Efficient Arithmetic on Hyperelliptic Koblitz Curves

Tanja Lange

Institute of Experimental Mathematics
University of Essen
Ellernstrasse 29
D-45326 Essen
Germany

lange@exp-math.uni-essen.de

May 23, 2001

1 Introduction

Due to the emerging market of electronic commerce public key cryptosystems gain more and more attention. Unlike for military purposes there is a need of flexible user groups. Besides RSA most cryptosystems and protocols like the Diffie-Hellman key exchange [3] and the ElGamal cryptosystem [5] are based on the discrete logarithm as the underlying one-way function. Given a cyclic subgroup of an abelian group generated by g and an integer m one can compute $g^m = b$. If $\langle g \rangle$ is a group suitable for cryptographic applications then it is computationally hard to retrieve m for given b and g. m is called the *discrete logarithm* of b to the base g. The problem of determining m given b and g is called the *discrete logarithm problem.* A group is suitable if

1. the group operation is fast,
2. the group order can be computed efficiently,
3. the discrete logarithm problem is hard,

4. the representation is easy and compact.

Two common kinds of groups used in practice are the multiplicative group of a finite field and the group of points on an elliptic curve over a finite field. The first group comes equipped with the fast arithmetic developed for finite fields but also with a subexponential algorithm for computing the discrete logarithm. Since this index calculus attack does not carry over to the elliptic curves, only general techniques like Pollard's rho and kangaroo method (see [40, 43, 44, 60]) apply, unless the curve has a special structure, for example is supersingular (see Frey and Rück [8] and Menezes, Okamoto, and Vanstone [32]) or the group order is divisible only by small primes, thus weak under the Pohlig-Hellman attack [41]. But there is a big drawback – one addition on an elliptic curve takes either 2 multiplications, 1 squaring, and 1 inversion or 12 multiplications and 4 squarings depending on the chosen representation of the curve. Doubling causes mainly the same complexity. To obtain a speed-up for the main operation – computing m-folds – Koblitz [22] proposed the use of a special kind of curves. These *Koblitz* or *subfield* curves are curves defined over a comparably small finite field $\mathbf{F}_q$. They are then considered as curves over a large extension field $\mathbf{F}_{q^n}$, where n is prime. The arithmetic makes use of the fact that if the curve C is defined over $\mathbf{F}_q$ and $P = (x, y) \in \mathbf{F}_{q^n} \times \mathbf{F}_{q^n}$ lies on C then the point $\sigma(P) = (x^q, y^q)$ lies on C, too, as can be seen by direct computation. Note that this only holds since the curve is defined over the small field. σ is an endomorphism of the curve called the Frobenius endomorphism. On the coordinates of the points it operates like the Frobenius automorphism of the underlying field $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$. These curves have thoroughly been studied by Koblitz [22, 23], Meier and Staffelbach [31], Müller [36], Smart [51], and Solinas [52, 53], where the last reference contains a detailed analysis of the maximal speed-up achievable for curves over $\mathbf{F}_2$.

In [21] Koblitz proposed the Picard group $\mathrm{Pic}^0(C/\mathbf{F}_q)$ of a hyperelliptic curve as a further group suitable for cryptographic applications. The advantages over the elliptic curves are the smaller field size and the larger variety of curves to choose from. The representation of the group elements is given by polynomials of bounded degrees. Hence, the group satisfies requirement 4. But there are several disadvantages:
At the moment no-one is able to compute the group order of a randomly generated hyperelliptic curve over a prime field with group order $\sim 2^{160}$. The best result obtained for curves of genus two is a curve over the prime field $\mathbf{F}_p$ with $p = 10^{19} + 51$ by Gaudry and Harley [14] which leads to a group order $\sim 10^{38} \sim 2^{129}$ which is smaller than recommended for cryptographic applications. Hence, one is forced to take special curves. Generalizing Atkin, Spallek [54] suggested the use of curves with complex multiplication, so called CM-curves. This approach was investigated in more detail by Weng [61] again for genus two. Recently she generalized it to work also for genus 3 curves but in both cases the

curves are defined over finite prime fields of odd characteristic or small extension fields (of degree at most 12). We propose a different class of curves in this article which allows to work in characteristic 2 as well.
Furthermore the group operation for a generic hyperelliptic curve is slower than for an elliptic curve. For larger genus there exists an index-calculus like method for computing the discrete logarithm by Adleman, DeMarrais, and Huang [1], Müller, Stein, and Thiel [37], and Enge [6]. Gaudry [13] modified this algorithm and gave a detailed analysis showing that his attack is faster than Pollard's rho method for $g \geq 4$. For smaller genus these groups are secure provided that the group order is sufficiently large and that one avoids curves for which special attacks are known.
In this article we investigate *hyperelliptic Koblitz curves*. The idea of elliptic Koblitz curves was generalized by Günther, Lange, and Stein [17]. There we investigate two special examples of binary curves of genus 2. We show in that paper that also in the hyperelliptic case the Frobenius endomorphism can be used to achieve fast arithmetic, i. e. to speed up scalar multiplication. This generalization offers a larger variety of curves to choose from. To compare – there are up to isogeny only two non supersingular elliptic curves over $\mathbf{F}_2$ whereas one can choose from 6 different curves of genus 2 over $\mathbf{F}_2$ and there are even much more curves for higher genus. We provide a list of suitable curves for genus 2,3, and 4 in this paper.
And we give a detailed analysis that the Frobenius endomorphism gives rise to a speed-up of at least a factor of 4 (for $q = g = 2$) and much more if many precomputations can be stored. The speed-up increases with q and g.

A further important advantage of Koblitz curves is that due to the construction the group order can be determined very efficiently. Since the group order corresponding to the field of definition $\mathbf{F}_q$ always divides the group order over $\mathbf{F}_{q^n}$ the best one can hope for are almost prime orders, i. e. orders being a product of this inevitable factor and a large prime. Experiments with various subfields and genera give evidence that among the Koblitz curves there are many providing a group of cryptographic relevance.

Hence, firstly the computation of m-folds is sped up considerably and can thus be regarded as fast. Secondly the group order can be computed very easily. The group elements can be represented by two polynomials of degree at most g over $\mathbf{F}_{q^n}$, thus the representation is compact and easy.
To the third point: The Picard group of Koblitz curves over $\mathbf{F}_{q^n}$ comes along with an automorphism group of order at least $2n$ – due to the Frobenius automorphism of order n and inversion. This can be used for cryptanalysis. The attack of Gallant, Lambert, and Vanstone [11] designed for elliptic curves was extended to hyperelliptic curves. Duursma, Gaudry, and Morain [4] make use of equivalence classes in Pollard's rho method and obtain a speed-up of $\sqrt{n}$

compared to a Picard group without automorphisms except for the inversion. This can be dealt with by choosing n some bits larger (at most 4 bits in the range considered here). Gaudry [13] used this automorphism group to speed-up his variant of the index-calculus method by n^2. For genus 2 and 3 this does not affect the security of our system. But for genus 4 we need to be aware of that effect and either avoid these curves or choose a larger exponent.

Furthermore there is an attack on anomalous curves investigated by Semaev [48] (see also Satoh and Araki [47], and Smart [50]) for elliptic and by Rück [46] for hyperelliptic curves. This works for groups of order a multiple of p^r where p is the characteristic of the ground field. But the hyperelliptic Koblitz curves we use do not lead to a curve which is weak under that attack since we work in the subgroup of large prime order and the characteristic of the fields is small, thus we always work in the prime to p part.

Certainly one has to be aware of the Frey-Rück attack [8]. It can be applied whenever the order of q^n, i.e. the cardinality of the finite field one works in, modulo l is small, where l is the order of the subgroup of the Picard group. Thus one has to compute this order before accepting a curve. All the examples of curves proposed here satisfy this requirement.

The Weil descent attack described for elliptic curves in [15] applies also to hyperelliptic curves. Thus we need to ensure that we consider curves over fields where the exponent is a prime and for characteristic 2 is not of the form $2^l - 1$ (see [34]) – or more generally – leads to a curve with such a large genus that the attack gets infeasible. Although Gaudry, Hess, and Smart [15] say that their attack does not work for curves defined over the ground field one can modify the curve to get an isogenous one defined over the extension field.
However we only consider prime degree extensions since otherwise the class number would contain more prime factors.

Hence, Koblitz curves provide a large source of hyperelliptic curves for every genus with an easy to compute group order and they allow the use of fields over characteristic two which is advantageous in implementations. And the security requirements are fulfilled as well.

Remark:

1. Although our approach is described for curves over arbitrary fields and of arbitrary genus in applications they are most likely used over small fields with $q \leq 7$ and genus 2, 3 or 4, since for larger genus the groups are insecure and for larger field size the number of precomputations to be stored increases and we loose too much due to inevitable factors of the group order.

2. We only consider the case of hyperelliptic curves, but all this generalizes to arbitrary abelian varieties, thus especially to those attached to C_{ab}-curves, as soon as the action of the Frobenius endomorphism can be used efficiently. This holds since we only work with the characteristic polynomial not with the curves themselves.

The remainder of this paper is organized as follows. In the next section we provide the necessary mathematical background followed by two sections dealing with the computation of the group order. We then give some experimental data concerning group orders of Koblitz curves over several finite fields. Section 6 is devoted to the standard ways of computing m-folds which will be used to compare our results with. In Section 7 we show how to make use of the Frobenius endomorphism to achieve a speed-up in computing m-folds. Sections 8, 9 and 10 give details on the algorithms and theoretical results concerning the length and density of expansions related to the Frobenius endomorphism. The following section lists some results on Koblitz curves and gives numerical evidence for the assumptions. In Section 12 we compare the new method with the standard double-and-add method. Then we investigate what happens if we cannot store precomputed values. In the following section we deal with a different set-up for cryptosystems based on Koblitz curves which is useful in implementations. Finally we give an outlook on what can be done as well.
After finishing this paper it was brought to our attention that Lee [26] has also generalized the results of Günther, Lange, and Stein [17] to arbitrary characteristic. His paper does not contain a proof of the finiteness and length of the representations obtained. Furthermore he uses larger ground fields than we recommend. We say more about this in Section 15.

2 Mathematical Background

This section provides the necessary background on algebraic curves with emphasis on hyperelliptic curves. Usually the results are stated for arbitrary curves respectively functions fields and the examples deal with the special case. Many results presented here have analogies in number theory. We decided to take a more algebraically motivated approach, hence, starting from function fields since the arithmetic we use later is based on this representation. On the other hand we make use of the geometric background as well to derive results concerning the structure. In the following we state the results without proofs. We follow the lines of Lorenzini [29] and also adopt his notation. Most of the results can be found as well in the book of Stichtenoth [58]. For the more geometric approach see the book of Fulton [9]. You can as well consider Gaudry's thesis [12] which contains a nice introduction with several pictures.
The reader only interested in the computational aspects might consult the introduction by Menezes, Wu and Zuccherato [35] to get an insight in hyperelliptic

curves and skip the first subsection. Furthermore Silverman's book [49] contains a lot of the theory not only for elliptic curves.

2.1 Notation and Definitions

Throughout this article let k denote a perfect field. Some of the results mentioned below hold also for arbitrary fields but since we consider hyperelliptic curves over finite fields in the other sections this means no restriction for us and eases to state the theorems. Our starting point is the following definition.

Definition 2.1 *A field L containing k is called a* function field over k *if the field L is a field of transcendence degree 1 over k, and k is algebraically closed in L.*

Example 2.2 *Let $k = \mathbf{F}_5$ and consider $f = y^2 - x^3 - x - 1$. f is absolutely irreducible, i. e. irreducible over k and any extension field. Thus f defines a function field $k(x, y)$.*

We now consider special maps from L^* to the integers called *valuations*

Definition 2.3 *A* valuation of L *is a map $v : L^* \to \mathbf{Z}$ such that the following properties are satisfied:*

1. $v(xy) = v(x) + v(y)$ *for all* $x, y \in L^*$,
2. $v(x + y) \geq \min\{v(x), v(y)\}$ *for all* $x, y \in L^*$.

A valuation is called surjective *if v is surjective.*
A valuation is called trivial on k *if $v(k^*) = \{0\}$.*
v is extended to L by putting $v(0) = \infty$.

For example the map $v(x) = 0$ for all $x \in L^*$ is a valuation. This valuation is called the trivial valuation. An example for a non-trivial valuation is the map $k(x)^* \to \mathbf{Z}$ where $v(\alpha) = \deg(\alpha)$ with the usual meaning of degree.

Let B be a Dedekind domain with field of fractions L. Let M be a maximal ideal of B. Then we can define the valuation for $\alpha = g/h \in L,\ g, h \in B$ via $v(\alpha) = v(g) - v(h)$ and define $v(g)$ for $g \in B$ to be the largest i such that $g \in M^i$. Thus to each maximal ideal corresponds a valuation. Now let v be a valuation such that $v(B) \geq 0$. Consider the set $\mathcal{O}_v = \{\alpha \in L | v(\alpha) \geq 0\}$. One can show that $\mathcal{O}_v$ is a local principal ideal domain and that $\mathcal{M}_v = \{\alpha \in L | v(\alpha) > 0\}$ is the maximal ideal in $\mathcal{O}_v$. Put $M = \mathcal{M} \cap B$. Then M is a maximal ideal of B. In fact one can show that the set of surjective valuations v with $v(B) \geq 0$ is in bijection with the set of maximal ideals of B.

Let $\mathcal{V}(L/k)$ be the set of all surjective valuations trivial on k. It is this set that we will consider as points of a curve. Before we give the formal definition let's see how this fits with the intuitive definition of a point as a zero of a given polynomial and a curve as a set of these zeros plus maybe some additionally elements at infinity.

Example 2.4 *Assume that k is an algebraically closed field. Since L/k is a function field we can find an element $x \in L$ such that $L/k(x)$ is a finite extension. Let α be a defining element of this extension, hence $L = k(x, \alpha)$, and consider the minimal polynomial $f(y) \in k(x)[y]$ of α. Without restriction we can assume that α is algebraic over $k(x)$, thus, f is monic in y and $k[x, y]/(f)$ is a Dedekind domain. Now let $a, b \in k$ with $f(a, b) = 0$. $\mathcal{P} = (x - a, y - b)$ is a maximal ideal in $k[x, y]/(f)$. Then $\mathcal{P}$ defines a valuation $v_{\mathcal{P}}$ as seen above. Since k is algebraically closed we can in fact find all valuations corresponding to maximal ideals this way. The set of these valuations is an example of an affine curve. But we are missing some valuations of L, namely those valuations that are extensions of the degree map* deg *from $k(x)$ respectively those that do not result from $k[x, y]/(f)$ but from the other ring $k[1/x, y]/(f)$ contained in L. Taking f as the defining equation of a curve over k and considering the zeros of f as points of the curve one is used to add points at infinity corresponding to the solutions of $\tilde{f}(t, y)$ at $t = 0$ after the change of variables $t = 1/x$. Considering the polynomial ring $k[t, y]/(\tilde{f})$ one obtains the corresponding valuations of L^* in a similar manner as above.*
The other way round one can associate to each valuation v a local principal ideal domain $\mathcal{O}_v$ and its maximal ideal $\mathcal{M}_v$. Assume that $M = \mathcal{M}_v \cap k[x, y]/(f)$ is nonempty. Since $k[x, y]/(f)$ is a Dedekind domain we can find a basis of M consisting of (at most) two elements as $M = (x - a, y - b)$. Then we find a zero of f namely $f(a, b) = 0$. If $\mathcal{M}_v$ contains no elements of $k[x, y]/(f)$ then it does of $k[1/x, y]/(\tilde{f})$, thus corresponds to a point 'at infinity'.

If k is algebraically closed we obtain each maximal ideal of $k[x, y]/(f)$ (and therefore such a valuation) via the zeroes of f. But if k is not algebraically closed we do not find all maximal ideals this way. If the basis of $\mathcal{M}_v \cap k[x, y]/(f)$ consists of polynomials of higher degree then the valuation corresponds to a class of conjugate points of a finite extension of k. The connection is as follows:
Denote by $\bar{k}$ an algebraic closure of k. Let $a, b \in \bar{k}$ and put

$$\bar{\varphi}_{(a,b)} : \bar{k}[x, y] \to \bar{k},\ g(x, y) \mapsto g(a, b).$$

Denote the restriction to $k[x, y]$ by $\varphi_{(a,b)}$. One can show that for any maximal ideal M of $k[x, y]$ there exists a pair $(a, b) \in \bar{k} \times \bar{k}$ such that $M = \mathrm{Ker}(\varphi_{(a,b)})$.

Furthermore let the minimal polynomial of a over k be $g(x)$. Since g is irreducible, $k[x,y]/(g(x))$ is a principal ideal domain and $M/(g(x))$ is generated by a single element, say by the class of $h(x,y)$. Therefore $M = (g(x), h(x,y))$. Hence, every maximal ideal is generated by two polynomials and both statements hold true when we restrict to the ring $k[x,y]/(f)$ with the additional property that $f(a,b) = 0$ for the tuple $(a,b) \in \bar{k} \times \bar{k}$ such that $M = \mathrm{Ker}(\varphi_{(a,b)})$.

The correspondence of zeros of f – or more generally for non-closed fields maximal ideals of $k[x,y]/(f)$ –, valuations, and local principal ideal domain is fundamental for the definition of curves.

Definition 2.5 *A* nonsingular complete curve X/k over k *is a pair* $(X, k(X)/k))$ *consisting in a function field* $k(X)/k$ *over* k, *and a set* X *identified with the set* $\mathcal{V}(k(X)/k)$ *through a given bijection. An element* P *of* X *is called a* point. *The field* $k(X)$ *is called the* field of rational functions on X. *To each point* P *corresponds a valuation* v_P *of* $\mathcal{V}(k(X)/k)$, *and a local principal ideal domain* $\mathcal{O}_P := \mathcal{O}_{v_P}$, *with maximal ideal* $\mathcal{M}_P$. *The ring* $\mathcal{O}_P$ *is called the* ring of rational functions defined at P. *An element of* $\mathcal{O}_P$ *is called a* function on X defined at P. *The* domain *of* $\alpha \in k(X)$ *is the set of points in* X *where* α *is defined. If* $U \subseteq X$, *then we let* $\mathcal{O}_X(U) := \cap_{P \in U} \mathcal{O}_P$, *and we call this ring the* ring of functions on X defined everywhere on U.

Note that with this definition we have $\mathcal{O}_X(X) = k$ since k is algebraically closed in $k(X)$.

As an example for a complete curve we consider the following definition

Definition 2.6 *The* projective line over k *is a nonsingular complete curve* $\mathbb{P}^1/k$ *such that the field of functions* $k(\mathbb{P}^1)$ *is isomorphic, as* k*-algebra, to the field of rational functions in one variable.*

If $k = \mathbf{C}$, thus algebraically closed, all valuations of $k(x)$ come from the ideals $(x-a), a \in \mathbf{C}$ except for the valuation v_∞ which is the degree-valuation. Hence, $\mathbb{P}^1/k$ can be identified with the Riemann sphere, i. e. $\mathbf{C}$ plus an additionally point.
In general we have

$$\mathbb{P}^1/k = \{v_{g(x)} | g(x) \in k[x], \text{ irreducible and monic } \} \sqcup \{v_\infty\},$$

since the maximal ideals of $k[x]$ are generated by the irreducible polynomials. Usually one denotes the point v_∞ of $\mathbb{P}^1$ simply by ∞.

Let X/k be the nonsingular complete curve associated to the field $k(X)/k$. Let $x \in k(X)$ such that $k(X)/k(x)$ is a finite extension. Since $\mathcal{O}_P$ is local for every P

we have that either $x \in \mathcal{O}_P$ or $1/x \in \mathcal{O}_P$. Now let U and U' denote respectively the domain of x and $1/x$ in X. Then we have

$$X = U \cup U'.$$

Furthermore $\mathcal{O}_X(U)$ is equal to the integral closure of $k[x]$ in $k(X)$. The complement of U in X is the set of points P such that $\mathcal{O}_P \supset k[1/x]_{(1/x)}$, where $k[1/x]_{(1/x)}$ denotes the localization of $k[1/x]$ at $(1/x)$.

Under the 'bijection' occurring in the definition of a curve we can thus understand for example that we consider the maximal ideals of $\mathcal{O}_X(U)$ and $\mathcal{O}_X(U')$ as points with the relation to valuations shown above.

Definition 2.7 *Let X/k and Y/k be two nonsingular complete curves over k. A* morphism $\varphi : X \to Y$ of nonsingular curves over k *is a map given by a homomorphism of k-algebras $\varphi^* : k(Y) \to k(X)$ in the following way: if $P \in X$ corresponds to the valuation v_P then $\varphi(P)$ corresponds in Y to the unique surjective valuation attached to the valuation $v_P \circ \varphi^*$.*
The degree *of φ is defined to be $[k(X) : \varphi^*(k(Y))]$.*

Let $P \in X$ and consider the rings associated to P and $\varphi(P)$. We define the integer e_P by $\mathcal{M}_{\varphi(P)}\mathcal{O}_P = \mathcal{M}_P^{e_P}$.

Definition 2.8 *$P \in X$ is* unramified *over Y if $e_P = 1$. Otherwise P is called ramified. The integer e_P is called the* ramification index *of φ at P. Let $Q \in Y$. The* fiber of Q *is the set of points $\varphi^{-1}(Q)$ of X mapped to Q under φ.*

If $\varphi^* : k(X) \to k(X)$ is an automorphism of k-algebras, then the corresponding morphism of curves is called an *automorphism* of X/k.

Let $k(X)/k(x)$ be a finite extension. Then we obtain a natural morphism $\pi : X \to \mathbb{P}^1$ which maps via the embedding $\pi^* : k(x) \to k(X)$. The degree of π is equal to $[k(X) : k(x)]$.

Definition 2.9 *A complete nonsingular curve X/k over k is called a* hyperelliptic curve *if it is not the projective line and if the corresponding function field $k(X)$ contains an element x such that $[k(X) : k(x)] = 2$.*

Alternatively one calls a curve X/k hyperelliptic if it is not the projective line and there exists a morphism $\pi : X \to \mathbb{P}^1$ over k of degree 2. For $\mathrm{char}(k) \neq 2$ a hyperelliptic curve X/k is given via $k(X) = k(x)[y]/(f)$, where $f(x, y) = y^2 - g(x) \in k[x, y]$ and $g(x)$ is squarefree. In characteristic 2 an extension of degree 2 of $k(x)$ means that we have an Artin-Schreier extension, thus an irreducible polynomial f is usually given in the following form $f(x, y) = y^2 - y - g(x)$ with

$g(x) \in k(x)$. Clearing denominators and changing variables one can as well obtain a representation via $\tilde{f}(u,v) = v^2 + h(u)v - \tilde{g}(u)$ such that the partial derivatives of $\tilde{f}$ do not vanish simultaneously at any $(a,b) \in \bar{k}^2$ with $\tilde{f}(a,b) = 0$, where $\bar{k}$ denotes the algebraic closure of k.

Example 2.10 *Let $k = \mathbf{F}_2$. The complete curve defined via $f(x,y) = y^2 + (x^2 + x + 1)y - x^5 - x^4 - 1$ is a hyperelliptic curve.*

Let $P \in \mathbb{P}^1/k$. Consider the fiber of π over P, i.e. the set $\pi^{-1}(P)$. If π is of degree n and this set contains less then n points, then P ramifies in X. The ramified points of X are called *Weierstrass points.*
The ramification behavior of ∞, i.e. the extensions of the degree-valuation, will be important for the group we consider later on. Let $v_{\mathfrak{P}_1}, \ldots, v_{\mathfrak{P}_r}$ denote the distinct elements in the fiber of ∞.

Example 2.11 *Let $\mathrm{char}(k) \neq 2$ and let $g(x) \in k[x]$ be a squarefree polynomial of degree d, put a_d the leading coefficient of g. Consider the function field $L = k(x)(\sqrt{g(x)})$ and the associated nonsingular complete curve X/k. Via the change of variables $t := 1/x$ one can study the behavior at infinity $t = 0$. Denote by B' the integral closure of $k[t]$ in L. Remember that we associated to each valuation a maximal ideal. To the extensions of v_∞ correspond the factors of the ideal (tB'). We have*

$$(tB') = \begin{cases} \mathfrak{P}_1\mathfrak{P}_2 & d \text{ is even and } a_d = b^2 \text{ for} b \in k \\ \mathfrak{P} := (tB') & d \text{ is even and } a_d \neq b^2 \text{ for all } b \in k \\ \mathfrak{P}^2 & d \text{ is odd} \end{cases}$$

If tB' splits into two different ideals then L is called a real quadratic function field, *otherwise it is called* imaginary quadratic. *These notations are used since the respective fields share many properties with the corresponding quadratic number fields.*

Let k' be a finite extension of k. Any curve defined over k can also be considered as a curve over k'. The topic of this article are Koblitz curves, these are curves which are defined over a small finite field and are then considered over a large extension field. Thus we need to define what we mean by this.

Definition 2.12 *Let X/k be a nonsingular complete curve. Let $k(X)$ denote the function field of X, and fix an algebraic closure $\overline{k(X)}$ of $k(X)$. Let k'/k be any algebraic extension of k contained in $\overline{k(X)}$. Let $k'(X) := k' \cdot k(X)$. Let $X_{k'}/k'$ denote the nonsingular complete curve associated to the function field $k'(X)/k'$. The curve is said to be obtained from X/k by* a constant field extension *or by* extension of the scalars, *or by* base change. *The extension $k'(X)/k(X)$ is called a* constant field extension.

If k'/k is a Galois extension in $\bar{k}$ one can show that the groups $\mathrm{Gal}(k'(X)/k(X))$ and $\mathrm{Gal}(k'/k)$ are isomorphic.

The other way round we also need to define

Definition 2.13 *Let $k \subseteq E$ be two fields. Let $\bar{X}/E$ be a nonsingular complete curve. We say that $\bar{X}/E$* is defined over k *if the function field $E(\bar{X})/E$ contains a function field L/k such that $EL = E(\bar{X})$.*
Let X/k be a complete nonsingular curve and let $P \in X_{\bar{k}}$. For all $\sigma \in \mathrm{Gal}(\bar{k}/k)$ let $\sigma(P)$ be such that $\mathcal{O}_{\sigma(P)} = \sigma(\mathcal{O}_P)$. Put $\mathrm{Stab}(P) := \{\sigma \in \mathrm{Gal}(\bar{k}/k) | \sigma(P) = P\}$. *The* field of definition of P *is $k(P) := \bar{k}^{\mathrm{Stab}(P)}$. We call* $\deg(P) := [k(P) : k]$ *the* degree of P.

It may happen that for two curves X/k and Y/k the curves $X/\bar{k}$ and $Y/\bar{k}$ are isomorphic as nonsingular curves over $\bar{k}$. Then the curve Y is called a twist of X. As we have seen at the beginning the maximal ideals M of $k[x,y]/(f)$ for an absolute irreducible polynomial f can be given as $\mathrm{Ker}(\varphi_{(a,b)})$ for a pair $(a,b) \in \bar{k} \times \bar{k}$ with $f(a,b) = 0$. Since $M \subset k[x,y]/(f)$ we could use any of the conjugates of (a,b) under $\mathrm{Gal}(\bar{k}/k)$ instead of (a,b). More precisely one can show

Lemma 2.14 *Let X/k be a nonsingular complete curve. Consider the map*

$$I : X_{\bar{k}} \to X, \ \bar{P} \mapsto P, \ \text{such that } \mathcal{O}_P := \mathcal{O}_{\bar{P}} \cap k(X).$$

The map I is surjective and X is in bijection with the set of orbits of $X_{\bar{k}}$ under the action of $\mathrm{Gal}(\bar{k}/k)$.

We also can extend the morphisms for a base change.

Definition 2.15 *Consider a morphism of curves over k $\varphi : X \to Y$, given by the inclusion $k(Y) \subseteq k(X)$. Now let $\bar{k}$ be the algebraic closure of k contained in $\overline{k(X)}$ and let k'/k be an extension of k contained in $\bar{k}$. Using the inclusion $k'(Y) \subseteq k'(X)$ the morphism* can be extended *to the morphism $\varphi' : X_{k'} \to Y_{k'}$.*

Consider again the example 2.11.

Example 2.16 *Let $f(x,y) := y^2 - g(x)$ with $g(x) \in \overline{k}[x]$, $\deg(g) = d$ odd, and $\mathrm{char}(k) \neq 2$. We consider the function field $\overline{k(X)}$ and the corresponding morphism $\bar{\pi} : \bar{X} \to \mathbb{P}^1(\bar{k})$ of degree 2 which is an extension of the morphism considered above. Let V denote the domain of x in $\bar{X}$. By the previous example – g has odd degree – we know that $\bar{X} \backslash V$ consists of a single point which is mapped to ∞ under $\bar{\pi}$, hence $\bar{\pi}$ is ramified at this point with ramification index 2. All other points of $\bar{X}$ correspond to maximal ideals M of $\bar{k}[x,y]/(f)$, and since $\bar{k}$ is algebraically closed $M = (x-a, y-b)$, $f(a,b) = 0$ with image under $\bar{\pi}$ corresponding to $(x-a)$. Since f is of degree 2 in y, the only ramification points of $\bar{\pi}$*

correspond to the d zeros of f of the form $(a_i, 0), g(a_i) = 0$. Thus, the morphism is ramified at $d+1$ points with ramification index 2.
If the degree e of g is even and the leading coefficient is a square in k, then $\bar{X}\backslash V$ consists of two points mapped to ∞ under $\bar{\pi}$. Hence, $\bar{\pi}$ is unramified at this point. Therefore the only ramification points correspond to the e zeros of f of the form $(a_i, 0), g(a_i) = 0$.
Thus, in both cases the number of ramification points is even and if in the second case one of the ramification points lies in k one can transform the equations such that the same curve is described by an equation with g of odd degree $e-1$. A transformation from the first to the second case is always possible.

We now introduce a class group related to the curve X called the *Picard group* of X/k or the *divisor class group* of X/k. First we need the following definition.

Definition 2.17 *Let $L/k(x)$ be a finite extension and consider the set of surjective valuations of L that are trivial on k, namely $\mathcal{V}(L/k)$. When $\mathcal{V}(L/k) \neq \emptyset$, the free abelian group* $\mathrm{Div}(L/k)$ *generated by the set $\{x_v | v \in \mathcal{V}(L/k)\}$,*

$$\mathrm{Div}(L/k) := \oplus_{v\in\mathcal{V}(L/k)} \mathbf{Z} x_v,$$

is called the group of divisors *of L/k.*

An element D is written as a sum $\sum a_v x_v$ with $a_v \in \mathbf{Z}$ and $a_v = 0$ for all but finitely may $v \in \mathcal{V}(L/k)$.
Such a *divisor* is called *effective* if $a_v \geq 0$ for all $v \in \mathcal{V}(L/k)$.
We now attach to a function a divisor defined by the map

$$\mathrm{div}_L : L^* \to \mathrm{Div}(L/k),\ f \mapsto \sum_{v\in\mathcal{V}(L/k)} v(f) x_v.$$

Divisors resulting from functions are called *principal divisors.*

Definition 2.18 *The* Picard group $\mathrm{Pic}(L/k)$ *is the quotient of the group* $\mathrm{Div}(L/k)$ *by the image of the map* div_L. *The following sequence of abelian groups is exact:*

$$(1) \longrightarrow \bigcap_{v\in\mathcal{V}(L/k)} \mathcal{O}_v^* \longrightarrow L^* \xrightarrow{\mathrm{div}_L} \mathrm{Div}(L/k) \xrightarrow{\mathrm{cl}} \mathrm{Pic}(L/k) \longrightarrow (0).$$

Let X/k be the curve associated to the function field $k(X)/k$. Using the identification of valuations and points we let $\mathrm{Div}(X/k) := \oplus_{P\in X} \mathbf{Z} P$.
Let $P \in X$ and consider the local principal ideal domain $\mathcal{O}_P$ in $k(X)$ corresponding to P. The *degree of P* is defined by $\deg(P) = [\mathcal{O}_P/\mathcal{M}_P : k]$. Note that this definition coincides with the one given above for $Q \in X_{\bar{k}}$. Without restriction let $k(X)/k(x)$ be finite and let P be in the domain of x. Let the maximal ideal $M = \mathrm{Ker}\varphi_{(a,b)}$ correspond to P and let Q correspond to $(x-a, y-b)$. Then the degree of $Q \in X(\bar{k})$, i. e. $[k(Q) : k]$ is equal to $\deg(P)$ as defined above.

Definition 2.19 *The degree of a divisor* $D \in \mathrm{Div}(X/k)$ *is defined to be* $\deg(D) = \sum a_P \deg(P)$.

Actually it will be the subgroup $\mathrm{Pic}^0(X/k)$ of degree zero divisors modulo the group of principal divisors that we will use as a group in cryptography. Note that this definition makes sense since the principal divisors have degree 0. For a finite field k and a nonsingular complete curve X/k we have that $\mathrm{Pic}^0(X/k)$ is finite. The order of $\mathrm{Pic}^0(X/k)$ is then called the *class number of* X/k.

Using the obvious group law would result in sums containing more and more terms if we do not have a powerful reduction theory. Furthermore to use this group in the applications we need some kind of unique representation of these divisor classes and an efficient group law on the reduced classes.
Therefore we now investigate a further class group associated to the function field L/k, or more generally to an extension field. Let B be a Dedekind domain. Consider the following equivalence relation on the set of non-zero ideals of B:

$$I \equiv J \text{ if and only if there exist } \alpha, \beta \in B\backslash\{0\} \text{ such that } (\alpha)I = (\beta)J.$$

The equivalence classes of these ideals modulo the principal ideals form a group $\mathrm{Cl}(B)$ called the *ideal class group of* B.

Now let L/k be the field of fractions of B and let $k \subset B$. We define

$$\mathrm{Div}(B) := \oplus_{\substack{v \in \mathcal{V}(L/k) \\ v(B) \geq 0}} \mathbf{Z} x_v,$$

and

$$\mathrm{div}_B : L^* \to \mathrm{Div}(B), f \mapsto \sum_{\substack{v \in \mathcal{V}(L/k) \\ v(B) \geq 0}} v(f) x_v,$$

Then the following map defines a group homomorphism (also called cl like above)

$$\mathrm{cl} : \mathrm{Div}(B) \to \mathrm{Cl}(B), \ x_v \mapsto \text{ class of } \mathcal{M}_v \cap B.$$

In fact, this map induces a group isomorphism from $\mathrm{Div}(B)/\mathrm{div}_B(L^*)$ to $\mathrm{Cl}(B)$ and therefore provides an additive description of the ideal class group.

For the restriction map

$$\mathrm{res} : \mathrm{Div}(L/k) \to \mathrm{Div}(B), \quad \sum_{v \in \mathcal{V}(L/k)} a_v x_v \mapsto \sum_{\substack{v \in \mathcal{V}(L/k) \\ v(B) \geq 0}} a_v x_v$$

we have $\mathrm{res} \circ \mathrm{div}_L = \mathrm{div}_B$.
This leads to the following lemma.

Lemma 2.20 *Let $k' := \bigcap_{v \in \mathcal{V}(L/k)} \mathcal{O}_v$. The map* res *induces the following commutative diagram with exact rows:*

$$\begin{array}{ccccccccccc}
(1) & \longrightarrow & (k')^* & \longrightarrow & L^* & \xrightarrow{\mathrm{div}_L} & \mathrm{Div}(L/k) & \longrightarrow & \mathrm{Pic}(L/k) & \longrightarrow & (0) \\
 & & \downarrow & & \| & & \downarrow \mathrm{res} & & \downarrow & & \\
(1) & \longrightarrow & B^* & \longrightarrow & L^* & \xrightarrow{\mathrm{div}_B} & \mathrm{Div}(B) & \longrightarrow & \mathrm{Cl}(B) & \longrightarrow & (0)
\end{array}$$

We consider the case of a nonsingular complete curve X/k corresponding to the function field $k(X)/k$. Let $x \in k(X)$ such that $k(X)/k(x)$ is finite and let B be the integral closure of $k[x]$ in $k(X)$. Then B is a Dedekind domain and due to the definition of a function field we have $\bigcap_{v \in \mathcal{V}(L/k)} \mathcal{O}_v = k$. For the morphism $\pi : X \to \mathbb{P}^1$ defined above let $\pi^{-1}(\infty) = \{P_1, \ldots, P_r\}$ and define $U := \{P \in X | \mathcal{O}_P \subset B\}$. Then $\pi^{-1}(\infty)$ is the complement of U in X.
The above lemma holds as well if we consider only the divisors of degree 0, denoted by $\mathrm{Div}^0(X)$. Thus we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccccc}
(1) & \longrightarrow & k^* & \longrightarrow & k(X)^* & \xrightarrow{\mathrm{div}} & \mathrm{Div}^0(X) & \longrightarrow & \mathrm{Pic}^0(X) & \longrightarrow & (0) \\
 & & \downarrow & & \| & & \downarrow \mathrm{res} & & \downarrow & & \\
(1) & \longrightarrow & B^* & \longrightarrow & k(X)^* & \xrightarrow{\mathrm{div}_B} & \mathrm{Div}(B) & \longrightarrow & \mathrm{Cl}(B) & \longrightarrow & (0)
\end{array}$$

We will use the correspondence between $\mathrm{Pic}^0(X)$ and $\mathrm{Cl}(B)$ to obtain an efficient arithmetic since the multiplication of ideals can be performed using operations in the polynomial ring $k[x, y]$. And as we have seen at the beginning each maximal ideals of $k[x, y]/(f)$ can be generated by two elements, hence we can also find a representative for each class by two polynomials. We discuss this in the next subsection in more detail.

Denote the map from $\mathrm{Pic}^0(X)$ to $\mathrm{Cl}(B)$ by φ. It is given by

$$\varphi : \mathrm{Pic}^0(X) \to \mathrm{Cl}(B), \quad \text{class of } \sum_{P \in X} a_P P \mapsto \prod_{P \in U} (\text{class of } \mathcal{M}_P \cap B)^{a_P}.$$

If φ is bijective we can identify the groups. This is the most interesting case for applications. However this cannot be the case if B^* is strictly larger than k^*, hence if $r > 1$, since one can show for finite fields k that B^* has rank $r - 1$ and torsion group k^*.

Let $k(X)/k(x)$ be a function field and consider the fiber of ∞, hence the points $P_1, \ldots, P_r$ of X that map to ∞ under π. The *regulator* R is an integer associated to these valuations providing information about the group of units B^*. If $r = 1$ we put $R = 1$. We do not go into the details here since we will be concerned with the imaginary quadratic case, hence with $R = 1$. The definition can be found like the other results in Lorenzini [29]. For the use of function fields of unit rank ≥ 1 and a comparison of both cases we refer to Paulus and Rück [42] and several works of Stein, for example [56].

The following lemma holds

Lemma 2.21

$$|\mathrm{Cl}(B)| \cdot R = |\mathrm{Pic}^0(X)| \cdot \prod_{i=1}^{r} \deg(P_i) \cdot \log(q)^{r-1}.$$

Example 2.22 *Consider the setting of Example 2.11.*
In the first case, i. e. the real quadratic case, $r = 2$ and the degree of each point at infinity is 1. In this case the regulator is nontrivial and the groups Cl *and* Pic^0 *can be of very different cardinality. In the third case we have that $r = 1$, hence, $R = 1$ and the point at infinity has degree 1. Thus the groups have equal cardinality and in fact $Ker(\varphi) = \{0\}$.*
By a change of variables we can transform a defining equation of the first kind into one of the third if there exists a k-rational Weierstrass point, i. e. a point defined over k such that the map $\pi : X \to \mathbb{P}^1(k)$ is ramified at this point.

Before we conclude this section we introduce a further invariant of the curves we will need – the genus of the curve. Take for example the hyperelliptic curves in odd characteristic. For all of them the function field can be defined via a polynomial $y^2 = f(x), f(x) \in k[x]$. However we can further discriminate by considering the degree of f. In the case of hyperelliptic curves this is just what the genus does. This invariant occurs for example in the formula for the size of $\mathrm{Pic}^0(X)$. We define it via the Theorem of Riemann-Roch. First we define a space associated to an effective divisor.

Definition 2.23 *Let D be an effective divisor. Consider the following partial order $\geq$ on* $\mathrm{Div}(L)$*:*

$$D' \geq D \Longleftrightarrow D' - D \textit{ is an effective divisor.}$$

Define for a divisor D

$$H^0(D) := \{\alpha \in L | \mathrm{div}(\alpha) + D \geq 0\}.$$

This set actually is a finite space over k. Put $h^0(D) = \dim H^0(D)$.

Hence, this dimension is the same for all elements of a divisor class. We do not further motivate the following theorem but a detailed treatment can be found in almost any book on the topic.

Theorem 2.24 (Riemann-Roch) *Let X/k be a nonsingular complete curve. Then there exists a divisor $K \in \mathrm{Div}(k(X))$ and a non-negative integer g such that for all $D \in \mathrm{Div}(k(X))$ we have*

$$h^0(D) = \deg(D) + 1 - g + h^0(K - D).$$

Definition 2.25 *The integer g occurring in the Riemann-Roch Theorem is called the* genus of the curve *X/k. A nonsingular complete curve of genus 1 is called an* elliptic curve.

An important property of the genus is that it does not chance with scalar extensions of the ground field.

For an arbitrary given curve it is hard to find the genus, however there are some examples where it can be read off from the polynomial defining the corresponding function field.

Example 2.26 *Let the curve X/k be given by a polynomial*

$$y^2 - f(x),$$

where f is squarefree and $\mathrm{char}(k) \neq 2$. Let $\deg(f) = 2g + \varepsilon$, $\varepsilon = 1$ or 2. Then the genus of X equals g.
In characteristic 2 we have seen that the defining equation of a quadratic function field is of the form $y^2 + h(x)y - f(x)$. Let $\deg(f) = 2g + \varepsilon$, $\varepsilon = 1$ or 2. Then the genus of X equals g and we even have that $\deg h \leq g$.

2.2 Algorithms for the Ideal Class Group

To summarize the previous subsection we state the case of function fields we consider in this article as a definition. Furthermore note that from now on we let $k = \mathbf{F}_q$ be a finite field of characteristic p. We deal with hyperelliptic curves in imaginary representation only, hence with those having at least a $\mathbf{F}_q$-rational Weierstrass point. Thus the class number and $|\mathrm{Cl}|$ are equal.

Definition 2.27 *Let $\mathbf{F}_q(X)/\mathbf{F}_q$ be a quadratic function field. Let $\mathbf{F}_q(X)$ be defined via an equation*

$$y^2 + h(x)y = f(x) \text{ in } \mathbf{F}_q[x, y], \tag{1}$$

where $f(x) \in \mathbf{F}_q[x]$ is a monic polynomial of degree $2g + 1$, $h(x) \in \mathbf{F}_q[x]$ is a polynomial of degree at most g, and there are no solutions $(x, y) \in \bar{\mathbf{F}}_q \times \bar{\mathbf{F}}_q$ which simultaneously satisfy the equation $y^2 + h(x)y = f(x)$ and the partial derivative equations $2y + h(x) = 0$ and $h'(x)y - f'(x) = 0$. The curve $C/\mathbf{F}_q$ associated to this function field is a hyperelliptic curve of genus g *defined over $\mathbf{F}_q$.*

We have seen that for odd characteristic is suffices to let $h(x) = 0$ and to have f squarefree.
We now provide some very basic examples.

Example 2.28 *Curve of genus* 1 *(elliptic curve) over* $\mathbf{F}_{1601}$

$$C:\ y^2 = x^3 + 598x + 1043.$$

Curve of genus 2 *over* $\mathbf{F}_4 = \mathbf{F}_2(\alpha)$, $\alpha^2 = \alpha + 1$

$$C:\ y^2 + (x^2 + \alpha x + 1)y = x^5 + \alpha x^4 + x^3 + x^2 + x + 1.$$

Curve of genus 3 *over* $\mathbf{F}_{100000007}$

$$\begin{aligned} C:\ y^2 &= x^7 - 3\,x^6 + 3\,x^5 + 25000003\,x^4 \\ &\quad +49999999\,x^3 + 75000009\,x^2 \\ &\quad +50000002\,x + 25000002. \end{aligned}$$

Curve of genus 4 *over* $\mathbf{F}_{2^{79}}$

$$C:\ y^2 + x^4 y = x^9 + x^8 + x^5 + x.$$

Note that if P is defined over $\mathbf{F}_{q^r}$ and P does not correspond to the valuation v_{P_1} – the extension of deg under π – this means that we can find a basis of the corresponding maximal ideal of $\mathbf{F}_{q^r}[x,y]/(y^2 + h(x)y - f(x))$ of the form $(x - a, y - b)$, $a, b \in \mathbf{F}_{q^r}$. Hence, for the points defined over a fixed extension field we can rely on the interpretation of a point as a zero of $y^2 + h(x)y - f(x)$ if we add the point associated to v_{P_1} which we denote from now on by ∞ like on $\mathbb{P}^1$.
We have seen in the previous subsection that the maximal ideals of $\mathbf{F}_q[x,y]/(y^2 + h(x)y - f(x))$ have a basis consisting of two polynomials. By the construction presented there, the first polynomial $\in \mathbf{F}_q[x]$, whereas the second one is of the form $y - z(x), z(x) \in \mathbf{F}_q[x]$, since we reduce modulo a polynomial of degree 2 in y. Now consider the ideal class group, i.e. the ideals modulo the principal ideals. We can even show that in each class there exists a unique representative $D = (a(x), y - b(x))$ such that a is monic of $\deg(a) \leq g$ and $\deg b < \deg a$. Since D is an ideal of $\mathbf{F}_q[x,y]/(y^2 + h(x)y - f(x))$ we additionally have that $a|(b^2 + bh - f)$. For short we denote this ideal by $[a, b]$. We refer to this representation as *Mumford representation.* We now denote the ideals and ideal classes by D due to the relation to the divisors. Computing in the ideal class group consists thus in a composition of the ideals and a first reduction to a basis of two polynomials. The output of this algorithm is said to be semireduced. Then we need a second algorithm which is usually called reduction to find the unique representative in the class referred to above. Such an ideal is called *reduced.* Due to the work of Cantor [2] (for odd characteristic only) and Koblitz [21] there

exists an efficient algorithm to do so which is similar to the computation in the number field case. The algorithms are given in detail in several publications including Cantor [2], Koblitz [21], Krieger [25], Menezes et.al. [35] and are therefore stated here without further comments. The running time estimates are $17g^2 + O(g)$ operations in $\mathbf{F}_q$ for a generic operation whereas doubling takes $16g^2+O(g)$ operations (see Stein [55]). Improvements are possible in special cases.

Algorithm 2.1 (Composition)
`INPUT:` $D_1 = [a_1, b_1], D_2 = [a_2, b_2]$,
$C : y^2 + h(x)y = f(x)$.
`OUTPUT:` $D = [a, b]$ *semireduced with* $D \equiv D_1 D_2$.

1. *compute* $d_1 = \gcd(a_1, a_2) = e_1 a_1 + e_2 a_2$;
2. *compute* $d = \gcd(d_1, b_1 + b_2 + h) =$;
   $= c_1 d_1 + c_2(b_1 + b_2 + h)$;
3. *let* $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$;
   $$d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h);$$
4. $a = \frac{a_1 a_2}{d^2}$;
   $b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d} \bmod a$.

Algorithm 2.2 (Reduction)
`INPUT:` $D = [a, b]$ *semireduced.*
`OUTPUT:` $D' = [a', b']$ *reduced with* $D \equiv D'$.

1. *let* $a' = \frac{f - bh - b^2}{a}$;
   $$b' = (-h - b) \bmod a';$$
2. *if* $\deg a' > g$ *put* $a := a', b := b'$ *goto step 1;*
3. *make a monic.*

The inverse of a class in the representation is represented by $[a, -h - b]$.

2.3 Cardinality of $\mathrm{Pic}^0(X/\mathbf{F}_{q^n})$

Note that later on we consider the case where the class group and the ideal class group are isomorphic, however the results presented here hold in general for the Picard group $\mathrm{Pic}^0(X)$. Unless stated otherwise the results hold for any nonsingular complete curve X defined over $\mathbf{F}_q$.
For cryptographic purposes it is necessary to know more about the group structure of the chosen group. For example to avoid the Pohlig-Hellman attack one has to guarantee that the class number contains a large prime factor. Let $\overline{\mathbf{F}}_q$ denote the algebraic closure of $\mathbf{F}_q$ contained in $\overline{\mathbf{F}_q(X)}$. Let $\mathbf{F}_{q^n}$ denote the unique subfield of $\overline{\mathbf{F}}_q$ of degree n. Extending the concept of extension of scalars to the Picard group we put

$$N_n = |\mathrm{Pic}^0(X/\mathbf{F}_{q^n})|.$$

For the group order we have the following bound depending only on the finite field and the genus of the curve.

Theorem 2.29 (Hasse-Weil)

$$(q^{n/2}-1)^{2g} \leq N_n \leq (q^{n/2}+1)^{2g}.$$

Thus $N_n \sim q^{ng}$.

Denote by M_r the number of points of $X_{\bar{\mathbf{F}}_q}$ that are defined over $\mathbf{F}_{q^r}$ or a subfield $\mathbf{F}_{q^s}$, $s|r$. There is a relationship between the N_i and the numbers M_r for $1 \leq r \leq g$. The power series $Z(X/\mathbf{F}_q, t) = \exp\left(\sum_{n=1}^{\infty} M_n t^n/n\right)$ is called the zeta-function of $X/\mathbf{F}_q$. One can show that the zeta function is rational and can also be written in the form $Z(X/\mathbf{F}_q, t) = \frac{L(t)}{(1-t)(1-qt)}$, where $L(t)$ is a polynomial $\in \mathbf{Z}[t]$ of degree $2g$. We are more interested in the related polynomial $P(T) = T^{2g}L(1/T)$. In the following theorem we list the most important properties of P.

Theorem 2.30 *Let the factorization of $P(T)$ over $\mathbf{C}$ be $P(T) = \prod_{i=1}^{2g}(T-\tau_i)$.*

1. *The roots of P satisfy $|\tau_i| = \sqrt{q}$.*
2. *They come in complex conjugate pairs such that there exists an ordering with $\tau_{i+g} = \bar{\tau}_i$, hence, $\tau_{i+g}\tau_i = q$.*
3. *$P(T)$ is of the following form*
$$T^{2g} + a_1T^{2g-1} + a_2T^{2g-2} + \cdots + a_gT^g + qa_{g-1}T^{g-1} + \cdots + q^{g-1}a_1T + q^g.$$
4. *For any integer n we have*
$$N_n = \prod_{i=1}^{2g}(1-\tau_i^n).$$

5. *For any integer n we have*
$$|M_n - (q^n + 1)| \leq g\lfloor 2q^{n/2} \rfloor.$$

6. *For any integer n we have*
$$M_n = q^n + 1 - \sum_{i=1}^{2g} \tau_i^n.$$

7. *Put $a_0 = 1$ then*
$$ia_i = (M_i - (q^i + 1))a_0 + (M_{i-1} - (q^{i-1} + 1))a_1 + \cdots + (M_1 - (q + 1))a_{i-1}$$
for $1 \leq i \leq g$.

Thus from the first g numbers of points on the curve M_i one can obtain the whole polynomial $P(T)$ and thus the class number. To illustrate this relation: for a genus 2 curve we have to count the number of points defined over $\mathbf{F}_q$ and $\mathbf{F}_{q^2}$ to obtain $a_1 = M_1 - q - 1$ and $a_2 = (M_2 - q^2 - 1 + a_1^2)/2$.
Hence, if the curve is defined over a small field, then we can easily obtain the polynomial $P(T)$ and therefore the class number for any extension field. A curve defined over a small finite field which is considered over a large extension field is called a *Koblitz curve*. We have just seen one advantage of Koblitz curves - $P(T)$ can be determined easily. In the following section we explain the details on the computation of $P(T)$ for Koblitz curves.

From *1.* and *5.* we can obtain bounds on the coefficients of P. For example we have $|a_1| \leq g\lfloor 2\sqrt{q} \rfloor$, $|a_2| \leq \binom{2g}{2}q$. In more detail and in dependence on a_1 Rück [45] shows for hyperelliptic curves of genus 2 that in the case of irreducible $P(T)$ we even have
$$2|a_1|\sqrt{q} - 2q < a_2 < a_1^2/4 + 2q, \tag{2}$$
and $a_1^2 - 4a_2 + 8q$ is not a square.
Furthermore the structure of $P(T)$, i.e. *3.* can be read off from *1.* and *2.*. *7.* follows by considering the derivative of $\ln Z(X/\mathbf{F}_q, t)$ in the representation as $\exp\left(\sum_{n=1}^{\infty} M_n t^n/n\right)$ and as $\frac{L(t)}{(1-t)(1-qt)}$.

Let $P(T) = T^{2g} + a_1 T^{2g-1} + a_2 T^{2g-2} + \cdots + a_g T^g + q a_{g-1} T^{g-1} + \cdots + q^{g-1} a_1 T + q^g$ correspond to the curve $X/\mathbf{F}_q$ and let $Y/\mathbf{F}_q$ be a twist of X. One can show that for Y the polynomial is of the form $T^{2g} - a_1 T^{2g-1} + a_2 T^{2g-2} + - \cdots + -a_g T^g + q a_{g-1} T^{g-1} + - \cdots - q^{g-1} a_1 T + q^g$.

In cryptographic applications we usually work in a subgroup of $\mathrm{Pic}^0(X_{\mathbf{F}_{q^n}})$ of prime order. Since two curves having the same polynomial $P(T)$ have the same class number over any extension of the ground field, we can classify the curves using this polynomial. The classes will be called *isogeny classes* due to the geometric concept of isogeny.

There are certain curves we want to avoid, since they are weak under a special attack. For the elliptic curves one can use the Weil pairing to map the discrete logarithm problem of the curve over $\mathbf{F}_{q^n}$ to an equivalent one in $\mathbf{F}_{q^{kn}}$, where k is such that the l-th roots of unity are in $\mathbf{F}_{q^{kn}}$, where the prime l is the order of the group used in the cryptosystem. Thus k is the order of q^n modulo l. Menezes, Okamato, and Vanstone [32] showed that for certain elliptic curves k is always ≤ 6 independent of the degree of extension n. This attack is a special case of the one by Frey and Rück [8] which works also for the Picard group of hyperelliptic curves. Thus before accepting a hyperelliptic curve to use in cryptography one should always check that k is large enough, i. e. $\geq 2000/\log_2 q^n$.

Usually k depends on the extension field $\mathbf{F}_{q^r}$ we consider, however there are some curves that are always weak under this attack. Galbraith [10] provides a list showing how large k can get for so called *supersingular curves* depending on the genus of the curve. Since the k is relatively small in any such case, supersingular hyperelliptic curves should be avoided.
Note that this is an abuse of notation since it is the *Jacobian variety* of the curve that is supersingular in this case. The Jacobian variety J is an abelian variety that corresponds in a functorial way to the Picard group of the curve X such that for any field $\mathbf{F}_{q^n} \subseteq \bar{\mathbf{F}}_q$ the group of $\mathbf{F}_{q^n}$-rational points of the Jacobian corresponds to the group $\mathrm{Pic}^0(X_{\mathbf{F}_{q^n}}/\mathbf{F}_q)$ and such that for a given $\mathbf{F}_q$-rational point P_0 there exists a morphism $X \to J$ that sends P_0 to the identity element of J. This morphism induces the map $P \mapsto$ class of $P - P_0$ on the $\bar{\mathbf{F}}_q$-rational points of X. Since we do only use the concept of supersingularity to exclude some curves we shall use the criterion to detect them (see Tate [59]) as a definition.

Definition 2.31 *Suppose* $q = p^r$ *and suppose* $\mathbf{J}$ *is the Jacobian variety of a hyperelliptic curve of genus* g *over* $\mathbf{F}_q$. *Suppose*

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

is the corresponding polynomial. Then $\mathbf{J}$ *is* supersingular *if and only if, for all* $1 \leq i \leq g$,

$$p^{\lceil ri/2 \rceil} | a_i.$$

Note that we have to be aware of k for every curve, but usually k can be large depending on n whereas for supersingular curves it is always small.

2.4 The Frobenius Endomorphism

Also in this subsection the results hold for arbitrary curves defined over the finite field $\mathbf{F}_q$.

Definition 2.32 *Let $X/\mathbf{F}_q$ be a nonsingular complete curve. The homomorphism $\sigma^* : \mathbf{F}_q(X) \to \mathbf{F}_q(X), \alpha \mapsto \alpha^q$ is a map of $\mathbf{F}_q$-algebras which enduces an endomorphism $\sigma : X \to X$ called the* Frobenius endomorphism.

The map σ^* can be extended to a map $\bar{\sigma}^* : \bar{\mathbf{F}}_q(X) \to \bar{\mathbf{F}}_q(X)$, $\sum_{i=1}^s a_i\alpha_i \mapsto \sum_{i=1}^s a_i\alpha_i^q$, where $a_i \in \bar{\mathbf{F}}_q, \alpha_i \in \mathbf{F}_q(X)$ and a corresponding map $\bar{\sigma} : X_{\bar{\mathbf{F}}_q} \to X_{\bar{\mathbf{F}}_q}$. In the first subsection we used the Galois group of $\bar{k}/k$ to define the field of definition of a point. For finite fields $k = \mathbf{F}_q$ this group is generated by the Frobenius automorphism F of $\bar{\mathbf{F}}_q$ over $\mathbf{F}_q$, where $F(\alpha) = \alpha^q$ for $\alpha \in \bar{\mathbf{F}}_q$. Furthermore we have seen that the groups $\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ and $\mathrm{Gal}(\bar{\mathbf{F}}_q(X)/\mathbf{F}_q(X))$ are isomorphic. Now consider the action of F on the function field $F : \bar{\mathbf{F}}_q(X) \to \bar{\mathbf{F}}_q(X)$, $\sum_{i=1}^s a_i\alpha_i \mapsto \sum_{i=1}^s a_i^q\alpha_i$, where like above $a_i \in \bar{\mathbf{F}}_q, \alpha_i \in \mathbf{F}_q(X)$. One can show that for points $P \in X_{\bar{\mathbf{F}}_q}$ the action of this map and $\bar{\sigma}(P)$ are equal. Thus, let $\bar{\mathbf{F}}_q(X)/\bar{\mathbf{F}}_q(x)$ be a finite extension, hence, $\bar{\mathbf{F}}_q(X) = \bar{\mathbf{F}}_q(x, y)/(f)$, and let P correspond to a maximal ideal of $\bar{\mathbf{F}}_q[x, y]/(f)$ given by $(x - a, y - b)$. Then using the second map we see that $\bar{\sigma}(P)$ corresponds to $(x - a^q, y - b^q)$. This motivates the following statement which could also have served as a definition of the field of definition of a point.

Lemma 2.33 *Let $X/\mathbf{F}_q$ be a nonsingular complete curve. A point $P \in X_{\bar{\mathbf{F}}_q}$ is defined over $\mathbf{F}_q$ if and only if $\bar{\sigma}(P) = P$.*

In the case of hyperelliptic Koblitz curves $C/\mathbf{F}_q$ we consider here, we identified a point with ∞ or with a zero of the defining polynomial. If $P \neq \infty$ is defined over $\mathbf{F}_{q^r}$, then $P = (a, b)$, $a, b \in \mathbf{F}_{q^r}$ and $\bar{\sigma}(P) = (a^q, b^q)$. For the point ∞ we have seen that it is defined over the ground field, hence $\bar{\sigma}(\infty) = \infty$.

The Frobenius endomorphism extends to the group of divisors and hence also to the Picard group $\mathrm{Pic}^0(X_{\bar{\mathbf{F}}_q}/\bar{\mathbf{F}}_q)$.

Example 2.34 *Consider the case of imaginary quadratic function fields. Then we represent the divisor classes via the ideal classes. If $D = (\sum_{i=0}^g a_ix^i, y - \sum_{i=0}^{g-1} b_ix^i)$ represents an ideal class, then we have that $\bar{\sigma}(D) = (\sum_{i=0}^g a_i^qx^i, y - \sum_{i=0}^{g-1} b_i^qx^i)$.*

Let $X/\mathbf{F}_q$ be a nonsingular complete curve of genus g. Denote by $J[m]$ the kernel of the multiplication by m map on $\mathrm{Pic}^0(X_{\bar{\mathbf{F}}_q}/\bar{\mathbf{F}}_q)$. One can show that the natural action of $\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ on $\mathrm{Pic}^0(X_{\bar{\mathbf{F}}_q}/\bar{\mathbf{F}}_q)$ restricts to an action on $J[m]$,

$\bar{\rho}_m : \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q) \to J[m]$. If m is prime to p then $J[m]$ is isomorphic to $(\mathbf{Z}/m\mathbf{Z})^{2g}$ as $\mathbf{Z}/m\mathbf{Z}$-module. Furthermore one can show that the image of $\bar{\rho}_m$ lies in the subgroup of endomorphisms of the $(\mathbf{Z}/m\mathbf{Z})$-module $J[m]$. Hence the image of a Galois automorphism corresponds to a matrix of $\mathrm{GL}_{2g}(\mathbf{Z}/m\mathbf{Z})$. We shall be interested in the image of the Frobenius automorphism.
Let l be a prime. The *Tate module* $T_l(X/\mathbf{F}_q)$ of $X/\mathbf{F}_q$ is defined as the projective limit of the projective system of multiplication by l-homomorphisms $\{J[l^{m+1}] \to J[l^m]\}$. Using the projective limit of the representations $\bar{\rho}_{l^r}$ leads to a representation ρ_l of $\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ in $\mathrm{GL}_s(\mathbf{Z}_l)$, where $\mathbf{Z}_l$ denotes the l-adic integers and $s = 2g$ for $l \neq p$.
Let now $F \in \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ denote the Frobenius automorphism. Put

$$P(F, l)(T) := \det(\rho_l(F) - T).$$

Then this polynomial is the characteristic polynomial of $\rho_l(F)$ in $\mathrm{GL}_{2g}(\mathbf{Z}_l)$. The following theorem will be important for our applications.

Theorem 2.35 *Let $X/\mathbf{F}_q$ be a nonsingular complete curve of genus $g \geq 1$. Then for all primes $l \neq p$ the polynomial $P(F,l)(T)$ is a polynomial with integer coefficients. Moreover the coefficients are independent of the choice of l. In fact this polynomial is equal to the polynomial $P(T)$, which is $T^{2g}L(1/T)$, where L is the numerator of the zeta-function $Z(X/\mathbf{F}_q, t)$.*

We will make intensive use of the Frobenius endomorphism of the curve to speed up the arithmetic in $\mathrm{Pic}^0(X/\mathbf{F}_{q^r})$ and use the fact, that for points the maps defined above correspond such that we can use the characteristic polynomial of the Frobenius automorphism of $\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ also as the characteristic polynomial of the Frobenius endomorphism of $X_{\bar{\mathbf{F}}_q}$ and of $\mathrm{Pic}^0(X/\mathbf{F}_{q^n})$, due to the representation of a divisor as a sum of points.

3 Computation of $P(T)$

From now on we only consider hyperelliptic Koblitz curves of genus g. In this section we state some details for computing $P(T)$ in the case of Koblitz curves. Since the coefficients of $P(T)$ do only depend on the number of points on the curve over $\mathbf{F}_q, \ldots, \mathbf{F}_{q^g}$, where the curve is defined over $\mathbf{F}_q$ and has genus g, we first need a way to count the points.
As $\mathbf{F}_q$ is of small cardinality since C is a Koblitz curve, this can be done by a brute-force search using some short-cuts. Stein and Teske [57] investigated a way to compute $P(T)$ by determining M_i only up to $i = g - 1$ respectively to $g - 2$ and computing N_1 (and also N_2 in the second case). Although the complexity of their algorithm is better we do not get into its details since our fields and genera are of such a small size that we can count at almost no effort even for $\mathbf{F}_{q^g}$.

Note that the following ideas can be found in Koblitz [21]. First, let q be odd, then C is given by $C : y^2 = f(x)$. $a \in \mathbf{F}_{q^i}$ leads to a single point iff $f(a) = 0$, hence, to $P = (a, 0)$. There are two points with first coordinate a iff $f(a)$ is a square in $\mathbf{F}_{q^i}$. Using the quadratic character χ of $\mathbf{F}_{q^i}$ with the convention $\chi(0) = 0$ we have

$$M_i = 1 + \sum_{a \in \mathbf{F}_{q^i}} (1 + \chi(f(a))) = q^i + 1 + \sum_{a \in \mathbf{F}_{q^i}} \chi(f(a)).$$

$\chi(f(a))$ can be computed by $f(a)^{(q^i-1)/2}$. Thus in the algorithm we simply compute $\sum_{a \in \mathbf{F}_{q^i}} \chi(f(a))$ and add $q^i + 1$.

In case of $q = 2^r$ the defining equation is $C : y^2 + h(x)y = f(x)$ and $h(x) \neq 1$ since otherwise the curve is supersingular (see Galbraith [10]). If $h(a)$ happens to be 0 then a gives rise to one special point. Otherwise we make a transformation by dividing through $h(a)^2$ which leads to the equation $v^2 + v = (f(a)/h(a)^2)$, $v = y/h(a)$. This equation is satisfied for two distinct values v iff $\mathrm{Tr}_{\mathbf{F}_{q^i}:\mathbf{F}_2}(f(a)/h(a)^2) = 0$. If we apply the trace map on both sides then $\mathrm{Tr}(v^2 + v) = \mathrm{Tr}(v^2) + \mathrm{Tr}(v) = 0$ since we are working in characteristic 2 and $\mathrm{Tr}(v^2) = \mathrm{Tr}(v)$. Thus to compute M_i we do the following. For every $a \in \mathbf{F}_q$ we first evaluate $h(a)$ and increase M_i by one if this is zero. Else we compute the trace of $f(a)/(h(a)^2)$ and increase M_i by two if this is zero. Finally we have to add one for the single point at infinity.

To build a list of all nonisogenous classes of hyperelliptic curves we make a brute force search though all possible curves i. e. all polynomials f (and h in characteristic 2), first check for nonsingularity, and then compute the polynomial $P(T)$. Since two curves are isogenous iff they have the same polynomial P our algorithm stores only one representative equation. If one chooses a curve – or rather a suitable polynomial P – it might be advantageous for implementation to search through all isogenous curves as the addition formulae depend on the representation of the curve.

Consider the same curve as defined over $\mathbf{F}_{q^n}$ and denote the corresponding polynomial by $\tilde{P}(T)$. Since due to $|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| = \tilde{P}(1)$ the class number is highly composite unless the polynomial for the corresponding field extension is irreducible we want to exclude the cases where P is reducible. On the other hand we only compute the polynomial P of the ground field. And it would be rather time-consuming to check all extension fields. However we can exclude some cases. Due to formula *4.* in Theorem 2.30 we have that if P is reducible then $\tilde{P}$ for any extension of the ground field is reducible, too. Hence, we only take into account those curves with irreducible P. Some of the results are included in Section 5, but most of the tabulars require to much space.

4 Counting Points

In this section we deal with the problem of evaluating an expression of the form $\prod_{i=1}^{r}(1-\alpha_i^n)$ where the α_i are the roots of a polynomial of degree r. This problem was considered by Pierce [39] and Lehmer [27] for arbitrary polynomials. They give explicit formulae to establish linear recurrence sequences to compute this expression for polynomials of degree at most 5. However, we can make use of the special structure of our polynomials and obtain recurrences of lower order for any degree.
In the age of computer algebra systems the more direct approach would be to factor the polynomial over the complex numbers with a suitable precision and to compute the expression directly. To get the result one takes the nearest integer or even better the nearest integer divisible by $\prod_{i=1}^{r}(1-\alpha_i)$, i. e. by the value of the polynomial at 1. However our approach has the advantage that it is fast, uses exact integer arithmetic only, and that due to the recurrences one saves even more computing the class numbers for various extensions subsequently.

Let

$$P(T) = T^{2g} + a_1T^{2g-1} + \cdots + a_gT^g + a_{g-1}qT^{g-1} + \cdots + a_1q^{g-1}T + q^g$$

be the characteristic polynomial of the Frobenius endomorphism associated to the hyperelliptic curve of genus g. In order to compute the order of $\mathrm{Pic}^0(C/\mathbf{F}_{q^n})$ we use Theorem 2.30

$$N_n = \prod_{i=1}^{g}((1-\tau_i^n)(1-\bar{\tau}_i^n)) = \prod_{i=1}^{g}((1+q^n)-(\tau_i^n+\bar{\tau}_i^n)).$$

For cryptographic purposes we are interested in groups which contain large prime order subgroups. For $n_1|n_2$ we immediately get by $N_n = \prod_{i=1}^{2g}(1-\tau_i^n)$ that N_{n_2} is divisible by N_{n_1}. Therefore we compute the number of divisor classes only for n prime in order to achieve a big subgroup of prime order. The results for various Koblitz curves can be found in the next section.

We know that the roots τ_i of P occur in conjugate pairs and $\tau_i \cdot \bar{\tau}_i = q$. So by grouping together these pairs we obtain g equations $T^2 - \mu_iT + q$ satisfied by the τ_i, i. e. $\tau_i + \bar{\tau}_i = \mu_i$.
As the following formulae get very complicated dealing with the coefficients of P we now introduce the related polynomial

$$Q(T) = \prod_{i=1}^{g}(T-\mu_i) = T^g + b_1T^{g-1} + \cdots + b_g.$$

The coefficients $Q(T)$ can be obtained recursively from the coefficients of the corresponding polynomial P (because the τ_i are the roots of P, and thus

the symmetric expressions in $(\tau_1 + \bar{\tau}_1), \ldots, (\tau_g + \bar{\tau}_g)$ depend only on those in $\tau_1, \bar{\tau}_1, \ldots, \tau_g, \bar{\tau}_g$, hence on the coefficients of P). This has the advantage that we can carry out the computation of the b_i using exact integer arithmetic. We first make use of the b_i, and then return to the computation of these coefficients.
To ease and speed up the computations we derive recursion formulae for the expressions $(\tau_i^n + \bar{\tau}_i^n)$ and state them in terms of the corresponding μ_i. In the final step we expand the given product using Q. Note, that we need not factor neither P nor Q.
Suppose that we already got $\tau_i^n + \bar{\tau}_i^n = A_{1,n} + \mu_i A_{2,n} + \cdots + \mu_i^{g-1} A_{g,n}$, where $A_{j,n} \in \mathbf{Z}$ (for the τ_i are algebraic integers and by $\tau_i^n + \bar{\tau}_i^n = \tau_i^n + (\mu_i - \tau_i)^n \in \mathbf{Q}(\mu_i)$). We immediately get:

$$
\begin{aligned}
&\tau_i^{n+1} + \bar{\tau}_i^{n+1} = (\tau_i + \bar{\tau}_i)(\tau_i^n + \bar{\tau}_i^n) - \tau_i \bar{\tau}_i (\tau_i^{n-1} + \bar{\tau}_i^{n-1}) \\
&= \mu_i (A_{1,n} + \mu_i A_{2,n} + \cdots + \mu_i^{g-1} A_{g,n}) - q(A_{1,n-1} + \mu_i A_{2,n-1} + \cdots + \mu_i^{g-1} A_{g,n-1}) \\
&= (q A_{1,n-1} - b_g A_{g,n}) + \mu_i (A_{1,n} + q A_{2,n-1} - b_{g-1} A_{g,n}) + \cdots + \\
&\qquad + \mu_i^{g-1} (A_{g-1,n} + q A_{g-2,n-1} - b_1 A_{g,n}).
\end{aligned}
$$

With the initial states $A_{1,0} = 2 = \tau_i^0 + \bar{\tau}_i^0$, $\quad A_{j,0} = 0$ for $j \neq 1$ and $A_{2,1} = 1$ (as $\tau_i^1 + \bar{\tau}_i^1 = \mu_i$), $A_{j,1} = 0$ for $j \neq 2$ we are lead to the following definitions of linear recursions:

$$
\begin{array}{rcll}
A_{1,n+1} & = & & q A_{1,n-1} - b_g A_{g,n} \\
A_{2,n+1} & = & A_{1,n} + & q A_{2,n-1} - b_{g-1} A_{g,n} \\
& \vdots & & \vdots \\
A_{j,n+1} & = & A_{j-1,n} + & q A_{j,n-1} - b_{g-j+1} A_{g,n} \\
& \vdots & & \vdots \\
A_{g,n+1} & = & A_{g-1,n} + & q A_{g,n-1} - b_1 A_{g,n}.
\end{array}
$$

In the expansion of the product

$$
\prod_{i=1}^{g} ((1 + q^n) - (\tau_i^n + \bar{\tau}_i^n)) = \prod_{i=1}^{g} ((1 + q^n) - (A_{1,n} + \mu_i A_{2,n} + \cdots + \mu_i^{g-1} A_{g,n}))
$$

the terms in the μ_i are symmetric polynomials in μ_i, and therefore they can be expressed in terms of the elementary symmetric functions, hence in the coefficients of Q.
For the implementation we explicitly computed these dependencies on the b_i for genera up to 4. For example in the case of genus two this formula is

$$
|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| = (1 + q^n)^2 - (2A_{1,n} - b_1 A_{2,n})(1 + q^n) + A_{1,n}^2 - b_1 A_{1,n} A_{n,2} + b_2 A_{2,n}^2.
$$

Thus to build the tables of group orders given in the next section we run the recurrence sequences from $n = 0$ to the maximal value of interest. This is almost for free. We compute the class number only for the cases of n prime. The evaluation of the expression in the b_i's is also fast and we gain from computing the values for several extensions.

We now deal with the computation of Q.

Theorem 4.1 *Let*

$$\begin{aligned} P(T) &= \prod_{i=1}^{2g}(T-\tau_i) \\ &= T^{2g} + a_1T^{2g-1} + \cdots + a_gT^g + a_{g-1}qT^{g-1} + \cdots + a_1q^{g-1}T + q^g \end{aligned}$$

and put $a_0 = 1$. *Then the following statements hold for the coefficients of* $Q(T) = \prod_{j=1}^{g}(T-\mu_i) = T^g + b_1T^{g-1} + \cdots + b_g$, $\mu_j = \tau_j + \bar{\tau}_j$:

$$\begin{aligned} b_{2k} &= a_{2k} - \left(\sum_{i=1}^{k} \binom{g-2(k-i)}{i} q^i b_{2(k-i)} \right), \\ b_{2k+1} &= a_{2k+1} - \left(\sum_{i=1}^{k} \binom{g-2(k-i)-1}{i} q^i b_{2(k-i)+1} \right). \end{aligned}$$

Proof. Choose the ordering of the roots τ_i of $P(T)$ as usual such that for $1 \le i \le g$ we have $\bar{\tau}_i = \tau_{g+i}$. The b_i are the elementary symmetric functions in the μ_i, thus $b_j = (-1)^j \sum_{i_1<\ldots<i_j}^{g} \mu_{i_1}\cdots\mu_{i_j}$. We have to consider two cases for odd and even index:

$$\begin{aligned} b_{2k} &= \sum_{i_1<i_2<\cdots<i_{2k}}^{g} \mu_{i_1}\mu_{i_2}\cdots\mu_{i_{2k}} \\ &= \sum_{i_1<i_2<\cdots<i_{2k}}^{g} (\tau_{i_1}+\bar{\tau}_{i_1})(\tau_{i_2}+\bar{\tau}_{i_2})\cdots(\tau_{i_{2k}}+\bar{\tau}_{i_{2k}}). \end{aligned}$$

Expanding and rearranging this product leads to the sum of all products of $2k$ different τ_i's with the property that no two conjugated τ_i's occur. Hence,

$$b_{2k} = \sum_{\substack{j_1<j_2<\cdots<j_{2k} \\ \text{no two conjugate}}}^{2g} \tau_{j_1}\tau_{j_2}\cdots\tau_{j_{2k}}.$$

Since the coefficients of P contain conjugate τ_i's, $(a_i = (-1)^i \sum_{j_1<\ldots<j_i}^{2g} \tau_{j_1} \cdots \tau_{j_i})$ we have to subtract from a_{2k} any cases of two or more conjugates. Then they are expressed with respect to the $b_{2k'}$, with $k' < k$.

$$\begin{aligned} b_{2k} &= \sum_{j_1<j_2<\cdots<j_{2k}}^{2g} \tau_{j_1}\tau_{j_2}\cdots\tau_{j_{2k}} - \sum_{\substack{j_1<\cdots<j_{2k-2} \\ \text{no two conjugate}}}^{2g} \sum_{\substack{l_1\leq g \\ l_1,l_1+g\neq j_1,\ldots,j_{2k-2}}} \tau_{l_1}\bar{\tau}_{l_1}\tau_{j_1}\cdots\tau_{j_{2k-2}} - \\ &- \sum_{\substack{j_1<\cdots<j_{2k-4} \\ \text{no two conjugate}}}^{2g} \sum_{\substack{l_1,l_2\leq g \\ l_i,l_i+g,\neq j_1,\ldots j_{2k-4}}} \tau_{l_1}\bar{\tau}_{l_1}\tau_{l_2}\bar{\tau}_{l_2}\tau_{j_1}\cdots\tau_{j_{2k-4}} - \cdots - \sum_{l_1,\ldots,l_k\leq g} \tau_{l_1}\bar{\tau}_{l_1}\cdots\tau_{l_k}\bar{\tau}_{l_k}. \end{aligned}$$

Once the $j_1 < \ldots < j_{2k-2i}$ are fixed, there are $\binom{g-2(k-i)}{i}$ choices for the $l_1, \ldots, l_i$. We have $\tau_{l_1}\bar{\tau}_{l_1}\cdots\tau_{l_i}\bar{\tau}_{l_i} = q^i$ and $\sum_{\substack{j_1<\cdots<j_{2k-2i} \\ \text{no two conjugate}}}^{2g} \tau_{j_1}\cdots\tau_{j_{2k-2i}} = b_{2k-2i}$. Thus

$$\begin{aligned} b_{2k} &= a_{2k} - (g-2k+2)qb_{2k-2} - \binom{g-2k+4}{2}q^2 b_{2k-4} - \cdots - \binom{g}{k}q^k b_0 \\ &= a_{2k} - \left(\sum_{i=1}^{k} \binom{g-2(k-i)}{i} q^i b_{2(k-i)}\right). \end{aligned}$$

The case of odd index is treated similarly. The difference lies in the fact that there is an odd number of τ_i's to deal with. Since we consider *pairs* of conjugates the number of elements to choose the respective l_i's from is decreased by 1.

$$\begin{aligned} b_{2k+1} &= - \sum_{i_1<i_2<\cdots<i_{2k+1}}^{g} \mu_{i_1}\mu_{i_2}\cdots\mu_{i_{2k+1}} \\ &= - \sum_{i_1<i_2<\cdots<i_{2k+1}}^{g} (\tau_{i_1}+\bar{\tau}_{i_1})(\tau_{i_2}+\bar{\tau}_{i_2})\cdots(\tau_{i_{2k+1}}+\bar{\tau}_{i_{2k+1}}) \\ &= - \sum_{\substack{j_1<j_2<\cdots<j_{2k+1} \\ \text{no two conjugate}}}^{2g} \tau_{j_1}\tau_{j_2}\cdots\tau_{j_{2k+1}} \\ &= - \sum_{j_1<j_2<\cdots<j_{2k+1}}^{2g} \tau_{j_1}\tau_{j_2}\cdots\tau_{j_{2k+1}} + \sum_{\substack{j_1<\cdots<j_{2k-1} \\ \text{no two conjugate}}}^{2g} \sum_{\substack{l_1\leq g \\ l_1,l_1+g\neq j_1,\ldots,j_{2k-1}}} \tau_{l_1}\bar{\tau}_{l_1}\tau_{j_1}\cdots\tau_{j_{2k-1}} + \\ &+ \sum_{\substack{j_1<\cdots<j_{2k-3} \\ \text{no two conjugate}}}^{2g} \sum_{\substack{l_1,l_2<\leq g \\ l_i,l_i+g\neq j_1,\ldots,j_{2k-3}}} \tau_{l_1}\bar{\tau}_{l_1}\tau_{l_2}\bar{\tau}_{l_2}\tau_{j_1}\cdots\tau_{j_{2k-3}} + \cdots + \sum_{j_1}^{2g} \sum_{\substack{l_1,\ldots,l_k\leq g \\ l_i,l_i+g\neq j_1}} \tau_{l_1}\bar{\tau}_{l_1}\cdots\tau_{l_k}\bar{\tau}_{l_k}\tau_{j_1} \\ &= a_{2k+1} - (g-2k+2-1)qb_{2k-1} - \binom{g-2k+4-1}{2}q^2 b_{2k-3} - \cdots - \binom{g-1}{k}q^k b_1 \end{aligned}$$

Table 1: Binary curves of genus 2

Equation of C	$P(T)$
$y^2+y=x^5+x^3$	$T^4+2T^3+2T^2+4T+4$
$y^2+y=x^5+x^3+1$	$T^4-2T^3+2T^2-4T+4$
$y^2+y=x^5+x^3+x$	T^4+2T^2+4
$y^2+xy=x^5+1$	T^4+T^3+2T+4
$y^2+xy=x^5+x^2+1$	T^4-T^3-2T+4
$y^2+(x^2+x+1)y=x^5+x^4+x^3$	T^4+T^2+4
$y^2+(x^2+x)y=x^5+x^4+x$	T^4-T^2+4
$y^2+(x^2+x+1)y=x^5+x^4$	$T^4+2T^3+3T^2+4T+4$
$y^2+(x^2+x+1)y=x^5+x^4+1$	$T^4-2T^3+3T^2-4T+4$

$$= \quad a_{2k+1}-\left(\sum_{i=1}^{k}\binom{g-2(k-i)-1}{i}q^i b_{2(k-i)+1}\right).$$

$\square$

5 Examples

This section provides several examples for the characteristic polynomials and the class number for hyperelliptic curves of genus 2,3 and 4. The algorithms described in the preceding sections have been implemented using the computer algebra system Magma. For all the examples we present as "nice examples" we checked that $q^{nk} \not\equiv 1 \bmod l$ for $k \leq \frac{2000}{\log_2 q^n}$, where l is the large prime dividing $|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})|$. Thus these curves are secure under the Frey-Rück attack.
The complete lists with all curves and all group orders for suitable extensions have been made public. They can be obtained from

`http://www.exp-math.uni-essen.de/~lange/KoblitzC.html`.

Remark: When we speak of *all* isogeny classes we consider only those hyperelliptic curves having at least one $\mathbf{F}_q$-rational Weierstrass point.

5.1 Binary Koblitz Curves

Over $\mathbf{F}_2$ we can classify up to isogenies the nine classes of hyperelliptic curves of genus 2 with irreducible $P(T)$ given in Table 1.
The first five examples were given in Koblitz [21]. Besides the first three classes these curves are non-supersingular. The fourth and fifth case were studied by Günter, Lange, and Stein in [17] where they also give tables stating the group

Table 2: Curve with $P(T) = T^4 + T^2 + 4$:

n	$\lvert \mathrm{Pic}^0(C/\mathbf{F}_{2^n}) \rvert$
61	531691198313966349295368021364532706=
	$2 \cdot 3 \cdot 28549 \cdot 1683601 \cdot 18436485874741919325168049$
67	21778071482940061661933311406888688670134=
	$2 \cdot 3 \cdot 1200109695244769627 \cdot 3024455676736879780907$
71	5575186299632655785387655742010246170856454=
	$2 \cdot 3 \cdot 89603 \cdot 205579223 \cdot 50443633667649128915517181261$
73	89202980794122492566135449435595199268083726=
	$2 \cdot 3 \cdot 1607 \cdot 230389 \cdot 40156005041388474897223374021340127$
79	365375409332725729550920124174223720018505058214=
	$2 \cdot 3 \cdot 47100403685197463 \cdot 1292895533602240063852543777463$
83	93536104789177786765035812824978038852703797931254=
	$2 \cdot 3 \cdot 167^2 \cdot 6143 \cdot 410175709 \cdot 20161744307 \cdot 11003137296258831609409$
89	383123885216472214589586756196910238039372229984597326=
	$2 \cdot 3 \cdot 49307 \cdot 15590885966106020183 \cdot 83063189494092733119300351841$
97	25108406941546723055343157692645817997961288373601574818286=
	$2 \cdot 3 \cdot 444649 \cdot 1107004113769 \cdot 8501613431704058621006174311112801040301$
101	6427752177035961102167848369366568644401251546953123398915006=
	$2 \cdot 3 \cdot 4243646561167484411070572401 \cdot 252446101263265107819810889340101$
103	102844034832575377634685573909818603313575101884725372017554054=
	$2 \cdot 3 \cdot 4709161 \cdot 39418138729 \cdot 92339645752877062571888142037449143716984561$
107	26328072917139296674479506920917301414787852721508015252463986134=
	$2 \cdot 3 \cdot 6421 \cdot 74994216391141 \cdot 9112496619561893347803980601085579631534736049$
109	421249166674228746791672110734682597034357074384641885294339640926=
	$2 \cdot 3 \cdot 34081415711260123261703 \cdot 2060014027601229583321512687759335041888307$
113	107839786668602559178668060348078516984115385385576512046713859188526=
	$2 \cdot 3 \cdot 227^2 \cdot 1583 \cdot 3824147 \cdot 6778085329 \cdot 2530945889145571847 \cdot 3358695792503140247319023$

orders. Remember that the class number is the same for any curve in an isogeny class. Therefore we need to care only about the corresponding polynomial $P(T)$. In Tables 2, 3, 4, and 5 we state the class numbers in the remaining cases in the range of cryptographic interest.

Note that $T^4 - T^2 + 4$ leads to very good groups for $n = 67$ and 79 and that the magnitude of these groups is in the region of cryptographic interest. The same holds for $T^4 + 2T^3 + 3T^2 + 4T + 4$ and $n = 67$ and for $T^4 - 2T^3 + 3T^2 - 4T + 4$ and $n = 89$.

For binary curves of genus three the classes of nonisogenous curves with irreducible $P(T)$ given in Table 6 are to be considered.

Table 3: Curve with $P(T) = T^4 - T^2 + 4$:

n	$\lvert \mathrm{Pic}^0(C/\mathbf{F}_{2^n}) \rvert$
61	5316911983139663490276776268597429604=
	$2^2 \cdot 1831 \cdot 34039 \cdot 21327224596069892980071644089$
67	21778071482940061661378638344377642396236=
	$2^2 \cdot 5444517870735015415344659586094410599059$
71	557518629963265578538020339431393458213756=
	$2^2 \cdot 26839 \cdot 148249 \cdot 35030092981145246548675945137 4849$
73	892029807941224925661502967455916927797596 04=
	$2^2 \cdot 8761 \cdot 442189471 \cdot 575648394745599178210750272537 1$
79	365375409332725729550922292183917789809461213276=
	$2^2 \cdot 91343852333181432387730573045979447452365303319$
83	9353610478917778676503584576270618766325556756 9676=
	$2^2 \cdot 14922571 \cdot 19492219 \cdot 31262449 \cdot 257152858687943139616882741 9$
89	383123885216472214589586757378244353769997331107203764=
	$2^2 \cdot 2671 \cdot 53497189 \cdot 670307974525390635096804382861885945480039$
97	25108406941546723055343157693015513330857555182110701284884=
	$2^2 \cdot 14551 \cdot 431386278289236531086233896175787116535934904510183171$
101	642775217703596110216784836936273217577637240330921928349600 4=
	$2^2 \cdot 59962489 \cdot 1898267731 \cdot 1204958581789 \cdot 231501457725649 \cdot 50609980118281999$
103	10284403483257537763468557390985020980926688131947211090102207 6=
	$2^2 \cdot 43261 \cdot 420859 \cdot 18751186669 \cdot 579776615513755189 \cdot 129896213174170756724641$
107	263280729171392966744795069209179147446596949787665403746915026 36=
	$2^2 \cdot 973257085699 \cdot 676287727672444629795783995546967793950518106423804 1$
109	421249166674228746791672110734680861516803688819751004740148179364=
	$2^2 \cdot 247885621 \cdot 598722031900039 \cdot 709581833294910782648588418537541414098739$
113	107839786668602559178668060348078528404981769994748067802115022805204=
	$2^2 \cdot 299464210429 \cdot 5149674762391 \cdot 27151900595462829709 \cdot 64386388554080955716385 1$

Table 4: Curve with $P(T) = T^4 + 2T^3 + 3T^2 + 4T + 4$:

n	$\lvert \mathrm{Pic}^0(C/\mathbf{F}_{2^n}) \rvert$
61	5316911977033364753140596481861826078=
	$2 \cdot 7 \cdot 8297 \cdot 84913 \cdot 539058824399606395941223457$
67	21778071483463258786186409694173819439362=
	$2 \cdot 7 \cdot 1555576534533089913299029263869558531383$
71	5575186299519090460509374439525583695134642=
	$2 \cdot 7 \cdot 569 \cdot 67217532937 \cdot 10412056438741229571321406751$
73	89202980794660877710779236197113745019927342=
	$2 \cdot 7 \cdot 5215121 \cdot 38961862367 \cdot 31357919011564553499404479$
79	365375409332684354222911973151271502086185656786=
	$2 \cdot 7 \cdot 765353 \cdot 34099616155895603935412060387379745227383$
83	93536104789160189806805423910911919572829943988546=
	$2 \cdot 7 \cdot 167^2 \cdot 16305189977 \cdot 23564064703 \cdot 114833530663 \cdot 5429670992567$
89	383123885216459517032176679352494921969133201300475502=
	$2 \cdot 7 \cdot 27535906720484993 \cdot 993829332695156643037204399999982801$
97	25108406941546475519266315021658437571181521793461683089038=
	$2 \cdot 7 \cdot 14551 \cdot 1233451320939473 \cdot 99925485729323135043380964652866217079$
101	6427752177035957907451442801389171479467324814535766520314942=
	$2 \cdot 7 \cdot 809 \cdot 173481667802057497 \cdot 3271364813643191699446032816977049688361$
103	102844034832575476719110810648132974252699547665638242275462706=
	$2 \cdot 7 \cdot 1031 \cdot 95791 \cdot 222905317476413119 \cdot 333693133335133257838716121713570521$
107	26328072917139294546040852041778359184739018933207502722451192098=
	$2 \cdot 7 \cdot 522048144436627468578695929 \cdot 3602304992325872016040102691473537183$
109	421249166674228723916622526297781673826606073095629781898923047134=
	$2 \cdot 7 \cdot 23327 \cdot 259285535870782740205972941431 \cdot 4974779536224541687872518393713$
113	107839786668602562144784569926136125127702549672855001914916536331214=
	$2 \cdot 7 \cdot 1583 \cdot 476183 \cdot 10218712550205474310417731984747447186313991554764219834409$

Table 5: Curve with $P(T) = T^4 - 2T^3 + 3T^2 - 4T + 4$:

n	$\lvert \mathrm{Pic}^0(C/\mathbf{F}_{2^n}) \rvert$
61	5316911989245962242818683728633489154=
	$2 \cdot 2432681 \cdot 2620439 \cdot 417032842527230298484303$
67	21778071482416864537446635953410062641118=
	$2 \cdot 1447182983 \cdot 7524297804162635229606840931673$
71	5575186299746221110262294379669429762239406=
	$2 \cdot 569 \cdot 86934124925851727 \cdot 56354270899593227398081$
73	89202980793584107421495344917337461052555634=
	$2 \cdot 439^2 \cdot 9199 \cdot 13288729471 \cdot 1893198935882080472609113$
79	365375409332767104878929811002998582341618884238=
	$2 \cdot 245582903177 \cdot 385470718084279 \cdot 1929833305427033271593$
83	93536104789195383723266271508981636974607166019998=
	$2 \cdot 1993 \cdot 742036103 \cdot 31624010819082508050012911382239813681$
89	383123885216484912146996836504217327230624063025829938=
	$2 \cdot 191561942608242456073498418252108663615312031512914969$
97	25108406941546970591420000365856734391746032187874605051154=
	$2 \cdot 8303783 \cdot 10811233 \cdot 4301079329 \cdot 18213582137 \cdot 33615921137 \cdot 53103128412343$
101	6427752177035964296884253937344652571417716786928117811276258=
	$2 \cdot 607 \cdot 39491718645242373390511 \cdot 134070862451207479415245154349528577$
103	102844034832575278550260337171619924730902372723788419368923438=
	$2 \cdot 1115115916567 \cdot 1194810566153 \cdot 38594910823239289818210723140302070969$
107	26328072917139298802918161800057517858600061794757601863017849022=
	$2 \cdot 857 \cdot 69337 \cdot 167875511 \cdot 49240121127292757087 \cdot 26800120525355732899584237047$
109	421249166674228769666721695171582786991896862126155481447535141442=
	$2 \cdot 2617 \cdot 5233 \cdot 6529319 \cdot 681135151789622559551 \cdot 3458226390504253310223905604769$
113	107839786668602556212551550770021002022143617259636900034540459252178=
	$2 \cdot 457026017248411887857047 \cdot 117979920834558666366991761541414920541129087$

Table 6: Binary curves of genus 3

Equation of C	$P(T)$
$y^2 + x^3y = x^7 + x^6 + x^5 + x$ $y^2 + x^3y = x^7 + x^5 + x$	$T^6 + T^5 + 4T + 8$ $T^6 - T^5 - 4T + 8$
$y^2 + x^3y = x^7 + x^6 + x^3 + x$ $y^2 + x^3y = x^7 + x^3 + x$	$T^6 + T^5 + 2T^4 + 2T^3 + 4T^2 + 4T + 8$ $T^6 - T^5 + 2T^4 - 2T^3 + 4T^2 - 4T + 8$
$y^2 + (x^3 + x^2)y = x^7 + x^6 + x$ $y^2 + (x^3 + x^2)y = x^7 + x^4 + x$	$T^6 - T^4 + 2T^3 - 2T^2 + 8$ $T^6 - T^4 - 2T^3 - 2T^2 + 8$
$y^2 + (x^3 + x^2 + x)y = x^7 + x^6 + x^5 + x$ $y^2 + (x^3 + x^2 + x)y = x^7 + x^6 + x$	$T^6 + T^5 + T^4 + 3T^3 + 2T^2 + 4T + 8$ $T^6 - T^5 + T^4 - 3T^3 + 2T^2 - 4T + 8$
$y^2 + y = x^7 + x^6$ $y^2 + y = x^7 + x^6 + 1$	$T^6 + 2T^5 + 2T^4 + 2T^3 + 4T^2 + 8T + 8$ $T^6 - 2T^5 + 2T^4 - 2T^3 + 4T^2 - 8T + 8$
$y^2 + y = x^7 + x^6 + x^4$ $y^2 + y = x^7 + x^6 + x^5$	$T^6 + 2T^4 + 2T^3 + 4T^2 + 8$ $T^6 + 2T^4 - 2T^3 + 4T^2 + 8$
$y^2 + y = x^7 + x^5 + x^4$ $y^2 + y = x^7$	$T^6 + 2T^3 + 8$ $T^6 - 2T^3 + 8$
$y^2 + y = x^7 + x^5$ $y^2 + y = x^7 + x^5 + 1$	$T^6 + 2T^5 + 4T^4 + 6T^3 + 8T^2 + 8T + 8$ $T^6 - 2T^5 + 4T^4 - 6T^3 + 8T^2 - 8T + 8$
$y^2 + (x^3 + x^2 + 1)y = x^7 + x^5$ $y^2 + (x^3 + x^2 + 1)y = x^7 + x^6 + x^5 + x^4 + 1$	$T^6 + 2T^5 + 2T^4 + T^3 + 4T^2 + 8T + 8$ $T^6 - 2T^5 + 2T^4 - T^3 + 4T^2 - 8T + 8$
$y^2 + (x^3 + x^2 + 1)y = x^7 + x^6 + x^5$ $y^2 + (x^3 + x^2 + 1)y = x^7$	$T^6 + 2T^4 + T^3 + 4T^2 + 8$ $T^6 + 2T^4 - T^3 + 4T^2 + 8$
$y^2 + (x^3 + x^2 + 1)y = x^7 + 1$ $y^2 + (x^3 + x^2 + 1)y = x^7 + x^6 + x^4$	$T^6 + T^3 + 8$ $T^6 - T^3 + 8$
$y^2 + (x^2 + x + 1)y = x^7 + x^4$ $y^2 + (x^2 + x + 1)y = x^7 + x^6 + x^5 + x^4 + 1$	$T^6 + 2T^5 + 3T^4 + 6T^3 + 6T^2 + 8T + 8$ $T^6 - 2T^5 + 3T^4 - 6T^3 + 6T^2 - 8T + 8$

According to the result of Galbraith [10] stated in Section 2 all these varieties are non-supersingular.

For binary curves of genus four there are 79 classes of nonisogenous curves with irreducible $P(T)$ only 6 of which are supersingular.

For all these curves of genus 3 and 4 we computed the class number for suitable extension fields. This means for genus 3 all prime degrees of extension in the range of 37 - 79 and for genus 4 in 29 – 67. Since the complete lists are to large to be included here, we only list some nice examples. By P_k we denote a prime with k *binary* digits.

Curve with $T^6 - T^5 - 4T + 8$, i.e. $g = 3$

$n = 37$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 25961127822503617821704847577705812 \\ &= 2^2 \cdot 6490281955625904455426211189426453 \\ &= 2^2 \cdot P_{109} \end{aligned}$$

$n = 47$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 2787592652971032115720725740533510746226316 \\ &= 2^2 \cdot 696898163242758028930181435133377686556579 \\ &= 2^2 \cdot P_{139} \end{aligned}$$

Curve with $T^6 + 2T^4 - T^3 + 4T^2 + 8$, i. e. $g = 3$
$n = 47$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 2787593652669850012488674859650329426543978 \\ &= 2 \cdot 7 \cdot 199113832333560715177762489975023530467427 \\ &= 2 \cdot 7 \cdot P_{137} \end{aligned}$$

Curve with $T^8 + T^7 - T^5 - 3T^4 - 2T^3 + 8T + 16$, i. e. $g = 4$
$n = 47$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 392319027687823966090793648631943976925199118618548227940 \\ &= 2^2 \cdot 5 \cdot 19615951384391198304539682431597198846259955930927411397 \\ &= 2^2 \cdot 5 \cdot P_{183} \end{aligned}$$

5.2 Curves over $\mathbf{F}_3$

For larger fields the number of curves to consider increases considerably. Therefore in this and the following subsections we only give some statistics on how many curves were found and provide some examples of curves suitable for cryptographic applications.

For genus 2 we found 22 nonisogenous classes of Koblitz curves with irreducible polynomial P, none of which is supersingular. In the genus 3 case there exist 145 classes containing no supersingular ones and there are 1068 classes of ternary curves of genus 4.
For all these curves we computed the class number in the range of cryptographic interest. In detail: for genus 2 we computed the group order for prime degrees of extension in 53 – 89, for genus 3 in 41 – 79 and for genus 4 in 31 – 67.

Some curves with almost prime $|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})|$:

Curve with $T^4 - 2T^3 + 2T^2 - 6T + 9$, i. e. $g = 2$
$n = 59$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 199667811101604967778690445389889887784425007041531467156 \\ &= 2^2 \cdot 49916952775401241944672611347472471946106251760382866789 \\ &= 2^2 \cdot P_{185} \end{aligned}$$

$n = 61$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 1617309269922994461435237637977909933697312681359090533204 \\ &= 2^2 \cdot 404327317480748615358809409494477483424328170339772633301 \\ &= 2^2 \cdot P_{191} \end{aligned}$$

$n = 67$,

$$\begin{aligned} &|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| \\ =\ & 859504455717142688366155125738799233830844745562404941035458 2196 \\ =\ & 2^2 \cdot 214876113929285672091538781434699808457711186390601235258864 5549 \\ =\ & 2^2 \cdot P_{210} \end{aligned}$$

Curve with $T^4 + T^3 + 5T^2 + 3T + 9$, i. e. $g = 2$
$n = 53$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 37571021261375006591159582348161439581978496614328 9 \\ &= 19 \cdot 1977422171651316136376820123587444188525184032333 1 \\ &= 19 \cdot P_{163} \end{aligned}$$

$n = 61$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 161730926992298825624868176782747046046939968744162240592 11 \\ &= 19 \cdot 85121540522262539802562198306708971603652615128506442416 9 \\ &= 19 \cdot P_{189} \end{aligned}$$

$n = 71$,

$$\begin{aligned} &|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| \\ =\ & 5639208733960173356449405291761786190428164015993197262259813732535 1 \\ =\ & 19 \cdot 296800459682114387181547646934830852127798106104905119066305985922 9 \\ =\ & 19 \cdot P_{220} \end{aligned}$$

Curve with $T^6 + T^5 + 5T^4 + 4T^3 + 15T^2 + 9T + 27$, i. e. $g = 3$
$n = 59$,

$$\begin{aligned} &|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| \\ =\ & 282138326095801751574884741760663210281935290729521975461021105070306125789369276016 2 \\ =\ & 2 \cdot 31 \cdot 455061816283551212217556035097843887551508533434712863646808233984364719015111735 51 \\ =\ & 2 \cdot 31 \cdot P_{274} \end{aligned}$$

Table 7: Numbers of nonisogenous classes of curves over $\mathbf{F}_4$ with irreducible $P(T)$

genus	number of classes	number of supersingular
2	25	4
3	240	0

Curve with $T^8 + 2T^7 + 2T^6 + 2T^5 + 8T^4 + 6T^3 + 18T^2 + 54T + 81$, i. e. $g = 4$
$n = 31$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 1455578222014158379694154241066021864378102882645003903734 54 \\ &= 2 \cdot 3 \cdot 29 \cdot 836539208054114011318479448888518312860978668186783\ 852721 \\ &= 2 \cdot 3 \cdot 29 \cdot P_{189} \end{aligned}$$

$n = 61$,

$$\begin{aligned} &|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| \\ = \quad &26156892745788177517252648760787890444759858866430831971120986438850449956797347409 2235288 \hookleftarrow \\ &\quad 11990323081262428727 1271574 \\ = \quad &2 \cdot 3 \cdot 29 \cdot 150326969803380330558923268740160289912412981990981792937476933556611781360904295 \hookleftarrow \\ &\quad 4553076368505190981681748777421101 \\ = \quad &2 \cdot 3 \cdot 29 \cdot P_{379} \end{aligned}$$

5.3 Curves over $\mathbf{F}_4$

Curves over $\mathbf{F}_4$ allow to work in extensions of binary fields. This is advantageous in hardware implementations. Compared to the $\mathbf{F}_2$ case there are more curves to choose from. Although there is a small drawback since the number of precomputations needed to obtain the speed-up considered in the next sections grows with the field size. Furthermore one needs to be aware of Weil descent attacks since now the field has composite degree of extension over $\mathbf{F}_2$. The following numbers of classes listed in Table 7 contain the classes of curves that are already obtained for $\mathbf{F}_2$, since every curve over $\mathbf{F}_2$ can be considered over $\mathbf{F}_4$.

For these classes we computed the class number. For genus 2 we chose all prime extensions in 29 – 59 and for genus 3 in 19 – 41. We did not carry out the computation for genus 4 since then the degrees of extension get even smaller – thus the computational advantages investigated in the following sections decrease – whereas the number of defining polynomials for the curves grows such that a brute force search trough all possible curves is rather time-consuming.

Some examples:
Curve with $T^4 - T^3 - 4T + 16$, i. e. $g = 2$

$n = 29$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 83076749829698992958942621500367388 \\ &= 2^2 \cdot 3 \cdot 6923062485808249413245218458363949 \\ &= 2^2 \cdot 3 \cdot P_{112} \end{aligned}$$

$n = 41$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 23384026197316960486422682358066130544236740957388 \\ &= 2^2 \cdot 3 \cdot 1948668849776413373868556863172177545353061746449 \\ &= 2^2 \cdot 3 \cdot P_{160} \end{aligned}$$

Curve with $T^4 + 2T^3 + 7T^2 + 8T + 16$, i. e. $g = 2$
$n = 59$,

$$\begin{aligned} & |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| \\ = \; & 110427941548649020343281285131795129969498221066698138419282824292856654 \\ = \; & 2 \cdot 17 \cdot 3247880633783794715978861327405739116749947678432298188802436008613431 \\ = \; & 2 \cdot 17 \cdot P_{230} \end{aligned}$$

Curve with $T^6 - T^5 + 5T^4 - 9T^3 + 20T^2 - 16T + 64$, i. e. $g = 3$
$n = 19$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 20769148196260031952815209804964032 \\ &= 2^6 \cdot 324517940566562999262737653202563 \\ &= 2^6 \cdot P_{107} \end{aligned}$$

$n = 23$

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 348449083479439714971877756379159944059328 \\ &= 2^6 \cdot 5444516929366245546435589943424374125927 \\ &= 2^6 \cdot P_{131} \end{aligned}$$

5.4 Curves over $\mathbf{F}_5$

As the field size grows the degree of the extension needed to obtain a class number of order $\sim 2^{160}$ decreases. Thus these fields allow us to work with smaller extension. Furthermore we obtain a larger variety of curves to choose from. But, as was said in the preceding section the number of precomputations – thus storage – grows also. Therefore the choice of a curve over $\mathbf{F}_5$ is only reasonable if these storage requirements are fulfilled. Furthermore the Theorem of Hasse-Weil 2.29 provides a lower bound on class number in the ground field, thus on the unused factor of the group size for the extension. This factor grows with g and q.

Over $\mathbf{F}_5$ there are 54 classes curves of genus 2 with irreducible polynomial P, none of which is supersingular. For genus 3 we even have 916 classes.
We have complete lists of the class numbers for all these classes in the relevant cases. For genus 2 we considered extensions of degree 29 – 43 and for genus 3 in 19 – 29. Like in the case of $\mathbf{F}_4$ we did not carry out the computation for genus 4.

Some nice examples:
Curve with $T^4 - 4T^3 + 12T^2 - 20T + 25$, i. e. $g = 2$
$n = 29$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 346944695223936320772129919992816854582 54 \\ &= 2 \cdot 7 \cdot 24781763944566880055152137142344061041 61 \\ &= 2 \cdot 7 \cdot P_{130} \end{aligned}$$

Curve with $T^4 - 3T^3 + 11T^2 - 15T + 25$, i. e. $g = 2$
$n = 31$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 216840434503348815900504814563209901242733 79 \\ &= 19 \cdot 1141265444754467452107920076648473164435441 \\ &= 19 \cdot P_{139} \end{aligned}$$

$n = 37$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 529395592034053700415956075316733460588981404011751 9 \\ &= 19 \cdot 27862925896529142127155582911407024241525337053250 1 \\ &= 19 \cdot P_{167} \end{aligned}$$

Curve with $T^6 + 5T^5 + 21T^4 + 51T^3 + 105T^2 + 125T + 125$, i. e. $g = 3$
$n = 19$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 6938889266073094641872874355228772937541 \\ &= 433 \cdot 16025148420492135431577077032860907477 \\ &= 433 \cdot P_{123} \end{aligned}$$

Curve with $T^6 - 2T^5 + 3T^4 - 8T^3 + 15T^2 - 50T + 125$, i. e. $g = 3$
$n = 23$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 1694065906185866506125847996570349388706047353412 \\ &= 2^2 \cdot 3 \cdot 7 \cdot 20167451264117458406260095197266064151262468493 \\ &= 2^2 \cdot 3 \cdot 7 \cdot P_{153} \end{aligned}$$

$n = 29$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 646234853600828989489680863502730439526283429214521063618232 4 \\ &= 2^2 \cdot 3 \cdot 7 \cdot 76932720666765355891628674226515528515033741573157269478361 \\ &= 2^2 \cdot 3 \cdot 7 \cdot P_{195} \end{aligned}$$

6 Standard ways of computing m-folds

We describe the standard algorithms to compute m times a group element D. The usual approach is the binary double-and-add method. It uses the binary expansion of the integer m. First we present the algorithm and then we provide some bounds on the density of these expansions. This method will serve as a base to compare our new results with. Thus by a speed-up by a factor of 7 we mean that the new algorithm is 7 times faster then the binary double-and-add method.

The algorithm is best described using an example: Instead of computing $11D$ by $11D = \underbrace{D + \cdots + D}_{11 \text{ times}}$ we use $11 = 2^3 + 2^1 + 2^0$ to obtain it by

$$11D = 2(2(2D) + D) + D,$$

thus requiring 2 generic additions and 3 doublings instead of 9 additions and one doubling.
This can be formalized in the following way:

Algorithm 6.1
INPUT: D, $m = \sum_{i=0}^{l-1} b_i 2^i$.
OUTPUT: $H = mD$.

1. *Initialize* $H := D$;
2. *For* $i = l - 2$ *to* 0 *do*
   (a) $H := 2H$;
   (b) *if* $(b_i = 1)$ $H := H + D$;
3. *output(H).*

To estimate the complexity of this algorithm we need bounds on the length and density of the binary expansion of m. If the expansion of m has length l the algorithm needs l doublings. $l - 1$ is the largest power of 2 occurring in the expansion of m, thus $l = \lfloor \log_2(m) \rfloor + 1$. For every coefficient 1 occurring in the binary expansion of m an addition occurs. The probability of a nonzero coefficient is $1/2$ as there are two possible coefficients. Since the complexity of an addition is approximately equal to that of a doubling we get an asymptotic complexity of

$$\sim (1 + \frac{1}{2}) \log_2(m).$$

The groups we consider are finite. Thus it is useless to take m larger then the group order. We therefore have $m \leq |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| \sim q^{gn}$ by the Hasse-Weil Bound 2.29. Thus to compute a multiple of a divisor class we need on average

$$\sim \frac{3}{2}\, g\, n\, \log_2(q)$$

group operations.

7 Representing Integers to the Base of τ

In this section we provide the basic tools for an efficient method of computing m-folds of divisor classes. Like in the double-and-add method we first expand the integer m to a given basis using a fixed set of coefficients. We also use the fact, that the negative of a divisor class can be computed with almost no effort (see Section 2).

The most important ingredient used in this chapter is the Frobenius endomorphism σ of the curve. As we stated in Section 2 we have that if a divisor class D is represented via a reduced ideal $(\sum_{i=0}^{g} a_i x^i, y - \sum_{i=0}^{g-1} b_i x^i)$, then $\sigma(D)$ is represented by $(\sum_{i=0}^{g} a_i^q x^i, y - \sum_{i=0}^{g-1} b_i^q x^i)$. Furthermore this ideal is reduced as well. Thus provided that $\mathbf{F}_{q^n}$ is represented with respect to a normal basis, $\sigma(D)$ is computed by at most $2g$ cyclic shiftings of the coefficients the costs of which can be neglected. Thus this endomorphism can be used efficiently – if we know how to use it in the arithmetic. We return to the choice of the ground field $\mathbf{F}_{q^n}$ in Section 15. Here we assume that the q-th power is easy to compute.
We have seen that the polynomial P introduced via the zeta-function of C is the characteristic polynomial of the Frobenius endomorphism of $\mathrm{Pic}^0(C/\bar{\mathbf{F}}_q)$. We now investigate how to use it. Remember that by the results of Section 3 for *Koblitz curves* we easily get $P(T)$.

Consider the hyperelliptic curve C with characteristic polynomial of the Frobenius endomorphism σ

$$P(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + a_{g-1} q T^{g-1} + \cdots + a_1 q^{g-1} T + q^g.$$

Since $P(\sigma) = 0$ we have for all divisor classes of $\mathrm{Pic}^0(C/\bar{\mathbf{F}}_q)$

$$\begin{aligned} q^g D &= -\sigma^{2g}(D) - a_1\sigma^{2g-1}(D) - \cdots - a_g\sigma^g(D) - \cdots - a_1 q^{g-1}\sigma(D) \\ &= -\sigma(\cdots\sigma(\sigma(\sigma(D) + a_1 D) + a_2 D) + \cdots + a_1 q^{g-1} D). \end{aligned}$$

This gives a first example where an m-fold is represented via a linear combination of $\sigma^j(D)$. The computation of a reduced representative of $\sigma(D)$ takes only cyclic shiftings the costs of which are negligible, provided that the coefficients of the

polynomials representing D are given with respect to a normal basis. (Even if they are not, this expansion leads to a speed-up since computing the respective powers of the coefficients is relatively fast compared to the operations with the divisor classes.)
Now we make use of this not only for multiples of q^g but also for arbitrary integers. Furthermore we provide a set of coefficients R such that for every integer m we can express mD as a sum of the above kind using only these coefficients.

Example 7.1 *Let the hyperelliptic curve of genus 2 be given by the polynomial $y^2+(x^2+x)y = x^5+x^4+x$. The characteristic polynomial of the Frobenius endomorphism is $P(T) = T^4 - T^2 + 4$. Using the set $R = \{0, \pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7\}$ one obtains the following expansion*

$$23D = 7D - 7\sigma^4(D) - \sigma^8(D).$$

Let τ be a complex root of $P(T)$. Since both τ and σ are roots of P, representing mD as a linear combination of the $\sigma^i(D)$ becomes equivalent to expanding m to the base of τ. The elements of $\mathbf{Z}[\tau]$ are of the form $c = c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}$ with $c_i \in \mathbf{Z}$.
To get an expansion of an integer m as $m = \sum_{i=0}^{l-1} u_i\tau^i$ using the restricted set of coefficients $u_i \in R$ we first need a criterion for an element to be divisible by τ.

Lemma 7.2 *$c = c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}$ is divisible by τ if and only if $q^g|c_0$.*

Proof. Let $q^g|c_0 \Leftrightarrow \exists \tilde{c_0} \in \mathbf{Z}$ such that $c = q^g\tilde{c_0} + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}$
$\Leftrightarrow c = (-\tau^{2g} - a_1\tau^{2g-1} - \cdots - a_g\tau^g - \cdots - a_1q^{g-1}\tau)\tilde{c_0} + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}$
$\Leftrightarrow c = \tau\left((c_1 - a_1q^{g-1}\tilde{c_0}) + \cdots + (c_g - a_g\tilde{c_0})\tau^{g-1} + \cdots + (c_{2g-1} - a_1\tilde{c_0})\tau^{2g-2} - \tilde{c_0}\tau^{2g-1}\right)$
$\Leftrightarrow \tau|c.$ □

Therefore the minimal set of coefficients R consists of a complete set of representatives of $\mathbf{Z}/q^g\mathbf{Z}$. Since taking the negative of a divisor class is essentially for free (to $-D$ corresponds $[a, h-b]$) we will use $R = \{0, \pm 1, \pm 2, \ldots, \pm\lceil\frac{q^g-1}{2}\rceil\}$ if just a representation is needed. Note that we would not need to include $-q^g/2$ in the case of even characteristic. But since we get it for free we will make use of it. Furthermore in the remainder of the text we shall impose conditions to achieve a sparse representation and therefore we will use different choices of the set of coefficients R depending on the structure of $P(T)$.
Now we state the algorithm for expanding an element of $\mathbf{Z}[\tau]$ to the base of τ. Note that at the moment we would only need to represent integers, but in the further sections we will reduce the length of the representation. Thereby we stumble over this more general problem.

Algorithm 7.1
`INPUT:` $c = c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}$, $P(T)$, *the set* R.
`OUTPUT:` $u_0, \ldots, u_{l-1}$ *with* $c = \sum_{i=0}^{l-1} u_i\tau^i$, $u_i \in R$.

1. *Put* $i := 0$;

2. *While for any* $0 \leq j \leq 2g-1$ *there exists an* $c_j \neq 0$ *do*
   if $q^g | c_0$ *choose* $u_i := 0$;
   else choose $u_i \in R$ *with* $q^g | c_0 - u_i$;
   /**in even characteristic choose* $u_i = c_0$ *if* $|c_0| = q^g/2$/*
   $d := (c_0 - u_i)/q^g$;
   for $0 \leq j \leq g-1$ *do*
   $c_j := c_{j+1} - a_{j+1} q^{g-j-1} d$;
   for $0 \leq j \leq g-2$ *do*
   $c_{g+j} := c_{g+j+1} - a_{g-j-1} d$;
   $c_{2g-1} := -d$;
   $i := i+1$;

3. *output* $(u_0, \ldots, u_{i-1})$.

The choice of $u \in R$ might also depend on further conditions to obtain a sparse representation of m.

8 On the Finiteness of the Representation

We now consider the finiteness of the τ-adic representations and establish the dependence of the length on an expression involving m in case of a finite representation. We show that for any curve the expansions are either finite or periodic and provide a means to find out what happens for a given individual curve.

To investigate the finiteness we now consider a $2g$ dimensional lattice associated to the elements of $\mathbf{Z}[\tau]$.
Consider the set of elements

$$\Lambda := \left\{ \left(\sum_{j=0}^{2g-1} c_j \tau_1^j, \ldots, \sum_{j=0}^{2g-1} c_j \tau_g^j \right) | c_j \in \mathbf{Z} \right\}.$$

These elements form a lattice in $\mathbf{C}^g$, since the sum of any two and integer multiples of the vectors are in Λ. Since the polynomial P is irreducible the lattice has full dimension $2g$. We now investigate the norm[1] of vectors in this lattice, where the norm is given by the usual Euclidean norm of $\mathbf{C}^g$

$$\mathcal{N} : (x_1, \ldots, x_g) \mapsto \sqrt{|x_1|^2 + \cdots + |x_g|^2},$$

[1]There are two notions of length – the length of the τ-adic expansion and the norm of the vector, which is often referred to as (Euclidean-)length in the literature. We hope not to confuse the reader and use norm in the second case.

where $|\ .\ |$ is the complex absolute value. We can also consider this lattice as a $2g$ dimensional lattice over $\mathbf{R}$ by the usual representation of $\mathbf{C}$ as $\mathbf{R}^2$.
By abuse of notation we write $\mathcal{N}(c)$ for $c = c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}$ and speak of the norm of c since these vectors are parameterized by the integers $c_0, \ldots, c_{2g-1}$. Thus then $\mathcal{N}(c)$ reads

$$\mathcal{N}(c) = \sqrt{\sum_{i=1}^{g} \left| \sum_{j=0}^{2g-1} c_j \tau_i^j \right|^2}.$$

Now we study the behaviour of the norm of the remainders during the expansion of c. Showing that the norm decreases down to a certain limit will be the important step to get the following

Theorem 8.1 *Let C be a hyperelliptic curve of genus g and let τ be a root of the characteristic polynomial of the Frobenius endomorphism. Then the expansion of $c = c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1} \in \mathbf{Z}[\tau]$ to the base of τ with coefficients in R is either finite or gets periodic.*

Proof. We first show that for elements of bounded norm the expansion cannot lead to a remainder with larger norm than that bound. Showing that the expansion of any element leads to a remainder of norm bounded by that constant concludes the proof.
Let $\mathcal{N}(c) < \frac{\sqrt{g}}{2}\frac{q^g}{\sqrt{q}-1}$ (respectively $< \frac{\sqrt{g}}{2}\frac{q^g+1}{\sqrt{q}-1}$ for even characteristic). Then using the Triangle inequality on $c = u + c - u =: u + c'\tau,\ u \in R$ we get $\mathcal{N}(c'\tau) \leq \mathcal{N}(c) + \mathcal{N}(u) \leq \mathcal{N}(c) + \sqrt{g}(q^g - 1)/2$ (respectively $\mathcal{N}(c) + \sqrt{g}q^g/2$) and $\mathcal{N}(\tau c') = \sqrt{q}\mathcal{N}(c')$. Now direct calculation shows that $\mathcal{N}(c')$ is bounded by the same constant.
Since we consider a lattice the number of elements with bounded norm is finite. Thus the expansion of these elements of bounded norm either ends after hitting at most one time all these elements or runs into a cycle since the choice of the u – and therefore the next remainder c' – is unique for given c. Hence, for these elements the expansion is either periodic or finite.
The following two lemmata show that expanding an element c to the base of τ leads to a remainder c' with $\mathcal{N}(c') < \frac{\sqrt{g}}{2}\frac{q^g}{\sqrt{q}-1}$ (or $< \frac{\sqrt{g}}{2}\frac{q^g+1}{\sqrt{q}-1}$ in even characteristic) after at most $2\log_q \frac{2(\sqrt{q}-1)\mathcal{N}(m)}{\sqrt{g}} + 1$ steps concluding the proof. □

Later we shall state an algorithm to find these elements of small norm and show how to recognize periods and how to deal with them. Hence the problem is solved in practice.

Lemma 8.2 *Let q be odd. For every $m \in \mathbf{Z}[\tau]$ we have an unique expansion*

$$m = \sum_{i=0}^{k-1} u_i\tau^i + m'\tau^k,$$

where $u_i \in \{0, \pm 1, \pm 2, \ldots, \pm \frac{q^g-1}{2}\}$,

$$\mathcal{N}(m') < \frac{\sqrt{g}}{2} \frac{q^g}{\sqrt{q}-1},$$

and

$$k \leq \lceil 2 \log_q \frac{2(\sqrt{q}-1)\mathcal{N}(m)}{\sqrt{g}} \rceil + 1.$$

Proof. Put $m_0 := m$. The expansion of m to the base of τ leads to

$$\begin{aligned} m_0 &= m_1\tau + u_0 = m_2\tau^2 + u_1\tau + u_0 \\ &= \sum_{i=0}^{j-1} u_i\tau^i + m_j\tau^j, \end{aligned}$$

where by Lemma 7.2 the $u_i \in \{0, \pm 1, \pm 2, \ldots, \pm \frac{q^g-1}{2}\}$ are uniquely determined. The Triangle inequality for $\mathcal{N}$ leads to $\sqrt{q}\mathcal{N}(m_j) \leq \mathcal{N}(m_{j-1}) + \mathcal{N}(u_{j-1}) \leq \mathcal{N}(m_{j-1}) + \sqrt{g}\frac{q^g-1}{2}$. Hence,

$$\begin{aligned} \mathcal{N}(m_j) &\leq \frac{\mathcal{N}(m_0) + \sqrt{g}(q^g-1)/2 \sum_{i=0}^{j-1} q^{i/2}}{q^{j/2}} \\ &< \frac{\mathcal{N}(m_0)}{q^{j/2}} + \frac{\sqrt{g}}{2} \frac{q^g-1}{\sqrt{q}-1}. \end{aligned}$$

If we choose $j \geq 2 \log_q \frac{2(\sqrt{q}-1)\mathcal{N}(m_0)}{\sqrt{g}}$, then $\frac{\mathcal{N}(m_0)}{q^{j/2}} \leq \frac{\sqrt{g}}{2(\sqrt{q}-1)}$ and the claim follows. □

For even characteristic we proceed similarly.

Lemma 8.3 *Let q be even. For every $m \in \mathbf{Z}[\tau]$ we have an expansion*

$$m = \sum_{i=0}^{k-1} u_i\tau^i + m'\tau^k,$$

where $u_i \in \{0, \pm 1, \pm 2, \ldots, \pm \frac{q^g}{2}\}$,

$$\mathcal{N}(m') < \frac{\sqrt{g}}{2} \frac{q^g+1}{\sqrt{q}-1},$$

and

$$k \leq \lceil 2 \log_q \frac{2(\sqrt{q}-1)\mathcal{N}(m)}{\sqrt{g}} \rceil + 1.$$

Proof. Put $m_0 := m$. The expansion of m to the base of τ leads to

$$\begin{aligned} m_0 &= m_1\tau + u_0 = m_2\tau^2 + u_1\tau + u_0 \\ &= \sum_{i=0}^{j-1} u_i\tau^i + m_j\tau^j, \end{aligned}$$

where the $u_i \in \{0, \pm 1, \pm 2, \ldots, \pm\frac{q^g}{2}\}$ are given like in Algorithm 7.1.
The Triangle inequality for $\mathcal{N}$ leads to $\sqrt{q}\mathcal{N}(m_j) \leq \mathcal{N}(m_{j-1}) + \mathcal{N}(u_{j-1}) \leq \mathcal{N}(m_{j-1}) + \sqrt{g}\frac{q^g}{2}$. Hence,

$$\begin{aligned} \mathcal{N}(m_j) &\leq \frac{\mathcal{N}(m_0) + \sqrt{g}q^g/2\sum_{i=0}^{j-1} q^{i/2}}{q^{j/2}} \\ &< \frac{\mathcal{N}(m_0)}{q^{j/2}} + \frac{\sqrt{g}}{2}\frac{q^g}{\sqrt{q}-1}. \end{aligned}$$

If we choose $j \geq 2\log_q \frac{2(\sqrt{q}-1)\mathcal{N}(m_0)}{\sqrt{g}}$ then $\frac{\mathcal{N}(m_0)}{q^{j/2}} \leq \frac{\sqrt{g}}{2(\sqrt{q}-1)}$ and the claim follows. □

We now investigate the norm $\mathcal{N}$ in more detail. Thus we state it explicitly in the coefficients of the polynomial $P(T)$ and express it in terms of the coefficients $c_0, \ldots, c_{2g-1}$. This can be done using the symmetric functions in the τ_i and with the help of the formulae derived in Section 4. Since $\mathcal{N}$ is the Euclidean norm its square leads to a positive definite quadratic form.
Before we do so let us see how the proof works for elliptic curves.

Example 8.4 *For curves of genus 1, i. e. elliptic curves, the finiteness was proved by Müller [36] for even characteristic and using the same idea by Smart [51] for odd characteristic. For $g = 1$ the norm simply reads $\mathcal{N}(c)^2 = c_0^2 - a_1c_0c_1 + qc_1^2$. The lattice defined above coincides then with the lattice spanned by 1 and τ. We present here the case of odd characteristic only. Hence the set of coefficients is $R = \{0, \pm 1, \ldots, \pm(q-1)/2\}$. After showing that the square of the norm decreases down to $(\sqrt{q}+2)^2/4$ giving a special case of Lemma 8.2 they rearrange*

$$\begin{aligned} \mathcal{N}(c)^2 &= c_0^2 - a_1c_0c_1 + qc_1^2 \\ &= \left(c_0 - \frac{a_1c_1}{2}\right)^2 + \frac{1}{4}(4q - a_1^2)c_1^2 \\ &= \left(\sqrt{q}c_1 - \frac{a_1c_0}{2\sqrt{q}}\right)^2 + \left(1 - \frac{a_1^2}{4q}\right)c_0^2 \end{aligned}$$

by completing the square. Since the curve is assumed to be non-supersingular, $|a_1| \leq 2\sqrt{q} - 1$, hence $4q - a_1^2 \geq 3$ and they get

$$|c_1| \leq \frac{\sqrt{q}+2}{\sqrt{3}}$$

and

$$|c_0| \leq \frac{q+2\sqrt{q}}{\sqrt{3}}.$$

Hence in any case $|c_1| \leq (q-1)/2$, *thus* c_1 *is in the set of remainders. But the best we can get for* $|c_0|$ *is* $|c_0| \leq (q-1)/2+q$. *Assuming* $c_0 > (q-1)/2$ *(the case of* $c_0 < -(q-1)/2$ *can be treated similarly) one can further expand to get*

$$c_0 + c_1\tau = (c_0 - q) + (c_1 - a_1)\tau - \tau^2.$$

Then $|c_1 - a_1| \leq \frac{\sqrt{q}+2}{\sqrt{3}} + 2\sqrt{q} < \frac{q-1}{2} + q$. *If again* $c_1 - a_1 > (q-1)/2$ *(again the other case follows the same lines) then*

$$c_0 + c_1\tau = (c_0 - q) + (c_1 - a_1)\tau - \tau^2 = (c_0 - q) + (c_1 - a_1 - q)\tau + (-a_1 - 1)\tau^2 - \tau^3.$$

Considering each occurrence of $|-a_1 - 1| > (q-1)/2$ *one finds that one needs to add the coefficients* $\pm(q+1)/2$ *in case of the pairs* (q, a_1) *equal to* $(5, \pm 4)$ *and* $(7, \pm 5)$.

Before we proceed we show what $\mathcal{N}(c)^2$ looks like after expanding the product for the cases of small genus.

Example 8.5 *For* $g = 2$ *we have for* $c = c_0 + c_1\tau + c_2\tau^2 + c_3\tau^3$

$$\begin{aligned}
\mathcal{N}(c)^2 &= 2c_0^2 - a_1c_0c_1 + (a_1^2 - 2a_2)c_0c_2 - (a_1^3 - 3(a_1a_2 - a_1q))c_0c_3 \\
&+ 2qc_1^2 - a_1qc_1c_2 + (a_1^2 - 2a_2)qc_1c_3 \\
&+ 2q^2c_2^2 - a_1q^2c_2c_3 \\
&+ 2q^3c_3^2.
\end{aligned}$$

For $g = 3$ *we have for* $c = c_0 + c_1\tau + c_2\tau^2 + c_3\tau^3 + c_4\tau^4 + c_5\tau^5$

$$\begin{aligned}
\mathcal{N}(c)^2 &= 3c_0^2 - a_1c_0c_1 + (a_1^2 - 2a_2)c_0c_2 - (a_1^3 - 3(a_1a_2 - a_3))c_0c_3 \\
&\quad +(a_1^4 - 4(a_1^2a_2 - a_1a_3 + a_2q) + 2a_2^2)c_0c_4 \\
&\quad -(a_1^5 - 5(a_1^3a_2 - a_1^2a_3 - a_1a_2^2 + a_1a_2q + a_2a_3 - a_1q))c_0c_5 \\
&+ 3qc_1^2 - a_1qc_1c_2 + (a_1^2 - 2a_2)qc_1c_3 - (a_1^3 - 3(a_1a_2 - a_3))qc_1c_4 \\
&\quad +(a_1^4 - 4(a_1^2a_2 - a_1a_3 + a_2q) + 2a_2^2)qc_1c_5 \\
&+ 3q^2c_2^2 - a_1q^2c_2c_3 + (a_1^2 - 2a_2)q^2c_2c_4 - (a_1^3 - 3(a_1a_2 - a_3))q^2c_2c_5 \\
&+ 3q^3c_3^2 - a_1q^3c_3c_4 + (a_1^2 - 2a_2)q^3c_3c_5 \\
&+ 3q^4c_4^2 - a_1q^4c_4c_5 \\
&+ 3q^5c_5^2.
\end{aligned}$$

In general $\mathcal{N}(c)^2$ is a quadratic form in the $2g$ variables $c_0, \ldots, c_{2g-1}$. The coefficient of c_i^2 is gq^i and of $c_ic_j, i < j$ is $q^i(q^\nu + 1 - M_\nu)$, where $\nu = j - i$ and M_ν is the number of points on the curve over $\mathbf{F}_{q^\nu}$ like in Section 2. Due to its origin in the interpretation as Euclidean norm in a lattice, $\mathcal{N}^2$ is a positive definite quadratic form.

Finke and Pohst [7] provide the following algorithm for finding all vectors in a lattice in $\mathbf{R}^s$ of bounded norm, respectively for finding all arrays $(x_0, \dots, x_{s-1})$ for which the value of the corresponding quadratic form with s variables is less than a constant. Let the quadratic form be given by $\sum_{i,j=0}^{s-1} a_{ij}x_ix_j,\ a_{ij} = a_{ji}$, and put K the bound on the norm.

Algorithm 8.1 (Finke, Pohst)
`INPUT:` *quadratic form, bound K.*
`OUTPUT:` *all arrays $(x_0, \dots, x_{s-1})$ leading to values less than K.*

1. */* Set up*/*
   for $0 \le i \le j \le s-1$ *do*
   $q_{ij} := a_{ij};$

2. *for* $0 \le i \le s-2$ *do*
   for $i+1 \le j \le s-1$ *do*
   $q_{ji} := q_{ij};$
   $q_{ij} := \frac{q_{ij}}{q_{ii}};$
   for $i+1 \le k \le s-1$ *do*
   for $k \le k \le s-1$ *do*
   $q_{kl} := q_{kl} - q_{ki}q_{il};$

3. *put* $i := s-1;\ T_i := K;\ U_i := 0;$

4. */*start of iteration*/*
   put $Z := (T_i/q_{ii})^{1/2};\ UB_i := \lfloor Z - U_i \rfloor;\ x_i := \lceil -Z - U_i \rceil - 1;$

5. *put* $x_i := x_i + 1;$
   if $x_i \le UB_i$ *goto step 7;*
   else goto step 6;

6. *put i:=i+1;*

7. *if* $i = 0$ *goto step 8;*
   else $i := i-1;$
   $U_i := \sum_{j=i+1}^{s-1} q_{ij}x_j;$
   $T_i := T_{i+1} - q_{(i+1)(i+1)}(x_{i+1} + U_{i+1})^2;$
   goto step 4;

8. */*solution found*/*
   if $x = (0, \dots, 0)$ *terminate;*
   else output $\pm(x_0, \dots, x_{s-1});$
   goto step 5.

They also proved the following upper bound on the number of elements of norm bounded by K:

$$(2\lfloor K^{1/2}\rfloor + 1)\binom{\lfloor 4K\rfloor + s - 1}{\lfloor 4K\rfloor}.$$

Thus for our constant K we have at most $O\left((\sqrt{g}\frac{q^g}{\sqrt{q}-1})^{(4g-1)/2}\right)$ vectors of small norm. This bounds the length of the expansion in the non-periodic case.We used the algorithm to find the elements of small norm for individual curves. For each of them we computed the expansion. These experiments show that for each such element $c = c_0 + \cdots + c_{2g-1}\tau^{2g-1}$ of small norm we have $c_i \in R$ for $1 \le g \le 2g-1$ and $|c_0| \le q^g$, and if $c_0 \notin R$ the other coefficients are fairly small. If no periods occur then every such element has an expansion of length at most $2g+1$, thus either all $c_i \in R$ or the next remainder in the expansion has all coefficients in this set.
Therefore if $P(T)$ is such that we do not have periods the length of the expansion of m is bounded by $\lceil 2\log_q \frac{2(\sqrt{q}-1)\mathcal{N}(m)}{\sqrt{g}}\rceil + 2g + 2$.

Now we try to get estimates supporting the experimental results on $|c_i|$. However we do not succeed in a proof since the expressions get too involved and the known bounds on the coefficients of $P(T)$ are too weak. But we provide a detailed example for the genus two case.
The proof would proceed as follows: Like in the algorithm we first compute the coefficients b_{ij} satisfying

$$\mathcal{N}(c)^2 = \sum_{i=0}^{2g-1} b_{ii}\left(c_i + \sum_{j=i+1}^{2g-1} b_{ij}c_j\right)^2$$

for the quadratic form $\mathcal{N}(c)^2$. Then starting from the index $2g-1$ we obtain an upper bound on the coefficient c_{2g-1} and as well on the other c_i's depending on the value chosen for the preceding c_j's, $i < j \le 2g-1$.
For a fixed positive definite quadratic form of arbitrary degree this is the idea behind the above algorithm given in Finke and Pohst [7]. Thus for each individual curve this can be carried out efficiently. But using the variables $a_1, \ldots, a_g$ the expressions get rather involved.
In the following long example we restrict ourselves to curves of genus 2.

Example 8.6 *In the genus 2 case we have*

$$\begin{aligned}\mathcal{N}^2(c) &= 2\left(c_0 - \frac{1}{4}a_1c_1 + \frac{a_1^2 - 2a_2}{4}c_2 + \frac{-a_1^3 + 3a_1a_2 - 3a_1q}{4}c_3\right)^2 \\ &\quad + \frac{-a_1^2 + 16q}{8}\left(c_1 + \frac{-a_1^3 + 2a_1a_2 + 4a_1q}{a_1^2 - 16q}c_2 + \frac{a_1^4 - 3a_1^2a_2 - a_1^2q + 8a_2q}{a_1^2 - 16q}c_3\right)^2\end{aligned}$$

$$+\frac{a_1^4q-6a_1^2a_2q+4a_1^2q^2+8a_2^2q-32q^3}{a_1^2-16q}\left(c_2+\frac{-a_1^3+5/2a_1a_2+a_1q}{a_1^2-2a_2-4q}c_3\right)^2$$
$$+\frac{a_1^4q^2-1/4a_1^2a_2^2q-5a_1^2a_2q^2+7a_1^2q^3+a_2^3q+2a_2^2q^2-4a_2q^3-8q^4}{a_1^2-2a_2-4q}c_3^2.$$

Thus for this usual ordering b_{33} reads:

$$b_{33}=q\frac{a_1^4q-1/4a_1^2a_2^2-5a_1^2a_2q+7a_1^2q^2+a_2^3+2a_2^2q-4a_2q^2-8q^3}{a_1^2-2a_2-4q}.$$

Since we have that $\mathcal{N}^2(c)<\frac{2}{4}\left(\frac{q^2}{\sqrt{q}-1}\right)^2$ (respectively $<\frac{2}{4}\left(\frac{q^2+1}{\sqrt{q}-1}\right)^2$ in the case of even characteristic), that all $b_{ii}>0$, and that the other expressions are squares we get the bound $|c_3|<\frac{\sqrt{2}}{2}\frac{q^2}{\sqrt{q}-1}\frac{1}{\sqrt{b_{33}}}$ (respectively $<\frac{\sqrt{2}}{2}\frac{q^2+1}{\sqrt{q}-1}\frac{1}{\sqrt{b_{33}}}$).
Choosing an appropriate ordering we obtain individual bounds on the $|c_i|$. Note that these cannot occur simultaneously. The highest coefficients read in these cases:

for c_2:

$$q\frac{a_1^4q-1/4a_1^2a_2^2-5a_1^2a_2q+7a_1^2q^2+a_2^3+2a_2^2q-4a_2q^2-8q^3}{a_1^4-3a_1^2a_2+3a_1^2q-2a_2q-4q^2},$$

for c_1:

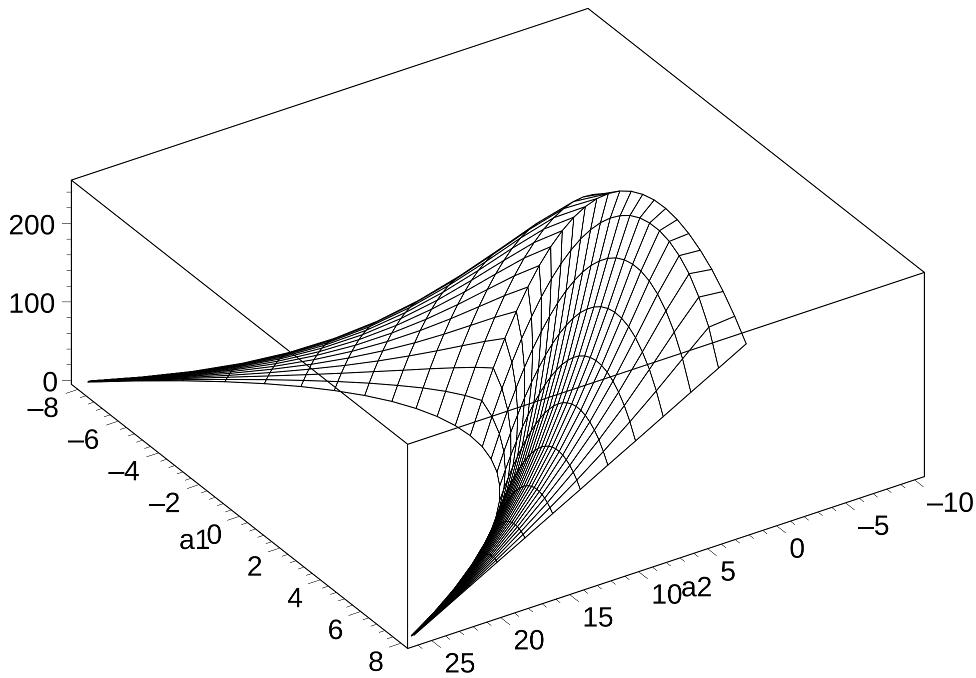
$$\frac{a_1^4q-1/4a_1^2a_2^2-5a_1^2a_2q+7a_1^2q^2+a_2^3+2a_2^2q-4a_2q^2-8q^3}{a_1^4-3a_1^2a_2+3a_1^2q-2a_2q-4q^2},$$

and for c_0:

$$\frac{a_1^4q-1/4a_1^2a_2^2-5a_1^2a_2q+7a_1^2q^2+a_2^3+2a_2^2q-4a_2q^2-8q^3}{q^2(a_1^2-2a_2-4q)}.$$

Note that the numerators in all 4 cases are equal and that looking only at the orders the power of q increases with growing index.
In the genus 2 case we have the bounds from Rück (2) $|a_1|\le 2\lfloor 2\sqrt{q}\rfloor$ and $2|a_1|\sqrt{q}-2q<a_2<a_1^2/4+2q$. Thus we see that the denominators are negative in both cases and we have that the integer $-a_1^2+2a_2+4q\in(0,8q)$ and the integer $-a_1^4+3a_1^2a_2-3a_1^2q+2a_2q+4q^2\in(0,\frac{81}{4}q^2)$.
Substituting $a_1=b_1\sqrt{q}$ and $a_2=b_2q$, thus $|b_1|<4$ and $b_1-2<b_2<b_1^2/4+2$ provides that the coefficient for c_i^2 is of order $O(q^i)$. Thus asymptotically we have $|c_i|<kq^{g-i/2}$ for some constant k. This corresponds to our experiments providing $c_i\in R$ for $i\ge 1$ but we shall try to get some knowledge about the constants implied.
Now we deal with the numerator $B=-a_1^4q+1/4a_1^2a_2^2+5a_1^2a_2q-7a_1^2q^2-a_2^3-2a_2^2q+4a_2q^2+8q^3$. Inserting the bounds for a_2 leads to $B=0$, but since we have

strict inequalities they are not attained. (The bounds would lead to reducible polynomials P, what we excluded.) Thus we have $B > 0$ what we knew in advance since $\mathcal{N}^2$ is positive definite.
The following picture illustrates the correspondence of b_{33} on a_1 and a_2 for the case of $q = 5$. The vertical axis gives the value of $b_{33}(a_1, a_2)$.



a_1 occurs only with even exponents in B. It grows towards the interior of the segment and is maximal for $a_1 = 0$ and $a_2 = 2/3q$. For this pair – which can occur only for characteristic 3 – the value of the respective b_{33} is $16/9q^i$ for all four cases. Hence, then we have $|c_i| < \frac{3\sqrt{2}}{8}\frac{q^{2-i/2}}{\sqrt{q}-1}$.

In the following we assume $a_1 \geq 0$ and provide the largest and the smallest value assumed, hence for $a_1 = 0$ and the maximal value of a_1.
Near the upper bound of a_2 we make the following observation:
Inserting $a_2 = (a_1^2 - 1)/4 + 2q$ in b_{33} yields for the coefficient of c_3^2 (the same holds for c_0 if we divide by q^3):

$$-1/32q\frac{1 - 2a_1^2 - 32q + 256q^2 - 32a_1^2q + a_1^4}{a_1^2 + 1 - 16q}.$$

For $a_1 = 0$ we get $1/32(-1 + 16q)q$, thus the coefficient is approximately $1/2q^2$ and for $a_1 = 4\sqrt{q} - 2$ we get $3/32q\frac{64q-32\sqrt{q}+3}{16\sqrt{q}-5}$ thus only the estimate $3/8q^{3/2}$.
Maisner and Nart [30] investigate in more detail which pairs a_1, a_2 satisfying the

conditions of Theorem 2.30 and leading to an irreducible polynomial P belong to a hyperelliptic curve. For example they conjecture that the choice of $a_2 = 2q + (a_1^2 - 1)/4$ does not belong to a hyperelliptic curve. If this holds the upper bound decreases to $a_2 \leq a_1^2/4 - 1 + 2q$ and the constants are improved to $2q^2$ and $5/3q^{3/2}$ respectively.
The lower bound on a_2 is much more subtle to handle unless q is a square. In that case one easily gets $2q^2 - 1/2q$ for $a_1 = 0$ and $5/4q\frac{16q+1-12\sqrt{q}}{12\sqrt{q}-7}$ for $a_1 = 4\sqrt{q} - 1$ by choosing $a_2 = a_1\sqrt{q} - 2q + 1$.
In the case q a non-square for $a_1 = 0$ we have $a_2 \geq 1 - 2q$, thus the bound $1/2(4q^2 - 441)q$. Now to consider the maximal value for a_1 put $a_1 = 2(2\sqrt{q} - \delta)$, where $\delta \in (0, 1)$. Hence, δ is such that $\lfloor 2\sqrt{q} \rfloor = 2\sqrt{q} - \delta$. Then $a_2 > 6q - 4\sqrt{q}\delta$ but from the upper bound we have as well $a_2 < 6q - 4\sqrt{q}\delta + \delta^2$. Therefore putting $a_2 = 6q - 4\sqrt{q}\delta + \epsilon$, $\epsilon \in (0, \delta^2)$ leads to

$$1/2q\epsilon\frac{16\delta^2 q - 16q\epsilon - 8\sqrt{q}\delta^3 + 8\sqrt{q}\delta\epsilon + \delta^2\epsilon - \epsilon^2}{4\sqrt{q}\delta - 2\delta^2 + \epsilon}.$$

Note that it is very likely that there does not exist any integer in this interval for a_2, we just consider the worst case. If such an integer does not exist this means that $a_1 \leq 2(2\sqrt{q} - \delta) - 1$ and the bounds for a_2 are changed adequately.
Putting $\epsilon = 1/2\delta^2$ provides

$$1/8q\delta^3\frac{32q - 16\sqrt{q}\delta + \delta^2}{8\sqrt{q} - 3\delta} \sim 1/2\delta^3 q^{3/2}.$$

Thus essentially we have at least $b_{33} \geq kq^{3/2}$ for large a_1 and $b_{33} \geq k'q^2$ for $a_1 = 0$, where k and k' are constants. This provides $|c_3| < \frac{1}{2k}\frac{q^{5/4}}{\sqrt{q}-1}$ respectively $|c_3| < \frac{1}{2k'}\frac{q}{\sqrt{q}-1}$ for odd characteristic and similar results for even characteristic.

The coefficients of c_1 and c_2 can be investigated in the same way leading to similar bounds.

Thus assuming the condition $c_3 \in R$ to hold from the bound on b_{33} – this is less then the above computations provide, it just uses $b_{33} \geq 2/(\sqrt{q} - 1)^2$ – we obtain that $|c_0| \leq q^{3/2} r_{\max}$, where $r_{\max}$ is the maximal coefficient of R, hence $(q^2 - 1)/2$ for odd and $q^2/2$ for even q. In the same manner we get $|c_1| \leq q r_{\max}$ and $|c_2| \leq q^{1/2} r_{\max}$. Sure these maximal bounds cannot be attained simultaneously since the coefficients b_{ij} for $(i, j) \neq (3, 3)$ lead to further restrictions and furthermore the maximal choices for for example c_0 probably cannot be extended to a vector with integer entries. This is the reason why we used the first ordering for the implementation – to avoid too many aborted vectors, thus to reduce the running time. But using these weak estimates provides a worst case bound on the size of these coefficients.

Furthermore in the experiments we even had $c_i \in R$ for $i \geq 1$, thus a proof of this would lead to $|c_0| \leq q^{1/2} r_{\max}$.

Note that these observations generalize to arbitrary genus. But there the bounds on the a_i's are less optimized. If the bound on $b_{(2g-1)(2g-1)}$ leads to $|c_{2g-1}| \leq k$ then an appropriate ordering of $\mathcal{N}^2(c)$ provides

$$|c_i| \leq k_i q^{(2g-1-i)/2},$$

with moderately adjusted constants k_i and all this is in the worst case which probably cannot happen.

One argument that can be used in the proof of the finiteness in the elliptic curve case is that periods of length larger than one (except for a change of sign) cannot occur since otherwise the coefficients c_0 and c_1 would be larger than allowed. Now we investigate in which situations periods can occur at all. For the elliptic curve case the expansion can become cyclic only if $|a_1| - 1 > (q-1)/2$ thus for $q < 14$. In fact only for the following cases such curves do exist: Smart [51] states that for odd characteristic we have periods if $q = 5$ and $a_1 = \pm 4$ or $q = 7$ and $a_1 = \pm 5$ respectively, i.e. in the cases of Example 8.4 where we included a further coefficient. For even characteristic it was shown in [36] by Müller that we always obtain a finite expansion if we use the set R as given above.
For curves of larger genus the situation is a bit different. First of all – although obvious from the experiments and motivated by the previous example in the genus 2 case – we have no proof how large the coefficients of c with $\mathcal{N}(c)^2$ bounded as above can get but we can obtain some information as well, which makes it easy to check for periods for an individual curve.

Assume that for

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

we have that

$$\begin{aligned} c &= c_0 + c_1 \tau + \cdots + c_{2g-1} \tau^{2g-1} \\ &= u_0 \pm \tau(c_0 + c_1 \tau + \cdots + c_{2g-1} \tau^{2g-1}) \end{aligned}$$

with $u_0 \in R$ and where $\mathcal{N}(c)^2$ is bounded by the constant from Lemma 8.2 or Lemma 8.3 respectively. (Otherwise we know that the norm decreases.) Without loss of generality we assume that $c_0 > 0$ and therefore $c_0 > \lceil (q^g - 1)/2 \rceil$. Put

$$d = (c_0 - u_0)/q^g > 0. \tag{3}$$

The rules for expanding an element lead to a system of equations

$$\begin{array}{lcll} \pm c_i &=& c_{i+1} - d a_{i+1} q^{g-i-1} & 0 \leq i \leq g-1 \\ \pm c_i &=& c_{i+1} - d a_{2g-1-i} & g \leq i \leq 2g-2 \ , \\ \pm c_{2g-1} &=& -d & \end{array}$$

where the signs are assumed simultaneously. If this system can be fulfilled for a curve with the positive sign for $(c_0, c_1, \ldots, c_{2g-1})$ then the equations hold for the quadratic twist of the curve with the opposite sign and the above coefficient vector with alternating signs. Thus we restrict ourselves to the case of positive sign. Inserting all equations in the one for c_0 yields

$$c_0 = -d - da_1 - \cdots - da_g - da_{g-1}q - \cdots - da_1q^{g-1},$$

thus $c_0 = dq^g - d|\mathrm{Pic}^0(C/\mathbf{F}_q)|$. Using (3) we obtain

$$u_0 = -d|\mathrm{Pic}^0(C/\mathbf{F}_q)|.$$

Since both d and $|\mathrm{Pic}^0(C/\mathbf{F}_q)|$ are non-negative and $u_0 \in R$ the crucial part to be fulfilled for either the curve or its twist is $\lceil (q^g-1)/2 \rceil \geq d|\mathrm{Pic}^0(C/\mathbf{F}_q)|$. Since a lower bound on the class number is given by the Theorem of Hasse-Weil 2.29, q and d have to be such that $\lceil (q^g-1)/2 \rceil \geq d(\sqrt{q}-1)^{2g}$. Thus we only have this problem if q is small enough.
We just have shown

Theorem 8.7 *Let C be a hyperelliptic curve of genus g with characteristic polynomial of the Frobenius endomorphism and let c be of norm less than $\frac{\sqrt{g}q^g}{2(\sqrt{q}-1)}$ (respectively $\frac{\sqrt{g}(q^g+1)}{2(\sqrt{q}-1)}$) and put $d = \lfloor (c_0 + u_{\max})/q^g \rfloor$, where $u_{\max}$ is the maximal coefficient contained in R. Then the expansion of c can become cyclic only if*

$$\lceil (q^g-1)/2 \rceil \geq d|\mathrm{Pic}^0(\tilde{C}/\mathbf{F}_q)|,$$

where $\tilde{C}$ is either the curve or its quadratic twist.

In the following example we assume that R consists of a complete set of remainders modulo q^g.

Example 8.8 *In the genus 2 case for odd characteristic we have the following tabular. In the experiments only $d = 1$ occurred.*

d	$q \leq$
1	*37*
2	*11*
3	*7*
4	*5*
11	*3*
15	*no such q*

If we assume that at least that $c_3 \in R$ holds then by $c_0 \leq q^{3/2}r_{\max}$ we have that d is additionally bounded from above by $d < q^{3/2}/2$. For example this leads to $d \leq 2$ for $q = 3$ and to $d \leq 5$ for $q = 5$, thus cutting the lower part of the tabular. If we even had $c_i \in R,\ i \geq 1$ and $|c_0| < k\sqrt{q}r_{\max}$ for a constant k then d is additionally bounded from above by $d < kq^{1/2}/2$.

For a given curve it is fairly easy to check whether the expansion can run into a cycle at all. Using the algorithm of Finke and Pohst we can compute all elements of such a small norm and expand all these elements to the base of τ. However, not all the curves for which the inequality of the theorem holds lead to cyclic expansions. In case this happens, we just need to include $\pm d(q^g - |\mathrm{Pic}^0(C/\mathbf{F}_q)|)$ in our set of coefficients and use it instead of the whole period that would follow to obtain a finite expansion as wanted. Thus if we choose such a curve for implementation we need to precompute and store one more element. Since d and q are bounded by relatively small constants the time for this further precomputation can be neglected.

Example 8.9 *Put $g = 2, q = 3$. Among all the isogeny classes of curves with irreducible $P(T)$ only $P(T) = T^4 \pm 2T^3 + 2T^2 \pm 6T + 9$, $P(T) = T^4 \pm T^3 - 2T^2 \pm 3T + 9$, and $T^4 \pm 3T^3 + 5T^2 \pm 9T + 9$ lead to periods. The coefficients to include are ± 5 in the first two cases and ± 6 in the last one.*

Example 8.10 *In the case of even characteristic the situation is even a bit more relaxed. If we choose coefficients from $\{0, \pm 1, \ldots, \pm q^g/2 - 1, q^g/2\}$ unless $c_0 = -q^g/2$ (cf. Algorithm 7.1) then for all classes of curves of genus two over $\mathbf{F}_2$ (see Tabular 1) the expansions are finite. For $\mathbf{F}_4$ we run into a cycle only for $P(T) = T^4 \pm 4T^3 + 9T^2 \pm 16T + 16$. To deal with this we include ± 10 in the set of coefficients.*

Now we look for longer periods. Without loss of generality let $c_0 > 0$. Put $c_0 - u_0 = dq^g$ and $c_1 - a_1 q^{g-1} d - u_1 = eq^g$. Then from the equation

$$\begin{aligned} c &= c_0 + c_1\tau + \cdots + c_{2g-3}\tau^{2g-3} + c_{2g-2}\tau^{2g-2} + c_{2g-1}\tau^{2g-1} \\ &= u_0 + \tau(u_1 \pm \tau(c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1})), \end{aligned}$$

the rules for expansion lead to the following system (again we allow a change of sign):

$$\begin{array}{lll} \pm c_i &= c_{i+2} - da_{i+2}q^{g-i-2} - ea_{i+1}q^{g-i-1} & 0 \le i \le g-2 \\ \pm c_i &= c_{i+2} - da_{2g-2-i} - ea_{2g-1-i} & g-1 \le i \le 2g-3 \\ \pm c_{2g-2} &= -d - ea_1 & \\ \pm c_{2g-1} &= -e. & \end{array}$$

Inserting all this (for positive sign) in the equations for c_0 and c_1 we get

$$\begin{array}{lllll} c_0 &= -d - ea_1 - da_2 - \cdots - dq^{g-2}a_2 - eq^{g-1}a_1 &= & dq^g + u_0 \\ c_1 &= -e - da_1 - ea_2 - \cdots - eq^{g-1}a_2 & = & dq^{g-1}a_1 + eq^g + u_1, \end{array}$$

where the last part comes from the definition of d respectively e. A necessary condition is that

$$-(d+e)|\mathrm{Pic}^0(C/\mathbf{F}_q)| = u_0 + u_1$$

can be fulfilled for $u_0, u_1 \in R$.
For $d = -e$ we get $u_0 = -u_1$, i. e. the case of period length one with a change of sign. And from the equations above we have the same restriction on the size of d as before.
In the other cases we see as well, that e and d are of the same order and that both and q have to be reasonably small. On the other hand except for $d = -e = 1$ this did not occur in the experiments and the same holds for periods of higher order.
Again this can be explained by the bounds on the coefficients. If we have $|c_0| < k\sqrt{q}r_{\max}$ and $|c_i| \in R,\ i \geq 1$, then $d < k\sqrt{q}/2$ and $e < 1 + kg$ in the worst case.

A different way to proof the finiteness of such expansions can be extended from Lesage [28]. He investigates expansions to the base α, where α is a root of a quadratic polynomial over $\mathbf{Z}$ and the set of remainders is of cardinality $|\alpha|^2$, symmetric to 0. He uses difference equations to prove the finiteness and succeeds in general for the case of complex roots (except special cases where one obtains periods). For a special polynomial he computes the expected length of the expansion as well. The approach generalizes to the kind of polynomials considered here due to the symmetry of $P(T)$ but again the expressions for the general case involving the a_i cannot be handled. Like before it is possible to get bounds for an individual curve with explicit coefficients.

9 Reducing the length of the representation

Now that we know the dependence between the length of the expansion of m and the value of $\mathcal{N}(m)$ we can try to shorten the representation. We have not made use of the fact that we are working in a fixed extension field of degree n, yet.
We now consider the action of the Frobenius endomorphism on the restricted group of $\mathrm{Pic}^0(C/\mathbf{F}_{q^n})$. For these divisor classes D we have that $\sigma^n(D) = D$. Thus two sums $\sum_{i=0}^{l_1-1} c_i\phi^i$ and $\sum_{i=0}^{l_2-1} d_i\phi^i$ represent the same endomorphism on $\mathrm{Pic}^0(C/\mathbf{F}_{q^n})$ if the corresponding sums in $\mathbf{Z}[\tau]$ are congruent modulo $\tau^n - 1$, i. e. if

$$\sum_{i=0}^{l_1-1} c_i\tau^i - \sum_{i=0}^{l_2-1} d_i\tau^i \in (\tau^n - 1)\mathbf{Z}[\tau].$$

Remark: Since we consider only irreducible polynomials P and since the constant term of P is $q^g \neq \pm 1$ the polynomials $P(T)$ and $T^n - 1$ are co-prime. Thus their gcd over $\mathbf{Q}[T]$ is one. But we are working in $\mathbf{Z}[T]$. The ideal generated by these polynomials is a principal ideal generated by an integer (since the gcd over $\mathbf{Q}[T]$ is 1).

Claim: In fact this number is equal to the cardinality of the Picard group over $\mathbf{F}_{q^n}$.

Note that this leads to a further way to compute the class number for a field extension using integer arithmetic only. The approach described in Section 4 has the advantage that it provides a fast means to compute the group order for various extensions.

Proof of claim. Write $P(T) = \prod_{i=1}^{2g}(T - \tau_i)$. Then in the ideal we have $T^n = 1$. Transforming $T \to T^n$ we have to evaluate

$$\prod_{i=1}^{2g}(T^n - \tau_i^n)_{|T^n=1} = \prod_{i=1}^{2g}(1 - \tau_i^n) = |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})|,$$

which is indeed the class number. □

To rephrase this, in $\mathbf{F}_l[T]$ these polynomials have a common factor $T-s$ of degree 1, where l is a prime factor of $|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})|$. Hence if we consider only the cyclic group of order l the operation of the Frobenius endomorphism on a divisor class corresponds to the multiplication of the divisor class by an integer s modulo l. For cryptographic purposes we work in the subgroup of prime order. From now on let l be the large prime factor of $|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})|$.
If we restrict to the subgroup of order l we can even reduce modulo $\frac{\tau^n-1}{\tau-1} = \tau^{n-1} + \tau^{n-2} + \cdots + \tau + 1$ since the operation of the Frobenius cannot correspond to 1 modulo l.
Therefore we shall search for elements $M \in \mathbf{Z}[\tau]$ that satisfy for a given $m \in \mathbf{Z}$ the equation $m \equiv M \bmod (\tau^n - 1)/(\tau - 1)$ and the τ-adic expansion of M is as short as possible. Hence, the value of $\mathcal{N}(M)$ is as small as possible.
We state the following

Theorem 9.1 *Let τ be a root of the characteristic polynomial $P(T)$ of the Frobenius endomorphism of the hyperelliptic curve C of genus g defined over $\mathbf{F}_q$. Consider the curve over $\mathbf{F}_{q^n}$ and let $m \in \mathbf{Z}$. There is an element $M \in \mathbf{Z}[\tau]$ such that*

1. $m \equiv M \bmod (\tau^n - 1)/(\tau - 1)$, *and*
2. $$2\log_q \frac{2(\sqrt{q}-1)\mathcal{N}(M)}{\sqrt{g}} < n + 2g.$$

The proof is constructive, thus it provides a way to compute such an element M. Let us fix some notation which shall be useful for the proof and to state the algorithms. For an element $r \in \mathbf{Q}$ let $z =$`nearest`(r) be the nearest integer to r, if ambiguity arises it is defined to be the integer with the least absolute value. This can be realized computationally by choosing $z = \lceil r - 0.5 \rceil$ if $r > 0$ and $r = \lfloor r + 0.5 \rfloor$ else.

Proof of the theorem. Taking the field $\mathbf{Q}[\tau]$ one can invert elements. Thus, put $r := m(\tau-1)/(\tau^n-1) \in \mathbf{Q}[\tau]$, so $r = \sum_{i=0}^{2g-1} r_i\tau^i$ where $r_i \in \mathbf{Q}$. For $0 \le i \le 2g-1$ put $z_i =$`round`(r_i) and put

$$z := \sum_{i=0}^{2g-1} z_i\tau^i \quad \text{and} \quad M := m - z(\tau^n - 1)/(\tau - 1).$$

Thus it is easy to see that $m \equiv M \bmod (\tau^n - 1)/(\tau - 1)$. To compute the value

$$\mathcal{N}(M) = \mathcal{N}\left(m - \frac{z(\tau^n-1)}{(\tau-1)}\right) = \mathcal{N}\left(\left(\frac{m(\tau-1)}{\tau^n-1} - z\right)\frac{\tau^n-1}{\tau-1}\right)$$

we need an estimate on $\mathcal{N}(\frac{m(\tau-1)}{\tau^n-1} - z) = \mathcal{N}(r - z)$.

$$\begin{aligned}
\mathcal{N}(r-z) &= \left(\sum_{j=1}^{g}\left|\sum_{i=0}^{2g-1}(r_i - z_i)\tau_j^i\right|^2\right)^{\frac{1}{2}} \\
&\le \left(\sum_{j=1}^{g}\left(\sum_{i=0}^{2g-1}|(r_i - z_i)\tau_j^i|\right)^2\right)^{\frac{1}{2}} \\
&\le \left(\sum_{j=1}^{g}\left(\frac{1}{2}\sum_{i=0}^{2g-1}\sqrt{q}^i\right)^2\right)^{\frac{1}{2}} \\
&= \left(\sum_{j=1}^{g}\left(\frac{1}{2}\frac{\sqrt{q}^{2g}-1}{\sqrt{q}-1}\right)^2\right)^{\frac{1}{2}} \\
&= \sqrt{g}\frac{1}{2}\frac{q^g-1}{\sqrt{q}-1}.
\end{aligned}$$

Therefore we have

$$\begin{aligned}
\mathcal{N}(m) &= \mathcal{N}\left(\left(\frac{m(\tau-1)}{\tau^n-1} - z\right)\frac{\tau^n-1}{\tau-1}\right) \le \sum_{i=0}^{n-1}\mathcal{N}\left(\left(\frac{m(\tau-1)}{\tau^n-1} - z\right)\tau^i\right) \\
&= \sum_{i=0}^{n-1}\left(\frac{\sqrt{g}}{2}\frac{q^g-1}{\sqrt{q}-1}q^{i/2}\right) = \frac{\sqrt{g}}{2}\frac{q^g-1}{\sqrt{q}-1}\frac{\sqrt{q}^n-1}{\sqrt{q}-1}.
\end{aligned}$$

It follows that

$$2\log_q \frac{2(\sqrt{q}-1)\mathcal{N}(M)}{\sqrt{g}} \leq 2\log_q(q^g-1) + 2\log_q\left(\frac{\sqrt{q}^n-1}{\sqrt{q}-1}\right) < n+2g.$$

□

Remark: This might not be the best choice, nevertheless it provides an efficient way to compute a length-reduced representation which works for every genus g, ground field $\mathbf{F}_q$, and degree of extension n. For the two binary elliptic curves Solinas investigates in more detail an optimal way of reduction. Considering the lattice spanned by $\{1, \tau\}$ he shows that for each element of $\mathbf{Q}[\tau]$ there is a unique lattice point within distance less than 4/7. For larger genus the computation of the nearest point is computationally hard to realize and we do not loose much choosing the "rounded" elements the way presented here.
Thus from the discussion of Section 8 we have the following result.

Theorem 9.2 (Main result on the Length)
Let C be a hyperelliptic curve of genus g and with characteristic polynomial of the Frobenius endomorphism $P(T)$. Let P be such that the τ-adic expansion is not periodic and that for an element c of $\mathbf{Z}[\tau]$ of norm $< \frac{g}{4}\left(\frac{q^g}{\sqrt{q}-1}\right)^2$ (respectively $< \frac{g}{4}\left(\frac{q^g+1}{\sqrt{q}-1}\right)^2$ for even characteristic) the τ-adic expansion is no longer than $2g+1$. Then we have:
For every element $m \in \mathbf{Z}$ we can compute a τ-adic expansion of length k using coefficients in the set R only, where

$$k \leq n + 4g + 2.$$

From the algorithmic point of view there are two problems left to consider:

- How to represent $(\tau^n - 1)/(\tau - 1)$ in $\mathbf{Z}[\tau]$?
- How to invert elements of $\mathbf{Z}[\tau]$?

These question are investigated in the following subsections.

9.1 Representing $(\tau^n - 1)/(\tau - 1)$ in $\mathbf{Z}[\tau]$

Let $P(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + a_{g-1} q T^{g-1} + \cdots + a_1 q^{g-1} T + q^g$ be the characteristic polynomial of the Frobenius endomorphism associated to the hyperelliptic curve C of genus g. Suppose that

$$\tau^{k-1} = d_{0,k-1} + d_{1,k-1}\tau + \cdots + d_{2g-1,k-1}\tau^{2g-1}$$

for integers $d_{0,k-1}, d_{1,k-1}, \ldots, d_{2g-1,k-1}$, then

$$\begin{aligned}
\tau^k &= d_{0,k-1}\tau + d_{1,k-1}\tau^2 + \cdots + d_{2g-1,k-1}\tau^{2g} \\
&= -q^g d_{2g-1,k-1} + (d_{0,k-1} - a_1 q^{g-1} d_{2g-1,k-1})\tau + (d_{1,k-1} - a_2 q^{g-2} d_{2g-1,k-1})\tau^2 + \\
&\quad \cdots + (d_{2g-2,k-1} - a_1 d_{2g-1,k-1})\tau^{2g-1}.
\end{aligned}$$

This leads to an algorithm to compute the coefficients of τ^k iteratively starting with $\tau^0 = 1$. Since $(\tau^n - 1)/(\tau - 1) = \tau^{n-1} + \tau^{n-2} + \cdots + \tau + 1$ we sum up the intermediate results after each exponentiation.

Algorithm 9.1
`INPUT:` $n \in \mathbf{N}$, $P(T)$.
`OUTPUT:` $e_0, \ldots, e_{2g-1} \in \mathbf{Z}$ *such that* $(\tau^n - 1)/(\tau - 1) = e_0 + e_1\tau + \cdots + e_{2g-1}\tau^{2g-1}$.

1. *Initialize:* $d_0 = 1$ *and* $d_i = 0$ *for* $1 \le i \le 2g-1$;
   $e_0 = 1$ *and* $e_i = 0$ *for* $1 \le i \le 2g-1$;
2. *for* $1 \le k \le n-1$ *do*
   (a) $d_{old} := d_{2g-1}$;
   (b) *for* $2g-1 \ge i \ge g$ *do*
   $d_i := d_{i-1} - a_{2g-i} d_{old}$;
   $e_i := e_i + d_i$;
   (c) *for* $g-1 \ge i \ge 1$ *do*
   $d_i := d_{i-1} - a_i q^{g-i} d_{old}$;
   $e_i := e_i + d_i$;
   (d) $d_0 := -q^g d_{old}$;
   $e_0 := e_0 + d_0$;
3. *output* $(e_0, e_1, \ldots, e_{2g-1})$.

9.2 Inversion of Elements $e_0 + e_1\tau + \cdots + e_{2g-1}\tau^{2g-1}$ in $\mathbf{Q}[\tau]$

Let $e_0 + e_1\tau + \cdots + e_{2g-1}\tau^{2g-1} \in \mathbf{Z}[\tau]$ where τ is a root of $P(T)$. As we only consider curves with irreducible $P(T)$ and as the degree of $S(T) := e_0 + e_1 T + \cdots + e_{2g-1}T^{2g-1}$ is less than $\deg P(T)$ the polynomials $P(T)$ and $S(T)$ are relatively prime, hence $\gcd(S(T), P(T)) \in \mathbf{Q}$. Since $\mathbf{Q}[T]$ is an Euclidean domain with respect to the degree map, there exist polynomials $V(T), U(T) \in \mathbf{Q}[T]$ such that

$$\gcd(S(T), P(T)) = U(T)S(T) + V(T)P(T)$$

and $\deg U < \deg P$. They can be computed using the extended Euclidean algorithm.
By inserting τ for T we get

$$(e_0 + e_1\tau + \cdots + e_{2g-1}\tau^{2g-1})^{-1} = U(\tau)/\gcd(S(T), P(T)).$$

9.3 Computing τ-adic Expansions of Reduced Length

Combining our results of the previous sections we are now in a position to state an algorithm for computing m-folds of divisor classes using τ-adic expansions of reduced length.
Let C be a hyperelliptic curve of genus g defined over $\mathbf{F}_q$ and $P(T)$ the corresponding characteristic polynomial of the Frobenius endomorphism. Consider the curve over the extension field $\mathbf{F}_{q^n}$. Take the unique reduced ideal $D = [a, b]$ in the ideal class corresponding to the divisor class as a representative. Assume that the coefficients of the polynomials are represented with respect to a normal basis.

Algorithm 9.2 (Computation of m-folds using τ-adic expansions)
`INPUT:` $m \in \mathbf{Z}, D = [a, b],\ a, b \in \mathbf{F}_{q^n}[x],\ P(T),\ R$ *the set of coefficients.*
`OUTPUT:`mD *represented by the reduced ideal* $H = [s, t],\ \ s, t \in \mathbf{F}_{q^n}[x]$.

1. *Precomputation: for* $i \in R, i > 0$ *compute*
   $D(i) := iD$;
   $D(-i) := -D(i)$; /* *for free*/*
2. /**compute a length reduced* $M \in \mathbf{Z}[\tau]$ *with* $m \equiv M \bmod (\tau^n - 1)/(\tau - 1)$;*/
   (a) *Initialize:* $d_0 = 1$ *and* $d_i = 0$ *for* $1 \le i \le 2g-1$;
   $e_0 = 1$ *and* $e_i = 0$ *for* $1 \le i \le 2g-1$;
   (b) *for* $1 \le k \le n-1$ *do*
      i. $d_{old} := d_{2g-1}$;
      ii. *for* $2g-1 \ge i \ge g$ *do*
         $d_i := d_{i-1} - a_{2g-i}d_{old}$;
         $e_i := e_i + d_i$;
      iii. *for* $g-1 \ge i \ge 1$ *do*
         $d_i := d_{i-1} - a_i q^{g-i} d_{old}$;
         $e_i := e_i + d_i$;
      iv. $d_0 := -q^g d_{old}$;
         $e_0 := e_0 + d_0$;
   (c) *let* $e := \sum e_i T^i$;
   (d) *compute* $e' := e^{-1} \bmod P$ *using extended GCD;*

(e) *compute* $M' :=\texttt{round}(m \cdot e')$;

(f) *let* $M = \sum_{i=0}^{2g-1} M_i T^i := m - e \cdot M' \bmod P$;

3. /*compute the τ-adic representation of M;*/

   (a) *Put* $i := 0$;

   (b) *While for any* $0 \leq j \leq 2g-1$ *there exists an* $M_j \neq 0$ *do*
   - *if* $q^g | M_0$ *choose* $u_i := 0$;
   - *else choose* $u_i \in R$ *with* $q^g | M_0 - u_i$;
   - /*in even characteristic choose $u_i = M_0$ if $|M_0| = q^g/2$/*
   - $d := (M_0 - u_i)/q^g$;
   - *for* $0 \leq j \leq g-1$ *do*
     - $M_j := M_{j+1} - a_{j+1} q^{g-j-1} d$;
   - *for* $0 \leq j \leq g-2$ *do*
     - $M_{g+j} := M_{g+j+1} - a_{g-j-1} d$;
   - $M_{2g-1} := -d$;
   - $i := i + 1$;

4. /* compute m-fold of D;*/

   (a) *initialize* $H := [1, 0]$;

   (b) *for* $l - 1 \leq 0$ *do*
   - $H := \sigma(H)$; /* this means cyclic shifting /*
   - *if* $u_i \neq 0$ *then*
     - $H := H + D(u_i)$;

5. *output(H).*

Remarks:

1. If the algorithm is carried out several times with the same divisor class D (like in the first step of the Diffie-Hellman key exchange) then we need to do the precomputations of Step 1 and the determination of e' (i. e. most of Step 2) only once and for all at the set-up of the system.

2. To obtain a sparse representation as described in the next section one changes Step 3 appropriately. If the curve is such that the expansion becomes cyclic after the coefficient γ, then include $D(\gamma) := \gamma D$ in the precomputations and choose γ as coefficient whenever $M_0 = \gamma$.

3. Note that when we restrict ourselves to the fixed extension $\mathbf{F}_{q^n}$ we can obtain a finite representation with restricted coefficients in any case since we can use $\tau^n - 1$ for computing the expansion as well. However these expansions would be much longer. Furthermore we took this approach (first considering the finiteness and dependence of the length on $\mathcal{N}$) to give

a motivation for the chosen strategy of reducing the length and to save the relation $(\tau^n - 1)/(\tau - 1)$ for the reduction.

10 Density of the Expansion

Besides the length the second important quantity to consider is the *density* of the representation. By density we mean the number of nonzero coefficients occurring in the representation divided by the length of the representation.
Naturally the density will depend heavily on the choice of the set R and therefore on the number of precomputations. As stated before the minimal set R simply to make possible the expansion is $\{0, \pm 1, \pm 2, \ldots, \pm\lceil\frac{q-1}{2}\rceil\}$. Using this set, we get a zero coefficient only at random, hence with a probability of $1/q^g$. (Remember $\tau | c_0 + \cdots + c_{2g-1}\tau^{2g-1} \Leftrightarrow q^g | c_0$.) Therefore the asymptotic density in that case is $(q^g - 1)/q^g$.
We can also double the number of remainders $R' = \{0, \pm 1, \ldots, \pm q^g - 1\}$ and use the fact that we can choose from two elements. This was used in [17] to obtain an asymptotic density of $\frac{489}{910}$ for a genus two curve over $\mathbf{F}_2$ and can be carried over to the general case as long as $p \not| a_1$. It leads to expansions satisfying that among any $2g$ coefficients there is at least one of value 0. Anyhow for larger genus and field size the interdependencies to be aware of while choosing the next coefficient become rather involved.

But by using other choices of R we can try to obtain more zero coefficients on the cost of more precomputations. This might be preferable if storage is no problem and the computations are to be carried out very often with the same divisor like in the first step of the Diffie-Hellman key exchange. Consider for example the curves with characteristic polynomial of the following form:

$$P(T) = T^{2g} + a_g T^g + q^g.$$

Let $q = p^r$. If $p^{\lceil gr/2\rceil}$ does not divide a_g then this curve is non supersingular and might be seen as the next best thing with respect to a sparse representation. (If also a_g were $\equiv 0 \bmod p^{\lceil gr/2\rceil}$ then the τ-adic expansion would become rather simple, but these curves are not suitable for cryptology.) Consider the division step in the expansion of $c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}$ and choose $u \in R$ to ensure $q^g | c_0 - u$. Then we get:
$c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1} =$
$= u + \tau(c_1 + c_2\tau + \cdots + (c_g - \frac{c_0-u}{q^g}a_g)\tau^{g-1} + \cdots + c_{2g-1}\tau^{2g-2} - \frac{c_0-u}{q^g}\tau^{2g-1}))$.
The next $g-1$ coefficients of the representation are not influenced by u at all. Thus we obtain g non interacting strands. Taking R to be a complete set of representatives modulo q^{2g} we can force $c_g - \frac{c_0-u}{q^g}a_g$ to be divisible by q^g provided that q and a_g are relatively prime. An example is given in the next section.
Now we observe that for q even $R = \{0, \pm 1, \pm 2, \ldots, \pm\frac{q^{2g}}{2} - 1\} \backslash \{q^g, 2q^g, \ldots, (q^g -$

$1)q^g\}$ and for q odd $R = \{0, \pm 1, \pm 2, \ldots, \pm \frac{q^{2g}-1}{2}\} \backslash \{q^g, 2q^g, \ldots, (q^g - 2)q^g\}$ are minimal choices with $|R| = (q^g - 1)q^g$ to ensure that we obtain at least one zero coefficient for every nonzero one. The proportion of nonzero coefficients visa zeros is $1 : 1 + \frac{1}{q^g} + \frac{1}{q^{2g}} + \cdots$ (the first one from the construction, the others by probability). Thus we get an asymptotic density of $\frac{q^g-1}{2q^g-1}$.
The same strategy and set R work if for $1 \le i < g$ we have $q^g | a_i q^{g-i}$, because then the remainder of the former $c_g - \frac{c_0 - u}{q^g} a_g$ modulo q^g does not change during the next $g - 2$ steps of expansion. Hence, we can obtain a representation of asymptotic density $\frac{q^g-1}{2q^g-1}$ using this strategy whenever

$$P(T) \equiv T^{2g} + a_g T^g + q^g \bmod q^g, \quad a_g \neq 0.$$

In the next section we provide some examples to explain and give evidence that the theoretical results hold even for the range of n considered here.

Remarks

1. Although we described this technique for the above sparse kind of P it is more likely to be used for the more general case since the sparse case corresponds to elliptic curves over $\mathbf{F}_{q^g}$ via Weil descent.

2. This might be regarded as an intelligent kind of windowing. Naturally the standard windowing methods carry through to τ-adic windowing, i. e. to considering $u_0 + u_1\tau + \cdots u_{k-1}\tau^{k-1}$ as *one* coefficient, too. One is naturally lead to considering sliding windows allowing a string of zeros between any nonzero coefficients. Let the length of the window be k like above. Then the density is $\frac{q^g-1}{k(q^g-1)+1}$ computed from the proportion $1 : (k-1) + \frac{1}{q^g} + \frac{1}{q^{2g}} + \cdots = \frac{(k-1)(q^g-1+1}{q^g-1}$.
   Note that the windowing method can be applied for any $P(T)$.
   In [17] we considered coefficients of the form $a + b\tau$ and showed how to slightly reduce the number of precomputations in the case of even characteristic. Instead of the obvious $q^{2g}/2$ precomputations we achieve $(q^g-1)q^g/2$ like above.

3. The bounds on the length hold here as well, but we need to be aware of new periods occurring.

11 Experimental results

This section provides several experimental results about the length and density of the τ-adic expansions for hyperelliptic binary curves of genus 2,3, and 4.
We achieved similar results for odd characteristics as well. Furthermore we only

Table 8: Average Length and Density,Curve with $T^4 - T^2 + 4$

n	average length	average density	n	average length	average density
61	62.35	0.4393	97	98.35	0.4352
67	68.36	0.4383	101	102.36	0.4351
71	72.34	0.4377	103	104.37	0.4347
73	74.33	0.4375	107	108.37	0.4349
79	80.32	0.4368	109	110.35	0.4345
83	84.35	0.4363	113	114.37	0.4345
89	90.36	0.4361			

mention results obtained for the reduced density. Using the minimal set of coefficients the experiments confirm the theoretical (and asymptotical) results, as well.

11.1 Curves of genus 2 over $\mathbf{F}_2$

Besides the supersingular curves and the two curves considered by Günter, Lange, and Stein [17] there are 4 classes of curves left to investigate. All of them allow to reduce the density by the strategy explained in Section 10.
To compute a τ-adic representation we use the following algorithms to realize the strategy that for each nonzero coefficient we obtain at least one zero coefficient as stated in Section 10. Let $M = c_0 + c_1\tau + c_2\tau^2 + c_3\tau^3$. Take $R = \{0, \pm1, \pm2, \dots, \pm7\}\backslash\{\pm4\}$. As in all four cases the coefficient of T is divisible by 4 we observe that there are two non interacting strands as c_1 is not influenced by the choice of u . Thus a nonzero coefficient is not necessarily succeeded by a zero coefficient. But we obtain for each nonzero coefficient

$$1 + 1/4 + 1/16 + \cdots = 4/3$$

zero coefficients (the first one from the construction, the others by probability), hence resulting in a ratio of $1 : 4/3$ thus in an expected density of $3/7$.

Experimental results with all four kinds of curves show that the density decreases for growing n and that a density of less than 0.434 thus slightly worse than $3/7 = 0.42857$ is achieved for extensions of degree at least $n \geq 71$.
In detail these results are given in Tables 8 till 11.

11.2 Curves of genus 3 over $\mathbf{F}_2$

Also for the genus 3 case we made use of the strategy, that we get at least one zero coefficient for each nonzero one. The results are stated in the following Tables 12 and 13.

Table 9: Average Length and Density,Curve with $T^4 + T^2 + 4$

n	average length	average density	n	average length	average density
61	62.36	0.4393	97	98.33	0.4351
67	68.34	0.4382	101	102.35	0.4349
71	72.37	0.4380	103	104.31	0.4348
73	74.34	0.4369	107	108.34	0.4343
79	80.34	0.4368	109	110.35	0.4345
83	84.37	0.4365	113	114.32	0.4344
89	90.36	0.4362			

Table 10: Average Length and Density,Curve with $T^4 + 2T^3 + 3T^2 + 4T + 4$

n	average length	average density	n	average length	average density
61	65.18	0.4348	97	101.13	0.4326
67	71.15	0.4343	101	105.13	0.4324
71	75.17	0.4339	103	107.19	0.4321
73	77.09	0.4338	107	111.15	0.4322
79	83.16	0.4333	109	113.13	0.4321
83	87.14	0.4331	113	117.18	0.4323
89	93.18	0.4327			

Table 11: Average Length and Density,Curve with $T^4 - 2T^3 + 3T^2 - 4T + 4$

n	average length	average density	n	average length	average density
61	65.18	0.4346	97	101.19	0.4326
67	71.20	0.4342	101	105.15	0.4326
71	75.17	0.4340	103	107.18	0.4324
73	77.16	0.4339	107	111.21	0.4320
79	83.19	0.43344	109	113.18	0.4318
83	87.17	0.4331	113	117.13	0.4320
89	93.17	0.4328			

Table 12: Average Length and Density,Curve with $T^8 - T^4 + 8$

n	average length	average density	n	average length	average density
37	40.21	0.4874	61	64.20	0.4793
41	44.30	0.4848	67	70.23	0.4783
43	46.23	0.4848	71	74.23	0.4777
47	50.30	0.4828	73	76.24	0.477
53	56.29	0.4810	79	82.24	0.4764
59	62.27	0.4795			

Table 13: Average Length and Density,Curve with $T^8 + T^4 + 8$

n	average length	average density	n	average length	average density
37	40.21	0.4876	61	64.24	0.4792
41	44.30	0.4844	67	70.24	0.4781
43	46.21	0.4848	71	74.23	0.4776
47	50.23	0.4825	73	76.22	0.4772
53	56.27	0.4812	79	82.22	0.4764
59	62.25	0.4793			

Table 14: Average Length and Density,Curve with $T^8 + T^4 + 16$

n	average length	average density	n	average length	average density
29	34.02	0.5042	47	51.86	0.5046
31	35.87	0.5154	53	57.90	0.4977
37	41.95	0.5018	59	63.69	0.4984
41	45.63	0.5101	61	65.94	0.4962
43	47.66	0.5034	67	71.72	0.4969

11.3 Curves of genus 4 over $\mathbf{F}_2$

Finally we considered genus 4 curves. Here we used two different strategies to compare the effects. First we reduced the density by the strategy of Section 10. These results are stated in Tables 14 and 15. In the second case we had to add a further coefficient since the expansion allowed a period of length 1. To compare we made use of a combination of the windowing technique with τ-adic expansions, allowing the coefficients to be of the form $a + b\tau$ with $|a|, |b| \leq q^g/2$. The corresponding facts can be found in Tables 16 and 17.
The results motivate that it might be preferable to use the usual windowing method. But in this implementation the number of precomputations was not optimized, thus there are more precomputations to store to achieve these results. Like in [17] one can also set up the system such that the number of precomputations for the windowing method is equal to that for the enlarged set presented in Section 10. This will probably lead to results similar to our new strategy, i. e. slightly increase the length.

12 Comparison

12.1 Complexity compared to binary double-and-add

In this section we compare the methods for computing m-folds of divisors. First taking the naive double-and-add method as basis to compare, we compute the

Table 15: Average Length and Density,Curve with $T^8 - T^4 + 16$, additional coefficient

n	average length	average density	n	average length	average density
29	40.22	0.4781	47	57.90	0.4816
31	41.90	0.4802	53	64.17	0.4810
37	48.23	0.4794	59	70.24	0.4806
41	51.96	0.4801	61	72.20	0.4810
43	54.29	0.4793	67	78.22	0.4813

Table 16: Average Length and Density,Curve with $T^8 + T^4 + 16$

n	average length	average density	n	average length	average density
29	31.10	0.4859	47	49.076	0.4850
31	33.11	0.4859	53	55.02	0.4850
37	39.03	0.4861	59	61.08	0.4849
41	43.03	0.4857	61	63.07	0.4849
43	45.09	0.4853	67	69.07	0.4848

Table 17: Average Length and Density,Curve with $T^8 - T^4 + 16$

n	average length	average density	n	average length	average density
29	32.72	0.4906	47	50.71	0.4878
31	34.75	0.4897	53	56.72	0.4876
37	40.71	0.4889	59	62.71	0.4872
41	44.68	0.4887	61	64.69	0.4872
43	46.72	0.4884	67	70.72	0.4867

Table 18: $q = 2$

g	binary	τ-adic	speed-up factor
2	$3n$	$3/7n$	7
3	$9/2n$	$7/15n$	9
4	$6n$	$15/31n$	12

speed-up obtained using the Frobenius endomorphism.
By Section 6 we know that for the standard method we have

$$\sim \frac{3}{2} \cdot g \cdot n \cdot \log_2 q$$

group operations if the *binary* representation is used. If we can make use of the enlarged set of coefficients to achieve a sparse representation we have costs of approximately

$$\sim \frac{q^g - 1}{2q^g - 1} n < \frac{1}{2} n$$

for the τ-adic expansion. The relation leading to the speed-up is given by

$$\frac{\text{binary}}{\tau\text{-adic}} > 3 \cdot g \cdot \log_2 q.$$

If we can only use the minimal set the density is $(q^g - 1)/q^g$ resulting in

$$\sim \frac{q^g - 1}{q^g} n < n$$

operations in the ideal class group and

$$\text{speed-up } > \frac{3}{2} \cdot g \cdot \log_2 q.$$

To fill these numbers with life the following Tables 18 and 19 provide some examples of the speed-up obtained using the larger set of coefficients. Note that the results for the larger set also hold if one makes use of the windowing technique with coefficients $a + b\tau$ since this leads to the same density.

12.2 Complexities taking into account the storage

If one also wants to take into consideration the storage, one can as well compare the results of the τ-adic expansions with binary windowing techniques. Using

Table 19: $q = 5$

g	binary	τ-adic	speed-up factor
2	$6n$	$24/49n$	12
3	$9n$	$124/249n$	18
4	12	$624/1249n$	24

Table 20: $q = 2$, comparison with windowing

g	window	τ-adic (small)	speed-up factor	window	τ-adic (large)	speed-up factor
2	$11/4n$	$3/4n$	$11/3$	$31/12n$	$3/7n$	$217/36 \sim 6$
3	$31/8n$	$7/8n$	$31/7$	$573/160n$	$7/15n$	$1719/224 \sim 7.6$
4	$79/16n$	$15/16n$	$79/15$	$1023/224n$	$15/31n$	$10571/1120 \sim 9.4$

the standard windowing method one simply computes the expansion to the base of 2^k, thus needing $2^k - 2$ precomputations. Even more advanced one can again allow the coefficients to be in the above set but use a sliding window of width k, thus trying to achieve strings of zeros between the entries. A survey on these methods can be found in Gordon's paper [16] and in the Handbook of applied cryptography [33].

The usual windowing method leads to an expansion for m of length $\lambda \sim (\log_2 m)/k$. Thus we need $\sim \lambda k$ doublings. The asymptotic density is $(2^k - 1)/2^k$. Therefore the complexity is of order

$$\lambda k + \lambda(2^k - 1)/2^k \sim \log m(1 + (2^k - 1)/(k2^k)) < (k + 1)/k \log m,$$

where $\log_2 m \sim gn \log_2 q$.

For $q = 2$ we have in the τ-adic method $2^{g-1} - 1$ precomputations in the minimal set and $2^{2g-1} - 2^{g-1} - 1$ precomputations for the larger one. Thus choosing $k = g$ in the first and $k = 2g - 1$ in the second case is more than fair. Then we have for the first case that the number of operations is of order $gn(1 + (2^g - 1))/(g2^g)$ and for the second case of order $gn(1 + (2^{2g-1} - 1))/(g2^{2g-1})$. Thus asymptotically the Frobenius method is faster by a factor of g respectively $2g$. Explicit numbers can be found in Table 20.

Table 21: $q = 5$, comparison with windowing for small set

g	k	window	τ-adic	speed-up factor
2	4	$47/8n$	$24/25n$	$1175/192 \sim 6$
3	7	$511/64n$	$124/125n$	$63875/7936 \sim 8$
4	9	$2559/256n$	$624/625n$	$533125/53248 \sim 10$

Table 22: $q = 5$, comparison with windowing for large set

g	k	window	τ-adic	speed-up factor
2	9	$1535/256n$	$24/49n$	$75215/6144 \sim 12$
3	13	$32767/4096n$	$124/249n$	$263193/16384 \sim 16$
4	18	$1310719/131072n$	$624/1249n$	$1637088031/81788928 \sim 20$

For larger q it gets harder to find the right choice of k to compare. We investigate $q = 5$ as an example. In Tables 21 and 22 we choose k such that $2^k - 2$ is greater or equal than the number of precomputations for the τ-adic method. In the speed-up factor we used 2 instead of $\log_2 5$, again in favor of the windowing method.
Concluding one can state that the speed-up over the windowing method is also remarkable.

12.3 Timings

For timings we used the binary curve $C : y^2 + (x^2 + x + 1)y = x^5 + x^4 + 1$ with characteristic polynomial $P(T) = T^4 - 2T^3 + 3T^2 - 4T + 4$ over $\mathbf{F}_{2^{89}}$. Its class number is $2 \cdot 191561942608242456073498418252108663615312031512914969$, thus this curve is appropriate for applications. For the computations we used Magma. Unfortunately Magma does not provide a representation of the finite fields using a normal basis. Thus instead of using the cyclic shifting as proposed we raise each coefficient to the q-th power. Thus we cannot get the whole speed-up.
We carried out 1000 random scalar multiplications using the τ-adic method in Magma. For the τ-adic method we needed only one precomputation for $2D$, thus the time and space needed for this is negligible. To compare we also used the built-in routine for computing m-folds in Magma.
The average length of the τ-adic expansion is 90.18 and the average time to compute the expansion is 0.005318. The complete multiplication takes 0.070261 on

average. The corresponding time with the usual function is 0.146036 on average. Hence, we obtained a speed-up by a factor of 2.
The program used for this comparison `FrobExample` and a program to play around with a user-defined curve `FrobSelf` can be obtained from
`http://www.exp-math.uni-essen.de/~lange/KoblitzC.html`.

13 Alternatives

In Section 10 we considered different strategies to obtain sparse representations at the cost of more precomputations. But what happens if absolutely no precomputations are allowed, hence, not even for the minimal set R. That means that instead of retrieving $iD, i \in R$ by table-look-up we need to compute with probability $\frac{q^g-3}{q^g}$ an i-fold of D where the binary length of i is approximately $g \log_2 q - 1$. Using the binary double-and-add method this takes $\frac{3}{2}(g \log_2 q - 1)$ operations each time. Thus instead of $\frac{3}{2} gn \log_2 q$ operations using the standard method throughout we arrive at $\frac{q^g-3}{q^g} n \frac{3}{2}(g \log_2 q - 1)$, which is still better since we consider small g and q. Not to waste space on saving the τ-adic expansion we perform the addition after each step.

Algorithm 13.1 (τ-adic, without precomputations)
`INPUT:` $M \in \mathbf{Z}[\tau]$ *with* $M \equiv m \bmod (\tau^n - 1)/(\tau - 1)$, $D = [a, b]$
`OUTPUT:` $H := mD$

1. *Initialize* $H := [1, 0]$
2. *While for any* $0 \le j \le 2g - 1$ *there exists an* $M_j \ne 0$ *do*
   if $q^g | M_0$ *choose* $u := 0$;
   else choose $u \in R$ *with* $q^g | M_0 - u$;
   /**in even characteristic choose* $u = M_0$ *if* $|M_0| = q^g/2$/*
   $d := (M_0 - u_i)/q^g$;
   for $0 \le j \le g - 1$ *do*
   $M_j := M_{j+1} - a_{j+1} q^{g-j-1} d$;
   for $0 \le j \le g - 2$ *do*
   $M_{g+j} := M_{g+j+1} - a_{g-j-1} d$;
   $M_{2g-1} := -d$;
   compute $H := H + uD$ *via binary double-and-add;*
   $D := \sigma(D)$;
3. *output(H);*

If enough storage is available to save the τ-adic representation but not the precomputed values for $u_i D, u_i \in R$ then the following algorithm is much faster reducing the amount of doublings needed. Let the expansion of m be of length l and put $r := \lfloor \log_2(\max_{u_i \in R} |u_i|) \rfloor + 1$, hence for the minimal set R we have $r \sim g \log_2 q$. Let the binary expansion of u_i be $u_i = \sum_{j=0}^{r-1} u_{ij} 2^j$.

Algorithm 13.2 (τ-adic, precomputed expansion)
`INPUT:` $D = [a, b]$, $m = \sum_{i=0}^{l-1} u_i \tau^i$, $u_i \in R$.

`OUTPUT:` $H = mD$

1. *Initialize* $H := [1, 0]$;
2. *For* $j = r - 1$ *to* 1 *do*
   (a) *For* $i = l - 1$ *to* 0 *do*
   $H := H + u_{ij} D$;
   (b) $H := 2H$;
3. *For* $i = l - 1$ *to* 0 *do*
   $H := H + u_{i0} D$;
4. *output(H).*

For this algorithm we need r doublings and asymptotically $\frac{1}{2} rl$ additions. Thus the complexity is approximately $\frac{1}{2} ng \log_2 q$ for large n and $l \sim n$. We can do even better if we use a binary non adjacent form (NAF) – signed binary representation with no two consecutive non-zeros – of the u_i which has an asymptotic density of $1/3$ resulting in a complexity of $\frac{1}{3} ng \log_2 q$. Note that the space requirement to compute and store the NAFs of the u_i is not much larger than storing the binary representation of the u_i's. Unfortunately this way we cannot get rid of the factor g in the complexity.

14 Koblitz curve cryptosystems revisited

To use a cryptosystem or protocol based on Koblitz curves it is not necessary to start with a secret integer m, compute its τ-adic expansion and use this to compute a secret multiple of a group element. One can as well start with an expansion of fixed length (padding with leading zeros if necessary) and use it as the hidden number – not caring to which integer it corresponds if at all. If we restrict ourselves to the cyclic subgroup of order l as usual, then we know by Section 9 that for the action of the Frobenius endomorphism we have $\sigma(D) = sD$, where s is an integer modulo l. Hence, any sum corresponds to an integer modulo l. Thus instead of computing a random number smaller than the group order we choose at random k elements from the set of coefficients R. This idea was pointed out to me by Schroeppel. In [22] Koblitz investigates a similar set-up for elliptic curves, where he credits the idea to Lenstra.

To apply this idea, we need to ensure that the corresponding multipliers occurring are equally distributed. Respectively we need to be aware of collisions.

Using the method described so far in a group of order l the probability of collision is $1/l$. This is the probability that two persons choose the same key if the key is chosen at random. As before we restrict ourselves to the points of order l of $\mathrm{Pic}^0(C/\mathbf{F}_{q^n})$, where we consider the large prime l dividing $|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})|$. Hence, the there exists an integer s modulo l such that $\sigma D = sD$ for all divisor classes D of order l. Since we know that $s^n \equiv 1 \bmod l$, because s corresponds to the Frobenius endomorphism on this restricted group, and $s \not\equiv 1 \bmod l$ the highest exponent of τ in the expansion should be less or equal to $n-2$, to avoid multiple occurrences of a number. There can be other combinations of powers of s with bounded coefficients depending on the chosen curve, but here we try to exclude those polynomials that occur in any case.
Note that the two known equivalences $1 + s + \cdots + s^{n-1} \equiv 0 \bmod l$ and $s^{2g} + a_1 s^{2g-1} + \cdots + a_g s^g + \cdots + a_1 q^{g-1} s + q^g \equiv 0 \bmod l$ do not lead to such a representation, since in the first one the highest power is $n-1$ and all powers $s^i \bmod l, 0 \leq i \leq n-2$ are different (n is prime), the second one contains the coefficient $q^g \notin R$, and any combination of both still has the maximal power of $n-1$ or too large coefficients unless $s^{n-1-2g}(s^{2g}+a_1 s^{2g-1}+\cdots+a_g s^g+\cdots+a_1 q^{g-1}s+q^g-1+s+\cdots+s^{n-1}) \equiv 0 \bmod l$.

Using $(u_0, \ldots, u_{n-2})$ as a key we can obtain at most $|R|^{n-1} = q^{g(n-1)}$ or l – whichever smaller – different numbers $u_0+\cdots+u_{n-2}s^{n-2} \bmod l$. This time we do not include $-q^g/2$ in R for even characteristic to avoid ambiguity. If $l < q^{g(n-1)}$ then we know that collisions do occur. We should exclude this case – or choose a shorter key-length if l is that small. Since the experiments showed that in fact there are elements with expansions longer than $n-1$ not all l multipliers can occur.

Now assume that for a given curve considered over $\mathbf{F}_{q^n}$ all $m \bmod l$ have an expansion of length at most $n+4g+2$ and that the large prime divisor l is of size $\sim q^{ng}$. Thus taking only those elements of length $\leq n-1$ we loose at most $q^{g(n+4g+2)} - q^{g(n-1)}$ multipliers. But since we started with l different numbers the left-over $\sim q^{gn} - (q^{g(n+4g+2)} - q^{g(n-1)})$ is negative, thus this bad case cannot happen. Furthermore we know from the experiments that there are expansions of length $\leq n-1$.
Now let N be the number of different elements $\leq l$ representable by $n-1$ digits. If two expansions represent the same number this means that they differ by a multiple of l if the root τ is identified with the integer s. Hence there exists a representation of $0 \bmod l$ given by $s_0 + s_1 s + \cdots + s_{n-2}s^{n-2}$, where $s_i \in \{0, \pm 1, \ldots, \pm q^g - 1\}$. The worst thing that could happen is that one element occurs all the possible $q^{g(n-1)} - N$ times. We now motivate that this case is impossible to happen.
If there are several ways of representing the same multiplier this means that there exists a representation $s_0 + s_1 s + \cdots + s_{n-2}s^{n-2} \equiv 0 \bmod l$ with very small

coefficients. Thus one can also add and subtract multiples of this representation to many other expansion. Take one expansion $(u_0, \ldots, u_{n-2})$ which satisfies $u_i + ks_i \in R$ for $0 \leq i \leq n-2$ for K integers k, then this multiplier occurs at least K times. If the length of the nontrivial representation of $0 \bmod l$ is shorter then we also have to take into account shifted combinations.
Therefore there are several integers $\bmod l$ that are represented by different expansions. Thus the amount of $q^{g(n-1)} - N$ multiple occurrences spreads over several elements.
Hence, one can say that the representable integers modulo l represented by the vectors $(u_0, \ldots, u_{n-2})$ are almost equally distributed. Furthermore before choosing a curve one should run some experiments to know whether representations of $0 \bmod l$ of small length and with small coefficients exist, since this would imply that many elements occur very often in the expansions of length $\leq n-1$, thus N would be comparably small. Hence, one should at least exclude representations of 0 involving only the digits $0, \pm 1$ (and ± 2 for $q > 2$). Equivalently one can use the method of τ-adic expansion described in the preceding sections to get statistical data on how many of the elements allow a short representation, thus an approximation of N.

Example 14.1 *Consider the binary curve of genus 2 given by*

$$C : y^2 + (x^2 + x + 1)y = x^5 + x^4 + 1$$

with characteristic polynomial of the Frobenius endomorphism $P(T) = T^4 - 2T^3 + 3T^2 - 4T + 4$. *For the extension of degree* 89 *the class number is almost prime*

$$|\mathrm{Pic}^0(C/\mathbf{F}_{q^{89}})| = 2 \cdot 191561942608242456073498418252108663615312031512914969.$$

Let l be this large prime number. The operation of the Frobenius endomorphism on the cyclic group of this prime order corresponds to the multiplication by $s = -10909476359861941088449855420776379666052262767680104 1 \bmod l$. *Choosing a sequence of* 88 *elements u_i from* $R := \{-1, 0, 1, 2\}$ *at random and computing* $\sum_{i=0}^{87} u_i s^i \bmod l$ *we get the multiplier corresponding to the key* $(u_0, \ldots, u_{87})$. *If two sums represent the same integer modulo l then their difference has coefficients in* $0, \pm 1, \pm 2, \pm 3$. *To get the correct probabilities of occurrence we used the following mulitset* $U := \{-3, -2, -2, -1, -1, -1, 0, 0, 0, 0, 1, 1, 1, 2, 2, 3\}$ *and computed 10,000,000 such sums modulo l. The zero sum never occurred.*
Hence, there are no obvious weaknesses and this curve is probably suitable for using this modified set-up.

Note that the security of the modified system is unchanged since only a brute-force search throughout the keyspace can make use of the reduced amount of possible keys. The standard algorithms for computing the discrete logarithms

cannot make use of the fact that the last digits of the base τ expansion of the exponent are zero.
To conclude one can say that using this modified system saves the time needed to compute the expansion without weakening the system.
Furthermore one can restrict the key size even more by choosing a smaller set of digits for the τ-adic expansion. This reduces the storage requirements and the possibility of collisions but for extreme choices – like $R' = \{0, \pm 1\}$, thus without precomputations – one has to be aware of brute force attacks. If one tries to get around these by using longer keys of length $n+k$ collisions get more likely since one has to deal with $1 + s + \cdots + s^{n-1} \equiv 0 \bmod l$, thus for example the zero element occurs at least $2\binom{k+r'_{\max}-1}{r'_{\max}} + 1$ times, where $r'_{\max}$ is the maximal coefficient of R'.
Another idea is to consider only sparse representations to reduce the complexity. But this reduces the size of the key-space, such that collisions get more likely.

15 Outlook

In this section we investigate to what extend these results can be generalized. Furthermore we consider some prerequisites the field has to satisfy.

Throughout the whole discussion we only made use of the characteristic polynomial of the Frobenius endomorphism and its structure. Thus all the bounds on the length and density hold as soon as we consider an expansion to the base of a root of a polynomial of this shape. Hence, as soon as we can make use of the Frobenius efficiently – as for superelliptic or more general for C_{ab} curves where the elements of $\mathrm{Pic}^0(X/\mathbf{F}_{q^n})$ are represented by polynomials – all results carry through. This is also true for the recurrence sequences to compute the class number given P for the ground field. In this paper we restrict to hyperelliptic curves to shorten the explanations. The reader interested in the arithmetic of C_{ab} curves may consult Gurel [18] and Harasawa and Susuki [19].

When choosing a curve for "real-life" application one should not only look for the right order and the other security issues pointed out here but also make sure that the finite field is such that the arithmetic can be performed efficiently. Thus the choice of curves – or more correctly field extensions – is reduced. First of all we need to ensure that we are working in a field for which a normal basis exists such that the arithmetic of the field is not significantly slower than for a polynomial basis with a sparse polynomial. Using Gauss periods and – if necessary – working with a polynomial basis of a small extension field one obtains a field arithmetic much faster than using a matrix based multiplication. Furthermore it is also possible to use the Frobenius automorphism of the finite field for the arithmetic in the ground field. This is extremely interesting if one works in characteristic 2 since then squarings in the usual square and multiply method are for free. A generalization to composite Gauss periods was recently investigated by Nöcker [38]. It is a topic of current research to find optimal choices for a pair curve and finite field. For hardware implementations it is also useful to work over fields of characteristic 2.

A different approach was used by Lee [26]. He considers optimal extension fields. In these fields one uses a polynomial basis but the defining polynomial of the extension is a binomial, thus the multiplication of two field elements is as fast as possible. The action of the Frobenius endomorphism is made efficient by precomputations and table look-ups – thus it is slower than for the normal basis representation. Therefore he stores $\sigma^i D$ for all powers needed. On the other hand he avoids to store the multiples of D with the elements of R since in his case the size of R is large and n is comparably small. Using this approach he is not able to exploit the full power of using the Frobenius endomorphism on the curve, for example he lets the Frobenius operate only on D. His algorithm is similar to that in Section 13 but after computing the τ-adic representation like in Section 9 he reduces the length to n using $\tau^n - 1$, allowing larger coefficients. Since for an average element the expansion is of length slightly larger than n he almost always obtains coefficients of double size. Therefore he needs twice as many doublings and approximately the same number of additions compared to our algorithm.
The provided example does not seem to be optimal since the degree of extension used is only 13, thus fairly small (and he proposes even smaller extensions) and one has to be aware of Weil descent attacks which might work for these degrees as well.

In this article we did not deal with the standard arithmetic in the ideal class group except for stating Cantor's algorithm. For hyperelliptic curves of genus two and over fields of odd characteristic there exists a different approach similar to the elliptic curve case. Spallek [54] developed in her thesis explicit formulae for addition and doubling that have also been used and modified by Krieger [25]. These formulae can only be used for ideal classes, where the first polynomial of the reduced ideal is of the maximal degree g, thus for those not corresponding to divisor classes in the thetadivisor. Optimized formulae have been obtained by Harley [14, 20] and can be downloaded from the second reference. We can also combine the use of the Frobenius endomorphism with these algorithms. For genus two these formulae seem to be faster than the standard algorithm but for larger genus the number of different cases to consider increases and the dependencies get too involved. But for an implementation on a small device it might be useful to take these equations and also generalize them to characteristic two.

To set up a system one needs a divisor class of full order. Let $|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| = kl$. Choosing a point $P = (a, b) \in C/\mathbf{F}_{q^n}$ at random as described in Koblitz [21], interpreting $C - \infty$ as a representative of a divisor class, i. e. taking the reduced ideal $D = [x - a, b]$ and computing kD either leads to an ideal class of order l or to the neutral element. In the second case one has to try again with a different choice of the point. If one uses the explicit formulae one has to work with reduced ideals with first polynomial of degree g. Then choosing points at random until one obtains a reduced divisor of full degree, computing the corresponding reduced ideal and then computing the k-fold can be used.
Like in the elliptic curve case one need not store both components of the divisor class – the first "coordinate" and appropriately chosen bits to remember the signs suffice.

16 Acknowledgments

This work is part of my Ph.D. thesis. Special thanks go to my supervisor Professor Gerhard Frey for good advice and encouragement.
I would also like to thank the people from the IEM in Essen and the members of the graduate school on "Mathematische und ingenieurwissenschaftliche Methoden für sichere Datenübertragung und Informationsvermittlung" for discussions and interest. I am deeply thankful to Andreas Stein for leading my attention to this interesting topic and for friendly support. I would also like to thank the people from the CACR in Waterloo for helpful discussions. Parts of the work were done during a research visit at the CACR. Furthermore I want to express my gratitude to Guillaume Hanrot, Hendrik W. Lenstra, Michael Pohst, and René Schoof for useful hints. Finally I would like to thank Caroline Ullrich for her patient listening and useful discussions and Claus Diem for proof reading.

References

[1] L. Adleman, J. DeMarrais, M.-D. Huang, A Subexponential Algorithm for Discrete Logarithms over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields, in: *Algorithmic Number Theory Seminar ANTS-I*, Lecture Notes in Computer Science **877**, (Springer 1994), 28-40.

[2] D. Cantor, Computing in the Jacobian of a Hyperelliptic Curve, *Mathematics of Computation* **48** (1987), 95-101.

[3] W. Diffie, M. E. Hellman, New Directions in Cryptography, *Mathematics of Computation* **48** (1976), 95-101.

[4] I. Duursma, P. Gaudry, F. Morain, Speeding up the discrete log computation on curves with automorphisms, in: *Advances in Cryptology, Asiacrypt'99*, Lecture Notes in Computer Science **1716**, (Springer 1999), 103-121.

[5] T. ElGamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Transactions on Information Theory* **IT-31** (1985), 469-472.

[6] A. Enge, Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time, *University of Waterloo Technical Report CORR 99-04* (2000), to appear in Mathematics of Computation.

[7] U. Finke, M. Pohst, Methods for Calculating Vectors of Short Length in a Lattice, *Mathematics of Computation* **44** (1985), 463-482.

[8] G. Frey, H.-G. Rück, A Remark concerning m-Divisibility and the Discrete Logarithm Problem in the Divisor Class Group of Curves, *Mathematics of Computation* **62** (1994), 865-874.

[9] W. Fulton, *Algebraic curves: An Introduction to Algebraic Geometry*, (Benjamin 1969).

[10] S. Galbraith, Supersingular Curves in Cryptography, to appear.

[11] R. Gallant, R. Lambert, S. Vanstone, Improving the Parallelized Pollard Lambda Search on Anomalous Binary Curves, *Mathematics of Computation* **69** (2000), 1699-1705.

[12] P. Gaudry, Algorithmique des courbes hyperelliptiques et applications à la cryptologie, *thèse de doctorat de l'École polytechnique*, (2000).

[13] P. Gaudry, An algorithm for solving the discrete log problem on hyperelliptic curves, in: *Advances in Cryptology, Eurocrypt'2000*, Lecture Notes in Computer Science **1807**, (Springer 2000), 19-34.

[14] P. Gaudry, R. Harley, Counting points on hyperelliptic curves over finite fields, in: *Algorithmic Number Theory Seminar ANTS-IV*, Lecture Notes in Computer Science **1838**, (Springer 2000), 313-332.

[15] P. Gaudry, F. Hess, N. P. Smart, Constructive and destructive facets of Weil descent on elliptic curves, *Preprint* (2000).

[16] D. Gordon, A Survey of fast Exponentiation Methods, *Journal of Algorithms* **27** (1998), 129-146.

[17] C. Günter, T. Lange, A. Stein, Speeding up the Arithmetic on Koblitz Curves of Genus Two, in: *Selected Areas in Cryptography SAC 2001*, Lecture Notes in Computer Science **2012**, (Springer 2001), 106-117; see also *University of Waterloo Technical Report CORR 00-04* (2000).

[18] N. Gurel, Arithmétique des courbes C_{ab}, DEA Algorithmique, Rapport de stage (2000).

[19] R. Harasawa and J. Suzuki, Fast Jacobian Group Arithmetic on C_{ab} Curves, in: *Algorithmic Number Theory Seminar ANTS-IV*, Lecture Notes in Computer Science **1838**, (Springer 2000), 359-376.

[20] R. Harley, Fast arithmetic on genus 2 curves, availiable at `http://cristal.inria.fr/~harley/hyper` (2000).

[21] N. Koblitz, Hyperelliptic Cryptosystems, *Journal of Cryptology* **1** (1989), 139 - 150.

[22] N. Koblitz, CM-curves with good cryptographic properties, in: *Advances in Cryptology - Crypto '91*, Lecture Notes in Computer Science **576**, (Springer 1992), 279-287.

[23] N. Koblitz, An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm, in: *Advances in Cryptology - Crypto '98*, Lecture Notes in Computer Science **1462**, (Springer 1998), 327-337.

[24] N. Koblitz, *Algebraic Aspects of Cryptography*, (Springer 1998).

[25] U. Krieger, Anwendung hyperelliptischer Kurven in der Kryptographie, *Diploma Thesis*, Universität Gesamthochschule Essen (1997).

[26] J. W. Lee, Speeding Up the Arithmetic on the Jacobians of Hyperelliptic Curves, Preprint.

[27] D. H. Lehmer, Factorisation of Certain Cyclotomic Functions, *Annals of Mathematics* **34**(1933), 461-479.

[28] J.-L. Lesage, Equations Diophantiennes et corps quadratiques, *Ph.D. Thesis*, Université de Caen (1998).

[29] D. Lorenzini, *An Invitation to Arithmetic Geometry*, (AMS Graduate studies in mathematics **9** 1996).

[30] D. Maisner, E. Nart, Abelian surfaces over finite fields as jacobians, *Universitat Autonòma de Barcelona, Prepublications 14/2000* (2000)

[31] W. Meier, O. Staffelbach, Efficient Multiplication on Certain Nonsupersingular Elliptic Curves, in: *Advances in Cryptology - Crypto '92*, Lecture Notes in Computer Science **740**, (Springer 1993), 333-344.

[32] A. Menezes, T. Okamoto, S. Vanstone, Reducing elliptic curve discrete logarithms to a finite field, *IEEE Transactions on Information Theory* **39** (1993), 1639-1646.

[33] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, (CRC Press 1996).

[34] A. Menezes, M. Qu, Analysis of the Weil Descent Attack of Gaudry, Hess and Smart, to appear in: *Proceedings of RSA* (2001).

[35] A. Menezes, Y.-H. Wu, R. Zuccherato, An Elementary Introduction to Hyperelliptic Curves, in: N. Koblitz, *Algebraic Aspects of Cryptography*, (Springer 1998), 155-178.

[36] V. Müller, Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two, *Journal of Cryptology* **11** (1998), 219-234.

[37] V. Müller, A. Stein, C. Thiel, Computing Discrete Logarithms in Real Quadratic Congruence Function Fields of Large Genus, *Mathematics of Computation* **68** (1999), 807-822.

[38] M. Nöcker, Data structures for parallel exponentiation, *Ph.D. Thesis*, Universität Paderborn (2001).

[39] T. A. Pierce, The Numerical Factors of the Arithmetic Forms $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$, *Annals of Mathematics* **18** (1916), 53-64.

[40] P. van Oorschot, M. J. Wiener, Parallel Collision Search with Cryptanalytic Applications, *Journal of Cryptology* **12** (1999), 1-28.

[41] S. Pohlig, M. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, *IEEE Transactions on Information Theory* **IT-24** (1978), 106-110.

[42] S. Paulus, H.-G. Rück, Real and imaginary quadratic representations of hyperelliptic function fields, *Mathematics of Computation* **68** (1999), 1233-1241.

[43] J. M. Pollard, Monte Carlo methods for index computation $(\mathrm{mod}\, p)$, *Mathematics of Computation* **32** (1978), 918-924.

[44] J. M. Pollard, Kangaroos, Monopoly and Discrete Logarithms, *Journal of Cryptology*, Online publication: 10 August 2000.

[45] H.-G. Rück, Abelian surfaces and Jacobian varieties over finite fields, *Compositio Math.* **76** (1990), 351-366.

[46] H.-G. Rück, On the discrete logarithm in the divisor class group of curves, *Mathematics of Computation* **68** (1999), 805-806.

[47] T. Satoh, K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, *Commentari Math. Univ. St. Pauli* **47** (1998), 81-92.

[48] I. A. Semaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, *Mathematics of Computation* **67** (1998), 353-356.

[49] J. H. Silverman, *The Arithmetic of Elliptic Curves*, (Springer 1986).

[50] N. P. Smart, The Discrete Logarithm Problem on Elliptic Curves of Trace One, *Journal of Cryptology* **12** (1999), 193-196.

[51] N. P. Smart, Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic, *Journal of Cryptology* **12** (1999), 141-151.

[52] J. Solinas, An Improved Algorithm for Arithmetic on a Family of Elliptic Curves, in: *Advances in Cryptology - Crypto '97*, Lecture Notes in Computer Science **1294**, (Springer 1997), 375-371.

[53] J. Solinas, Efficient arithmetic on Koblitz curves, *Journal of Designs, Codes and Cryptography* **19** (2000), 195-249.

[54] A. M. Spallek, Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen, *Ph.D. Thesis*, Universität Gesamthochschule Essen (1994).

[55] A. Stein, Sharp Upper Bounds for Arithmetic in Hyperelliptic Function Fields, *University of Waterloo Technical Report CORR 99-23* (1999).

[56] A. Stein, Introduction to the Arithmetic in Real Quadratic Function Fields, availiable at
`http://www.math.uiuc.edu/ andreas/articles/introcfe.ps.gz`
(1999).

[57] A. Stein, E. Teske, Explicit bounds and heuristics on class numbers in hyperelliptic function fields, *University of Waterloo Technical Report CORR 99-26* (1999).

[58] H. Stichtenoth, *Algebraic Function Fields and Codes*, (Springer 1993).

[59] J. Tate, Endomorphisms of Abelian Varieties over Finite Fields, *Inventiones mathematicae* **2** (1966), 134-144.

[60] E. Teske, Speeding up Pollard's rho method for computing discrete logarithms, in: *Algorithmic Number Theory Seminar ANTS-III*, Lecture Notes in Computer Science **1423**, (Springer 1998), 541-554.

[61] A. Weng, Constructing hyperelliptic curves of genus 2 suitable for cryptography, *Preprint*, Universität Gesamthochschule Essen (2000).