Supersingular Curves in Cryptography

Steven D. Galbraith*

Mathematics Department,
Royal Holloway University of London,
Egham, Surrey TW20 0EX, UK.
Steven.Galbraith@rhul.ac.uk

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 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 which imply that supersingular curves are weaker than the general case for cryptography. 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. The generalised scheme provides a significant reduction in bandwidth compared with the original scheme.

1 Introduction

Frey and Rück [8] described how the Tate pairing can be used to map the discrete logarithm problem in 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 large prime order l of the divisor class group $\mathrm{Pic}_C^0(\mathbb{F}_q)$ is such that $l|(q^k-1)$. In general the value of k depends on both the field and the curve and is very large (i.e., $\log(k) \approx \log(q)$).

Menezes, Okamoto and Vanstone [23] showed that for supersingular elliptic curves the value k above is always less than or equal to 6. This important result

* 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.

C. Boyd (Ed.): ASIACRYPT 2001, LNCS 2248, pp. 495–513, 2001.

implies that supersingular elliptic curves are weaker than the general case for cryptography.

Elliptic curve cryptography was generalised to higher genus curves by Koblitz [16]. Our main result is Theorem 3 which states 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 (see Table 1) that supersingular curves should be considered weaker than the general case for cryptography.

It is important to be able to detect these weak cases in advance, especially when one is considering curves defined over small fields and using the zeta function to compute the group order over extension fields. Sakai, Sakurai and Ishizuka [27] were unable to find any secure hyperelliptic curves of genus two over $\mathbb{F}_2$. In Section 5 we show why the authors of [27] failed in their search and we explain how to avoid equations for supersingular curves in characteristic two. As an illustration we overcome the problem encountered in [27] and provide examples of secure genus two curves over $\mathbb{F}_2$.

Recently, beginning with the work of Joux [14], the Weil pairing has found positive applications in cryptography. In Section 3 we generalise an identity-based cryptosystem due to Boneh and Franklin [2]. Our scheme provides a significant improvement in bandwidth over the scheme of Boneh and Franklin.

2 The Tate Pairing

In this section we summarise various known results. Throughout the paper C is 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 $\mathbb{F}_q$. The $\mathbb{F}_q$-rational points on the Jacobian correspond to the divisor class group of the curve over $\mathbb{F}_q$, which we denote $\mathrm{Pic}^0_C(\mathbb{F}_q)$ (for background details see [4], [16], [29], [33]).

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 The Tate Pairing

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 The Tate pairing is a mapping

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

where the right hand side is the quotient group of elements of $\mathbb{F}^*_{q^k}$ modulo lth powers. Note that all three groups $G[l]$, G/lG and $\mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^l$ have exponent l. The Tate pairing satisfies the following properties [8]:

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.

The Tate pairing is computed as follows: Let P be a divisor of order l. There is a function f whose divisor, which we write as (f), is equal to lP. 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 [8], [9]).

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

One subtlety when implementing the Tate pairing is finding a divisor 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 $(Q) - (\infty)$ is the target divisor and where S is an arbitrary point (not necessarily of order l). In the higher genus case general Riemann-Roch algorithms can be used to 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 $\langle P, Q'\rangle \notin (\mathbb{F}_{q^k}^*)^l$.

In the case of elliptic curves one can compare the Tate pairing with the Weil pairing. 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 this field to be larger than that used for the Tate pairing, however at ECC '97 Koblitz observed that these fields are usually the same. Finally, the Weil pairing requires roughly twice the computation time as the Tate pairing, although this is partly offset by the added cost of a finite field exponentiation (to the power $(q^k - 1)/l$) in the case of the Tate pairing if a unique value is required.

2.2 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 [8]). Let $D_1, D_2 \in \mathrm{Pic}_C^0(\mathbb{F}_q)$ 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 the pairing is non-degenerate (hence $l | (q^k - 1)$). 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. Raise ζ_i to the power $(q^k-1)/l$ (this stage is optional since the linear algebra in the index calculus method below should be performed modulo l).
4. Solve the discrete logarithm problem $\zeta_2 = \zeta_1^\lambda$ in 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:

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 curves for which the Frey-Rück attack applies (e.g., elliptic curves over $\mathbb{F}_p$ with $p-1$ points).

2.3 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 $P \in \mathrm{Pic}^0_C(\mathbb{F}_q)$ then $\langle P, P\rangle \in \mathbb{F}^*_q$, but if l is prime and if l does not divide $(q-1)$ then $\langle P, P\rangle \in (\mathbb{F}^*_{q^k})^l$ since every element of $\mathbb{F}^*_{q^k}$ is an lth power in that case. Hence to have $\langle P, P\rangle$ nontrivial it is necessary (but not sufficient) that $l|(q-1)$ and so $k = 1$.

The following result originates from the work of [2] and [36]. It provides a very useful technique for finding points where the pairing is non-degenerate.

Lemma 1. *Let E be an elliptic curve. 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 $G[l] \cong G/lG$). Let ψ be an endomorphism of E which is not defined over $\mathbb{F}_q$. If $\psi(P) \notin E(\mathbb{F}_q)$ then $\langle P, \psi(P)\rangle^{(q^k-1)/l} \neq 1$.*

For the proof see the full version [11]. We refer to the maps ψ as 'non-$\mathbb{F}_q$-rational endomorphisms' (Verheul [36] calls them 'distortion maps').

In the case of curves of genus greater than one then this result is no longer true. On the other hand, in this setting there are usually many endomorphisms ψ available. Indeed, for supersingular abelian varieties it will generally be true that, for all P, there is some endomorphism ψ such that $\langle P, \psi(P)\rangle^{(q^k-1)/l} \neq 1$.

3 Identity-Based Cryptosystems Using the Tate Pairing

Identity based cryptography was proposed by Shamir [28] 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 [2] developed a new identity-based cryptosystem using the Weil pairing on a specific supersingular elliptic curve. In this section we show that the use of other supersingular curves leads to significant efficiency improvements over the original scheme.

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, 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 [2]). 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 of [2] as random oracles.

3.2 User's Public and Private Key

We now discuss how a user's identity gives rise to a public key. There must be a procedure to convert the identity of user A (such as their name or email address). to a divisor $Q_A \in G = \mathrm{Pic}^0_C(\mathbb{F}_{q^k})$ such that:

1. $\langle P, Q_A\rangle \notin (\mathbb{F}^*_{q^k})^l$.
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 [2] 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. We now sketch a generalisation of their method.

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 $\mathrm{Pic}^0_C(\mathbb{F}_q)$. 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 non-$\mathbb{F}_q$-rational endomorphism from the available possibilities where m is the cofactor $\#\mathrm{Pic}^0_C(\mathbb{F}_q)/l$. This process is repeated until $\langle P, Q_A\rangle^{(q^k-1)/l} \neq 1$.

A more general scheme, which does not require non-$\mathbb{F}_q$-rational endomorphisms, is given in [11].

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

3.3 Encryption and Decryption

Let the message M be a bitstring of length N and suppose we want to send this to user A. First derive the public key Q_A from the identity of A and obtain the dealer's public keys P and P'. The remaining steps are

1. Choose a random integer $1 \leq r \leq l$.
2. Compute $R = rP$.
3. Compute $S = M \oplus H_2(\langle P', Q_A\rangle^{r(q^k-1)/l})$. (Recall that $\langle P', Q_A\rangle \in \mathbb{F}^*_{q^k}$.)
4. Send (R, S).

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

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

A more versatile encryption process is obtained by using $H_2(\langle P', Q_A\rangle^{r(q^k-1)/l})$ as the key for a fixed symmetric encryption function.

3.4 Security

The security of this system relies on the following variant of the Diffie-Hellman problem:

Definition 1. *The* **Tate-Diffie-Hellman problem (TDH)** *is the following: Let G and l be as above. Given divisors $P, P' = sP, R = rP$ and $Q_A \in G$ of order l such that $\langle P, Q_A\rangle^{(q^k-1)/l} \neq 1$ 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 l. We make the assumption that the Tate-Diffie-Hellman problem is hard over random P', R, Q_A,

i.e., where $Q_A = \psi(Q)$ (for a suitable non-$\mathbb{F}_q$-rational endomorphism) and where $P', R, Q \in \langle P \rangle$ are chosen uniformly at random.

If one can solve the elliptic curve Diffie-Hellman problem then one can compute rsP and thus $\langle rsP, Q_A \rangle$. Similarly, if one can solve the Diffie-Hellman problem in $\mathbb{F}^*_{q^k}$ then one can solve the TDH.

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 [2]. First it is necessary to establish that the basic scheme has the 'one-way encryption' (ID-OWE) security property (see Section 2 of [2]). The security proof for the scheme above is completely analogous to the proof of Theorem 4.1 of [2] and it holds under the assumptions that the hash functions H_1 and H_2 are random oracles and that the TDH problem is hard.

3.5 Parameter Sizes and Performance

For security it is necessary that $q^g \geq 2^{160}$ and $q^k \geq 2^{1024}$. Boneh and Franklin [2] use $g = 1$ and $k = 2$ and so they must take q to be of size at least 512 bits[1]. 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 Section 3.6 we give the details for a curve with $k = 6$. Hence there are the following advantages of the generalised scheme compared with the scheme of [2].

- The bandwidth (number of bits) of an encryption (R, S) can be reduced (see Section 3.6 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. Since this involves computations in the large field $\mathbb{F}_{q^k}$ the cost of encryption and decryption is roughly comparable for both schemes, although there are some savings available in characteristic two.

As mentioned in [2], the computation of the Weil and Tate pairings can be made much faster by choosing the prime l of size around 160 bits.

3.6 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 [18].

[1] Actually, in [2] it is specified that q have 1024 bits, but 512 bits seems to be sufficient.

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

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

where $i \in \mathbb{F}_{3^2}$ satisfies $i^2 = -1$ and $\alpha \in \mathbb{F}_{3^3}$ satisfies $\alpha^3 - \alpha + 1 = 0$.

We list some values of m such that the group order of $E_i(\mathbb{F}_{3^m})$ is equal to a small cofactor c 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	1	259	1
167	1	262	7
167	2	237	$8017 \cdot 44089$
173	2	241	16420688749
193	2	306	1
239	2	379	1

Consider, say, the case $m = 163$ 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.

3.7 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 [2].

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 $\mathbb{F}_2$. 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 $P_{E_2}(X) = X^2 - 2X + 2$.

We list some values of m such that $\#E_i(\mathbb{F}_{2^m}) = cl$ 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 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 using the Magma computer algebra package. 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.

3.8 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 question of Section 2.2

For supersingular curves we will show in Section 4.3 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 seems that one cannot realise these large values for $k(g)$ with suitable Jacobians of curves. It seems that the supersingular elliptic curves with $k = 4$ and $k = 6$ are the optimal choice for the identity-based cryptosystem and other applications using supersingular curves. More research is needed to clarify this.

It is not necessary to insist on using supersingular curves for the identity-based cryptosystem, since there should exist non-supersingular elliptic curves E over certain finite fields $\mathbb{F}_q$ with relatively small values of k. However, for such E 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 $p = 2l+1$, but these only have $k = 1$). This phenomenon is indicated by the results of Balasubramanian and Koblitz [1] and is confirmed by computer experiments. It would be extremely interesting to have a construction for non-supersingular curves with relatively small values of k.

4 Supersingular Curves over Finite Fields

In this section we recall some facts about supersingular curves and we give our main result (Theorem 3). More details can be found in the full version of this paper [11].

As before, C is a non-singular, irreducible curve of genus g over a finite field $\mathbb{F}_q$. The Frobenius endomorphism π on $\mathrm{Jac}(C)$ satisfies a characteristic polynomial $P(X)$ of degree $2g$ with integer coefficients. 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. In particular:

1. The numbers α_i satisfy $|\alpha_i| = \sqrt{q}$ and they can be indexed such that $\alpha_i\alpha_{g+i} = q$.
2. $P(X)$ has the following form

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

3. For any integer $r \geq 1$ we have $\#C(\mathbb{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$.
4. For any integer $r \geq 1$ we have $\#\mathrm{Jac}(C)(\mathbb{F}_{q^r}) = \prod_{i=1}^{2g}(1 - \alpha_i^r)$.

The formula of property 4 for $\#\mathrm{Jac}(C)(\mathbb{F}_{q^r})$ 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 Appendix 1 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 and such that the group resists the known attacks ([8], [26]) on the discrete logarithm problem.

A common strategy is to try values of r until one is found for which the large prime l satisfies $\gcd(l, q) = 1$ and $q^{kr} \not\equiv 1 \pmod{l}$ 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.

4.1 Supersingularity

Recall that an elliptic curve E over $\mathbb{F}_{p^m}$ is supersingular if $E(\overline{\mathbb{F}}_p)$ has no points of order p (see [29]).

Definition 2. *(Oort [24]) An abelian variety A over $\mathbb{F}_q$ is called* **supersingular** *if A is isogenous to a product of supersingular elliptic curves. A curve C over $\mathbb{F}_q$ is called* **supersingular** *if $\mathrm{Jac}(C)$ is supersingular.*

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

Theorem 1. *The following conditions on an abelian variety A over $\mathbb{F}_q$ of dimension g are equivalent.*

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

The fourth property is the one which is most important for our application.

4.2 A Criterion for Supersingularity

The following result follows from Proposition 1 of Stichtenoth and Xing [34]. It gives a simple test for whether or not an abelian variety is supersingular, once $P(X)$ has been computed.

Theorem 2. *Suppose $q = p^n$ and suppose that A is an abelian variety of dimension g over $\mathbb{F}_q$. Let $P(X) = X^{2g} + a_1 X^{2g-1} + \cdots + a_g X^g + \cdots + q^g$ be the characteristic polynomial of the Frobenius endomorphism on A. Then A is supersingular if and only if, for all $1 \le j \le g$,*

$$p^{\lceil jn/2 \rceil} \mid a_j.$$

4.3 The Bound on the Extension Degree

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*

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

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

Theorem 3. *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 the group $A(\mathbb{F}_{q^r})$ divides $q^{kr} - 1$.*

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 [24] 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 2 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 [21], 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 $\pi^k = q_0^{k/2}$. For all points $P \in \mathrm{Pic}^0_C(\mathbb{F}_{q^r})$ we have $P = \pi^r(P) = [q_0^{rk/2}]P$. It follows that the exponent of $A(\mathbb{F}_{q_0^k})$ divides $q_0^{k/2}-1$ (also see Stichtenoth and Xing [34] Proposition 2). Since $q_0^{k/2}-1 = q^{rk}-1$ 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 [19] VI.3). The polynomials $\Phi_n(X)$ have degree $\varphi(n)$ (this is the Euler φ-function) so the values of $k'(g)$ are 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. 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 $\varphi(N) = 14$).

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

Table 1 gives some values for $k(g)$. We only list values for $g \leq 8$ since there are various algorithms (see [12]) for solving the discrete logarithm problem on high-genus curves. The notation 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 [35]) would have embedding degree 30. However, we have not found a curve whose Jacobian is isogenous to such an abelian variety.

The bounds given are 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 (note also that we recover the bound $k = 6$ in the elliptic curve case). However, we are more interested in Jacobian varieties of curves than in general abelian varieties. It is therefore important to determine which values for k can arise as the Jacobian of a curve. We return to this problem in Section 4.4.

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 the ratio $k(g)/g$, which is seen in Table 1 to grow rather slowly. This supports the notion that supersingular curves are weaker than the general case for standard discrete logarithm based cryptosystems.

4.4 Are Large Values of k Attained for Curves?

In this section some examples of curves with relatively large values for k are given (see Table 2). When $g > 2$ it is seen that the values are much smaller than the upper bounds given in Table 1. It is an interesting open problem to find the exact largest values of k for each genus, and we hope that this paper motivates further work on the problem.

The fact that the maximum value of k is attained in the case of genus one and two curves 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. Simple abelian varieties of dimension three should be isogenous to a Jacobian of a genus three curve (not necessarily hyperelliptic) over some extension field. However, we have not found any supersingular curves giving large values of k. Further, we have not found any supersingular hyperelliptic curves of genus three in characteristic two.

The reason for only listing curves defined over small fields is 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.

Table 2. Table of curves with large k. 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 $z^3 = x^4 + \theta x^2$.

Field	Curve	Genus	# points	k
$\mathbb{F}_p$ (1)	$y^2 = x^3 + a$	1	$p+1$	2
$\mathbb{F}_3$	$y^2 = x^3 + 2x \pm 1$	1	7,1	6
$\mathbb{F}_2$	$y^2 + y = x^5 + x^3$	2	13	12
$\mathbb{F}_3$	$y^2 = x^6 + x + 2$	2	13	3
$\mathbb{F}_5$	$y^2 = x^5 + 2x^4 + x^3 + x + 3$	2	11	5
$\mathbb{F}_{2^2} = \mathbb{F}_2(\theta)$	$x^4 + \theta x y^3 + y z^3$ (2)	3	57	9
$\mathbb{F}_3$	$y^2 = x^7 + 1$	3	28	6
$\mathbb{F}_5$	$y^2 = x^8 + 2x^4 + 3x^2 + 2$	3	66	10
$\mathbb{F}_7$	$y^2 = x^8 + x^4 + 5x^3$	3	911	14
$\mathbb{F}_2$	$y^2 + y = x^9 + x^4 + 1$	4	5	12

5 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 [27] suggested some hyperelliptic curves for use in cryptography. On page 172 they state that they were unable to find any secure genus 2 curves over $\mathbb{F}_2$ and speculated that this was caused by their restriction to the field $\mathbb{F}_2$ (instead of using $\mathbb{F}_{2^n}$). In fact, the reason for this is that they only considered equations of the form $C : y^2 + y = f(x)$ with $f(x) \in \mathbb{F}_2[x]$ monic of degree 5. We will show that all genus two curves of this form over all fields $\mathbb{F}_{2^n}$ 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, but 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 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. Indeed, there are curves of this form which are not supersingular when the genus is three or more. Our main result in this section is that all such curves are supersingular in the case of genus two.

Theorem 4. *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.*

Before giving the proof of the theorem it is necessary to obtain the following result about the polynomials $P(X)$ 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 2 implies that the curve is supersingular. In the general case we need a further argument.

Proof. (of Theorem 4) Using Lemma 2 we see that $P(X) \equiv X^4 \pmod 2$. By a result of Manin [22] (also see Stichtenoth [32] 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 [20] 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 2 (see Rück [25] for details of this approach).

Note that both of these arguments rely heavily on the fact that we are in the genus two case. In the case of genus three it is possible to give 'safe' examples. For instance, the curve $C : y^2 + y = x^7$ of [27] 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.

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 [27] could 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 2 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

$$\#\mathrm{Jac}(C)(\mathbb{F}_{2^{97}}) = 2 \cdot 389 \cdot 1747 \cdot 184733924638688269103187946767540719407 16909907019619$$

$$\#\mathrm{Jac}(C)(\mathbb{F}_{2^{1103}}) = 2 \cdot 47381 \cdot 10852877190495703277390509258459145399489273609233701 10769$$

where the large numbers are proven primes according to Magma. In both cases the Frey-Rück embedding degree exceeds 10^{50}.

The above arguments suggest that, in characteristic two, only curves of the form $y^2 + h(x)y = f(x)$ where $\deg(h(x)) \geq 1$ 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 [30] Section 1 and [7] Theorem 14).

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.

Acknowledgements. It is a pleasure to thank Hans-Georg Rück for indicating both proofs of Theorem 4; 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 version of the paper.

References

1. 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.
2. D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, in J. Kilian (ed.), Crypto 2001, Springer LNCS 2139 (2001) 213–229.
3. J. Buhler and N. Koblitz, Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems, *Bull. Aust. Math. Soc.*, **58**, No.1 (1998) 147–154.
4. D. G. Cantor, Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.*, **48** (1987) 95–101.
5. H. Cohen, A course in computational number theory, Springer GTM 138 (1993).
6. I. Duursma, P. Gaudry and F. Morain, Speeding up the discrete log computation on curves with automorphisms, in K. Y. Lam et al (eds.), Asiacrypt '99, Springer LNCS 1716, (1999) 103–121.
7. A. Enge, The extended Euclidean algorithm on polynomials and the computational efficiency of hyperelliptic cryptosystems, *Designs, Codes and Cryptography*, **23** (2001) 53–74.
8. G. Frey, 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.
9. 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.
10. S. D. Galbraith, S. Paulus and N. P. Smart, Arithmetic on superelliptic curves, To appear in *Math. Comp.*
11. S. D. Galbraith, Supersingular curves in cryptography (full version), available from the author's web pages.
12. 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.

13. R. Harley, Rump session talk, EUROCRYPT 2001, (2001).
14. A. Joux, A one round protocol for tripartite Diffie-Hellman, in W. Bosma (ed.), ANTS-IV, Springer LNCS 1838 (2000) 385–393.
15. K. S. Kedlaya, Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology, preprint (2001).
16. N. Koblitz, Hyperelliptic cryptosystems, *J. Cryptology*, **1**, no. 3 (1989) 139–150.
17. N. Koblitz, A family of jacobians suitable for discrete log cryptosystems, in S. Goldwasser (ed.), CRYPTO '88, Springer LNCS 403 (1990) 94–99.
18. 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.
19. S. Lang, Algebra, 3rd ed., Addison-Wesley, 1993.
20. K.-Z. Li and F. Oort, Moduli of supersingular abelian varieties, Springer LNM 1680 (1998).
21. Yu. I. Manin, The theory of commutative formal groups over fields of finite characteristic, *Russ. Math. Surv.*, **18**, No. 6 (1963) 1–83.
22. Yu. I. Manin, The Hasse-Witt matrix of an algebraic curve, *Translations, II Ser.*, Am. Math. Soc., **45** (1965) 245–264.
23. 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.
24. F. Oort, Subvarieties of moduli spaces, *Inv. Math.*, **24** (1970) 95–119.
25. H.-G. Rück, Abelsche varietäten niderer dimension über endlichen körpern, Habilitation Thesis, University of Essen (1990).
26. H.-G. Rück, On the discrete logarithm in the divisor class group of curves, *Math. Comp.*, **68**, No.226 (1999) 805–806.
27. 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.
28. A. Shamir, Identity-based cryptosystems and signature schemes, In G.R. Blakley and D. Chaum (eds.), CRYPTO '84, Springer LNCS 196 (1985) 47–53.
29. J. H. Silverman, The arithmetic of elliptic curves, Springer GTM 106, (1986).
30. N. Smart, On the performance of hyperelliptic cryptosystems, in J. Stern (ed.), EUROCRYPT '99, Springer LNCS 1592 (1999) 165–175.
31. A. Stein and E. Teske, Explicit bounds and heuristics on class numbers in hyperelliptic function fields, To appear in *Math. Comp.*, University of Waterloo technical report CORR 99-26 (1999).
32. H. Stichtenoth, Die Hasse-Witt-invariante eines kongruenzfunktionenkörpers, *Arch. Math.*, **33**, No. 4 (1980) 357–360.
33. H. Stichtenoth, Algebraic function fields and codes, Springer Universitext (1993).
34. 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.
35. 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.
36. 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.

Appendix 1. Methods to Compute $P(X)$

Very recently there have been some breakthroughs [15], [13] in algorithms for counting points and computing $P(X)$ on higher genus curves in the case of small characteristic. Nevertheless there is still interest in using subfield curves. We discuss some methods to compute $P(X)$ for curves C defined over small fields $\mathbb{F}_q$.

First we give the most elementary method. 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 [5] 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 [31] 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 [31]. This method has the superior complexity $O(q^{g-2+\epsilon})$ when $g = 4$ or $g \geq 6$. This trick cannot be extended.

Appendix 2. Superelliptic Curves

The case of hyperelliptic curves has been fairly thoroughly explored in the past [16], [17], [3], [27], [30]. In particular, Buhler and Koblitz [3] mention cases which are guaranteed to be non-supersingular.

A superelliptic curve (see [10]) is a curve given by 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 $\frac{1}{2}(n-1)(\deg f(x) - 1)$.

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 field. In other words, when g is odd, one can compute $P(X)$ in

time $O(q^{g-1+\epsilon})$. On the other hand, such curves do not have full 2-torsion and so they are not fully general among all superelliptic curves.

Table 3 lists some non-supersingular superelliptic curves. In all cases the large numbers l are proven primes according to Magma, and the curves are resistant to the Frey-Rück attack. 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 [6], [12].

Table 3. Examples of superelliptic curves suitable for cryptography.

$g = 3$ $\quad C : y^3 = x^4 + x^3 + \alpha x^2 + x + \alpha$ 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 $\mathbb{F}_{2^5}$ $P(X) = X^6 + 39X^4 + 1248X^2 + 2^{15}$ $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{5\cdot 23}}) = 2^4 \cdot 3^2 \cdot 5^5 \cdot 7 \cdot 11 \cdot 83 \cdot$ 24921097984905764960391575993390085577862674124762402677018464681 5 709788699839224081758315379 59 (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 $\mathbb{F}_2$ $P(X) = X^8 + 2X^6 + 6X^4 + 8X^2 + 16$ $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{43}}) = 3 \cdot 11 \cdot$ 18140335474265631308087819230436531735 4825710535649 (167 bit) $\#\mathrm{Jac}(C)(\mathbb{F}_{2^{61}}) = 3 \cdot 11 \cdot 12323 \cdot$ 69516604910881473963537569029137158267066937810090081 343111639513643 (226 bit)