2 also satisfy the condition of Theorem 6 (see Rück [32] for details of this approach).

Note that both of these arguments rely heavily on the fact that we are in the genus 2 case (indeed, below we give a secure genus three example).

We note that $\#C(\mathbb{F}_2)$ and $\#C(\mathbb{F}_{2^2})$ being odd does not alone imply that C is supersingular. An example is the genus two curve $y^2+(x^2+x+1)y = x^5+1$ which has 3 points over $\mathbb{F}_2$ and 7 points over $\mathbb{F}_{2^2}$ and so $P(X) = X^4+X^2+4$ and C is not supersingular.

The authors of [35] could also have considered curves of the form $y^2+xy = f(x)$ (with degree five $f(x) \in \mathbb{F}_2[x]$). In these cases it is clear that $\#C(\mathbb{F}_{2^n})$ is always even, in which case a_1 is always odd and, by Theorem 6 the curve cannot be supersingular. Indeed, the same argument shows that curves of the form $y^2+xy = f(x)$ with $f(x) \in \mathbb{F}_{2^n}[x]$ of odd degree are an infinite family of non-supersingular hyperelliptic curves. It is easy to find suitable examples of genus 2 curves of this form, for instance $C : y^2+xy = x^5+x^2+1$ has $P(X) = X^4-X^3-2X+4$. One can show that

$$\begin{aligned}\#\mathrm{Jac}(C)(\mathbb{F}_{2^{97}}) &= 2 \cdot 389 \cdot 1747 \cdot \\ &\quad 184733924638688269103187946767540719407160990701961 9 \\ \#\mathrm{Jac}(C)(\mathbb{F}_{2^{103}}) &= 2 \cdot 47381 \cdot \\ &\quad 10852877190495703277390509258459145399489273609233701107 69\end{aligned}$$

where the large numbers are proven primes according to Magma. In both cases the Frey-Rück embedding degree exceeds 10^{50} so there are no worries here.

The above arguments suggest that, in characteristic two, only curves of the form $y^2+h(x)y = f(x)$ with $\deg(h(x)) \geq 1$ should be used in cryptography. However, this is not necessarily the conclusion one wants to draw, since equations of the form $y^2+y = f(x)$ give some implementation efficiency (see Smart [39] Section 1 and [12] Theorem 14). In the case of genus three it is possible to give 'safe' examples. For instance, the curve $C : y^2+y = x^7$ of [35] has $P(X) = X^6-2X^3+2^3$ and the fact that a_3 is not divisible by $2^{\lceil 3/2 \rceil}$ means that C is not supersingular. Note however that such a curve is necessarily very special (i.e., it has no 2-torsion).

Another strategy would be to use genus two curves of the form $y^2+h(x)y = f(x)$ over $\mathbb{F}_{2^n}$ which always have two points at infinity (i.e., $\deg(h(x)) = 3$ such that $h(x)$ has no root in the ground field). In these cases one also has a_1 odd, and so the curves are not supersingular.

13. Some Examples of Superelliptic Curves

The case of hyperelliptic curves has been fairly thoroughly explored in the past [20], [21], [6], [35], [39]. In particular, [6] mention cases which are guaranteed to be non-supersingular. We give some examples of superelliptic curves with group orders suitable for cryptography. (When they were first written then these were the first examples; nowadays there are much better examples available using the p-adic point counting methods [17]).

In all cases the large numbers l are proven primes according to Magma. In all cases the curves are resistant to the Frey-Rück attack (to calculate the exact embedding degree involves factoring $l-1$ but it is sufficient to find all factors of $l-1$ less than say 1000 to convince oneself that the curve is acceptable).

Note that the curve $y^3 = f(x)$ over $\mathbb{F}_{2^n}$ has exactly 2^n+1 points when n is odd (since in those cases 3 is coprime to the order of $\mathbb{F}_{2^n}^*$). This means that, in the case where the ground field is an odd degree extension of $\mathbb{F}_2$, to compute $P(X)$ it is only necessary to count the number of points over even degree extensions of the ground

$g = 3$ $\quad C : y^3 = x^4 + x^3 + \alpha x^2 + x + \alpha$ over $\mathbb{F}_{2^2}$ $P(X) = X^6 + 3X^4 + 4X^3 + 12X^2 + 2^6$ $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{2\cdot 41}}) = 2^2 \cdot 3 \cdot 7 \cdot 1231 \cdot 12547 \cdot 839353 \cdot$ 1038381756516645166417655013254676491970300083007611871486 61 (197 bit)
$g = 3$ $\quad C : y^3 = x^4 + x^3 + \alpha x + 1$ over $\mathbb{F}_{2^5}$ $P(X) = X^6 + 39X^4 + 1248X^2 + 2^{15}$ $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{5\cdot 23}}) = 2^4 \cdot 3^2 \cdot 5^5 \cdot 7 \cdot 11 \cdot 83 \cdot$ 2492109798490576496039157599339008557786267412476240267701846468 15 7097886998392240817583153795 9 (314 bit)
$g = 4$ $\quad C : y^3 = x^5 + 1$ over $\mathbb{F}_2$ $P(X) = X^8 - 2X^4 + 16$ $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{43}}) = 3 \cdot 5 \cdot 4129 \cdot$ 96654730063895670508796204430057604912608599311 (157 bit)
$g = 4$ $\quad C : y^3 = x^5 + x + 1$ over $\mathbb{F}_2$ $P(X) = X^8 + 2X^6 + 6X^4 + 8X^2 + 16$ $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{43}}) = 3 \cdot 11 \cdot$ 18140335474265631308087819230436531735482571053564 9 (167 bit) $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{61}}) = 3 \cdot 11 \cdot 12323 \cdot$ 69516604910881473963537569029137158267066937810090081 343111639513643 (226 bit)

TABLE 2. Examples of superelliptic curves suitable for cryptography.

field. In other words, when g is odd, one can compute $P(X)$ in time $O(q^{g-1+\epsilon})$ without using the tricks of Section 5. Note however that while such curves are not supersingular, they are also not ordinary (i.e., they do not have full 2-torsion).

Table 2 lists some non-supersingular superelliptic curves. In all cases the symbol α represents a generator of the multiplicative group of the field of definition. As usual, one must be careful about the use of curves such as these due to the large automorphism group [10], [16].

14. Conclusion

We have studied the impact of the Frey-Rück attack on supersingular curves. We emphasise that even in the non-supersingular case one should be careful: Given a divisor class group of a curve of genus g over $\mathbb{F}_q$ such that the group order is divisible by a large prime l one should always check that $\gcd(l, q) = 1$ and that

$$q^k \not\equiv 1 \pmod{l}$$

for all k between 1 and, say, $20g$.

15. Acknowledgements

It is a pleasure to thank Hans-Georg Rück for indicating both proofs of Theorem 9; Nigel Smart, Dan Boneh and Keith Harrison for discussions on the Boneh and Franklin scheme; Pierrick Gaudry for discussions about hyperelliptic curves in characteristic two; and Alice Silverberg for helpful comments on an earlier draft of the paper.

References

1. S. Arita, Algorithms for computations in Jacobian group of $C_{a,b}$ curve and their application to discrete-log-based public key cryptosystems, in A. Odlyzko et al (ed.), "The mathematics of public key cryptography", Fields Institute, 1999.
2. R. Balasubramanian and N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm., *J. Cryptology*, **11** no. 2 (1998) 141–145.
3. E. R. Barreiro, J.-P. Cherdieu and J. E. Sarlabous, Efficient reduction on the jacobian variety of picard curves, in J. Buchmann et al (eds.), "Coding theory, cryptography and related areas", Springer, 2000.
4. D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, in J. Kilian (ed.) Crypto 2001, Springer LNCS 2139 (2001).
5. B. W. Brock, Superspecial curves of genera two and three, Ph.D. Thesis, Princeton, 1993.
6. J. Buhler and N. Koblitz, Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems, *Bull. Aust. Math. Soc.*, **58**, No.1 (1998) 147–154.
7. D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.*, **48** (1987) 95–101.
8. C. Cocks, Identity based cryptosystems, talk at the University of Bristol on May 29th, 2001. More information available from: `http://www.cesg.gov.uk/id-pkc/`
9. H. Cohen, A course in computational number theory, Springer GTM 138 1993.
10. I. Duursma, P. Gaudry and F. Morain, Speeding up the discrete log computation on curves with automorphisms, in Lam et al (ed.), Asiacrypt '99, Springer LNCS 1716, 1999.
11. T. Ekedahl, On supersingular curves and abelian varieties, *Math. Scand.*, **60** (1987) 151–178.
12. A. Enge, The extended Euclidean algorithm on polynomials and the computational efficiency of hyperelliptic cryptosystems, *Designs, Codes and Cryptography*, **23** (2001) 53–74.
13. G. Frey and H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, *Math. Comp.*, **62**, No.206 (1994) 865–874.
14. G. Frey, M. Müller and H.-G. Rück, The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, *IEEE Trans. Inform. Theory*, **45**, no. 5 (1999) 1717–1719.
15. S. D. Galbraith, S. Paulus and N. P. Smart, Arithmetic on superelliptic curves, To appear in *Math. Comp.*
16. P. Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves, in B. Preneel (ed.), Eurocrypt 2000, Springer, LNCS 1807 (2000) 19–34.
17. P. Gaudry, N. Gurel, An extension of Kedlaya's algorithm for counting points of superelliptic curves, to appear in Asiacrypt 2001 (2001).
18. A. Joux, A one round protocol for tripartite Diffie-Hellman, in W. Bosma (ed.), Ants-IV, Springer LNCS 1838 (2000) 385–393.
19. A. Joux and K. Nguyen, Separating Decision Diffie-Hellman from Diffie-Hellman in cryptographic groups, preprint (2001)
20. N. Koblitz, Hyperelliptic cryptosystems, *J. Cryptology*, **1**, no. 3 (1989) 139–150.
21. N. Koblitz, A family of jacobians suitable for discrete log cryptosystems, in S. Goldwasser (ed.), Crypto '88, Springer LNCS 403 (1990) 94–99.
22. N. Koblitz, An elliptic curve implementation of the finite field digital signature algorithm, in H. Krawczyk (ed.), Crypto '98, Springer LNCS 1462 (1998) 327–337.
23. S. Lang, Algebra, 3rd ed., Addison-Wesley, 1993.
24. K.-Z. Li and F. Oort, Moduli of supersingular abelian varieties, Springer LNM 1680 1998.
25. Yu. I. Manin, The theory of commutative formal groups over fields of finite characteristic, *Russ. Math. Surv.*, **18**, No. 6 (1963) 1–83.
26. Yu. I. Manin, The Hasse-Witt matrix of an algebraic curve, *Translations, II Ser.*, Am. Math. Soc., **45** (1965) 245–264.
27. A. J. Menezes, T. Okamoto and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inf. Theory*, **39**, No. 5 (1993) 1639–1646.
28. F. Oort, Subvarieties of moduli spaces, *Inv. Math.*, **24** (1970) 95–119.
29. S. Paulus and H.-G. Rück, Real and imaginary quadratic representations of hyperelliptic function fields, *Math. Comp.*, **68**, No. 227 (1999) 1233–1241.
30. S. Paulus and A. Stein, Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves, in J. Buhler, (ed.), Ants III, Springer LNCS 1423 (1998) 576–591.

31. J. Pila, Frobenius maps of abelian varieties and finding roots of unity in finite fields, *Math. Comp.*, **55**, No.192 (1990) 745–763.
32. H.-G. Rück, Abelsche varietäten niderer dimension über endlichen körpern, Habilitation Thesis, University of Essen, 1990.
33. H.-G. Rück, Abelian surfaces and Jacobian varieties over finite fields, *Comp. Math.*, **76** (1990) 351–366.
34. H.-G. Rück, On the discrete logarithm in the divisor class group of curves, *Math. Comp.*, **68**, No.226 (1999) 805–806.
35. Y. Sakai, K. Sakurai and H. Ishizuka, Secure hyperelliptic cryptosystems and their performance, in H. Imai et al. (eds.), PKC '98, Springer LNCS 1431 (1998) 164–181.
36. R. Scheidler, Ideal arithmetic and infrastructure in purely cubic function fields, to appear in *J. Th. Nomb. Bord.*
37. A. Shamir, Identity-based cryptosystems and signature schemes, In G.R. Blakley and D. Chaum (eds.), CRYPTO '84, Springer LNCS 196 (1985) 47–53..
38. J. H. Silverman, The arithmetic of elliptic curves, Springer GTM 106, 1986.
39. N. Smart, On the performance of hyperelliptic cryptosystems, in J. Stern (ed.), EUROCRYPT '99, Springer LNCS 1592 (1999) 165–175.
40. A. Stein and E. Teske, Explicit bounds and heuristics on class numbers in hyperelliptic function fields, University of Waterloo technical report CORR 99-26 (1999), to appear in *Math. Comp.*
41. H. Stichtenoth, Die Hasse-Witt-invariante eines kongruenzfunktionenkörpers, *Arch. Math.*, **33**, No. 4 (1980) 357–360.
42. H. Stichtenoth, Algebraic function fields and codes, Springer Universitext, 1993.
43. H. Stichtenoth and C. Xing, On the structure of the divisor class group of a class of curves over finite fields, *Arch. Math.*, Vol. **65** (1995) 141–150.
44. J. Tate, Endomorphisms of abelian varieties over finite fields, *Inv. Math.*, **2** (1966) 134–144.
45. J. Tate, Classes d'isogénie de variétés abéliennes sur un corps fini (d'après T. Honda), *Sém. Bourbaki*, Exp. 352, Springer LNM 179 (1971) 95–110.
46. E. R. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, in B. Pfitzmann (ed.), EUROCRYPT 2001, Springer LNCS 2045 (2001), 195–210.
47. W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.*, 4^e série, t. 2 (1969) 521–560.

MATHEMATICS DEPARTMENT, ROYAL HOLLOWAY UNIVERSITY OF LONDON, EGHAM, SURREY TW20 0EX, UK.

E-mail address: Steven.Galbraith@rhul.ac.uk