Efficient Arithmetic on Hyperelliptic Curves

Dissertation

zur Erlangung des Grades eines
Doktors der Naturwissenschaften
(Dr. rer. nat.)

Dem Fachbereich 6
(Mathematik und Informatik)
der
Universität-Gesamthochschule Essen
vorgelegt von

Tanja Lange
aus Bad Gandersheim

Essen, 21.08.2001

Tag der Disputation: 15.01.2002

Vorsitzender:	Prof. Dr. K.J. Witsch
1. Gutachter:	Prof. Dr.Dr.h.c. G. Frey
2. Gutachter:	Prof. Dr. Y.J. Choie
3. Gutachter:	Prof. Dr. Dobbertin

To Wolfgang,
to my parents

Zusammenfassung der Dissertation

Als Koblitz-Kurven bezeichnet man hyperelliptische Kurven vom Geschlecht g, die über einem Körper kleiner Ordnung definiert sind, allerdings über einem Erweiterungskörper dieses Körpers betrachtet werden. Ein großer Vorteil dieser Kurven ist es, dass die Klassenzahl einfach bestimmbar ist. Um zu garantieren, dass die Pohlig-Hellman-Attacke nicht funktioniert, muss die Gruppenordnung durch eine große Primzahl teilbar sein, so dass es wichtig ist, die Gruppenordnung zu kennen. Für eine beliebige Kurve über einem Primkörper kann diese allerdings noch nicht in der Größenordnung der kryptographischen Sicherheit bestimmt werden. Die Arbeit liefert über Körpern der Charakteristik $2, 3$ und 5 Kurven vom Geschlecht $2, 3$ und 4, deren Klassenzahlen einen Primfaktor in der gewünschten Größenordnung haben. Die vollständigen Listen sind im Internet öffentlich zugänglich gemacht worden
(siehe http://www.exp-math.uni-essen.de/∼lange/KoblitzC.html).
Da für diese Kurven Körper der Charakteristik zwei besonders interessant sind, jedoch bislang noch niemand für diese Körper explizite Formeln für die Arithmetik in den Divisorklassengruppen bestimmt hat, werden diese für Kurven vom Geschlecht zwei ermittelt. Für Kurven größeren Geschlechts würden solche Formeln eine noch umfangreichere Fallunterscheidung bedeuten, so dass der allgemeine Algorithmus von Cantor schneller ist.

Der Frobeniusautomorphismus des endlichen Körpers hat eine natürliche Fortsetzung auf die Funktionenkörper und damit auch auf die Divisoren. Werden die Elemente des Erweiterungskörpers bezüglich einer Normalbasis dargestellt, so bedeutet die Operation des Frobenius nur zyklisches Vertauschen, welches keine Kosten verursacht. Die Hauptoperation im ElGamal-Kryptosystem, beim Diffie-Hellman-Schlüsselaustausch und auch beim Signieren ist die Berechnung des m-Fachen eines Gruppenelements. Üblicherweise wird hierzu die double-and-add-Methode benutzt, die eine binäre Entwicklung von m voraussetzt. Die Operation des Frobeniusendomorphismus lässt sich auch auf den Divisorklassen in der (üblichen) Darstellung mit Hilfe zweier Polynome quasi kostenlos durchführen. Um diesen Kostenvorteil ausnutzen zu können, wird der Multiplikator m nun zur Basis τ entwickelt, wobei τ eine komplexe Zahl ist, so dass die Anwendung des Frobenius genau der Multiplikation mit τ entspricht. Hierdurch kann eine Beschleunigung der Arithmetik erzielt werden. Koblitz hatte ein solches Verfahren für elliptische Kurven vorgeschlagen, in einer Folgearbeit von Solinas wird für elliptische Kurven die größtmögliche Beschleunigung erreicht. Gemeinsam mit C. Günther und A. Stein habe ich das Konzept auf hyperelliptische Kurven verallgemeinert und zwei Kurven vom Geschlecht 2 über Körpern der Charakteristik 2 untersucht. Hierbei wurde eine Beschleunigung um einen Faktor von 5 bzw. bei mehr Vorberechnungen von 7 erzielt.
Ich habe die entsprechenden Ergebnisse auf beliebige endliche Körper und hyperelliptische Kurven höheren Geschlechts verallgemeinert. In der Dissertation habe ich das Problem

der Endlichkeit solcher Darstellungen untersucht und ein Verfahren angegeben, das es erlaubt, die Endlichkeit für eine gegebene Klasse von Kurven nachzuweisen, und dieses für etliche Beispiele durchgeführt. Es werden Algorithmen geliefert, die eine solche Entwicklung berechnen und die leicht an die Bedürfnisse der Implementationsumgebung angepasst werden können, und zwar insofern, als je nach vorhandenem Speicherplatz mehr oder weniger Vorberechnungen gemacht werden, wobei sich Vorberechnungen durch eine Beschleunigung auszahlen. Die Arbeit gibt Längenabschätzungen für die erwähnten Entwicklungen, eine Strategie, um die Länge zu reduzieren, und beschäftigt sich mit dem Auftreten von periodischen Entwicklungen. All diese Abschätzungen werden mit einer Fülle experimenteller Daten belegt, so dass erkennbar wird, dass für die betrachteten Erweiterungskörper bereits die asymptotischen Ergebnisse mit hoher Genauigkeit zutreffen. Die Beschleunigung ist für Kurven höheren Geschlechts und größerer Charakteristik größer, jedoch wird dann auch mehr Speicher benötigt. Den Fall, dass gar kein Speicher zur Verfügung steht, habe ich ebenfalls behandelt und dabei theoretische Abschätzungen über die dennoch zu erwartende Beschleunigung geliefert.
Außerdem stelle ich eine alternative Konstruktion des Systems vor, bei der – anstatt eine zufällig gewählte Zahl mit den angegebenen Algorithmen zu entwickeln – als Schlüssel eine Entwicklung fester Länge gewählt wird, deren Koeffizienten aus einer beschränkten Menge stammen. Ich habe untersucht, wie sich die üblichen Protokolle für diese Konstruktion übertragen lassen, mich mit Kollisionen beschäftigt und die Sicherheit gegen einen aus Arbeiten von Nguyen und Shparlinski verallgemeinerten Angriff untersucht.
Im letzten Teil der Arbeit wird der konstruktive Weil-Descent beschrieben. Ausgangspunkt ist eine hyperelliptische Kurve vom Geschlecht 2, definiert über einem hinreichend großen primen Grundkörper $\mathbf{F}_p$, so dass $p^4 \sim 2^{160}$ ist, deren Klassenzahl für die Kurve über $\mathbf{F}_{p^3}$ einen großen Primfaktor der Ordnung p^4 hat. Wird nun der Weil-Descent durchgeführt und zieht man nur solche Elemente in Betracht, die in der Spur-Null-Varietät liegen, so erhält man eine Abelsche Varietät mit einer Gruppe der Ordnung der großen Primzahl. Das Gruppengesetz und auch die Ausnutzung des Frobeniusendomorphismus kann man von der ursprünglichen Kurve übertragen. Somit erhält man eine weitere Gruppe, die in der Kryptographie genutzt werden kann und die zusätzlich eine Arithmetik unter Ausnutzung des Frobeniusendomorphismus ermöglicht. Für diese Gruppe schlage ich das Verfahren vor, das für die Koblitz-Kurven oben als alternative Konstruktion beschrieben wurde. Die Komplexität der Berechnung von Vielfachen einen Gruppenelements wird für die Spur-Null-Varietät und algebraische Gruppen gleicher Sicherheit bestimmt. Ist der Körper so gewält, dass es ein kleines Element η gibt, das keine dritte Potenz ist, so ist die Arithmetik in dieser Varietät schneller als in der Divisorklassengruppe einer hyperelliptischen Kurve, die über einem Primkörper definiert ist und gleiche Gruppengröße hat. Vergleichen mit elliptischen Kurven ist die Arithmetik stets langsamer.

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen verwendet habe.

Tanja Lange
Essen, den 21.08.2001

Acknowledgments

First of all I would like to express my gratitude to my supervisor Professor Gerhard Frey for good advice and encouragement.
Thanks to Guido Blady for providing me with the timings and to him and to Roberto Avanzi for pointing out some details for the arithmetic in the finite fields in Section 6.3, to Annegret Weng for computing the example presented in Section 6.5 for the trace zero subgroup, and to Claus Diem and Ralf Gerkmann for proofreading parts of the thesis. 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. Furthermore I would 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. Finally I want to express my gratitude to Guillaume Hanrot, Hendrik W. Lenstra, Michael Pohst, and René Schoof for useful hints.

Contents

Chapter 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 [9] and the ElGamal cryptosystem [11] 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 C 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 [55, 58, 59, 75]) apply, unless the curve has a special structure, for example is supersingular (see Frey and Rück [14] and Menezes, Okamoto, and Vanstone [44]) or the group order is divisible only by small primes, thus weak under the Pohlig-Hellman attack [56]. But there is a big drawback – an addition on an elliptic curve takes 2 multiplications, 1 squaring, and 1 inversion in the underlying field. To obtain a speed-up for the main operation – computing m-folds – Koblitz [34] 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 a map on the curve that induces an endomorphism on the Jacobian of C 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 [34, 35], Meier and Staffelbach [43], Müller [48], Smart [66], and Solinas [67, 68], where the last reference contains a detailed analysis of the maximal speed-up achievable for curves over $\mathbf{F}_2$.

In [33] 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 [22] 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 [69] suggested the use of curves with complex multiplication, so called CM-curves. This approach was investigated in more detail by Weng [76]. 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 here 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 [49], and Enge [12]. Gaudry [21] 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 only the generic attacks apply provided that the group order is sufficiently large and that one avoids curves for which special attacks are known.

In this thesis we investigate *hyperelliptic Koblitz curves*. The idea of elliptic Koblitz curves was generalized by Günther, Lange, and Stein [26]. In that article 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.
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.
For Koblitz curves it is interesting to work over a field of even characteristic. In the case of odd characteristic it is reported that explicit formulae are faster than Cantors algorithm. However, no-one has generalized these equations to even characteristic so far.

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: For fixed n 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 [18] designed for elliptic curves was extended to hyperelliptic curves. Duursma, Gaudry, and Morain [10] 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 [21] 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 [63] (see also Satoh and Araki [62], and Smart [65]) for elliptic and by Rück [61] 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 [14]. 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 [23] 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 [46]) – or more generally – leads to a curve with such a large genus that the attack gets infeasible. Although Gaudry, Hess, and Smart [23] 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.

Naumann [51] and Diem [7] propose a further abelian group constructed by means of algebraic geometry for use in cryptography. They start with an elliptic curve defined over the prime field $\mathbf{F}_p$ and consider it over $\mathbf{F}_{p^3}$. Then they impose the condition $\sigma^2(P) + \sigma(P) + P = 0$ on the points and obtain the *Trace-zero-hypersurface*. It is an abelian variety of dimension 2 defined over the above prime field which is not isogenous to the Jacobian of a curve. Hence, it is a new way to construct suitable groups. The drawback is that to perform the arithmetic one can only make use of the formulae for the elliptic curve over $\mathbf{F}_{p^3}$ which involves more variables than would actually be needed, but the group has the advantage that we can also make use of the Frobenius endomorphism to speed up the computation of m-folds and the security is equivalent to that of a curve defined over a prime field.

In the second part of the thesis we investigate the trace zero subgroup in case of a genus two curve defined over a comparably large prime field ($p \sim 2^{40}$) considered over $\mathbf{F}_{p^3}$. This group can be viewed as a 4-dimensional abelian variety over the prime ground field, but still we can use the Frobenius endomorphism of the original curve. We show that the curve itself and the divisor classes belonging to the ground field lie outside this group. Like for elliptic curves one can use the arithmetic from the larger divisor class group for $\mathbf{F}_{p^3}$ and also the speed-up from the endomorphism. We compare the complexity of computing m-folds in this group to other groups with similar parameters like the Divisor class group of a genus two curve over $\mathbf{F}_{p'}$, $p' \sim p^2$ prime, and an elliptic curve over the prime field $F_{p''}$, $p'' \sim p^4$.

The remainder of this paper is organized as follows. In the next chapter we provide the necessary mathematical background, followed by a chapter on the computation in the Picard group in the case of even characteristic. The next chapter deals with the computation of the group order. We include some experimental data concerning group orders of Koblitz curves over several finite fields. Chapter 5 is the core of this thesis dealing with the arithmetic in the Picard group for Koblitz curves. Section 5.1 is devoted to the standard ways of computing m-folds which will be used to compare our results with. In Section 5.2 we show how to make use of the Frobenius endomorphism to achieve a speed-up in computing m-folds. Sections 5.3, 5.4 and 5.5 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 5.7 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.
In Chapter 6 we deal with the trace zero subgroup, where in the first section we show which kinds of divisor classes can lie in this subgroup, then we try to find equations describing the subgroup using less variables, i. e. such that the length of an element is not too large for a group of order p^4. In Section 6.4 the computation in the subgroup is investigated in more detail, and in the next section we compare the efficiency of the group operation in this group to others obtained using algebraic geometry which have similar security parameters. Finally, we present some examples in Section 6.5. To conclude we deal with side-channel attacks and give an outlook on what can be done as well in Chapter 7.

After finishing this thesis it was brought to our attention that Lee [38] has also generalized the results of Günther, Lange, and Stein [26] 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 5.8.

Chapter 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 [41] and also adopt his notation. Most of the results can be found as well in the book of Stichtenoth [73]. For the more geometric approach see Fulton [15]. You can as well consider Gaudry's thesis [20] 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 [47] to get an insight in hyperelliptic curves and skip the first section. Furthermore Silverman's book [64] contains a lot of the theory not only for elliptic curves.

2.1 Notation and Definitions

Throughout this thesis 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 *An* algebraic function field L/k in one variable over k *is an extension field $L \supseteq k$ such that L is a finite algebraic extension of $k(x)$ for an element $x \in L$, where x is transcendental over k. The* constant field *is $\{x \in L | x \text{ is algebraic over } k\}$. It is a subfield of L containing k and L is an algebraic function field over this field as well.*

We only consider algebraic function fields in one variable L/k where k is the full constant field. Hence, we always implicitly mean this when speaking of a function field.

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 as the field of fractions of $k[x,y]/(F)$.*

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 $g \in M^i$. As M/M^2 is nonempty there is an element $g \in B$ with $v(g) = 1$. Thus to each maximal ideal corresponds a surjective valuation. Now let v be a surjective valuation such that $v(B) \geq 0$. Consider the sets $\mathcal{O}_v = \{\alpha \in L | v(\alpha) \geq 0\}$ and $\mathcal{M}_v = \{\alpha \in L | v(\alpha) > 0\}$. Then $\mathcal{O}_v$ is a local Noetherian domain with $\mathcal{M}_v$ as its maximal ideal, and $\mathcal{M}_v$ is principal as it is generated by an $\alpha \in L$ with $v(\alpha) = 1$. Put $M = \mathcal{M}_v \cap B$. Then M is a maximal ideal of B. This way one sets up a bijection between the set of surjective valuations v with $v(B) \geq 0$ and the set of maximal ideals of B.

Let $\mathcal{V}(L/k)$ be the set of all surjective valuations of L that are 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 additional elements at infinity.

Example 2.4 *Assume that* k *is an algebraically closed field. Let* $F \in k[x, y]$ *be an absolutely irreducible polynomial of degree* > 1 *monic in* y. *Put* L *the function field obtained as the quotient field of* $k[x, y]/(F)$. *First of all we establish a bijection between the maximal ideals of* $k[x, y]/(F)$ *and the tuples* $(a, b) \in k^2$ *with* $F(a, b) = 0$. *Note that the maximal ideals in* $k[x, y]/(F)$ *correspond to maximal ideals of* $k[x, y]$ *containing* F.

Let $a, b \in k$ *with* $F(a, b) = 0$. $\mathcal{P} = (x - a, y - b)$ *is a maximal ideal in* $k[x, y]/(F)$ *as* $k[x, y]/(x - a, y - b)$ *is isomorphic to* k *and* $F \in (x - a, y - b)$ *as* $F(a, b) = 0$.
Let M *be a maximal ideal of* $k[x, y]/(F)$ *and let* $\tilde{M}$ *be the corresponding maximal ideal in* $k[x, y]$ *containing* F. *Put* $P = \tilde{M} \cap k[x]$. P *is a nonzero prime ideal of* $k[x]$, *and as* k *is algebraically closed we have* $P = (x - a)$ *for some* $a \in k$. *Consider the image of* $\tilde{M}$ *in* $k[x, y]/(x - a) \cong k[y]$. *It is given by* $(y - b)$ *for* $b \in k$, *hence* $\tilde{M} = (x - a, y - b)$. *As* $F \in \tilde{M}$ *we have that* $F(a, b) = 0$ *and* $M = (x - a, y - b)$.
Now we can associate to $M = (x - a, y - b)$ *the local ring* $\mathcal{O}_M = \{\alpha \in L | \alpha$ *is defined at* $(a, b)\}$ *with maximal ideal* $\mathcal{M}_M = \{\alpha \in \mathcal{O}_M | \alpha(a, b) = 0\}$ *of* $\mathcal{O}_M$. *The maximal ideal* $M = (x - a, y - b)$ *leads to a surjective valuation iff* $\mathcal{M}_M$ *is a principal ideal. These* (a, b) *are*

called nonsingular points. If all points are nonsingular, i. e. $\mathcal{O}_M$ is a local principal Noetherian domain for all (a,b) with $F(a,b) = 0$, then $k[x,y]/(F)$ is a Dedekind domain and we can use the above construction to establish the bijection between maximal ideals and surjective valuations. Hence, to each nonsingular point corresponds a surjective valuation. The set of these valuations is an example of an affine curve. But we are missing some valuations of L, namely those that do not result from $k[x,y]/(F)$ but from other rings contained in L.

Assume now that for an absolutely irreducible polynomial $F \in k[x,y]$ we have that $B = k[x,y]/(F)$ is a Dedekind domain. If k is algebraically closed we obtain each maximal ideal of $k[x,y]/(F)$ via the zeros of F. Let k be not algebraically closed and consider the maximal ideal $\mathcal{M}_v$ of $\mathcal{O}_v$ corresponding to the valuation v with $v(B) \geq 0$. 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 zeroes of F in 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 $\varphi_{(a,b)}$. Like above one shows 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 $u(x)$. Since u is irreducible, $k[x,y]/(u(x))$ is a principal ideal domain and $M/(u(x))$ is generated by a single element, say by the class of $v(x,y)$. Therefore $M = (u(x), v(x,y))$. 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 maximal ideals of $k[x,y]/(F)$, valuations, and local principal ideal domains is fundamental for the definition of curves.

Definition 2.5 *A* nonsingular complete absolutely irreducible 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*. Each point P corresponds to 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 we have $\mathcal{O}_X(X) = k$ since we assume that k is algebraically closed in $k(X)$.
The curves we consider are always absolutely irreducible, thus we implicitly mean this when speaking of a curve.
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 $[k(X) : \varphi^*(k(Y))]$. φ is called* separable *if the extension $k(X)/\varphi^*(k(Y))$ is separable.*
If $\varphi^* : k(Y) \to k(X)$ is an isomorphism of k-algebras, then the corresponding morphism of curves is called an isomorphism*.*

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.*

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 $[k(X) : k(x)]$. Let $P \in \mathbb{P}^1/k$ and let $k(X)/k(x)$ be separable and finite. 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 it contains at least one ramified point of 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 $[k(X) : k(x)] = 2$ and $k(X)/k(x)$ is a Galois extension.*
The map $\iota : X \to X$ that maps $P \in X$ to the other point in the fiber of $\pi(P)$ and fixes the ramified points is called the hyperelliptic involution*.*

Alternatively one calls a curve X/k hyperelliptic if it is not the projective line and there exists a separable 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 $F(x,y) = y^2 - f(x) \in k[x,y]$ and $f(x)$ is squarefree. In characteristic 2 a separable 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 $F(x,y) = y^2 - y - f(x)$ with $f(x) \in k(x)$. Clearing denominators and changing variables one can as well obtain a representation via $\tilde{F}(u,v) = v^2 + h(u)v - \tilde{f}(u)$ with $h, \tilde{f} \in k[u]$. The curve is nonsingular if 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.*

The ramification behavior of ∞, i.e. the extensions of the degree-valuation, will be important for the group we consider later on. Let $v_{\mathfrak{P}_1}, \dots, v_{\mathfrak{P}_r}$ denote the distinct elements in the fiber of ∞.

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

$$(tB') = \begin{cases} \mathfrak{P}_1\mathfrak{P}_2 = (t, \sqrt{\tilde{f}(t)} - b)(t, \sqrt{\tilde{f}(t)} + b) & d \text{ is even and } f_d = b^2 \text{ for a } b \in k, \\ \mathfrak{P} := (tB') & d \text{ is even and } f_d \neq b^2 \text{ for all } b \in k, \\ \mathfrak{P}^2 = (t, \sqrt{\tilde{f}(t)})^2 & d \text{ is odd.} \end{cases}$$

If tB' splits into two different ideals then $L/k(x)$ is called a real quadratic function field, *otherwise it is called* imaginary quadratic. *These notations are used since the respective function 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'. One major topic of this thesis 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 an algebraic extension of k contained in $\overline{k(X)}$. Put $k'(X) := k' \cdot k(X)$ and denote by $X_{k'}/k'$ 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 $\sigma \in \mathrm{Gal}(\bar{k}/k)$ 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.
Consider again $B = k[x, y]/(F)$ for an absolutely irreducible polynomial F such that B is a Dedekind domain. As we have seen at the beginning, the maximal ideals M of B 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). This motivates the following lemma.

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 $\varphi : X \to Y$ of curves over k, 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 φ* can be extended *to the morphism $\varphi' : X_{k'} \to Y_{k'}$. The morphism corresponding to $\bar{k}(Y) \subseteq \bar{k}(X)$ is denoted by $\bar{\varphi}$.*

Consider again Example 2.11.

Example 2.16 *Let $F(x, y) := y^2 - f(x)$ with $f(x) \in k[x]$, $\mathrm{char}(k) \neq 2$, and f has no multiple roots in $\bar{k}$. 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. Assume first that $\deg(f) = d$ is odd. Let V denote the domain of x in $\bar{X}$. By the previous example 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 other ramification points of $\bar{\pi}$ correspond to the d zeros of F of the form $(a_i, 0), f(a_i) = 0$. Thus, the morphism is ramified at $d + 1$ points with ramification index 2.*
If $\deg(f) = e$ is even and the leading coefficient is a square in k, then $\bar{X} \backslash V$ consists of two different 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 $(a_i, 0), f(a_i) = 0$.
Thus, in both cases the number of ramification points is $2\lceil \deg(f)/2 \rceil$ and if in the second case one of the ramification points lies in k one can transform the equations such that an isomorphic curve is described by an equation with f 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 be a function field 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 many $v \in \mathcal{V}(L/k)$.
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 $f \in L^*$ 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 elements of $X_{\bar{k}}$: Let $k(X)/k(x)$ be finite and let P be in the domain of x. Let the maximal ideal M corresponding to P be $M = \mathrm{Ker}\varphi_{(a,b)}$ and put $Q \in X_{\bar{k}}$ the point corresponding to $(x-a, y-b)$. Then $[k(Q) : k] = [\mathcal{O}_P/\mathcal{M}_P : k]$.

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:

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

These equivalence classes of the 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 $\mathrm{Div}(B)/\mathrm{div}_B(L^*)$ (with the group-operation addition of divisor classes) to $\mathrm{Cl}(B)$ (with the group-operation multiplication of ideal classes).

For the restriction map

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

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:*

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

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:

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

We will use the correspondence between $\text{Pic}^0(X)$ and $\text{Cl}(B)$ 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. The same way we can also find a representative for each class by two polynomials. We discuss this in the next section in more detail.

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

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

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 $|\pi^{-1}(\infty)| = r > 1$, 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 $P_1, \dots, P_r$ 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 [41]. For the use of function fields of unit rank ≥ 1 and a comparison of both cases we refer to Paulus and Rück [57] and several works of Stein, for example [71].

Lemma 2.21 *Let $X/\mathbf{F}_q$ be a curve defined over the finite field $\mathbf{F}_q$. Let $\pi^{-1}(\infty) = \{P_1, \dots, P_r\}$. Then we have the following relation between the class number, the ideal class number and the regulator:*

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

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(φ) $= \{0\}$.*

Before we conclude this section we introduce a further invariant of the curves we will need – the genus. 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* $\mathrm{Div}(L)$*:*

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

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 with at least one point is called an* elliptic curve*.*

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

There are some curves where one can read off the genus 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 section, 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 one $\mathbf{F}_q$-rational ramification point of π. Thus the class number $\mathrm{Pic}^0(C/\mathbf{F}_q)|$ and the ideal class number $|\mathrm{Cl}|$ are equal.

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

$$y^2 + h(x)y = f(x) \text{ in } \mathbf{F}_q[x,y], \tag{2.1}$$

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 $\mathbf{F}_q$.*

Furthermore we can identify points P associated to valuations v_P with $v_P(k[x,y]/(F)) \geq 0$ and $\deg P = 1$ with tuples $(a,b) \in \mathbf{F}_q^2$ with $F(a,b) = 0$. And there is a single point not in the domain of x. We denote it by ∞ like in $\mathbb{P}^1(\mathbf{F}_q)$.
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 $\mathbf{F}_{2^{79}}$

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

Consider a point $P \neq \infty$ of C, if $\deg P = n$ then we can find $a, b \in \mathbf{F}_{q^n}$ such that we can identify P with (a,b). Hence, for the points defined over a fixed extension field we can rely on the interpretation of a point as a zero of $y^2 + h(x)y - f(x)$. We have $\iota P = (a, -b - h(a))$, where ι is the hyperelliptic involution. The function $(x - a)$ leads to a divisor $P + \iota P - 2\infty$. Hence, we can achieve that we represent a divisor class by a divisor $D = \sum_{i=1}^r P_i - r\infty$, where $P_i \neq \infty$ and $P_i \neq \iota P_j$ for $i \neq j$. Furthermore one finds a representative with $r \leq g$. Note that D defined over $\mathbf{F}_{q^n}$ does not imply that each P_i is defined over the same field. If P_i is defined over $\mathbf{F}_{q^{nl}}$ then all l conjugates of P_i must also occur in D. Therefore l is bounded by g.

We have seen in the previous section 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 is in $\mathbf{F}_q[x]$, whereas the second one is of the form $y - v(x), v(x) \in \mathbf{F}_q[x]$, 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. In Mumford [50][page 3.17] the following representation is introduced which as well makes explicit the correspondence of ideal classes and divisor classes:

Theorem 2.29 (Mumford Representation)
Let the function field be given via the irreducible polynomial $y^2 + h(x)y = f(x)$, where $h, f \in \mathbf{F}_q[x]$, $\deg f = 2g+1$, $\deg h \leq g$. Each nontrivial ideal class over $\mathbf{F}_{q^n}$ can be represented via a unique ideal generated by $u(x)$ and $y - v(x)$, $u, v \in \mathbf{F}_{q^n}[x]$, where

1. *u is monic,*
2. *$\deg v < \deg u \leq g$,*
3. *$u | v^2 + vh - f$.*

Let $D = \sum_{i=1}^{r} P_i - r\infty$, where $P_i \neq \infty, P_i \neq \iota P_j$ for $i \neq j$ and $r \leq g$. Put $P_i = (x_i, y_i)$. Then the corresponding ideal class is represented by $u = \prod_{i=1}^{r}(x - x_i)$ and if P_i occurs n_i times then $\left(\frac{d}{dt}\right)^j \left[v(x)^2 + v(x)h(x) - f(x)\right]_{|x=x_i} = 0,\ 0 \leq j \leq n_i - 1$.

For short we denote this ideal by $[u, v]$. The inverse of a class is represented by $[u, -h - v]$, where the second polynomial is understood modulo u if necessary. The zero divisor is represented by $[1, 0]$. We now denote the ideals and ideal classes by D due to the relation to the divisors.

The second part of the theorem means that for all points $P_i = (x_i, y_i)$ occurring in the support of D we have that $u(x_i) = 0$ and the third condition guarantees that $v(x_i) = y_i$ with appropriate multiplicity.

Addition of divisor classes means multiplication of ideal classes which consists 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 [4] (for odd characteristic only) and Koblitz [33] 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 [4], Koblitz [33], Krieger [37], Menezes et.al. [47] 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 addition whereas doubling takes $16g^2 + O(g)$ operations (see Stein [70]). Improvements are possible in special cases.

Algorithm 2.30 (Composition)
`INPUT:` $D_1 = [u_1, v_1], D_2 = [u_2, v_2]$,
$C : y^2 + h(x)y = f(x)$.
`OUTPUT:` $D = [u, v]$ *semireduced with* $D \equiv D_1 D_2$.

1. *compute* $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$;
2. *compute* $d = \gcd(d_1, v_1 + v_2 + h) =$
$= c_1 d_1 + c_2(v_1 + v_2 + h)$;
3. *let* $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$;
i.e. $d = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2 + h)$;

4. $u = \frac{u_1 u_2}{d^2}$;
$v = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \bmod u$.

Algorithm 2.31 (Reduction)
`INPUT:` $D = [u, v]$ *semireduced.*
`OUTPUT:` $D' = [u', v']$ *reduced with* $D \equiv D'$.

1. *let* $u' = \frac{f - vh - v^2}{u}$;

   $v' = (-h - v) \bmod u'$;

2. *if* $\deg u' > g$ *put* $u := u', v := v'$ *goto step 1;*

3. *make* u' *monic.*

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 over $\mathbf{F}_q$. Extending the concept of extension of scalars to the Picard group we put

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

From now on we omit the index of X unless confusion might occur.
For the group order we have the following bound depending only on the finite field and the genus of the curve:

Theorem 2.32 (Hasse-Weil)

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

Thus $N_n = q^{ng} + O(q^{n(g-1/2)})$.

Denote by M_r the number of points of $X_{\overline{\mathbf{F}}_q}$ 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 $X/\mathbf{F}_q$. The zeta function is proved to be rational (see [41][Chapter VIII] and [73][Chapter V]). It can 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 2.33 *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. *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 as $P(1)$. 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.
For further reference we give the following rather inexact definition:

Definition 2.34 *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 Chapter 4 we explain the details on the computation of $P(T)$ and the class number for extension fields 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 [60] shows for hyperelliptic curves of genus 2 that in the case of irreducible $P(T)$ we even have

$$2|a_1|\sqrt{q} - 2q < a_2 < a_1^2/4 + 2q, \tag{2.2}$$

$a_1^2 - 4a_2 + 8q$ is not a square, and some conditions on the divisibility of a_1 and a_2 by p hold. 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 both representations – as $\exp\left(\sum_{n=1}^{\infty} M_n t^n/n\right)$ and as $\frac{L(t)}{(1-t)(1-qt)}$.

Let $P(T) = T^{2g}+a_1T^{2g-1}+a_2T^{2g-2}+\cdots+a_gT^g+qa_{g-1}T^{g-1}+\cdots+q^{g-1}a_1T+q^g$ correspond to the curve $X/\mathbf{F}_q$ and let $Y/\mathbf{F}_q$ be a quadratic twist of X. One can show that for Y the polynomial is of the form $T^{2g}-a_1T^{2g-1}+a_2T^{2g-2}+-\cdots+-a_gT^g+-qa_{g-1}T^{g-1}+-\cdots-q^{g-1}a_1T+q^g$.

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* as the Jacobian varieties of the curves are isogenous. The *Jacobian variety* $\mathbf{J}$ associated to a curve is an abelian variety, i. e. a nonsingular, complete variety with group operations given by regular maps. It 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 is in bijection with the group $\mathrm{Pic}^0(X_{\bar{\mathbf{F}}_q}/\bar{\mathbf{F}}_q)^{\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_{q^n})}$ and such that for a given $\mathbf{F}_q$-rational point P_0 of X there exists a morphism $\phi : X \to \mathbf{J}$ that sends P_0 to the identity element of $\mathbf{J}$. This morphism induces the map $\mathrm{Div}^0(X/\bar{\mathbf{F}}_q) \to \mathbf{J} : \sum n_iP_i \mapsto \sum n_i\phi(P_i)$ which gives an isomorphism $\mathrm{Pic}^0(X/\bar{\mathbf{F}}_q) \to \mathbf{J}(\bar{\mathbf{F}}_q)$. The dimension of $\mathbf{J}$ is the genus of X. Two abelian varieties A and B are isogenous if there exists a surjective homomorphism $\lambda : A \to B$ whose kernel is finite.

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 $\mathbf{F}_{q^{kn}}$, and 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, Okamoto, and Vanstone [44] 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 [14] which works as well 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 [16] 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.
Since we do only use the concept of supersingularity to exclude some curves, we shall use the criterion to detect them (see Galbraith [16] and Tate [74]) as a definition.

Definition 2.35 *Suppose $q = p^r$ and suppose $\mathbf{J}$ is the Jacobian variety of a hyperelliptic curve of genus g over $\mathbf{F}_q$. Suppose*

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

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 will be large depending on n, whereas for supersingular curves it is always small.

Example 2.36 *Put $p = 2$. Galbraith [16] shows that every nonsingular curve of the form*

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

is supersingular.

2.4 The Frobenius Endomorphism

In this section we define the Frobenius endomorphism of a curve and give its characteristic polynomial. Also in this section the results hold for arbitrary curves defined over a finite field $\mathbf{F}_q$.

Let k be a perfect field of characteristic $p > 0$ and denote by $\bar{k}$ its algebraic closure.
Let us first motivate our studies by an example:

Example 2.37 *Let $F \in \bar{k}[x,y]$ be irreducible and assume that $\bar{k}[x,y]/(F)$ is a Dedekind domain. For $F = \sum a_{ij}x^i y^j$ put $F^{(p^n)} = \sum a_{ij}^{p^n} x^i y^j$. Then the map*

$$(\varphi^n)^* : \bar{k}[x,y]/(F^{(p^n)}) \to \bar{k}[x,y]/(F), \text{ class of } g(x,y) \mapsto \text{ class of } g(x^{p^n}, y^{p^n})$$

is a homomorphism of $\bar{k}$-algebras. It induces a morphism of the corresponding curves whose restriction to the zeros of F respectively $F^{(p^n)}$ maps (a,b) to (a^{p^n}, b^{p^n}). The image of $(\varphi^n)^*$ in $\bar{k}[x,y]/(F)$ is the set of p^n-th powers as $(g^{(1/p^n)}(x,y))^{p^n} = g(x^{p^n}, y^{p^n})$.

For a k-algebra R let $\mathrm{Frob}_R : R \to R, r \mapsto r^p$ and denote by R^p the image of Frob_R in R. Now let $K/k(x)$ be a finite extension. The diagram

$$\begin{array}{ccccc}
K & \overset{(\mathrm{Frob}_K)^n}{\to} & K^{p^n} & \subseteq & K \\
\uparrow & & \uparrow & & \uparrow \\
k(x) & \overset{(\mathrm{Frob}_{k(x)})^n}{\to} & k(x)^{p^n} & \subseteq & k(x).
\end{array}$$

together with $k(x)^{p^n} = k(x^{p^n})$ shows that $[K : K^{p^n}] = p^n$. The inclusion $K^{p^n} \subseteq K$ leads to a homomorphism of k-algebras .

Definition 2.38 *Let k be a perfect field. Let $k(X)/k(x)$ be the function field of a complete nonsingular curve X/k. Then $k(X)^{p^n}/k$ is the function field of a complete nonsingular curve denoted by $X^{(p^n)}/k$. The inclusion $k(X)^{p^n} \subseteq k(X)$ defines a completely inseparable morphism of complete curves over k of degree p^n:*

$$\varphi^n : X \to X^{(p^n)}.$$

Now let $k = \mathbf{F}_q$ where $q = p^r$ and let X/k be a nonsingular complete curve. Then $(\mathrm{Frob}_{k(X)})^r : k(X) \to k(X)^{p^r}$ induces the identity restricted to k and hence leads to an isomorphism of k-algebras. It induces an isomorphism of curves $\psi : X^{(p^r)} \to X$. The concatenation of φ^r and ψ leads to an endomorphism of X.

Definition 2.39 *Let $X/\mathbf{F}_q$ be a nonsingular complete curve. The endomorphism $\sigma : X \to X$ given by $\sigma = \psi \circ \varphi^r$ is called the* Frobenius endomorphism of X over $\mathbf{F}_q$.

The map σ^* can be extended to a map $\bar{\sigma}^* : \bar{\mathbf{F}}_q(X) \to \bar{\mathbf{F}}_q(X)$, $\sum_{i=1}^s u_i \alpha_i^{1/q} \mapsto \sum_{i=1}^s u_i \alpha_i$, where $u_i \in \bar{\mathbf{F}}_q, \alpha_i \in \mathbf{F}_q(X)$ and a corresponding map $\bar{\sigma} : X_{\bar{\mathbf{F}}_q} \to X_{\bar{\mathbf{F}}_q}$.
In the first section 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 Fr of $\bar{\mathbf{F}}_q$ over $\mathbf{F}_q$, where $Fr(u) = u^q$ for $u \in \bar{\mathbf{F}}_q$. 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 Fr on the function field $Fr : \bar{\mathbf{F}}_q(X) \to \bar{\mathbf{F}}_q(X)$, $\sum_{i=1}^s u_i \alpha_i \mapsto \sum_{i=1}^s u_i^q \alpha_i$, where like above $u_i \in \bar{\mathbf{F}}_q, \alpha_i \in \mathbf{F}_q(X)$. One can show that for points $P \in X_{\bar{\mathbf{F}}_q}$ we have that $Fr(P) = \bar{\sigma}(P)$. 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 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 2.40 *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 the points with ∞ or with a zero of the defining polynomial over an appropriate extension field. If $P \neq \infty$ is defined over $\mathbf{F}_{q^n}$, then $P = (u,v)$, $u, v \in \mathbf{F}_{q^n}$ and $\bar{\sigma}(P) = (u^q, v^q)$. 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 2.41 *Consider the case of imaginary quadratic function fields. Then we represent the divisor classes via the ideal classes. If $D = \sum n_i P_i - r\infty$ is represented by $(\sum_{i=0}^r u_i x^i, y - \sum_{i=0}^{r-1} v_i x^i)$ then $\bar{\sigma}(D) = \sum n_i \bar{\sigma}(P_i) - r\infty$ is represented by $(\sum_{i=0}^r u_i^q x^i, y - \sum_{i=0}^{r-1} v_i^q x^i)$.*

Let $X/\mathbf{F}_q$ be a nonsingular complete curve of genus g. One can use $\mathrm{Pic}^0(X_{\bar{\mathbf{F}}_q}/\bar{\mathbf{F}}_q)$ to get a representation of $\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$. Denote by $\mathbf{J}[m]$ the kernel of the multiplication by m map on $\mathrm{Pic}^0(X_{\bar{\mathbf{F}}_q}/\bar{\mathbf{F}}_q)$. If m is prime to p then $\mathbf{J}[m]$ is isomorphic to $(\mathbf{Z}/m\mathbf{Z})^{2g}$ as $\mathbf{Z}/m\mathbf{Z}$-module. 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 $\mathbf{J}[m]$. Denote by $\bar{\rho}_m : \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q) \to \mathrm{Perm}(\mathbf{J}[m])$ the group homomorphism associated to this action. The image of $\bar{\rho}_m$ lies in the subgroup of endomorphisms of $(\mathbf{Z}/m\mathbf{Z})$-modules of $\mathbf{J}[m]$. 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 $\{\mathbf{J}[l^{m+1}] \to \mathbf{J}[l^m]\}$. 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 $Fr \in \mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q)$ denote the Frobenius automorphism. Put

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

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

Theorem 2.42 *Let $X/\mathbf{F}_q$ be a nonsingular complete curve of genus $g \geq 1$. Then for all primes $l \neq p$ the polynomial $P(Fr, l)(T)$ is a polynomial with integer coefficients. Moreover the coefficients are independent of l. In fact this polynomial is equal to the polynomial $P(T) = T^{2g}L(1/T)$, 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 $\mathrm{Pic}^0(X/\mathbf{F}_{q^n})$ 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 $\mathrm{Pic}^0(X/\mathbf{F}_{q^n})$.

Chapter 3

Computing in the Divisor Class Group for Genus 2

Like for elliptic curves it is also possible to perform the group operations using explicit formulae in the divisor class groups of curves of larger genus. In her thesis, Spallek [69] develops such equations for genus 2 in the most common case of divisor classes whose representing polynomial u is of degree 2 and for odd characteristic. These formulae are also used by Krieger [37]. Harley [29] takes a slightly different approach to optimize the running time. In their record for computing the group order for a genus 2 curve, Gaudry and Harley [22] make use of these formulae as they allow faster arithmetic than Cantor's algorithm. Harley also only considers the case of odd characteristic but allows all kinds of divisor classes making an extensive case study. 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. As for our purposes the finite fields of even characteristic are of special importance, we follow Harley's approach and develop formulae for characteristic two. We consider the case of genus 2 only.
To do so, we first make a case study of what can be the input of the combination algorithm and proceed in considering these different cases. We determine the exact number of operations needed to perform addition and doubling in the most common cases. In the other cases the operations are usually cheaper.
From these expressions we can as well derive explicit formulae. For example instead of $v(x_1)$ we could as well write $v_1x_1 + v_0$ and the modular reduction can be made explicit as well. This is used when we implement the arithmetic. However the way we present the expressions here is hopefully more transparent.

Note that some older articles report on the advantages of the computation in the divisor class group in characteristic two over that in others characteristics. But they assume $h = 1$. Then in the doubling step of the composition one can always take $d = 1$ and $s_1 = s_2 = 0,\ s_3 = 1$. Therefore $u = u_1^2$ and $v = v_1^2 + f \bmod u$. However as we stated in the previous chapter, these curves are always supersingular and thus they should be avoided. To our knowledge no one has cared about the arithmetic in even characteristic in other cases.

Unless stated otherwise the formulae hold independently of the characteristic, thus they allow the computation for the more general model $C : y^2 + h(x)y = f(x)$. Therefore we take care of the signs; in characteristic two $2y$ is understood as zero.

3.1 Different Cases

Consider the composition step of Cantors Algorithm 2.30. The input are two classes represented by two polynomials $[u_i, v_i]$ each. As we consider curves of genus two the following holds from Theorem 2.29:

1. u is monic,
2. $\deg v < \deg u \leq 2$,
3. $u | v^2 + vh - f^2$.

We now consider all possible cases. Without loss of generality let $\deg u_1 \leq \deg u_2$.

1. u_1 is of degree 0, this is only possible in the case $[u_1, v_1] = [1, 0]$, i.e. for the zero element. The result of the combination and reduction is the second class $[u_2, v_2]$.

2. If u_1 is of degree one, then either u_2 is of degree 1 as well or it has full degree.

   (a) Assume $\deg u_2 = 1$, i.e. $u_i = x + u_{i0}$ and the v_i are constant. Then if $u_1 = u_2$ we obtain for $v_1 = -v_2 - h(-u_{10})$ the zero element $[1, 0]$ and for $v_1 = v_2$ we double the divisor to obtain

$$\begin{aligned} u &= u_1^2, \\ v &= ((f'(-u_{10}) - v_1 h'(-u_{10}))x + (f'(-u_{10}) - v_1 h'(-u_{10}))u_{10})/(2v_1 + h(-u_{10})) + v_1. \end{aligned} \tag{3.1}$$

   Otherwise the composition leads to $u = u_1 u_2$ and
   $v = ((v_2 - v_1)x + v_2 u_{10} - v_1 u_{20})/(u_{10} - u_{20})$.
   In all cases the results are already reduced.

   (b) Now let the second polynomial be of degree two, $u_2 = x^2 + u_{21}x + u_{20}$. Then the corresponding divisors are given by $D_1 = P_1 - \infty$ and $D_2 = P_2 + P_3 - 2\infty$, $P_i \neq \infty$.

      i. If $u_2(-u_{10}) \neq 0$ then P_1 and $-P_1$ do not occur in D_2. This general case will be dealt with below in Section 3.3.

      ii. Otherwise if $v_2(-u_{10}) = v_1 + h(-u_{10})$ then $-P_1$ occurs in D_2 and the resulting class is given by $u = x + u_{21} - u_{10}$ and $v = v_2(-u_{21} + u_{10})$ as $-u_{21}$ equals the sum of the x-coordinates of the points.
      Otherwise one first doubles $[u_1, v_1]$ by (3.1) and then adds $[x + u_{21} - u_{10}, v_2(-u_{21} + u_{10})]$, hence, reduces the problem to the case of 2(b)i.

3. Let $\deg u_1 = \deg u_2 = 2$.

   (a) Let first $u_1 = u_2$. This means that for an appropriate ordering $D_1 = P_1 + P_2 - 2\infty$, $D_2 = P_3 + P_4 - 2\infty$ the x-coordinates of P_i and P_{i+2} are equal.

      i. If $v_1 \equiv -v_2 - h \bmod u_1$ then the result is $[1, 0]$.

ii. If $v_1 = v_2$ then we are in the case where we double a class not of order two and with first polynomial of full degree. Again we need to consider two sub-cases: If $D_1 = P_1 + P_2 - 2\infty$ where P_1 is equal to its opposite, then the result is $2P_2$ and can be computed like above. $P_1 = (x_{P_1}, y_{P_1})$ is equal to its opposite, iff $h(x_{P_1}) = -2y_{P_1}$. To check for this case we compute the resultant of $h + 2v_1$ and u_1.

A. If $\mathrm{res}(h + 2v_1, u_1) \neq 0$ then we are in the usual case where both points are not equal to their opposite. This will be considered in Section 3.4.

B. Otherwise we compute the $\gcd(h+2v_1, u_1) = (x - x_{P_1})$ to get the coordinate of P_1 and double $[x + u_{11} + x_{P_1}, v_1(-u_{11} - x_{P_1})]$.

iii. Now we know that without loss of generality $P_1 = P_3$ and $P_2 \neq P_4$ is the opposite of P_4. Let $v_i = v_{i1}x + v_{i0}$, then the result is $2P_1$ obtained by doubling $[x - (v_{10} - v_{20})/(v_{21} - v_{11}), v_1((v_{10} - v_{20})/(v_{21} - v_{11}))]$ using (3.1).

(b) Now we consider the remaining case $u_1 \neq u_2$. We need to consider the following cases.

i. If $\mathrm{res}(u_1, u_2) \neq 0$ then no point of D_1 is equal to a point or its opposite in D_2. This is the most frequent case. We deal with it in Section 3.2.

ii. If the above resultant is zero then $\gcd(u_1, u_2) = x - x_{P_1}$ and we know that either $D_1 = P_1 + P_2 - 2\infty$, $D_2 = P_1 + P_3 - 2\infty$ or D_2 contains the opposite of P_1 instead. This can be checked by inserting x_{P_1} in both v_1 and v_2.

A. If the results are equal then we are in the first case and proceed by computing $D' = 2(P_1 - \infty)$, then $D'' = D' + P_2 - \infty$ and finally $D = D'' + P_3 - \infty$ by the formulae in 2. We extract the coordinates of P_2 and P_3 by $P_2 = (-u_{11} + x_{P_1}, v_1(-u_{11} + x_{P_1})), P_3 = (-u_{21} + x_{P_1}, v_2(-u_{21} + x_{P_1}))$.

B. In case $v_1(x_{P_1}) \neq v_2(x_{P_1})$ the result is $P_2 + P_3 - 2\infty$.

If one uses the resultant as recommended in 3(a)ii and 3(b)i then one needs to compute a greatest common divisor as well to extract the coordinates of P_1. However most frequently we are in the case of resultant nonzero and thus we save on average.

3.2 Addition in Most Common Case

In this case the two divisor classes to be combined consist of 4 points different from each other and from each other's negative. The results of the composition Algorithm 2.30 are u_1u_2 and a polynomial v of degree ≤ 3 satisfying $u | v^2 + vh - f$ (see Theorem 2.29). As we started with $u_i | v_i^2 + v_ih - f$ we can obtain v using Chinese remaindering:

$$\begin{aligned} v &\equiv v_1 \bmod u_1, \\ v &\equiv v_2 \bmod u_2. \end{aligned} \tag{3.2}$$

Then we compute the resulting first polynomial u' by making $(f - vh - h^2)/(u_1u_2)$ monic and taking $v' = (-h - v \bmod u')$.

To optimize the computations we do not follow this literally. We now list the needed subexpressions and then show that we obtain in fact the desired result. Again this is generalized from Harley.

$$\begin{aligned}
k &= (f - v_2h - v_2^2)/u_2 \\
s &\equiv (v_1 - v_2)/u_2 \bmod u_1 \\
l &= s \cdot u_2 \\
u &= (k - s(l + h + 2v_2))/u_1 \\
u' &= u \text{ made monic} \\
v' &\equiv -h - (l + v_2) \bmod u'
\end{aligned}$$

The divisions made to get k and u are exact divisions due to the definition of the polynomials. Let us first verify that $v = l + v_2 = s \cdot u_2 + v_2$ satisfies the system of equations (3.2). This is obvious for the second equation. For the first one we consider $v \equiv s \cdot u_2 + v_2 \equiv (v_1 - v_2)/u_2 \cdot u_2 + v_2 \equiv v_1 \bmod u_1$.
Now we check that $u = (f - vh - v^2)/(u_1u_2)$ by expanding out

$$u_1 \cdot u_2 \cdot u = u_2(k - s(l + h + 2v_2)) = f - v_2h - v_2^2 - l(l + h) - 2lv_2 = f - vh - v^2.$$

In the case study we have already computed the resultant of u_1 and u_2 when we arrive at this algorithm. Hence, we can assume that $\tilde{u}_2 = u_2 \bmod u_1$ and $\text{res}(\tilde{u}_2, u_1)$ are known. However we include the costs here as we use these expressions to compute $1/\tilde{u}_2 \bmod u_1$.

In the course of computing we do not need all coefficients of the polynomials defined above. As $f = x^5 + \sum_{i=0}^{4} f_i x^i$ is monic and of degree 5, u_2 is monic of degree 2, $\deg h \leq 2$, and $\deg v_2 = 1$ we have that $k = x^3 + (f_4 - u_{21})x^2 + cx + c'$, where c, c' are some constants. In the computation of u we divide an expression involving k by a polynomial of degree 2, thus we only need the above known part of k. There are other coefficients we do not use but we get them almost for free, as they are obtained by additions in the finite field. In the following Table 3.1 we list the intermediate steps together with the number of multiplications (M), squarings (S) and inversions (I) needed. Note that when we assume that our field is represented via a normal basis and work in characteristic two, the squarings are virtually for free.
In the computation of a product of polynomials we use the following Karatsuba style formula to save one multiplication:

$$(ax + b)(cx + d) = acx^2 + ((a + b)(c + d) - ac - bd)x + bd.$$

To reduce a polynomial of degree 3 modulo a monic one of degree 2 we use

$$ax^3 + bx^2 + cx + d \equiv (c - (i + j)(a + (b - ia) - ia - j(b - ia)))x + d - j(b - ia) \bmod x^2 + ix + j$$

using only 3 multiplications instead of four.
Note that the generalization to consider $h \neq 0$ in odd characteristic does not increase the complexity as Harley obtains the same number of operations and for characteristic 2 we even save as the squarings need not be counted.
It might happen that s is constant. Then the number of operations reduces further, the amount depends on the coefficients of h.

Table 3.1: Operations to Add in $\mathrm{Pic}^0(C/\mathbf{F}_{q^n})$ in General Case

Expression	operations needed
$k = (f - v_2h - v_2^2)/u_2$	free
Subexpressions:	
$d = u_{11}u_{21}$	M
$t = u_{20} - d + u_{11}^2 - u_{10}$	S
Resultant:	
$r = u_{20}(t - u_{10}) + u_{10}(u_{21}^2 - d + u_{10})$	S, 2M
Inverse of u_2 modulo u_1:	
$inv = ((u_{11} - u_{21})x + t)/r$	I, 2M
$s = (v_1 - v_2)inv \bmod u_1$	5M
$l = s \cdot u_2$	3M
$u = (k - s(l + h + 2v_2))/u_1$	S, 6M
make u monic	I, 2M
$v' \equiv -h - (l + v_2) \bmod u'$	3M
Total:	2I, 3S, 24 M

Table 3.2: Operations to Add in Special Case

Expression	operations needed
$k = (f - v_2h - v_2^2)/u_2$	2M
$r \equiv u_2 \bmod u_1$	M
Inverse of u_2 modulo u_1 $inv = 1/r$	I
$s = (v_1 - v_2)inv \bmod u_1$	2M
$l = s \cdot u_2$	2M
$u = (k - s(l + h + 2v_2))/u_1$	3M
u is monic	
$v' \equiv -h - (l + v_2) \bmod u'$	2M
Total:	I, 12 M

3.3 Addition in Case $\deg u_1 = 1,\ \deg u_2 = 2$

By the above considerations we can assume that for $u_1 = x + u_{10}$ we have that $u_2(-u_{10}) \neq 0$. In principle we follow the same algorithm as stated in the previous section. But to obtain u we divide by a polynomial of degree 1, therefore we need an additional coefficient of k and save a lot in the other operations. This leads to Table 3.2.
Hence, one sees that this case is much cheaper than the general one, however it is not too likely to happen.

3.4 Doubling

The above case study left open how one computes the double of a class where the first polynomial has degree two and both points of the representing divisor are not equal to their opposite. Put $u = x^2 + u_1x + u_0,\ v = v_1x + v_0$. Combining $[u, v]$ with itself should result in a class $[u_{\text{new}}, v_{\text{new}}]$, where $u_{\text{new}} = u^2$,

$$(*) \quad v_{\text{new}} \equiv v \bmod u$$

and

$$(**) \quad u_{\text{new}} | v_{\text{new}}^2 + v_{\text{new}}h - f.$$

Then this class is reduced to obtain $[u', v']$. We use the following subexpressions:

$$\begin{aligned} k &= (f - hv - v^2)/u \\ s &\equiv k/(h+2v) \bmod u \\ l &= (k - (h+2v)s)/u \\ u_1 &= l - s^2 \\ u' &= u_1 \text{ made monic} \\ v' &\equiv -h - (su+v) \bmod u' \end{aligned}$$

Note that like above we did not compute the semireduced divisor explicitely, here $v_{\text{new}} = su + v$. Hence, we see that $(*)$ holds. To prove $(**)$ we consider

$$v_{\text{new}}^2 + v_{\text{new}}h - f = s^2u^2 + 2suv + v^2 + hsu + hv - f = s^2u^2 + u(hs + 2vs - k)$$

and

$$(h+2v)s - k \equiv (h+2v)k/(h+2v) - k \equiv 0 \bmod u.$$

Finally one finds by

$$(f - v_{\text{new}}h - v_{\text{new}}^2)/u_{\text{new}} = (k - (h+2v)s)/u - s^2 = l - s^2$$

that u_1 is in fact obtained like in the reduction algorithm.
We now list the numbers of elementary operations needed in Table 3.3; unlike in the addition case we need the exact polynomial k here to compute d. Like before we include the costs to compute $\tilde{h} = (h + 2v \bmod u)$ and $\operatorname{res}(\tilde{h}, u)$.

In the following we consider the worst case when $h = h_2x^2 + h_1x + h_0$ and $h_2, h_1 \notin \{0,1\}$ and when the resulting s is of degree 1 and not monic. By a linear change of variables we can achieve $h_2 = 1$ in case of nonzero h_2 by replacing y by h_2^5y' and x by h_2^2x' and dividing the equation by h_2^{10}. Therefore for $h_2 = 1$ and $h_1 \notin \{0,1\}$ we state the number of operations as well. There we also show the effects when s is constant, however usually it will be of degree 1.
If $h_2, h_1 \in \{0,1\}$ then the number of operations drops down to 2I, 6S and 24 M for $\deg s = 1$ and to 1I, 3S and 19 M for s constant. If like later on we assume that C is defined over $\mathbf{F}_2$, then we are in this cheaper case. For $h_2 = 0$ we can furthermore replace one multiplication by a squaring.

In the case of odd characteristic Harley needs 2I, 6S and 24M for s of full degree and 1I, 3S and 19 M otherwise. Hence, the comparison of the number of operations needed depends heavily on the structure of h. If we take a curve defined over $\mathbf{F}_2$ and assume that $\mathbf{F}_{2^n}$ is represented by a normal basis then we only need 2I and 24M for a doubling and 2I and 24M for a general addition which is faster than for odd characteristic.

Table 3.3: Operations to Double in $\mathrm{Pic}^0(C/\mathbf{F}_{q^n})$

Expression	operations needed $h_2, h_1 \notin \{0,1\}$	$h_2 = 1, h_1 \notin \{0,1\}$ $\deg s = 1$	$s = s_0$
$k = (f - hv - v^2)/u$	S, 6M	S, 4M	
$d \equiv k \bmod u$	2M	2M	
Subexpressions:			
$\tilde{h} \equiv (h + 2v) \bmod u$	2M	free	
$t = \tilde{h}_1 u_1$	M	M	
Resultant $\mathrm{res}(\tilde{h}, u)$:			
$r = \tilde{h}_0^2 + u_0 \tilde{h}_1^2 - \tilde{h}_0 t$	2S,2M	2S, 2M	
Inverse of $\tilde{h}$ modulo u_1:			
$e = (\tilde{h}_1 x + \tilde{h}_0 - t)/r \bmod u$	I, 2M	I, 2M	
$s \equiv de \bmod u$	5M	5M	
$l = (k - hs)/u$	4M	2M	free
$u' = l - s^2$	3S	3S	S
make u' monic	I, 2M	I, 2M	free
$v' \equiv -h - (su + v) \bmod u'$	6M	6M	4M
Total:	2I, 6S, 32 M	2I,6S,26 M	I,4S,20M

Note that for even characteristic we need only two squarings to compute u' for s of full degree. Furthermore in this case squarings can be assumed to be for free.

Chapter 4

Efficient Determination of the Class Number for Koblitz Curves

For the next two chapters we only consider hyperelliptic Koblitz curves of genus g. In the first section of this chapter we state some details for computing $P(T)$ in the case of Koblitz curves. In the second section we find recurrence relations allowing to compute $|\mathrm{Pic}^0(X/\mathbf{F}_{q^n})|$ from the coefficients of P and n. Finally we provide examples computed by these algorithms.

4.1 Computation of $P(T)$

By Theorem 2.33 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. Hence, 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 [72] 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 [33]. 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. If $h(a)$ happens to be 0, then $a \in \mathbf{F}_{q^i}$ gives rise to one point. Otherwise we make a transformation by dividing through by $h(a)^2$ 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 absolute trace map on both sides then $\mathrm{Tr}_{\mathbf{F}_{q^i}:\mathbf{F}_2}(v^2+v) = \mathrm{Tr}_{\mathbf{F}_{q^i}:\mathbf{F}_2}(v^2) + \mathrm{Tr}_{\mathbf{F}_{q^i}:\mathbf{F}_2}(v) = 0$ since we are working in characteristic 2 and $\mathrm{Tr}_{\mathbf{F}_{q^i}:\mathbf{F}_2}(v^2) = \mathrm{Tr}_{\mathbf{F}_{q^i}:\mathbf{F}_2}(v)$. Thus to compute M_i we do the following. For every $a \in \mathbf{F}_{q^i}$ 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 non-isogenous classes of hyperelliptic curves we make a brute force search through 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 would like to exclude the cases where $\tilde{P}$ 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 2.33 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 4.3, but most of the tabulars require to much space.

4.2 Recurrence Formulae for the Class Number

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 [54] and Lehmer [39] 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

2.33
$$N_n = \prod_{i=1}^{g}((1-\tau_i^n)(1-\bar{\tau}_i^n)) = \prod_{i=1}^{g}((1+q^n)-(\tau_i^n+\bar{\tau}_i^n)).$$

For cryptographic purposes we are interested in groups which contain large prime order subgroups. For $n_1|n_2$ we immediately get by $(1-\tau_i^{n_1})|(1-\tau_i^{n_2})$ that N_{n_2} is divisible by N_{n_1}. Therefore we compute the cardinality of $\mathrm{Pic}^0(C/\mathbf{F}_{q^n})$ 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 $T^2 - \mu_i T + q$ 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 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 $A_{j,n} \in \mathbf{Z}$, which can be shown by induction like below.
We immediately get:

$$\begin{aligned}
&\tau_i^{n+1} + \bar{\tau}_i^{n+1} = (\tau_i + \bar{\tau}_i)(\tau_i^n + \bar{\tau}_i^n) - \tau_i\bar{\tau}_i(\tau_i^{n-1} + \bar{\tau}_i^{n-1})\\
&= \mu_i(A_{1,n} + \mu_i A_{2,n} + \cdots + \mu_i^{g-1}A_{g,n}) - q(A_{1,n-1} + \mu_i A_{2,n-1} + \cdots + \mu_i^{g-1}A_{g,n-1})\\
&= (-qA_{1,n-1} - b_gA_{g,n}) + \mu_i(A_{1,n} - qA_{2,n-1} - b_{g-1}A_{g,n}) + \cdots +\\
&\qquad +\mu_i^{g-1}(A_{g-1,n} - qA_{g-2,n-1} - b_1A_{g,n}).
\end{aligned}$$

With the initial states $A_{1,0} = 2 = \tau_i^0 + \bar{\tau}_i^0$, $A_{j,0} = 0$ 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:

$$\begin{array}{rcll}
A_{1,n+1} & = & & -qA_{1,n-1} - b_gA_{g,n}\\
A_{2,n+1} & = & A_{1,n} & -qA_{2,n-1} - b_{g-1}A_{g,n}\\
& \vdots & & \vdots\\
A_{j,n+1} & = & A_{j-1,n} & -qA_{j,n-1} - b_{g-j+1}A_{g,n}\\
& \vdots & & \vdots\\
A_{g,n+1} & = & A_{g-1,n} & -qA_{g,n-1} - b_1A_{g,n}.
\end{array}$$

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*

$$\begin{aligned} P(T) &= \prod_{i=1}^{2g}(T-\tau_i) \\ &= T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + a_{g-1} q T^{g-1} + \cdots + a_1 q^{g-1} T + q^g \end{aligned}$$

and put $a_0 = 1$. *Then the following statements hold for the coefficients of* $Q(T) = \prod_{j=1}^{g}(T-\mu_j) = T^g + b_1 T^{g-1} + \cdots + b_g$, $\bar{\tau}_j = \tau_{g+j}$, $\mu_j = \tau_j + \bar{\tau}_j$, $b_0 = 1$*:*

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

Proof. The b_j are the elementary symmetric functions in the μ_j, 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.

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

□

Table 4.1: 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
$y^2+(x^2+x+1)y=x^5+x^4$	$T^4+2T^3+3T^2+4T+4$
$y^2+(x^2+x+1)y=x^5+x^4+1$	$T^4-2T^3+3T^2-4T+4$

4.3 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`.

By the results of Diem [7][Theorem 5] the variety of cardinality $|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})|/|\mathrm{Pic}^0(C/\mathbf{F}_q)|$, n prime, belonging to the curve is simple, unless $\mathbf{Q}(\zeta_n)$ contains the endomorphism ring of the Picard group, where ζ_n is a primitive n-th root of unity. Hence, there is no reason against this number being prime. The experiments show that indeed there are many examples where this number is prime. For details see Chapter 6, were we consider this variety.

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

4.3.1 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 4.1.
The first five examples were given in Koblitz [33]. Besides the first three classes these curves are non-supersingular. The fourth and fifth case were studied by Günter, Lange, and Stein in [26] where we also give tables stating the group 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 4.2, 4.3, 4.4, and 4.5 we state the class numbers in the remaining cases in the range of cryptographic interest.

Table 4.2: Curve with $P(T) = T^4 + T^2 + 4$:

n	$\lvert \mathrm{Pic}^0(C/\mathbf{F}_{2^n}) \rvert$
61	5316911983139663492953680213645327006=
	$2 \cdot 3 \cdot 28549 \cdot 1683601 \cdot 18436485874741919325168049$
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=
	$2 \cdot 3 \cdot 227^2 \cdot 1583 \cdot 3824147 \cdot 6778085329 \cdot 2530945889145571847 \cdot 3358695792503140247319023$

Table 4.3: 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	$5575186299632655785380203394313934582133756 =$ $2^2 \cdot 26839 \cdot 148249 \cdot 350300929811452465486759451374849$
73	$89202980794122492566150296745591692779759604 =$ $2^2 \cdot 8761 \cdot 442189471 \cdot 5756483947455991782107502725371$
79	$365375409332725729550922292183917789809461213276 =$ $2^2 \cdot 91343852333181432387730573045979447452365303319$
83	$93536104789177786765035845762706187663255567569676 =$ $2^2 \cdot 14922571 \cdot 19492219 \cdot 31262449 \cdot 25715285868794313961688827419$
89	$383123885216472214589586757378244353769997331107203764 =$ $2^2 \cdot 2671 \cdot 53497189 \cdot 670307974525390635096804382861885945480039$
97	$25108406941546723055343157693015513330857555182110701284884 =$ $2^2 \cdot 14551 \cdot 431386278289236531086233896175787116535934904510183171$
101	$6427752177035961102167848369362732175776372403309219283496004 =$ $2^2 \cdot 59962489 \cdot 1898267731 \cdot 1204958581789 \cdot 231501457725649 \cdot 50609980118281999$
103	$102844034832575377634685573909850209809266881319472110901022076 =$ $2^2 \cdot 43261 \cdot 420859 \cdot 18751186669 \cdot 579776615513755189 \cdot 1298962131741707567246 41$
107	$2632807291713929667447950692091791474465969497876654037469150 2636 =$ $2^2 \cdot 973257085699 \cdot 676287727672444629795783995546967793950518106423 8041$
109	$4212491666742287467916721107346808615168036888197510047401481 79364 =$ $2^2 \cdot 247885621 \cdot 598722031900039 \cdot 70958183329491078264858841853754141409 8739$
113	$10783978666860255917866806034807852840498176999474806780211502 2805204 =$ $2^2 \cdot 299464210429 \cdot 5149674762391 \cdot 27151900595462829709 \cdot 64386388554080955716 3851$

Table 4.4: 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=
	$2 \cdot 7 \cdot 155557653453308991329902926386955853 1383$
71	5575186299519090460509374439525583695134642=
	$2 \cdot 7 \cdot 569 \cdot 67217532937 \cdot 1041205643874122957132140 6751$
73	89202980794660877710779236197113745019927342=
	$2 \cdot 7 \cdot 5215121 \cdot 38961862367 \cdot 31357919011564553499404479$
79	365375409332684354222911973151271502086185656786=
	$2 \cdot 7 \cdot 765353 \cdot 340996161558956039354120603873797452 27383$
83	93536104789160189806805423910911919572829943988546=
	$2 \cdot 7 \cdot 167^2 \cdot 16305189977 \cdot 23564064703 \cdot 114833530663 \cdot 5429670992567$
89	383123885216459517032176679352494921969133201300475502=
	$2 \cdot 7 \cdot 27535906720484993 \cdot 99382933269515664303720439999998 2801$
97	25108406941546475519266315021658437571181521793461683089038=
	$2 \cdot 7 \cdot 14551 \cdot 1233451320939473 \cdot 99925485729323135043380964652866217079$
101	6427752177035957907451442801389171479467324814535766520314942=
	$2 \cdot 7 \cdot 809 \cdot 173481667802057497 \cdot 32713648136431916994460328169770496883 61$
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 4.5: 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 4.6: Binary curves of genus 3

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

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 4.6 are to be considered. According to Definition 2.35 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. $g = 3$
$n = 37$,

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

$n = 47$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 27875926529710321157207257405335107462263 16 \\ &= 2^2 \cdot 6968981632427580289301814351333776865565 79 \\ &= 2^2 \cdot P_{139} \end{aligned}$$

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

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 278759365266985001248867485965032942654397 8 \\ &= 2 \cdot 7 \cdot 199113832333560715177762489975023530467427 \\ &= 2 \cdot 7 \cdot P_{137} \end{aligned}$$

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

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

4.3.2 Curves over $\mathbf{F}_3$

For larger fields the number of curves to consider increases considerably. Let $k(C)/\mathbf{F}_q$ be a hyperelliptic function field of genus g given by $y^2 = f(x)$ As we have seen in Section 2.1 the map $C/\mathbf{F}_q \to \mathbb{P}^1(\mathbf{F}_q)$ is ramified in $2g + 2$ points and to each $2g + 2$ distinct points $x_1, \ldots, x_{2g+2}$ of $\mathbb{P}^1(\mathbf{F}_q)$ corresponds one curve. Now two curves are isomorphic if the sets of the corresponding $2g+2$ points can be mapped onto each other by an automorphism of $\mathbb{P}^1(\mathbf{F}_q)$. Using such an automorphism φ, we can always achieve that $\varphi(x_1) = 0, \varphi(x_2) = 1, \varphi(x_3) = \infty$. Hence, we allow the right hand side to be of the shape $f(x) = x(x-1)\prod_{i=1}^{2g-1}(x - x_i)$ for distinct x_i. This leads to $O(q^{2g-1})$ curves to consider, as the number of $(2g-1)$-tuples with multiple occurrences of one element and the number of curves identified via isogenies is of lower order.
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. $g = 2$
$n = 59$,

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

$n = 61$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 16173092699229944614352376379779099336973126813590905333204 \\ &= 2^2 \cdot 4043273174807486153588094094944774834243281703397726333301 \\ &= 2^2 \cdot P_{191} \end{aligned}$$

$n = 67$,

$$\begin{aligned} &|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| \\ =\ & 85950445571714268836615512573879923383084474556240494103545821 96 \\ =\ & 2^2 \cdot 21487611392928567209153878143469980845771118639060123525886455 49 \\ =\ & 2^2 \cdot P_{210} \end{aligned}$$

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

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 37571021261375006591159582348161439581978496614 3289 \\ &= 19 \cdot 1977422171651316136376820123587444188525184032 3331 \\ &= 19 \cdot P_{163} \end{aligned}$$

$n = 61$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 16173092699229882562486817678274704604693996874416224059211 \\ &= 19 \cdot 851215405222625398025621983067089716036526151285064424169 \\ &= 19 \cdot P_{189} \end{aligned}$$

$n = 71$,

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

Table 4.7: 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 $T^6 + T^5 + 5T^4 + 4T^3 + 15T^2 + 9T + 27$, i.e. $g = 3$
$n = 59$,

$$\begin{aligned}
&|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| \\
= \;& 2821383260958017515748847417606632102819352907295219754610211050703061257893692760162 \\
= \;& 2 \cdot 31 \cdot 45506181628355121221755603509784388755150853343471286364680823398436471901511173551 \\
= \;& 2 \cdot 31 \cdot P_{274}
\end{aligned}$$

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

$$\begin{aligned}
|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 14555782220141583796941542410660218643781028826450039037345 4 \\
&= 2 \cdot 3 \cdot 29 \cdot 8365392080541140113184794488885183128609786681867 83\ 852721 \\
&= 2 \cdot 3 \cdot 29 \cdot P_{189}
\end{aligned}$$

$n = 61$,

$$\begin{aligned}
&|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| \\
= \;& 2615689274578817751725264876078789044475985886643083197112098643885044995679734740922352 88 \hookleftarrow \\
&\qquad 119903230812624287271271574 \\
= \;& 2 \cdot 3 \cdot 29 \cdot 15032696980338033055892326874016028991241298199098179293747693355661178136090429 5 \hookleftarrow \\
&\qquad 4553076368505190981681748777421101 \\
= \;& 2 \cdot 3 \cdot 29 \cdot P_{379}
\end{aligned}$$

4.3.3 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. But 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 $\mathbf{F}_2$. Galbraith [17] shows how to weaken certain curves over $\mathbf{F}_4$ by this strategy.
The following numbers of classes listed in Table 4.7 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. $g = 2$
$n = 29$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 830767498296989929589426215003673388 \\ &= 2^2 \cdot 3 \cdot 69230624858082494132452184583636949 \\ &= 2^2 \cdot 3 \cdot P_{112} \end{aligned}$$

$n = 41$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 233840261973169604864226823580661305442367409573 88 \\ &= 2^2 \cdot 3 \cdot 19486688497764133738685568631721775453530617464 49 \\ &= 2^2 \cdot 3 \cdot P_{160} \end{aligned}$$

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. $g = 3$
$n = 19$,

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

$n = 23$,

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

4.3.4 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 subsection 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 2.32 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. $g = 2$
$n = 29$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 34694469522393632077212991999281685458254 \\ &= 2 \cdot 7 \cdot 2478176394456688005515213714234406104161 \\ &= 2 \cdot 7 \cdot P_{130} \end{aligned}$$

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

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 21684043450334881590050481456320990124273379 \\ &= 19 \cdot 1141265444754467452107920076648473164435441 \\ &= 19 \cdot P_{139} \end{aligned}$$

$n = 37$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 5293955920340537004159560753167334605889814040117519 \\ &= 19 \cdot 278629258965291421271555829114070242415253370532501 \\ &= 19 \cdot P_{167} \end{aligned}$$

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. $g = 3$
$n = 23$,

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

$n = 29$,

$$\begin{aligned} |\mathrm{Pic}^0(C/\mathbf{F}_{q^n})| &= 6462348536008289894896808635027304395262834292145210636182324 \\ &= 2^2 \cdot 3 \cdot 7 \cdot 76932720666765355891628674226515528515033741573157269478361 \\ &= 2^2 \cdot 3 \cdot 7 \cdot P_{195} \end{aligned}$$

Chapter 5

Speeding Up the Computation of m-folds for Koblitz Curves

The second advantage of Koblitz curves is that they allow to obtain a faster way to compute multiples of divisor classes by making use of the Frobenius endomorphism of the curve. We first show how this computation is carried out in arbitrary groups and then investigate the action of the Frobenius endomorphism on $\mathrm{Pic}^0(C/\mathbf{F}_{q^n})$. Note that although we consider a base extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ we still denote the endomorphism by σ. The characteristic polynomial P was studied in the previous chapter. Let τ be a complex root of P. We provide a means to compute an expansion of the integer m to the base of τ and show how to use it to obtain a speed-up in the computation of m-folds. The following sections deal with the finiteness, length, and density of these expansions. These theoretical results are confirmed by examples. For space reasons we only list results for binary curves although we made successful experiments with other characteristics as well. In Section 5.7 we compare this 'τ-adic' method with the binary double-and-add method and as well with the more advanced windowing method to get estimates for the speed-up obtained depending on the degree of extension n, the genus g and the field size q. Considering a different set-up for the multipliers for Koblitz curves concludes this chapter.

5.1 Standard ways of computing m-folds

We describe the standard algorithm 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 1 doubling. This can be formalized in the following way:

Algorithm 5.1
`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* $b_i = 1$ *then* $H := H + D$;
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 $l-1$ 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 2.32. Thus to compute a multiple of a divisor class we need on average

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

group operations.

In the divisor class group we can easily compute the negative of an element. Therefore it is useful to consider signed expansions. By a non-adjacent form (NAF) we mean an expansion to the base of two with coefficients $0, \pm 1$ such that no two consecutive coefficients are nonzero. Each integer has a unique NAF, its length is at most one bit longer than the usual binary expansion and the asymptotic density is $1/3$. For the computation of the expansion consider Gordon [25] and Solinas [68].

5.2 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.

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 $(\sum_{i=0}^{g} u_i x^i, y - \sum_{i=0}^{g-1} v_i x^i)$, then $\sigma(D)$ is represented by $(\sum_{i=0}^{g} u_i^q x^i, y - \sum_{i=0}^{g-1} v_i^q x^i)$. 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. (Even if 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.) 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 7.3. 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 $\mathrm{Pic}^0(C/\bar{\mathbf{F}}_q)$. Remember that by the results of Section 4.1 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 $\sigma^j(D)$. 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. This means that as soon as we have precomputed and stored the multiples rD for all $r \in R$, the computation of mD can be performed by using table-look-ups, applications of the Frobenius endomorphism and some additions.

Example 5.2 *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 $R = \{0, \pm1, \pm2, \pm3, \pm5, \pm6, \pm7\}$ one obtains the following expansion*

$$23D = 7D - 3\sigma^4(D) - \sigma^6(D).$$

This leads to two additions, two table-look-ups, and 6 applications of the Frobenius endomorphism which is by far less than the four doublings and three additions needed using the double-and-add method.

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 $m = \sum_{i=0}^{l-1} r_i \tau^i$ using the restricted set of coefficients $r_i \in R$ we first need a criterion for an element to be divisible by τ.

Lemma 5.3 $c = c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}$ *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 $[u, h-v]$) we will use $R = \{0, \pm1, \pm2, \ldots, \pm\lceil\frac{q^g-1}{2}\rceil\}$ if just a representation is needed. Note that we would not need to include $-q^g/2$ in the case of even characteristic. But as we get it for free we will make use of it. Furthermore later on in 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 5.4
`INPUT:` $c = c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}$, *$P(T)$, the set R.*
`OUTPUT:`$r_0, \ldots, r_{l-1}$ *with* $c = \sum_{i=0}^{l-1} r_i\tau^i,\ r_i \in R$.

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* $r_i := 0$;
   else choose $r_i \in R$ *with* $q^g|c_0 - r_i$;
   /**in even characteristic choose* $r_i = c_0$ *if* $|c_0| = q^g/2$/*
   $d := (c_0 - r_i)/q^g$;
   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* $(r_0, \ldots, r_{i-1})$.

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

5.3 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 way to find out what happens for a given individual curve and how to deal with periods.

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 $\mathbf{C}^g$

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

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 prove the following theorem:

Theorem 5.5 *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 $R = \{0, \pm 1, \ldots, \pm\lceil \frac{q^g-1}{2} \rceil\}$ 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 $c = r + c - r =: r + c'\tau$, $r \in R$ chosen according to Algorithm 5.4, we get $\mathcal{N}(c'\tau) \leq \mathcal{N}(c) + \mathcal{N}(r) \leq \mathcal{N}(c) + \sqrt{g}(q^g - 1)/2$ (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 r – and therefore the next remainder c' – is unique for given c. Hence, for these elements the expansion is either periodic

[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.

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. $\square$

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

Lemma 5.6 *Let q be odd. For every $m \in \mathbf{Z}[\tau]$ we have a unique expansion*

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

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

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

and

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

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

$$\begin{aligned} m_0 &= m_1\tau + r_0 = m_2\tau^2 + r_1\tau + r_0 \\ &= \sum_{i=0}^{j-1} r_i\tau^i + m_j\tau^j, \end{aligned}$$

where by Lemma 5.3 the $r_i \in \{0, \pm 1, \pm 2, \ldots, \pm\frac{q^g-1}{2}\}$ are uniquely determined.
The Triangle inequality for $\mathcal{N}$ leads to $\sqrt{q}\mathcal{N}(m_j) \leq \mathcal{N}(m_{j-1}) + \mathcal{N}(r_{j-1}) \leq \mathcal{N}(m_{j-1}) + \sqrt{g}\frac{q^g-1}{2}$.
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. $\square$

For even characteristic we proceed similarly.

Lemma 5.7 *Let q be even. For every $m \in \mathbf{Z}[\tau]$ we have an expansion*

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

where $r_i \in \{0, \pm 1, \pm 2, \dots, \pm\frac{q^g}{2}\}$,

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

and

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

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

$$\begin{aligned} m_0 &= m_1\tau + r_0 = m_2\tau^2 + r_1\tau + r_0 \\ &= \sum_{i=0}^{j-1} r_i\tau^i + m_j\tau^j, \end{aligned}$$

where the $r_i \in \{0, \pm 1, \pm 2, \dots, \pm\frac{q^g}{2}\}$ are given like in Algorithm 5.4.
The Triangle inequality for $\mathcal{N}$ leads to $\sqrt{q}\mathcal{N}(m_j) \leq \mathcal{N}(m_{j-1}) + \mathcal{N}(r_{j-1}) \leq \mathcal{N}(m_{j-1}) + \sqrt{g}\frac{q^g}{2}$.
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 $c_0, \dots, c_{2g-1}$. This can be done using the symmetric functions in the τ_i and with the help of the formulae derived in Section 4.2. 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 5.8 *For curves of genus 1, i. e. elliptic curves, the finiteness was proved by Müller [48] for even characteristic and using the same idea by Smart [66] 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 $R = \{0, \pm 1, \dots, \pm(q-1)/2\}$. After showing that the square of the norm decreases down to $(\sqrt{q}+2)^2/4$ giving a special case of Lemma 5.6 one rearranges*

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

by completing the square. Since the curve is assumed to be non-supersingular ($\Rightarrow a_1 \neq 2\sqrt{q}$), and a_1 is an integer, therefore $a_1^2 \equiv 0, 1 \bmod 4$, one has that $4q - a_1^2 \geq 3$, and gets

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

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 $|-a_1| - 1 > (q-1)/2$ (by the above $a_1 < 0$) – this can only happen if $q \leq 14$ – one finds that one needs to allow the coefficients $\pm(q+1)/2$ for the expansions 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 5.9 *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 $c_i c_j, i < j$ 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 [13] provide the following algorithm for finding all vectors of bounded norm in a lattice in $\mathbf{R}^s$, respectively for finding all arrays $(x_0, \ldots, x_{s-1})$ for which the value of the corresponding quadratic form in s variables is less than a given constant. Let the quadratic form be given by $\sum_{i,j=0}^{s-1} a_{ij} x_i x_j,\ a_{ij} = a_{ji}$, and put K the bound on the norm.

Algorithm 5.10 (Finke, Pohst)
`INPUT:` *quadratic form, bound K.*
`OUTPUT:` *all arrays $(x_0, \ldots, x_{s-1})$ leading to values less than K.*

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

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

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

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

They also prove 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, and also the length of the period. We use the algorithm to find the elements of small norm for individual curves. For each of them we compute 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 $1 \leq g \leq 2g-1$ and $|c_0| \leq q^g$, 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. Hence, the above bound is appropriate for the number of elements of small norm, however the expansions are by far shorter than hitting each element.
Therefore if $P(T)$ is such that we do not have periods, the length of the expansion of m is bounded by $\lceil 2\log_q \frac{2(\sqrt{q}-1)\mathcal{N}(m)}{\sqrt{g}}\rceil + 2g + 1$.

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, $i < j \leq 2g-1$.
For a fixed positive definite quadratic form of arbitrary degree this is the idea behind the above algorithm given in Finke and Pohst [13]. 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 5.11 *In the genus 2 case the reordered equation reads:*

$$\begin{aligned}
\mathcal{N}^2(c) \;=\;& 2\left(c_0 - \frac{1}{4}a_1c_1 + \frac{a_1^2-2a_2}{4}c_2 + \frac{-a_1^3+3a_1a_2-3a_1q}{4}c_3\right)^2 \\
&+\frac{-a_1^2+16q}{8}\left(c_1 + \frac{-a_1^3+2a_1a_2+4a_1q}{a_1^2-16q}c_2 + \frac{a_1^4-3a_1^2a_2-a_1^2q+8a_2q}{a_1^2-16q}c_3\right)^2 \\
&+\frac{a_1^4q-6a_1^2a_2q+4a_1^2q^2+8a_2^2q-32q^3}{a_1^2-16q}\left(c_2 + \frac{-a_1^3+5/2a_1a_2+a_1q}{a_1^2-2a_2-4q}c_3\right)^2 \\
&+\frac{a_1^4q^2-1/4a_1^2a_2^2q-5a_1^2a_2q^2+7a_1^2q^3+a_2^3q+2a_2^2q^2-4a_2q^3-8q^4}{a_1^2-2a_2-4q}c_3^2.
\end{aligned}$$

Thus for this usual ordering we have

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

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*:*

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

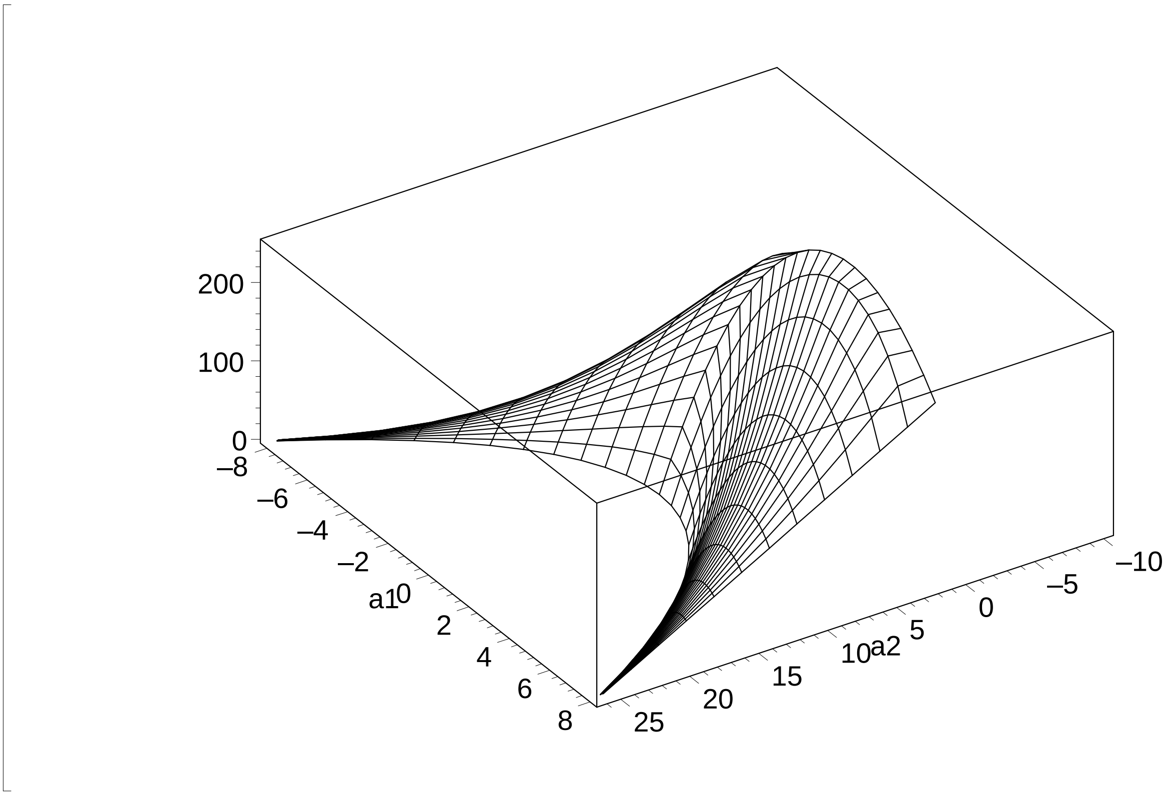
for c_1*:*

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

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 (2.2) $|a_1| \leq 2\lfloor 2\sqrt{q}\rfloor$ *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 $a_1 = \alpha_1\sqrt{q}$ *and* $a_2 = \alpha_2 q$*, thus* $|\alpha_1| < 4$ *and* $\alpha_1 - 2 < \alpha_2 < \alpha_1^2/4 + 2$ *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* $i \geq 1$ *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 dependence of b_{33} *for* c_3 *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. b_{33} 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 consider b_{33} for c_3 (and therefore also for c_0). For c_1 and c_2 similar observations hold. Furthermore 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_0^2 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 [42] investigate in more detail which pairs a_1, a_2 satisfying the conditions of Theorem 2.33 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 $2q^2 - q/2$ 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 e. g.* 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 $q < 14$. For odd characteristic these are just the cases of Example 5.8 where we included a further coefficient. For even characteristic it was shown in [48] 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.

In the following we assume that R consists of a complete set of remainders modulo q^g. For larger sets R' similar observations hold.

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

$$\begin{aligned} c &= c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1} \\ &= r_0 \pm \tau(c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}) \end{aligned}$$

with $r_0 \in R$ and where $\mathcal{N}(c)^2$ is bounded by the constant from Lemma 5.6 or Lemma 5.7 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

$$d = (c_0 - r_0)/q^g > 0. \tag{5.1}$$

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

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

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

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

thus $c_0 = dq^g - d|\mathrm{Pic}^0(C/\mathbf{F}_q)|$. Using (5.1) we obtain

$$r_0 = -d|\mathrm{Pic}^0(C/\mathbf{F}_q)|.$$

Since both d and $|\mathrm{Pic}^0(C/\mathbf{F}_q)|$ are non-negative and $r_0 \in R$ the crucial part to be fulfilled for either the curve or its twist is $\lceil (q^g - 1)/2 \rceil \ge d|\mathrm{Pic}^0(C/\mathbf{F}_q)|$. Since a lower bound on the class number is given by the Theorem of Hasse-Weil 2.32, q and d have to be such that $\lceil (q^g - 1)/2 \rceil \ge d(\sqrt{q} - 1)^{2g}$. Thus we only have this problem if q is small enough.
We just have shown

Theorem 5.12 *Let C be a hyperelliptic curve over $\mathbf{F}_q$ of genus g 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 $d = \lfloor (|c_0| + r_{\max})/q^g \rfloor$, where $r_{\max}$ is the maximal coefficient contained in R. Then the expansion of c can become cyclic only if*

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

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

Example 5.13 *In the genus 2 case for odd characteristic this theorem leads to 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 $c_3 \in R$ 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 $|c_0| < \sqrt{q} r_{\max}$ then d is additionally bounded from above by $d < (\sqrt{q}+1)/2$.

For a given curve it is fairly easy to check whether the expansion can run into a cycle at all by applying the bound of Theorem 5.12. Furthermore it shows which additional coefficients might have to be included in the set R. 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 5.14 *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 $P(T) = T^4 \pm 3T^3 + 5T^2 \pm 9T + 9$ lead to periods. The coefficients to include are ± 5 in the first two cases and ± 6 in the last one.*

Example 5.15 *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 5.4) then for all classes of curves of genus two over $\mathbf{F}_2$ (see Tabular 4.1) 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 $c_0 - r_0 = dq^g$ and $c_1 - a_1 q^{g-1} d - r_1 = eq^g$. Then from the equation

$$\begin{aligned} c &= c_0 + c_1\tau + \cdots + c_{2g-3}\tau^{2g-3} + c_{2g-2}\tau^{2g-2} + c_{2g-1}\tau^{2g-1} \\ &= r_0 + \tau(r_1 \pm \tau(c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1})) \end{aligned}$$

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

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

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

$$\begin{array}{rcl c r} c_0 & = & -d - ea_1 - da_2 - \cdots - dq^{g-2}a_2 - eq^{g-1}a_1 & = & dq^g + r_0 \\ c_1 & = & -e - da_1 - ea_2 - \cdots - eq^{g-1}a_2 & = & dq^{g-1}a_1 + eq^g + r_1, \end{array}$$

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

$$-(d+e)|\mathrm{Pic}^0(C/\mathbf{F}_q)| = r_0 + r_1$$

can be fulfilled for $r_0, r_1 \in R$.
For $d = -e$ we get $r_0 = -r_1$, 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 $|c_0| < \sqrt{q}r_{\max}$ and $|c_i| \in R,\ i \geq 1$, then $d < (\sqrt{q}+1)/2$ and $|e| < 1 + g + 1/\sqrt{q}$ in the worst case.

A different way to proof the finiteness of such expansions can be extended from Lesage [40]. 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 non-real roots (except some 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.

5.4 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 4.2 has the advantage that it provides a fast way 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 under consideration 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, modulo $|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})|$ these polynomials have a common linear factor. Hence, if we consider only the cyclic group of order l, the polynomials have a common factor $T-s$ in $\mathbf{F}_l[T]$, where l is a prime factor of $|\mathrm{Pic}^0(C/\mathbf{F}_{q^n})|$. This means that the operation of the Frobenius endomorphism on a divisor class corresponds to the multiplication of the divisor class by the integer s modulo l. For cryptographic purposes we work in a subgroup of prime order, anyway. 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 and l is prime.
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 that 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 5.16 *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. $$2\log_q \frac{2(\sqrt{q}-1)\mathcal{N}(M)}{\sqrt{g}} < n + 2g.$$

where $\mathcal{N}$ denotes the norm defined in the previous section.

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 $Q \in \mathbf{Q}$ let $z =$`nearest`(Q) be the nearest integer to Q, if ambiguity arises it is defined to be the integer with the least absolute value. This can be realized computationally by choosing $z = \lceil Q - 0.5 \rceil$ if $Q > 0$ and $z = \lfloor Q + 0.5 \rfloor$ else. We will also use `nearest`(.) for elements of $\mathbf{Q}[\tau]$ where it is understood coefficient-wise.

Proof. In the field $\mathbf{Q}[\tau]$ one can invert elements. Thus, put $Q := m(\tau-1)/(\tau^n-1) \in \mathbf{Q}[\tau]$, so $Q = \sum_{i=0}^{2g-1} Q_i \tau^i$ where $Q_i \in \mathbf{Q}$. For $0 \le i \le 2g-1$ put $z_i =$ `nearest`(Q_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

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

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

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

Therefore we have

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

It follows that

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

$\square$

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 5.3 we have the following result:

Theorem 5.17 (Main result on the Length)
Let C be a hyperelliptic curve over $\mathbf{F}_q$ 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

$$k \leq n + 4g + 1.$$

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. In the third subsection we collect the algorithms developed so far.

5.4.1 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 over $\mathbf{F}_q$ 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 5.18
`INPUT:` $n \in \mathbf{N}$, $P(T)$.
`OUTPUT:` $e_0, \ldots, e_{2g-1} \in \mathbf{Z}$ *such that* $(\tau^n - 1)/(\tau - 1) = e_0 + e_1\tau + \cdots + e_{2g-1}\tau^{2g-1}$ *in* $\mathbf{Z}[\tau]$.

1. *Initialize:* $d_0 = 1$ *and* $d_i = 0$ *for* $1 \leq i \leq 2g-1$;
   $e_0 = 1$ *and* $e_i = 0$ *for* $1 \leq i \leq 2g-1$;

2. *for* $1 \leq k \leq n-1$ *do*

   (a) $d_{old} := d_{2g-1}$;

   (b) *for* $2g-1 \geq i \geq g$ *do*
   $d_i := d_{i-1} - a_{2g-i} d_{old}$;
   $e_i := e_i + d_i$;

   (c) *for* $g-1 \geq i \geq 1$ *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* $(e_0, e_1, ..., e_{2g-1})$.

Assuming $n \geq 2g$ we can as well start with $d_{2g-1} = 1, d_i = 0, i \neq 2g-1$ and $c_i = 1$ for all $0 \leq i \leq 2g-1$ and let k run from $2g$ till $n-1$. For values of $n < 2g$ no algorithm would be needed as one can directly read off the result. However this way the algorithm works universally.

5.4.2 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

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

If the algorithm is carried out on a restricted device like chip cards, the computation of the extended greatest common divisor and of $M := m - ze \bmod P$ can be made explicit by using polynomial arithmetic (see von zur Gathen, Gerhard [19] for details). For example then a sparse polynomial P is advantageous.

5.4.3 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 $D = [u, v]$ 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 5.19 (Computation of m-folds using τ-adic expansions)
`INPUT:` *$m \in \mathbf{Z}, D = [u, v]$, $u, v \in \mathbf{F}_{q^n}[x]$, $P(T)$, 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*
   $D(i) := iD$; /* use double-and-add/*
   $D(-i) := -D(i)$; /* for free, can also be computed from $D(i)$ when used/*
2. */*Compute a length reduced $M \in \mathbf{Z}[\tau]$ with $m \equiv M \bmod (\tau^n - 1)/(\tau - 1)$;*/*
   (a) *compute $e := \sum e_i T^i \equiv (T^n - 1)/(T - 1) \bmod P$ using Algorithm 5.18;*
   (b) *compute $e' :\equiv e^{-1} \bmod P$ using extended GCD;*
   (c) *compute $z :=$`nearest`$(m \cdot e')$;*
   (d) *let $M = \sum_{i=0}^{2g-1} M_i T^i :\equiv m - e \cdot z \bmod P$;*
3. */*Compute the τ-adic representation of M (see Algorithm 5.4);*/*
   (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 $r_i := 0$;
      else choose $r_i \in R$ with $q^g | M_0 - r_i$;
      */*in even characteristic choose $r_i = M_0$ if $|M_0| = q^g/2$/**
      $d := (M_0 - r_i)/q^g$;
      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 $H := D(r_{i-1})$;*
   (b) *for $i - 2 \leq j \leq 0$ do*
      i. *$H := \sigma(H)$;* /* this means cyclic shifting /*
      ii. *if $r_j \neq 0$ then*
         $H := H + D(r_j)$; /* this means one table-look-up and one addition/*
   (c) *output(H).*

Remarks:

1. The determination of e' (i.e. most of Step 2) depends only on the chosen curve and not on the respective divisor class D and integer m, thus it is done only once and for all at the set-up of the system. 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 also only once and store them along with the curve parameters to obtain further speed-up.

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 M_0 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.

5.5 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.

Example 5.20 *We used this in [26] for a genus two curve over $\mathbf{F}_2$ by the following choice $R' = \{0, \pm 1, \pm 2, \pm 3\}$. Let $c = c_0 + c_1\tau + c_2\tau^2 + c_3\tau^3$. Choose the remainder $r \in R'$ in the following way:*

1. *If $4 \mid c_0$, then $\tau \mid c$ and we clearly use $r = 0$.*

2. *If $4 \nmid c_0$, then we have exactly two choices for r and we can try to make one of the subsequent c_0's divisible by 4:*

   (a) *If $2 \mid c_1$, then there is exactly one $r \in R$ such that $4 \mid c_0 - r$ and $4 \mid ((c_0 - r)/2 + c_1)$, namely*

$c_1 \bmod 4 \backslash c_0 \bmod 8$	1	2	3	5	6	7
0	1	2	3	−3	−2	−1
2	−3	−2	−1	1	2	3

   Using these values for r, the actual r is not zero but the next one will be zero.

(b) *If $2 \nmid c_1$, then we are only able to make the third successor of the actual c_0 at the latest be divisible by 4 by using.*

$c_3 \bmod 2 \backslash c_0 \bmod 8$	1	2	3	5	6	7
0	1	2	3	-3	-2	-1
1	-3	-2	-1	1	2	3

This strategy produces expansions $m = \sum_{i=0}^{l-1} r_i\tau^i$ with coefficients r_i in R', where $r_ir_{i+1}r_{i+2}r_{i+3} = 0 \quad (i \in \{0, \ldots, l-4\})$.
The asymptotic density is $\frac{489}{910}$.

The idea 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. Consider for example the curves with characteristic polynomial of the following form:

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

Let $q = p^r$. If $p^{\lceil gr/2\rceil}$ does not divide a_g, then this curve is not 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 cryptography.) Consider the division step in the expansion of $c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1}$ and choose $r \in R$ to ensure $q^g|c_0 - r$. Then we get:
$c_0 + c_1\tau + \cdots + c_{2g-1}\tau^{2g-1} =$
$= r + \tau(c_1 + c_2\tau + \cdots + (c_g - \frac{c_0-r}{q^g}a_g)\tau^{g-1} + \cdots + c_{2g-1}\tau^{2g-2} - \frac{c_0-r}{q^g}\tau^{2g-1}))$.
The next $g-1$ coefficients of the representation are not influenced by r at all. Thus we obtain g non interacting strands. Taking R to be a complete set of representatives modulo q^{2g} we can force $c_g - \frac{c_0-r}{q^g}a_g$ to be divisible by q^g provided that q and a_g are relatively prime.
We observe that for q even $R = \{0, \pm1, \pm2, \ldots, \pm\frac{q^{2g}}{2} - 1\}\backslash\{\pm$ multiples of $q^g\}$ and for q odd $R = \{0, \pm1, \pm2, \ldots, \pm\frac{q^{2g}-1}{2}\}\backslash\{\pm$ multiples of $q^g\}$ are minimal choices needing $(q^g-1)q^g/2-1$ precomputations 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 $1 \leq i < g$ we have $q^g|a_iq^{g-i}$, because then the remainder of the former $c_g - \frac{c_0-r}{q^g}a_g$ 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

$$P(T) \equiv T^{2g} + a_1T^{2g-1} + \cdots + a_gT^g \bmod q^g, \quad a_g \not\equiv 0 \bmod q.$$

In the next section we provide some examples to explain the procedure for genus 2 curves more directly and give evidence that the theoretical results hold not only asymptotically but also 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. The arithmetic on elliptic curves is faster and the degree of extension – ng – allows to use the Frobenius endomorphism as well, therefore these curves are bad choices as hyperelliptic curves.

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 $r_0 + r_1\tau + \cdots r_{k-1}\tau^{k-1}$ 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 $1 : (k-1) + \frac{1}{q^g} + \frac{1}{q^{2g}} + \cdots = k - 2 + \frac{q^g}{q^g-1}$.
Note that the windowing method can be applied for any $P(T)$.

   Example 5.21 *In [26] we considered coefficients of the form $a + b\tau$ and showed how to slightly reduce the number of precomputations in the case of $q = g = 2$. Let*

$$R' = \{0, \pm 1, \pm 2, \pm(1+\tau), \pm(1-\tau), \pm(1-2\tau), \pm 2 + \tau\}$$

   be the domain of coefficients. This choice enables us to realize a sparse τ-adic expansion in the sense that no two consecutive coefficients are nonzero. Using r as in the following table we force $c_0 + c_1\tau + c_2\tau^2 + c_3\tau^3 - r$ to be divisible by τ^2, i. e. the next coefficient will be zero. If $4|c_0$ then $r = 0$, else take

$c_1 \bmod 4 \backslash c_0 \bmod 8$	1	2	3	5	6	7
0	1	2	$-(1-2\tau)$	$1-2\tau$	-2	-1
1	$1+\tau$	$2+\tau$	$-(1+\tau)$	$1-\tau$	$-2+\tau$	$-(1-\tau)$
2	$1-2\tau$	-2	-1	1	2	$-(1-2\tau)$
3	$1-\tau$	$-2+\tau$	$-(1-\tau)$	$1+\tau$	$2+\tau$	$-(1+\tau)$

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

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

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

Besides the supersingular curves and the two curves considered by Günter, Lange, and Stein [26] there are 4 classes of curves left to investigate. All of them allow to reduce the density by the strategy explained in Section 5.5.
To compute a τ-adic representation we use the following algorithms to realize the strategy

Table 5.1: 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			

Table 5.2: 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			

that for each nonzero coefficient we obtain at least one zero coefficient as stated in Section 5.5. Let $M = c_0 + c_1\tau + c_2\tau^2 + c_3\tau^3$. Take $R = \{0, \pm1, \pm2, \ldots, \pm7\} \backslash \{\pm4\}$. 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 r . 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 5.1 till 5.4 which also list the average length, showing that in fact it is bounded by n plus some constant even less than $2g$.

5.6.2 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 5.5 and 5.6. The expected value for the density is $7/15 = 0.4\bar{6}$. Again we list the average length as well.

Table 5.3: 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 5.4: 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 5.5: 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 5.6: 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 5.7: 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

Table 5.8: 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

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

Finally we consider genus 4 curves. Here we use two different strategies to compare the effects. First we reduce the density by the strategy of Section 5.5. These results are stated in Tables 5.7 and 5.8. In the second case we have to add a further coefficient since the expansion allows a period of length 1. To compare we make 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 5.9 and 5.10.

In all cases the average length is bounded by n plus some small constant however 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 [26] 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 5.5. This will probably lead to results similar to our new strategy, i. e. slightly increase the length.

Table 5.9: 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 5.10: 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

5.7 Comparison

In this section we compare the complexity of the τ-adic method with some standard methods that apply to the divisor class group in general. Furthermore we present timings to confirm the previous results.

5.7.1 Complexity compared to binary double-and-add

We first take the naive double-and-add method as basis to compare and compute the speed-up obtained using the Frobenius endomorphism.
By Section 5.1 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 5.11 and 5.12 provide some examples of the speed-up obtained. 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.

Table 5.11: $q = 2$

g	binary	τ-adic (small)	speed-up factor	τ-adic (large)	speed-up factor
2	$3n$	$3/4n$	4	$3/7n$	7
3	$9/2n$	$7/8n$	$36/7 \sim 5$	$7/15n$	$105/14 \sim 9$
4	$6n$	$15/16n$	$32/5 \sim 6$	$15/31n$	$62/5 \sim 12$

Table 5.12: $q = 5$

g	binary	τ-adic (small)	speed-up factor	τ-adic (large)	speed-up factor
2	$6n$	$24/25n$	$25/4 \sim 6$	$24/49n$	$49/4 \sim 12$
3	$9n$	$124/125n$	~ 9	$124/249n$	~ 18
4	12	$624/625n$	~ 12	$624/1249n$	~ 24

5.7.2 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 the standard windowing method one simply computes the expansion to the base of 2^k, thus needing $2^k - 2$ precomputations. We can even allow the coefficients to be in the above set but use a sliding window of width k to achieve strings of zeros between the entries. A survey on these methods can be found in Gordon's paper [25] and in the Handbook of applied cryptography [45].
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 here $\log_2 m \sim gn \log_2 q$.
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 5.13.

For larger q it gets harder to find the right choice of k to compare. We investigate $q = 5$ as an example. In Tables 5.14 and 5.15 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.

Table 5.13: $q = 2$, 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	$79/16n$	$15/16n$	$79/15$	$1023/224n$	$15/31n$	$10571/1120 \sim 9.4$

Table 5.14: $q = 5$, 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 5.15: $q = 5$, 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	$1310719/131072n$	$624/1249n$	$1637088031/81788928 \sim 20$

5.7.3 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 cyclic shiftings as proposed we square each coefficient. Thus we cannot get the whole speed-up.
We carried out 1000 random scalar multiplications using the τ-adic method with the minimal set of coefficients $R = \{0, \pm 1, \pm 2\}$ 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`.

5.8 Alternatives

In Section 5.5 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 5.22 (τ-adic, without precomputations)
`INPUT:` *$M \in \mathbf{Z}[\tau]$ with $M \equiv m \bmod (\tau^n - 1)/(\tau - 1)$, $D = [u, v]$*
`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 $r := 0$;
   else choose $r \in R$ with $q^g | M_0 - r$;
   */*in even characteristic choose $r = M_0$ if $|M_0| = q^g/2$/**
   $d := (M_0 - r)/q^g$;
   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 $H := H + rD$ *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 $r_i D, r_i \in R$ then the following algorithm is much faster reducing the amount of doublings needed. We adapt the idea of Lee [38] (see below). Let the expansion of m be of length $n \leq \lambda < 2n$. For our choices of g and n this is to be expected by the previous sections. Using $\tau^n - 1 = 0$, we can reduce the length to n accepting coefficients that are at most twice as large. We assume that $\lambda \sim n + 2g$, therefore only the first $2g$ coefficients will be of size at most twice as large. Put $k := \lfloor \log_2(\max_{r_i \in R'} |r_i|) \rfloor + 1$, for this new set of coefficients R', hence $k \sim g \log_2 q + 1$. Let the binary expansion of r_i be $r_i = \sum_{j=0}^{k-1} r_{ij} 2^j$.

Algorithm 5.23 (τ-adic, precomputed expansion)
`INPUT:` $D = [u, v]$, $m = \sum_{i=0}^{\lambda-1} r_i \tau^i$, $r_i \in R'$.

`OUTPUT:` $H = mD$

1. *Initialize* $H := [1, 0]$*;*

2. *for* $j = k - 1$ *to* 1 *do*

   (a) *for* $i = n - 1$ *to* 0 *do*
   $H := H + r_{ij} \sigma^i(D)$*;*

   (b) $H := 2H$*;*

3. *for* $i = n - 1$ *to* 0 *do*
   $H := H + r_{i0} \sigma^i(D)$*;*

4. *output(H).*

For this algorithm we need k doublings and asymptotically $\frac{1}{2}kn$ additions. Thus the complexity is approximately $\frac{1}{2}ng \log_2 q$ for large 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 r_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 r_i is not much larger than storing the binary representation of the r_i's. Unfortunately the way presented in this section does not allow to get rid of the factor g in the complexity.

In general, Lee's [38] approach to use Koblitz curves differs from ours. Also for only moderately large primes he does not use a normal basis representation but 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. 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 the set of remainders 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 the one just presented but he

obtains the $\sigma^i(D)$ via table-look-ups.
The example he provides does not seem to be optimal since the degree of extension used is only 13, thus fairly small (and he proposes even smaller extensions – but larger than 3) and one has to be aware of Weil descent attacks which might work for these degrees as well since the restriction of scalars leads to a variety over the ground field with moderately large dimension that could be handled by the index calculus algorithm. On the other hand Diem [7] shows that for odd characteristic the generalization of the Gaudry-Hess-Smart [23] attack is very unlikely to work faster than attacking the original system.

5.9 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 5.4 that for the action of the Frobenius endomorphism we have $\sigma(D) = sD$, where s is an integer modulo l. Hence, any sum $\sum r_i \tau^i$ corresponds to an integer modulo l. Thus instead of computing a random number smaller than the group order we choose at random λ elements from the set of coefficients R. This idea was pointed out to me by Schroeppel. In [34] Koblitz investigates a similar set-up for elliptic curves, where he credits the idea to Lenstra.

5.9.1 Protocols

We first care about the practicability of these new keys and show that we can still use the standard protocols.
In the *Diffie-Hellman key-exchange* [9] the two parties **A** and **B** agree on a secret key in first selecting secret integers a and b. Then **A** sends aD to **B** and receives bD, where D is the generator of the group they work in. Then both parties can compute the common key abD by using their own (stored) secret integer. Here, one can simply use the vector as the secret number and the whole protocol carries through.
Nearly the same holds for the *ElGamal cryptosystem*. To set up the system each user selects a secret integer, say **A** selects a, and then publishes this multiple of the generator, hence $E_{\mathbf{A}} = aD$. To send a message to **A**, **B** looks up $E_{\mathbf{A}}$ and chooses a random integer k, usually called the nonce. Then he computes both $K = kD$ and $m + kE_{\mathbf{A}}$, where m is the message. Now **A** can decrypt by subtracting aK from the second part. In this system one can replace both, the hidden integer and the nonce by τ-adic expansions with randomly chosen coefficients. Therefore again both parties gain from the speed-up.
In the *signature scheme* for abelian varieties we choose an inversion-free version. For an overview of applicable schemes consider the Handbook of Applied Cryptography [45][Note 11.70]. Let $H(.)$ and $h(.)$ be hash functions from the message space respectively from the first polynomial of a divisor class to the integers modulo the group order l. The hash functions are public. **A** secretly chooses a and publishes $E_{\mathbf{A}} = aD$. To sign a message m, she chooses a nonce k and sends $\rho(k) = kD$ and $\mu(k,m) = aH(m) + kh(kD) \bmod l$ together with the message m. To check the validity of the signature one compares μD and $H(m)E_{\mathbf{A}} + h(\rho)\rho$,

where the addition is understood as addition of divisors. The signature is accepted if these divisors are equal. Note that for space efficiency we need not send both polynomials for $\rho(k)$, the first one and signs to determine the corresponding y-coordinates of the points suffice once one has agreed on a fixed ordering of the finite field. As one can see, the secret numbers are not only taken as multiples of a divisor class but also as integers modulo l. To use the alternative system one can start with the expansions and compute the corresponding integers modulo l using the correspondence of τ and s. To compute k as an integer, we need at least $n-3$ multiplications modulo l plus some additions for the coefficients. It depends on the device whether these modular operations can be performed faster than computing the key as presented in the previous sections. Note that we can compute the integer and kD on the run as we need not store the coefficients and for both computations we start from the highest power. Thus we take $n-1$ times a random element r of R and each time compute the intermediate results $\sigma(\rho)+rD$ and $sk+r \bmod l$.
To obtain a we proceed the same way, but we save a together with its expansion.
One can as well think of transmitting $\mu(k,m)$ as a tau-adic expansion. But then each coefficient can be of size l which is rather ineffective. Thus we do not recommend this.

5.9.2 Collisions

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, 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 $s^{2g}+a_1s^{2g-1}+\cdots+a_gs^g+\cdots+a_1q^{g-1}s+q^g \equiv 0 \bmod l$ 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 and also not equal to the negative of another power (n is an odd 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.

Using $(r_0,\ldots,r_{n-2})$ as a key we can obtain at most $|R|^{n-1} = q^{g(n-1)}$ or l – whichever smaller – different numbers $r_0+\cdots+r_{n-2}s^{n-2} \bmod l$. 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 $n+4g+1$ and that the large prime divisor l is of size $\sim q^{ng}$. Thus taking only those elements of length $\leq n-1$ we lose at most $q^{g(n+4g+1)} - q^{g(n-1)}$ multipliers. But since

we started with l different numbers the left-over $\sim q^{gn} - (q^{g(n+4g+1)} - q^{g(n-1)})$ 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 $(r_0, \ldots, r_{n-2})$ which satisfies $r_i + ts_i \in R$ for $0 \leq i \leq n-2$ for T integers t, then this multiplier occurs at least T 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 integers modulo l represented by the vectors $(r_0, \ldots, r_{n-2})$ 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.
In Chapter 6 we consider the special case of $n = 3$ and derive conditions on the coefficients to ensure that no collisions occur. Unfortunately the method does not generalize to the relatively large kind of n we work with here.

Example 5.24 *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*

$$|\mathrm{Pic}^0(C/\mathbf{F}_{q^{89}})| = 2 \cdot 19156194260824245607349841825210866361531203151291 4969.$$

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 $s = -109094763598619410884498554207763796660522627676801041 \bmod l$. *Choosing a sequence of* 88 *elements r_i from* $R := \{-1, 0, 1, 2\}$ *at random and computing* $\sum_{i=0}^{87} r_i s^i \bmod l$ *we get the multiplier corresponding to the key* $(r_0, \ldots, r_{87})$. *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 multi-set* $S := \{-3, -2, -2, -1, -1, -1, 0, 0, 0, 0, 1, 1, 1, 2, 2, 3\}$ *and computed 10 000 000 such sums modulo l. The zero sum never occurred.*
Hence, there is no obvious weakness and this curve is probably suitable for using this modified set-up.

5.9.3 Attacks

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. Hence, only a brute-force search throughout the keyspace can make use of the reduced amount of possible keys. As usual the group automorphism weakens the system slightly as we remarked in the introduction.

If we consider digital signatures we have to pay more attention. We first outline what happens if parts of the binary expansion of the nonces are known and then show that this attack does not apply for our case. Building upon the work of Boneh and Venkatesan [3] and Howgrave-Graham and Smart [31], Nguyen and Shparlinski [52] invented a way to reveal the secret signing key a if only some bits of the nonces k are known. Our notation and signature scheme differ from the one presented in [52] and they deal with the case of elliptic curves only, however we now present essentially their ideas.
The task of computing a is transformed to a hidden number problem, which can be solved then by lattice reduction. Assume that the highest j bits of k are known, i. e. one knows k' such that $0 \leq k - k' = \kappa < l/2^j$, where as before l denotes the prime group order. As $aH(m) \equiv \mu(k,m) - kh(kD) \equiv \mu(k,m) - (k' + \kappa)h(kD) \bmod l$, the attacker can compute

$$T(k,m) = h(\rho(k))^{-1}H(m), \quad U(k,m) = -k' + \mu(k,m)h(\rho(k))^{-1}$$

from the publicly knows values and gets the problem of finding a such that

$$(U(k,m) - aT(k,m) \bmod l) < l/2^j.$$

This hidden number problem can be solved assumed that one receives enough instances and that the nearest vector problem in the associated lattice can be solved (this is probable as the dimension is relatively low). Nguyen and Shparlinski verified this experimentally for elliptic curves and succeeded even for a small number of known bits as 3. Hence, this attack has to be taken serious.
Using our alternative scheme, the attacker knows that the "most significant τ-adic bits" of k are zero, respectively as the corresponding integer s is easy to compute, that the highest powers of s do not occur. On the other hand we can bound s as an integer from below:
We have that $s^{2g} + a_1 s^{2g-1} + \cdots + a_g s^g + \cdots + a_1 q^{g-1} s + q^g \equiv 0 \bmod l,\ s^n - 1 \equiv 0 \bmod l$ and that $l \sim q^{ng}$. Due to the second equivalence s is at least $> q^g$. Hence, the first equivalence one cannot hold in the integers, hence, $s^{2g} + a_1 s^{2g-1} + \cdots + a_g s^g + \cdots + a_1 q^{g-1} s + q^g > l$. Neglecting lower order terms we can conclude that s is even at least of order $q^{n/2}$, i. e. $l^{1/(2g)}$. Therefore the above considerations reveal only that modulo l the coefficients of s^{n-1} till s^{n+j} are zero (assuming that expansions of length $n + 4g + 1$ could occur in an expansion of an integer modulo l, we can use $j \leq 4g$). But this does only lead to the similar expression

$$(U(k,m) - aT(k,m) \bmod l) < (l/s^j \bmod l),$$

where we can use $k' = 0$ as approximation. As the right hand side is also considered modulo l we cannot extract a hidden number problem from this and this attack fails for τ-adic expansions.

To conclude one can say that using this modified system saves the time needed to compute the expansion without weakening the system.

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 $n + \lambda$ 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 $2\binom{\lambda + r'_{\max} - 1}{r'_{\max}} + 1$ 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 as well.

Chapter 6

Trace-Zero Variety

So far we have considered the case of very small characteristic and of large degree of extension. The reason for this is that for larger characteristic one would need to store many precomputed values if one follows the strategy described so far. Furthermore when the degree of extension is in a medium range the Weil descent attack has to be taken more seriously. However if we consider the case of large characteristic and small degree of extension, the situation becomes interesting again. For example then the field size is still small enough to compute the class number and the characteristic polynomial but the amount of curves is by far larger than for small characteristics as considered so far.
Since the class number attached to the ground field always divides the class number for any extension field, the unused factor is of size q^g, hence fairly large. But we can try to get rid of this factor by restricting to a subgroup. As we have seen before, all divisor classes in the subgroup of large prime order satisfy the equation $(\sigma^n - 1)/(\sigma - 1)(D) = 0$. The last statement is equivalent to saying that these divisor classes have trace zero. In general the elements of trace zero form a subgroup as they are the kernel of a homomorphism and thus they form an abelian sub-variety of dimension $g(n-1)$. For short we denote this abelian variety by G. For this chapter we restrict ourselves to prime ground fields $\mathbf{F}_p$.

If we represent the elements of G like in the larger group $\mathrm{Pic}^0(C/\mathbf{F}_{p^3})$, then the keys are relatively long compared to the group size. We try to establish relations describing this subgroup using fewer variables. To do so we use an explicit description of the field extension as $\mathbf{F}_{p^n} = \mathbf{F}_p[\xi]$ and write each coefficient of the representing polynomials of the divisor class via this basis. Expanding out the defining equations and sorting by the powers of ξ we derive a set of equations over the prime field. The strategy described so far is known as 'Weil restriction' or 'Galois descent'. For a detailed treatment in case of arbitrary characteristic see Diem [7] and Naumann [51]. Then we similarly expand the condition to be of trace zero and get additional equations that allow to reduce the number of variables needed. In the case of elliptic curves the trace-zero variety was studied by Diem and Naumann (see also [8]).

We turn our attention to the special case of genus two curves defined over a prime field and we consider an extension of degree $n = 3$ and appropriate large p. Requiring a group order of 2^{160}, p has to be of size 2^{40}. Therefore the characteristic is unequal to $2, 3$ and 5. Let the hyperelliptic curve be given by an equation of the form $C : y^2 = f(x)$, where $f = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \in \mathbf{F}_p[x]$. The change of variables $x \to x' - f_4/5$

leads to a polynomial where the coefficient of x'^4 is zero. This is the kind of defining equation we consider from now on, i. e. without loss of generality put $f_4 = 0$. Furthermore to ease the following computations we assume the case of Kummer extensions, i. e. that $p \equiv 1 \bmod 3$, hence, to construct $\mathbf{F}_{p^3} = \mathbf{F}_p[\xi]$ we use the polynomial $y^3 - \alpha$, which is irreducible when α is no third power in $\mathbf{F}_p$. As $\mathbf{F}_p$ contains a third root of unity η the roots of $y^3 - \alpha$ are $\xi, \eta\xi, \eta^2\xi$. To get rid of further variables, namely α, we even assume that $\alpha^3 = 1$, say $\alpha = \eta$, and since $y^3 - \alpha$ is assumed to be irreducible, $\mathbf{F}_p$ does not contain ninth roots of unity, hence $p \equiv 4, 7 \bmod 9$. Note that this last restriction is not necessary, it just saves space to write down the equations which are clumsy nevertheless.

The remainder of this chapter is organized as follows: We first investigate which kinds of divisor classes lie in the trace zero part, then we find equations describing this part in any case. However we do not succeed in finding shorter expansions. In the following section we consider the efficiency of the arithmetic in this group and finally we deal with security issues and compare the efficiency to that of groups with the same parameters. We conclude providing an examples of a suitable curve for which the trace zero subgroup is of prime order, the arithmetic is fast and the set of multipliers we use in the cryptosystem is of appropriate size.

6.1 Different Kinds of Divisor Classes on Trace-Zero Variety

In the case of a genus two curve each divisor class has a unique representative of the form $D = P_1 + P_2 - 2\infty$, $D = P_1 - \infty$ or $D = 0$. We now study which kinds of divisor classes can occur in the trace-zero variety, where the field is of degree 3 over a prime field.

First of all the zero element satisfies the trace zero relation and this is also obvious from the fact that the relation defines a subgroup.

If the divisor class $D \neq 0$ is defined over the ground field $\mathbf{F}_p$ – this is equivalent to $\sigma(D) = D$ – then D has to be of order 3 to satisfy $\sigma^2(D) + \sigma(D) + D = 0$. If we want to describe this part of the group geometrically we need to deal with Cantors division polynomials for hyperelliptic curves (see Cantor [5] for the describing equations). On the other hand for the applications we want the subgroup to be cyclic – and not to contain a factor from the group over the ground field. Hence, we restrict to divisor class groups containing no class of order three over $\mathbf{F}_p$. This can be checked easily since we assume that the characteristic is small enough to allow the computation of the group order.

From now on we assume that D is not defined over the ground field, hence $\sigma(D) \neq D$. As was stated in Section 2.2 we can associate to each divisor class two polynomials $u(x), v(x) \in \mathbf{F}_{p^3}[x]$, where $\deg(v) < \deg(u) \leq g$ and u is monic. Since we consider curves of genus two besides the zero element there are only two cases left to consider – that of $\deg u = 1$ and that of $\deg u = 2$.

Let first $\deg u = 1$. Then the divisor class can be represented by $P_1 - \infty$, where $P_1 = (x_1, y_1) \in C(\mathbf{F}_{p^3}) \setminus C(\mathbf{F}_p)$. As we consider a degree three extension x_1 cannot be in $\mathbf{F}_p$, hence, $x_1 \neq \sigma(x_1)$.

In the first step of the composition of two classes (Algorithm 2.30), the greatest common divisor of the two first polynomials is computed. In this case of $D + \sigma(D)$ it is one, thus the corresponding semi-reduced ideal class is simply $[x^2 - (x_1 + \sigma(x_1))x + x_1\sigma(x_1), ((y_1 - \sigma(y_1))x + x_1\sigma(y_1) - \sigma(x_1)y_1)/(x_1 - \sigma(x_1))]$. Furthermore the first polynomial is of degree 2 and thus will not be reduced further in the reduction Algorithm 2.31. The divisor class is in G iff this resulting class equals $-\sigma^2(D)$ which is represented by $[x - \sigma^2(x_1), -\sigma^2(y_1)]$. This cannot happen as the degrees are different.
Via $P \mapsto P - \infty$ the curve is embedded into the divisor class group. Hence this result shows, that the curve lies completely outside the variety under consideration.

To investigate the case of $\deg(u) = 2$ we must further distinguish the ways the representing divisor is built. Let the class of D be represented by $P_1 + P_2 - 2\infty$, where P_1, P_2 may lie in a quadratic extension of $\mathbf{F}_{p^3}$. If so, then P_2 has to be the conjugate of P_1 under this extension. Assume first that $P_2 = \sigma(P_1)$, where as usual σ denotes the Frobenius endomorphism corresponding to the degree three extension. Then both points are in $C(\mathbf{F}_{p^3})$. The trace zero relation means that $P_1 + \sigma(P_1) + \sigma(P_1 + \sigma(P_1)) + \sigma^2(P_1 + \sigma(P_1)) - 6\infty = 0$. Rearranging leads to $2(P_1 + \sigma(P_1) + \sigma^2(P_1) - 3\infty) = 0$. This can happen if either $P_1 + \sigma(P_1) + \sigma^2(P_1) - 3\infty = 0$ or if it is of order two. The first case is excluded by the $\deg(u) = 1$ case and the second by requiring additionally that $\mathrm{Pic}^0(C/\mathbf{F}_{p^3})$ contains no element of order two not in $\mathrm{Pic}^0(C/\mathbf{F}_p)$. The proof to exclude the case of $D = 2P_1 - 2\infty$ follows the same lines.

We have just shown:

Theorem 6.1 *Let $\mathrm{Pic}^0(C/\mathbf{F}_{p^3})$ contain no elements of order 2 or 3. Then the elements of the trace zero variety G are the divisor classes represented by*

$$P_1 + P_2 - 2\infty,$$

where $P_1 \neq P_2, \sigma(P_2), \sigma^2(P_2)$ and not both $P_1, P_2 \in C(\mathbf{F}_p)$.

6.2 Describing Equations

As we have seen the divisor classes not defined over the ground field are represented by $[u(x), v(x)] = [x^2 + u_1x + u_2, v_1x + v_2]$, $u_i, v_i \in \mathbf{F}_{p^3}$, where $u | f - v^2$. Hence, these elements can also be described via the remainder of dividing $f - v^2$ by a monic degree two polynomial. This leads to an explicit description of an open affine part of $\mathrm{Pic}^0(C/\mathbf{F}_{p^3})$ by the vanishing of the following polynomials:

$$\begin{aligned} F_1(u_1, u_2, v_1, v_2) &:= -f_1 + f_2u_1 - f_3(u_1^2 - u_2) - (u_1^2 - u_2)^2 + u_1^2u_2 - u_1v_1^2 + 2v_1v_2, \\ F_2(u_1, u_2, v_1, v_2) &:= -f_0 + f_2u_2 - f_3u_1u_2 - u_1u_2(u_1^2 - 2u_2) - u_2v_1^2 + v_2^2. \end{aligned}$$

Since the curve was defined over the ground field, $f_i \in \mathbf{F}_p$. We now expand the variables via $u_i = U_{i0} + U_{i1}\xi + U_{i2}\xi^2, v_i = V_{i0} + V_{i1}\xi + V_{i2}\xi^2$ where $\mathbf{F}_{p^3} = \mathbf{F}_p[\xi]$. This leads to the following system of equations that have to vanish simultaneously:
from F_1:

$-U_{10}^4 - 12\eta U_{10}^2U_{11}U_{12} + 3U_{10}^2U_{20} - U_{10}^2f_3 - 4\eta U_{10}U_{11}^3 + 6\eta U_{10}U_{11}U_{22} - 4\eta^2U_{10}U_{12}^3 + 6\eta U_{10}U_{12}U_{21} - U_{10}V_{10}^2 - 2\eta U_{10}V_{11}V_{12} + U_{10}f_2 - 6\eta^2U_{11}^2U_{12}^2 + 3\eta U_{11}^2U_{21} + 6\eta U_{11}U_{12}U_{20} -$

$2\eta U_{11}U_{12}f_3 - 2\eta U_{11}V_{10}V_{12} - \eta U_{11}V_{11}^2 + 3\eta^2 U_{12}^2 U_{22} - 2\eta U_{12}V_{10}V_{11} - \eta^2 U_{12}V_{12}^2 - U_{20}^2 + U_{20}f_3 - 2\eta U_{21}U_{22} + 2V_{10}V_{20} + 2\eta V_{11}V_{22} + 2\eta V_{12}V_{21} - f_1,$

$-4U_{10}^3 U_{11} - 6\eta U_{10}^2 U_{12}^2 + 3U_{10}^2 U_{21} - 12\eta U_{10}U_{11}^2 U_{12} + 6U_{10}U_{11}U_{20} - 2U_{10}U_{11}f_3 + 6\eta U_{10}U_{12}U_{22} - 2U_{10}V_{10}V_{11} - \eta U_{10}V_{12}^2 - \eta U_{11}^4 + 3\eta U_{11}^2 U_{22} - 4\eta^2 U_{11}U_{12}^3 + 6\eta U_{11}U_{12}U_{21} - U_{11}V_{10}^2 - 2\eta U_{11}V_{11}V_{12} + U_{11}f_2 + 3\eta U_{12}^2 U_{20} - \eta U_{12}^2 f_3 - 2\eta U_{12}V_{10}V_{12} - \eta U_{12}V_{11}^2 - 2U_{20}U_{21} + U_{21}f_3 - \eta U_{22}^2 + 2V_{10}V_{21} + 2V_{11}V_{20} + 2\eta V_{12}V_{22},$

$-4U_{10}^3 U_{12} - 6U_{10}^2 U_{11}^2 + 3U_{10}^2 U_{22} - 12\eta U_{10}U_{11}U_{12}^2 + 6U_{10}U_{11}U_{21} + 6U_{10}U_{12}U_{20} - 2U_{10}U_{12}f_3 - 2U_{10}V_{10}V_{12} - U_{10}V_{11}^2 - 4\eta U_{11}^3 U_{12} + 3U_{11}^2 U_{20} - U_{11}^2 f_3 + 6\eta U_{11}U_{12}U_{22} - 2U_{11}V_{10}V_{11} - \eta U_{11}V_{12}^2 - \eta^2 U_{12}^4 + 3\eta U_{12}^2 U_{21} - U_{12}V_{10}^2 - 2\eta U_{12}V_{11}V_{12} + U_{12}f_2 - 2U_{20}U_{22} - U_{21}^2 + U_{22}f_3 + 2V_{10}V_{22} + 2V_{11}V_{21} + 2V_{12}V_{20},$

and from F_2:

$-U_{10}^3 U_{20} - 3\eta U_{10}^2 U_{11}U_{22} - 3\eta U_{10}^2 U_{12}U_{21} - 3\eta U_{10}U_{11}^2 U_{21} - 6\eta U_{10}U_{11}U_{12}U_{20} - 3\eta^2 U_{10}U_{12}^2 U_{22} + 2U_{10}U_{20}^2 - U_{10}U_{20}f_3 + 4\eta U_{10}U_{21}U_{22} - \eta U_{11}^3 U_{20} - 3\eta^2 U_{11}^2 U_{12}U_{22} - 3\eta^2 U_{11}U_{12}^2 U_{21} + 4\eta U_{11}U_{20}U_{22} + 2\eta U_{11}U_{21}^2 - \eta U_{11}U_{22}f_3 - \eta^2 U_{12}^3 U_{20} + 4\eta U_{12}U_{20}U_{21} - \eta U_{12}U_{21}f_3 + 2\eta^2 U_{12}U_{22}^2 - U_{20}V_{10}^2 - 2\eta U_{20}V_{11}V_{12} + U_{20}f_2 - 2\eta U_{21}V_{10}V_{12} - \eta U_{21}V_{11}^2 - 2\eta U_{22}V_{10}V_{11} - \eta^2 U_{22}V_{12}^2 + V_{20}^2 + 2\eta V_{21}V_{22} - f_0,$

$-U_{10}^3 U_{21} - 3U_{10}^2 U_{11}U_{20} - 3\eta U_{10}^2 U_{12}U_{22} - 3\eta U_{10}U_{11}^2 U_{22} - 6\eta U_{10}U_{11}U_{12}U_{21} - 3\eta U_{10}U_{12}^2 U_{20} + 4U_{10}U_{20}U_{21} - U_{10}U_{21}f_3 + 2\eta U_{10}U_{22}^2 - \eta U_{11}^3 U_{21} - 3\eta U_{11}^2 U_{12}U_{20} - 3\eta^2 U_{11}U_{12}^2 U_{22} + 2U_{11}U_{20}^2 - U_{11}U_{20}f_3 + 4\eta U_{11}U_{21}U_{22} - \eta^2 U_{12}^3 U_{21} + 4\eta U_{12}U_{20}U_{22} + 2\eta U_{12}U_{21}^2 - \eta U_{12}U_{22}f_3 - 2U_{20}V_{10}V_{11} - \eta U_{20}V_{12}^2 - U_{21}V_{10}^2 - 2\eta U_{21}V_{11}V_{12} + U_{21}f_2 - 2\eta U_{22}V_{10}V_{12} - \eta U_{22}V_{11}^2 + 2V_{20}V_{21} + \eta V_{22}^2,$

$-U_{10}^3 U_{22} - 3U_{10}^2 U_{11}U_{21} - 3U_{10}^2 U_{12}U_{20} - 3U_{10}U_{11}^2 U_{20} - 6\eta U_{10}U_{11}U_{12}U_{22} - 3\eta U_{10}U_{12}^2 U_{21} + 4U_{10}U_{20}U_{22} + 2U_{10}U_{21}^2 - U_{10}U_{22}f_3 - \eta U_{11}^3 U_{22} - 3\eta U_{11}^2 U_{12}U_{21} - 3\eta U_{11}U_{12}^2 U_{20} + 4U_{11}U_{20}U_{21} - U_{11}U_{21}f_3 + 2\eta U_{11}U_{22}^2 - \eta^2 U_{12}^3 U_{22} + 2U_{12}U_{20}^2 - U_{12}U_{20}f_3 + 4\eta U_{12}U_{21}U_{22} - 2U_{20}V_{10}V_{12} - U_{20}V_{11}^2 - 2U_{21}V_{10}V_{11} - \eta U_{21}V_{12}^2 - U_{22}V_{10}^2 - 2\eta U_{22}V_{11}V_{12} + U_{22}f_2 + 2V_{20}V_{22} + V_{21}^2,$
where the respective first equations belong to 1, the second to ξ and the last to ξ^2.

We now consider the condition to be of trace zero in more detail and use the addition formulae of Spallek [69] to compose two classes. They have been obtained making explicit what is done in the composition and reduction algorithms. She considers only the case of $\deg(u) = 2$ which means no restriction in our case. By the above theorem we have that each divisor class in G is represented by $P_1 + P_2 - 2\infty$, where $P_1 \neq P_2, \sigma(P_2), \sigma^2(P_2)$ and $P_1, P_2 \notin C(\mathbf{F}_p)$. Hence, in adding $D + \sigma(D)$ we compose two classes corresponding to four distinct points. This case is abbreviated by $p1234$ by Spallek. Let the corresponding ideal class of D be given by $[x^2 + u_1 x + u_2, v_1 x + v_2]$.
We use the following abbreviations:

$$\begin{aligned}
v_1^* &= ((v_2 - \sigma(v_2))(u_1 - \sigma(u_1)) - (v_1 - \sigma(v_1))(u_2 - \sigma(u_2))),\\
v_2^* &= ((v_1 - \sigma(v_1))(\sigma(u_1)\sigma(u_2) - u_1u_2) + (v_2 - \sigma(v_2))((u_1 - \sigma(u_1))(u_1 + \sigma(u_1)) - (u_2 - \sigma(u_2)))),\\
v_3^* &= \sigma(v_1)(u_2(u_2 - \sigma(u_2)) + u_1\sigma(u_2)(u_1 - \sigma(u_1)) - v_1(\sigma(u_1)u_2(u_1 - \sigma(u_1)) + \sigma(u_2)(u_2 - \sigma(u_2))) +\\
&\quad +(v_2 - \sigma(v_2))(u_1\sigma(u_1)(u_1 - \sigma(u_1)) - \sigma(u_1)u_2 + u_1\sigma(u_2)),\\
n &= (u_2 - \sigma(u_2))^2 - (u_1 - \sigma(u_1))(u_2\sigma(u_1) - u_1\sigma(u_2))).
\end{aligned}$$

In G we have that $D + \sigma(D) = -\sigma^2(D)$, hence in the representation via polynomials the result of the composition should be

$$[x^2 + \sigma^2(u_1)x + \sigma^2(u_2), -(\sigma^2(v_1)x + \sigma^2(v_2))].$$

We can express the coefficients for the first polynomial via

$$\begin{aligned} \sigma^2(u_1) &\stackrel{!}{=} -(u_1 + \sigma(u_1)) + 2v_2^*/v_1^* - (n/v_1^*)^2, \\ \sigma^2(u_2) &\stackrel{!}{=} -(u_2 + \sigma(u_2)) + (u_1 + \sigma(u_1))^2 - u_1\sigma(u_1) + 2(v_3^* - v_2^*(u_1 + \sigma(u_1)))/v_1^* + \\ &\quad +(v_2^*/v_1^*)^2 + (u_1 + \sigma(u_1))(n/v_1^*)^2. \end{aligned}$$

Due to the construction of the finite field we have that $u_i + \sigma(u_i) + \sigma^2(u_i) = 3U_{i0}$. This allows to simplify the equations a little leading to
$3U_{10}v_1^{*2} = 2v_1^*v_2^* - n^2$ and
$3U_{20} + 3(u_1 + \sigma(u_1))U_{10} = (v_2^*/v_1^*)^2 + 2v_3^*/v_1^* + (u_1 + \sigma(u_1))^2 - u_1\sigma(u_1)$.

However using these formulae the expanded equations do still cover several pages, to get a taste: From the first equation we obtain upon dividing out $3\eta^2$ respectively 3:

$U_{10}U_{11}^2V_{22}^2 + 4U_{10}U_{11}U_{12}V_{21}V_{22} - 2U_{10}U_{11}U_{21}V_{12}V_{22} - 2U_{10}U_{11}U_{22}V_{11}V_{22} - 2U_{10}U_{11}U_{22}V_{12}V_{21} + 3U_{10}U_{12}^2V_{21}^2 - 2U_{10}U_{12}U_{21}V_{11}V_{22} - 2U_{10}U_{12}U_{21}V_{12}V_{21} - 2U_{10}U_{12}U_{22}V_{11}V_{21} + U_{10}U_{21}^2V_{12}^2 + 4U_{10}U_{21}U_{22}V_{11}V_{12} + U_{10}U_{22}^2V_{11}^2 = 3(-U_{10}^2U_{11}^2U_{22}^2 - 4U_{10}^2U_{11}U_{12}U_{21}U_{22} - U_{10}^2U_{12}^2U_{21}^2 - 2U_{10}U_{11}^3U_{21}U_{22} + 6U_{10}U_{11}^2U_{12}U_{20}U_{22} + 2U_{10}U_{11}^2U_{12}U_{21}^2 + 4U_{10}U_{11}^2V_{22}^2 + 6U_{10}U_{11}U_{12}^2U_{20}U_{21} + 2\eta U_{10}U_{11}U_{12}^2U_{22}^2 + 16U_{10}U_{11}U_{12}V_{21}V_{22} + 6U_{10}U_{11}U_{21}U_{22}^2 - 6U_{10}U_{11}U_{21}V_{12}V_{22} - 6U_{10}U_{11}U_{22}V_{11}V_{22} - 6U_{10}U_{11}U_{22}V_{12}V_{21} - 2\eta U_{10}U_{12}^3U_{21}U_{22} + 4U_{10}U_{12}^2V_{21}^2 + 6U_{10}U_{12}U_{21}^2U_{22} - 6U_{10}U_{12}U_{21}V_{11}V_{22} - 6U_{10}U_{12}U_{21}V_{12}V_{21} - 6U_{10}U_{12}U_{22}V_{11}V_{21} + 2U_{10}U_{21}^2V_{12}^2 + 8U_{10}U_{21}U_{22}V_{11}V_{12} + 2U_{10}U_{22}^2V_{11}^2 + 2U_{11}^4U_{20}U_{22} - 2U_{11}^3U_{12}U_{20}U_{21} + 2\eta U_{11}^3U_{12}U_{22}^2 + 4U_{11}^3V_{21}V_{22} - 6U_{11}^2U_{12}^2U_{20}^2 - 4\eta U_{11}^2U_{12}^2U_{21}U_{22} + 2U_{11}^2U_{12}V_{21}^2 - 2U_{11}^2U_{20}U_{22}^2 - 2U_{11}^2U_{20}V_{12}V_{22} + 2U_{11}^2U_{21}^2U_{22} - 4U_{11}^2U_{21}V_{11}V_{22} - 4U_{11}^2U_{21}V_{12}V_{21} - 2U_{11}^2U_{22}V_{11}V_{21} - 2\eta U_{11}U_{12}^3U_{20}U_{22} + 2\eta U_{11}U_{12}^3U_{21}^2 + 2\eta U_{11}U_{12}^2V_{22}^2 - 8U_{11}U_{12}U_{20}U_{21}U_{22} - 4U_{11}U_{12}U_{20}V_{11}V_{22} - 4U_{11}U_{12}U_{20}V_{12}V_{21} - 2U_{11}U_{12}U_{21}^3 - 2U_{11}U_{12}U_{21}V_{11}V_{21} - 2\eta U_{11}U_{12}U_{22}^3 - 2\eta U_{11}U_{12}U_{22}V_{12}V_{22} + 2U_{11}U_{20}U_{21}V_{12}^2 + 4U_{11}U_{20}U_{22}V_{11}V_{12} + 4U_{11}U_{21}^2V_{11}V_{12} + 2U_{11}U_{21}U_{22}V_{11}^2 - 2U_{11}U_{21}V_{22}^2 - 4U_{11}U_{22}V_{21}V_{22} + 2\eta U_{12}^4U_{20}U_{21} + 4\eta U_{12}^3V_{21}V_{22} - 2U_{12}^2U_{20}U_{21}^2 - 2U_{12}^2U_{20}V_{11}V_{21} + 2\eta U_{12}^2U_{21}U_{22}^2 - 2\eta U_{12}^2U_{21}V_{12}V_{22} - 4\eta U_{12}^2U_{22}V_{11}V_{22} - 4\eta U_{12}^2U_{22}V_{12}V_{21} + 4U_{12}U_{20}U_{21}V_{11}V_{12} + 2U_{12}U_{20}U_{22}V_{11}^2 + 2\eta U_{12}U_{21}U_{22}V_{12}^2 - 4U_{12}U_{21}V_{21}V_{22} + 4\eta U_{12}U_{22}^2V_{11}V_{12} - 2U_{12}U_{22}V_{21}^2 - 6U_{21}^2U_{22}^2 + 2U_{21}^2V_{12}V_{22} + 4U_{21}U_{22}V_{11}V_{22} + 4U_{21}U_{22}V_{12}V_{21} + 2U_{22}^2V_{11}V_{21})$,

$U_{10}U_{11}^2V_{21}^2 - 2\eta U_{10}U_{11}U_{12}V_{22}^2 - 2U_{10}U_{11}U_{21}V_{11}V_{21} + 2\eta U_{10}U_{11}U_{22}V_{12}V_{22} - 2\eta U_{10}U_{12}^2V_{21}V_{22} + 2\eta U_{10}U_{12}U_{21}V_{12}V_{22} + 2\eta U_{10}U_{12}U_{22}V_{11}V_{22} + 2\eta U_{10}U_{12}U_{22}V_{12}V_{21} + 1U_{10}U_{21}^2V_{11}^2 - 2\eta U_{10}U_{21}U_{22}V_{12}^2 - 2\eta U_{10}U_{22}^2V_{11}V_{12} = 3(-U_{10}^2U_{11}^2U_{21}^2 + 2\eta U_{10}^2U_{11}U_{12}U_{22}^2 + 2\eta U_{10}^2U_{12}^2U_{21}U_{22} + 2U_{10}U_{11}^3U_{20}U_{21} + 2\eta U_{10}U_{11}^3U_{22}^2 + 2\eta U_{10}U_{11}^2U_{12}U_{21}U_{22} + 4U_{10}U_{11}^2V_{21}^2 - 6\eta U_{10}U_{11}U_{12}^2U_{20}U_{22} - 4\eta U_{10}U_{11}U_{12}^2U_{21}^2 - 8\eta U_{10}U_{11}U_{12}V_{22}^2 + 2U_{10}U_{11}U_{21}^3 - 6U_{10}U_{11}U_{21}V_{11}V_{21} - 2\eta U_{10}U_{11}U_{22}^3 + 6\eta U_{10}U_{11}U_{22}V_{12}V_{22} - 2\eta U_{10}U_{12}^3U_{20}U_{21} - 8\eta U_{10}U_{12}^2V_{21}V_{22} - 6\eta U_{10}U_{12}U_{21}U_{22}^2 + 6\eta U_{10}U_{12}U_{21}V_{12}V_{22} + 6\eta U_{10}U_{12}U_{22}V_{11}V_{22} + 6\eta U_{10}U_{12}U_{22}V_{12}V_{21} + 2U_{10}U_{21}^2V_{11}^2 - 4\eta U_{10}U_{21}U_{22}V_{12}^2 - 4\eta U_{10}U_{22}^2V_{11}V_{12} - U_{11}^4U_{20}^2 - 6\eta U_{11}^3U_{12}U_{20}U_{22} - 2\eta U_{11}^3V_{22}^2 + 6\eta U_{11}^2U_{12}^2U_{20}U_{21} - \eta^2U_{11}^2U_{12}^2U_{22}^2 - 4\eta U_{11}^2U_{12}V_{21}V_{22} - 2U_{11}^2U_{20}U_{21}^2 - 2U_{11}^2U_{20}V_{11}V_{21} - 4\eta U_{11}^2U_{21}U_{22}^2 + 4\eta U_{11}^2U_{21}V_{12}V_{22} + 2\eta U_{11}^2U_{22}V_{11}V_{22} + 2\eta U_{11}^2U_{22}V_{12}V_{21} + 4\eta U_{11}U_{12}^3U_{20}^2 + 2\eta^2U_{11}U_{12}^3U_{21}U_{22} + 2\eta U_{11}U_{12}^2V_{21}^2 + 4\eta U_{11}U_{12}U_{20}U_{22}^2 + 4\eta U_{11}U_{12}U_{20}V_{12}V_{22} + 2\eta U_{11}U_{12}U_{21}^2U_{22} + 2\eta U_{11}U_{12}U_{21}V_{11}V_{22} +$

$2\eta U_{11}U_{12}U_{21}V_{12}V_{21} - 2\eta U_{11}U_{12}U_{22}V_{11}V_{21} + 2U_{11}U_{20}U_{21}V_{11}^2 - 2\eta U_{11}U_{20}U_{22}V_{12}^2 - 2\eta U_{11}U_{21}^2V_{12}^2 - 4\eta U_{11}U_{21}U_{22}V_{11}V_{12} - 2U_{11}U_{21}V_{21}^2 + 2\eta U_{11}U_{22}V_{22}^2 + -\eta^2U_{12}^4U_{21}^2 - 2\eta^2U_{12}^3V_{22}^2 + 4\eta U_{12}^2U_{20}U_{21}U_{22} + 2\eta U_{12}^2U_{20}V_{11}V_{22} + 2\eta U_{12}^2U_{20}V_{12}V_{21} + 2\eta U_{12}^2U_{21}^3 - 2\eta U_{12}^2U_{21}V_{11}V_{21} + 4\eta^2U_{12}^2U_{22}V_{12}V_{22} - 2\eta U_{12}U_{20}U_{21}V_{12}^2 - 4\eta U_{12}U_{20}U_{22}V_{11}V_{12} + 2\eta U_{12}U_{21}U_{22}V_{11}^2 + 2\eta U_{12}U_{21}V_{22}^2 - 2\eta^2U_{12}U_{22}^2V_{12}^2 + 4\eta U_{12}U_{22}V_{21}V_{22} - U_{21}^4 + 2U_{21}^2V_{11}V_{21} + 4\eta U_{21}U_{22}^3 - 4\eta U_{21}U_{22}V_{12}V_{22} - 2\eta U_{22}^2V_{11}V_{22} - 2\eta U_{22}^2V_{12}V_{21}),$

$-2U_{10}U_{11}^2V_{21}V_{22} - 2U_{10}U_{11}U_{12}V_{21}^2 + 2U_{10}U_{11}U_{21}V_{11}V_{22} + 2U_{10}U_{11}U_{21}V_{12}V_{21} + 2U_{10}U_{11}U_{22}V_{11}V_{21} + \eta U_{10}U_{12}^2V_{22}^2 + 2U_{10}U_{12}U_{21}V_{11}V_{21} - 2\eta U_{10}U_{12}U_{22}V_{12}V_{22} - 2U_{10}U_{21}^2V_{11}V_{12} - 2U_{10}U_{21}U_{22}V_{11}^2 + \eta U_{10}U_{22}^2V_{12}^2 = 3(2U_{10}^2U_{11}^2U_{21}U_{22} + 2U_{10}^2U_{11}U_{12}U_{21}^2 - \eta U_{10}^2U_{12}^2U_{22}^2 - 2U_{10}U_{11}^3U_{20}U_{22} - 6U_{10}U_{11}^2U_{12}U_{20}U_{21} - 4\eta U_{10}U_{11}^2U_{12}U_{22}^2 - 8U_{10}U_{11}^2V_{21}V_{22} + 2\eta U_{10}U_{11}U_{12}^2U_{21}U_{22} - 8U_{10}U_{11}U_{12}V_{21}^2 - 6U_{10}U_{11}U_{21}^2U_{22} + 6U_{10}U_{11}U_{21}V_{11}V_{22} + 6U_{10}U_{11}U_{21}V_{12}V_{21} + 6U_{10}U_{11}U_{22}V_{11}V_{21} + 2\eta U_{10}U_{12}^3U_{20}U_{22} + 2\eta U_{10}U_{12}^3U_{21}^2 + 4\eta U_{10}U_{12}^2V_{22}^2 - 2U_{10}U_{12}U_{21}^3 + 6U_{10}U_{12}U_{21}V_{11}V_{21} + 2\eta U_{10}U_{12}U_{22}^3 - 6\eta U_{10}U_{12}U_{22}V_{12}V_{22} - 4U_{10}U_{21}^2V_{11}V_{12} - 4U_{10}U_{21}U_{22}V_{11}^2 + 2\eta U_{10}U_{22}^2V_{12}^2 - \eta U_{11}^4U_{22}^2 + 4U_{11}^3U_{12}U_{20}^2 + 2\eta U_{11}^3U_{12}U_{21}U_{22} - 2U_{11}^3V_{21}^2 + 6\eta U_{11}^2U_{12}^2U_{20}U_{22} - \eta U_{11}^2U_{12}^2U_{21}^2 + 2\eta U_{11}^2U_{12}V_{22}^2 + 4U_{11}^2U_{20}U_{21}U_{22} + 2U_{11}^2U_{20}V_{11}V_{22} + 2U_{11}^2U_{20}V_{12}V_{21} + 4U_{11}^2U_{21}V_{11}V_{21} + 2\eta U_{11}^2U_{22}^3 - 2\eta U_{11}^2U_{22}V_{12}V_{22} - 6\eta U_{11}U_{12}^3U_{20}U_{21} - 4\eta U_{11}U_{12}^2V_{21}V_{22} + 4U_{11}U_{12}U_{20}U_{21}^2 + 4U_{11}U_{12}U_{20}V_{11}V_{21} + 2\eta U_{11}U_{12}U_{21}U_{22}^2 - 2\eta U_{11}U_{12}U_{21}V_{12}V_{22} + 2\eta U_{11}U_{12}U_{22}V_{11}V_{22} + 2\eta U_{11}U_{12}U_{22}V_{12}V_{21} - 4U_{11}U_{20}U_{21}V_{11}V_{12} - 2U_{11}U_{20}U_{22}V_{11}^2 - 2U_{11}U_{21}^2V_{11}^2 + 2\eta U_{11}U_{21}U_{22}V_{12}^2 + 4U_{11}U_{21}V_{21}V_{22} - 2U_{11}U_{22}V_{21}^2 - \eta U_{12}^4U_{20}^2 - 2\eta U_{12}^3V_{21}^2 - 2\eta U_{12}^2U_{20}U_{22}^2 - 2\eta U_{12}^2U_{20}V_{12}V_{22} - 4\eta U_{12}^2U_{21}^2U_{22} + 2\eta U_{12}^2U_{21}V_{11}V_{22} + 2\eta U_{12}^2U_{21}V_{12}V_{21} + 4\eta U_{12}^2U_{22}V_{11}V_{21} - 2U_{12}U_{20}U_{21}V_{11}^2 + 2\eta U_{12}U_{20}U_{22}V_{12}^2 - 4\eta U_{12}U_{21}U_{22}V_{11}V_{12} + 2U_{12}U_{21}V_{21}^2 - 2\eta U_{12}U_{22}^2V_{11}^2 - 2\eta U_{12}U_{22}V_{22}^2 + 4U_{21}^3U_{22} - 2U_{21}^2V_{11}V_{22} - 2U_{21}^2V_{12}V_{21} - 4U_{21}U_{22}V_{11}V_{21} - \eta U_{22}^4 + 2\eta U_{22}^2V_{12}V_{22}).$

We did not succeed in finding relations among these equations that allow to reduce the number of variables needed to represent the elements of G. Clearly – like in $\mathrm{Pic}^0(C/\mathbf{F}_{p^3})$ – one can compute the V_{ij} from the knowledge of all U_{ij} and some bits determining the signs of the second coordinates of the points involved.

6.3 Computing in the Trace Zero Variety

We now turn our attention to the arithmetic in G. Since G is a subgroup of $\mathrm{Pic}^0(C/\mathbf{F}_{p^3})$. We can use the equations stated in Chapter 3. However this implies that the computation in the subgroup is as slow as in the whole group. On the other hand as finding a description using fewer variables was not possible, obtaining addition formulae for this variety is a hopeless task; it even is for the somewhat easier case of elliptic curves.

Remember that we represent $\mathbf{F}_{p^3}$ by a polynomial basis via the irreducible polynomial $y^3 - \eta$. Using Karatsuba multiplication we need 8 multiplications in the ground field to compute a product. Squaring can be performed by either 6 squarings and 2 multiplications or 5 multiplications and 3 squarings in the ground field. It depends on the system used which is faster, we chose the first for implementation. To compute the inverse of w we make use of Cramer's rule, i.e. use the resultant. Let $\Delta = w_2^3\eta^2 + w_1^3\eta + w_0^3 - 3w_0w_1w_2\eta$. Then $(w_2\xi^2 + w_1\xi + w_0)^{-1} = (v_2\xi^2 + v_1\xi + v_0)/\Delta$, where $v_2 = w_1^2 - w_2w_0, v_1 = w_2^2\eta - w_1w_0, v_0 = w_0^2 - w_2w_1\eta$. In total this takes 1 inversion, 2 squarings and 12 multiplications in $\mathbf{F}_p$.

Since we did not succeed in finding shorter representations for the elements of the trace-zero variety, we do not need that η is a third root of unity. To have that $y^3 - \eta$ is irreducible we simply need to assure that η is no third power in $\mathbf{F}_p$. It is highly likely that there exists such an η of comparably small size that we need not count computing η times an element as a multiplication but perform it by adding. When the field has been chosen to allow this the costs reduce to 6 squarings for a squaring in $\mathbf{F}_{p^3}$, 6 multiplications for a multiplication and 1 inversion in the large field corresponds to 3 squarings, 9 multiplications and 1 inversion in the small field. We thank Avanzi for pointing out this idea.

Now as we work in odd characteristic we can use Harley's analysis for the complexity of the operations in G (see Chapter 3). From the above considerations we know that we are always in the general case where the first polynomials have degree two. A general addition in G can be performed using 2 inversions, 3 squarings, and 24 multiplications in $\mathbf{F}_{p^3}$ whereas a doubling needs 3 more squarings.
By the above computations this equals 162 (222) multiplications, 24 (22) squarings, and 2 inversions in $\mathbf{F}_p$ for an addition. The numbers in brackets refer to the case when no small η is avaliable. To double we need 162 (228) multiplications, 42 (40) squarings, and 2 inversions in $\mathbf{F}_p$.
Note that these considerations hold true for the whole divisor class group and do not depend on the restriction to G. However, we can try to speed up the computation in G:
Like in the first part of this thesis the Frobenius endomorphism in this variety satisfies its characteristic polynomial inherited from $\mathrm{Pic}^0(C/\mathbf{F}_{p^3})$ and from the construction it also satisfies $T^2+T+1=0$. Since now n is smaller than $2g$ we cannot use the reduction technique described in the first part since this would lead to longer expressions than needed, and we cannot use the asymptotic bound for the length as n but also take into account the $4g$. We proceed like in Section 5.9: Instead of using an integer m as the secret number hidden in mD we take a tuple (r_1, r_2) of integers and take $r_1D + r_2\sigma(D)$ as our secret key.
Again we need to be aware of collisions but in this special case we can show:

Theorem 6.2 *Let C be a hyperelliptic curve of genus two over $\mathbf{F}_p$, let $T^4 + a_1T^3 + a_2T^2 + a_1pT + p^2$ be the characteristic polynomial of the Frobenius endomorphism and consider a base field extension of degree 3. Let D be a generator of a subgroup of prime order l of the trace zero variety G.*
Put

$$\mathbf{r} := \min\left\{ \left\lfloor \frac{l}{\max\{p^2 + a_1p - 2a_2 + a_1 + 1, p^2 + a_1 - a_1p - 1\}} \right\rfloor, \frac{p^2 - a_2 + a_1}{\gcd(p^2 - a_2 + a_1, a_1p - a_2 + 1)} \right\}.$$

Then the $\mathbf{r}^2$ divisor classes $r_0D + r_1\sigma(D)$, $0 \le r_i < \mathbf{r}$ are distinct.

Proof. Since for the elements of G the Frobenius endomorphism satisfies T^2+T+1 and its characteristic polynomial we can combine these equations to obtain

$$(*) \qquad (a_1p - a_2 + 1)T + p^2 - a_2 + a_1 = 0$$

by inserting subsequently the trace zero relation.
Now assume that $r_0 + r_1\sigma = r_0' + r_1'\sigma$ as endomorphisms. Subtracting we obtain $(r_0 - r_0') + (r_1 - r_1')\sigma = 0$, where by construction $|r_i - r_i'| < \mathbf{r}$. We multiply this equation by $a_1p - a_2 + 1$ and use $(*)$

$$(a_1p - a_2 + 1)(r_0 - r_0') - (p^2 - a_2 + a_1)(r_1 - r_1') = 0.$$

By the choice of $\mathbf{r}$ we have $|(a_1p - a_2 + 1)(r_0 - r_0') - (p^2 - a_2 + a_1)(r_1 - r_1')| < \max\{p^2 + a_1p - 2a_2 + a_1 + 1, p^2 + a_1 - a_1p - 1\} \cdot \mathbf{r} < l$ and therefore this equality not only holds modulo l but also in the integers. But again by the choice of $\mathbf{r}$ and as $p > 3$ this implies that $(r_0 - r_0') = (r_1 - r_1') = 0$. □

Hence, if $\mathbf{r}$ is comparably large – we assume l to be of size p^4 and if the involved greatest common divisor is not too large we can hope for $\mathbf{r} \sim p^2$ – then there are sufficiently many elements obtainable using this construction. The size of $\mathbf{r}$ can be computed from the knowledge of the characteristic polynomial. We now assume that $\mathbf{r} \sim p^2$, thus $\mathbf{r}^2 \sim |G|$.

Remarks:

1. For this small choice of n, $(*)$ enables us to compute the s of Section 5.9 in terms of a_1 and a_2. This and the short length of a suitable expansion allow us to deal with collisions and to find choices of the coefficients to avoid them. Note however that here like in that section the length is $n-1$ and one can hope that $\mathbf{r} \sim p^2 = p^g$. This resembles the set up we have chosen before, hence giving evidence that the assumptions on the probability of collisions made there hold true.

2. Like with the alternative set-up it is possible to use the usual protocols with this tuple as key. For signing we again choose a scheme without inversions. Furthermore as we have seen in the proof, the integer s modulo l which corresponds to τ can be computed by two multiplications and one inversion modulo l. The value of s can be saved as a parameter of the curve. To get the multiplier belonging to the tuple we need one further multiplication modulo l.

Put $\rho = \lfloor \log_2 \mathbf{r} \rfloor + 1 \sim 2 \log_2 p$. Naumann [51] uses the following strategy to compute $r_0 D + r_1 \sigma(D)$ from the binary representations $r_i = \sum_{j=0}^{\rho-1} r_{ij} 2^j$. As we start from the least significant bits, we need not precompute these expansions but can as well compute them on the run dividing by two with remainder in each step. For implementations in software where one has no access to the binary representation of the integers this might be advantageous.

Algorithm 6.3
`INPUT:` $D = [u, v], r_0, r_1, r_i = \sum_{j=0}^{\rho-1} r_{ij} 2^j, r_{ij} \in \{0,1\}$;
`OUTPUT:` $H = r_0 D + r_1 \sigma(D)$;

1. *initialize* $T := D$;
   if $r_{00} = 1$ *then*
   if $r_{10} = 0$ *then* $H := T$;
   else $H := -\sigma^2(T)$;
   else if $r_{10} = 1$ *then* $H := \sigma(T)$;
   else $H := [1, 0]$;

2. *for* $j = 1$ *to* $\rho - 1$ *do*

   (a) $T := 2T$;

   (b) *if* $r_{0j} = 1$ *then*
   if $r_{1j} = 0$ *then* $H := H + T$;

else $H := H - \sigma^2(T)$;
else if $r_{1j} = 1$ *then* $H := H + \sigma(T)$;

3. *output* (H).

Note that in step j we have that $T = 2^j D$ and that in G the following holds: $T + \sigma(T) = -\sigma^2(T)$. $\sigma(T)$ and $-\sigma^2(T)$ can be computed easily from T.
Using this algorithm the computation of $r_0 D + r_1 \sigma(D)$ takes ρ doublings and asymptotically $3/4$ this number of additions, i.e. approximately $7/2 \log_2 p$ compositions over $\mathbf{F}_{p^3}$. Note that although we do not use a normal basis here, we can still assume the operation of the Frobenius endomorphism to be almost for free as $\sigma(D)$ and $\sigma^2(D)$ need only 8 multiplications in $\mathbf{F}_p$ each for precomputed η^2. This is cheap compared to the costs of a usual group operation.

To be more exact with probability of $1/2$ we need to compute either $\sigma(T)$ or $\sigma^2(T)$ and therefore the computation of an m-fold in G needs

$$7 \log_2 p \text{ inversions, } 120(113) \log_2 p \text{ squarings and } 575(797) \log_2 p \text{ multiplications}$$

on average, where again the numbers in brackets denote the costs for arbitrary η.

We can also use a *NAF representation* of the integers r_i. These representations allow coefficients in $\{0, \pm 1\}$ and have an asymptotic density of $1/3$ and are at most one bit longer than the usual binary expansions. We may assume that 1 and -1 occur equally often, i.e. with probability $1/6$. As the digits of r_1 and r_0 are uncorrelated we obtain the case of $r_{0j} = r_{1j} = 0$ with probability $4/9$. In all other cases we need to perform at least one addition in G. With probability $2 \cdot 1/9$ we have $r_{0j} = \pm 1$ and $r_{1j} = 0$. In all other cases we need to compute either $\pm\sigma(T)$ or $\pm\sigma^2(T)$. If both coefficients are nonzero and of opposite sign we use $\pm(T - \sigma(T)) = \pm(2T + \sigma^2(T))$, thus with probability $1/18$ we need two additions. Note here that $2T$ is computed the following step anyway and that due to the non-adjacency property both r_{ij+1} are zero, thus an overflow due to the carries cannot occur. This amounts to ρ doublings and $11/18\rho$ additions in G plus $8/3\rho$ further multiplications in $\mathbf{F}_p$ which is equivalent to

$$6.\bar{4} \log_2 p \text{ inversions, } 113.\bar{3}(106.\bar{8}) \log_2 p \text{ squarings and } 500.\bar{2}(729.\bar{7}) \log_2 p \text{ multiplications}$$

in $\mathbf{F}_p$ on average which is faster than the method presented before. However a bit more bookkeeping is needed to be aware of the carries.

6.4 Security and Comparison

Before being able to compare this group to other suitable ones we need to investigate the security parameters. As we have seen G is contained in an open affine part of dimension two of the associated abelian variety over $\mathbf{F}_{p^3}$. The restriction of scalars transforms this to a 6-dimensional variety over $\mathbf{F}_p$. Restricting to the trace zero variety forces the dimension to drop down by two. Hence, we can view G as a four dimensional abelian variety defined over the prime field $\mathbf{F}_p$. Other varieties of dimension four are for example the Jacobians of hyperelliptic curves of genus four. Note however that by results of Diem usually the resulting variety is not principally polarized, hence, does not belong to a hyperelliptic curve.

Table 6.1: Number of Elementary Operations for Elliptic Curves, Operations in $\mathbf{F}_{p''}$, $m \sim p^4$

Operation	Inversion	Squaring	Multiplication
Addition	1	1	2
Doubling	1	2	2
m-fold	$6\log_2 p$	$10\log_2 p$	$12\log_2 p$
m-fold, NAF	$5.\bar{3}\log_2 p$	$9.\bar{3}\log_2 p$	$10.\bar{6}\log_2 p$

Varieties of dimension 4 may still be considered as sufficiently secure since Gaudry's version of the index calculus attack is not faster than Pollard's rho method. However this justifies our rather special choice of the parameters – for larger genus and/or for larger degree of extension the resulting variety would be of larger dimension, thus less suitable.
From what was said above we can compare the arithmetic on G to that of the divisor class group of a genus two curve defined over a field $\mathbf{F}_q$, where $q = p'^2 \sim p^2$ or $q = p'$, p' a prime, and also to that of an elliptic curve defined over a field of size $\sim p^4$, this field can be assumed to be prime or of extension degree 2 or 4.
On the one hand we need to take into consideration the efficient-to-compute group automorphism that can be used in the attacks. On the other hand as far as we can see one cannot use it in G itself since we could not find shorter formulae to describe the variety and the arithmetic on it. Therefore the attacker has to work in $\mathrm{Pic}^0(C/\mathbf{F}_{p^3})$ which is by far larger ($\sim 2^{240}$). Therefore we decide to take for comparison only the curves defined over prime fields.

Since we consider the other curves over prime fields we can only use the double-and-add method to compute m-folds (see Section 5.1) there. We also take into consideration the effects of using a NAF of the multiplier. For both groups – the elliptic curve as well as for the divisor class group of the genus two curve – the group-size is $\sim p^4$, therefore we assume that the binary representation of the multiplier is on average of length $4\log_2 p$. In the double-and-add method we need $4\log_2 p$ doublings and $2\log_2 p$ additions, using the NAF we need $4/3\log_2 p$ additions.

We first consider the arithmetic on an *elliptic curve*. For a general addition we need 1 inversion, 1 squaring, and 2 multiplications in the finite field $\mathbf{F}_{p''}$, $p'' \sim p^4$, prime. To double a point we need one more squaring. This results in the following Table 6.1.
For the *genus two curve* we can make use of the formulae in Chapter 3 to perform the arithmetic. This leads to Table 6.2.

Put $\kappa = \log_2 \lambda$. In the prime field $\mathbf{F}_\lambda$ the complexity of division, multiplication and squaring is $\tilde{O}(\kappa)$, where the *soft-O* notation suppresses logarithmic terms. Therefore we can assume that an operation in $\mathbf{F}_{p'}$ takes at least 2 times as long as in $\mathbf{F}_p$ and in $\mathbf{F}_{p''}$ it takes at least 4 times as long. Assuming this to hold true we can make a theoretical comparison in Table 6.3.
From this Table 6.3 we see that the comparison depends heavily on the trade-off between the complexities of inversion and multiplication in the respective ground field. But one sees as well that the arithmetic on the elliptic curve will be faster than in the divisor class of the genus two curve for both kinds of expansions. If one assumes that squarings take

Table 6.2: Number of Elementary Operations for Curve of Genus 2, Operations in $\mathbf{F}_{p'}$, $m \sim p^4$

Operation	Inversion	Squaring	Multiplication
Addition	2	3	24
Doubling	2	6	24
m-fold	$12 \log_2 p$	$30 \log_2 p$	$144 \log_2 p$
m-fold, NAF	$10.\bar{6} \log_2 p$	$28 \log_2 p$	$128 \log_2 p$

Table 6.3: Theoretical Comparison

	Inversion	Squaring	Multiplication
Elliptic Curve	24	40	48
Genus 2 Curve	24	60	288
Trace-Zero Group	7	120	575
no small η	7	113	797
Elliptic Curve, NAF	21	37	43
Genus 2 Curve, NAF	21	48	256
Trace-Zero Group, NAF	6	113	500
no small η	6	107	730

All entries are to be multiplied by $\log_2 p$. Entries are rounded to nearest integer.

Table 6.4: Timings

	Inversion	Squaring	Multiplication
$p \sim 2^{40}$	2.1e-05	1e-06	2e-06
$p \sim 2^{80}$	6.5e-05	4e-06	5e-06
$p \sim 2^{160}$	1.3e-04	1.3e-05	1.5e-05

Table 6.5: Experimental Costs, in Multiplications in $\mathbf{F}_p$

	Inversion	Squaring	Multiplication
$p \sim 2^{40}$	21/2	1/2	**1**
$p \sim 2^{80}$	65/2	2	5/2
$p \sim 2^{160}$	65	13/2	15/2

approximately as long as multiplications and consider the case of small η only, we obtain that it is also faster than in G as otherwise an inversion would take more than 36 times as long as one multiplication (respectively even 38 times for the NAF). For the comparison of G and the genus two curve one inversion must take at least 21 times as long as a multiplication for G to be faster using the double-and-add method or the NAF. From these considerations, using G does not seem to be promising as elliptic curves are always faster, but we might be able to beat genus two curves.

However the proportion of the complexities of multiplication and inversion depends on the size of the prime field. Furthermore we will see that the computations in the larger fields are more expensive than expected by these theoretical considerations and that the difference between multiplication and squaring cannot be neglected. Therefore we need experimental data to compare the efficiencies of the group operations. Using the NTL-library Blady [2] obtains the timings in Table 6.4.

To compare the complexities we now use the above tabular to express all operations in multiplications in $\mathbf{F}_p$. We use this table for the exchange ratios (Table 6.5). Note that the performance in the larger fields is not as good as we expected in the theoretical comparison, especially the inversions are more expensive. This shows that the constants and logarithmic terms in the complexity are relevant for our comparison.

This allows us to get the experiment-based performances in Table 6.6 for the group order of size 2^{160} in all cases. We only rounded the result.
Hence, for this size of $p \sim 2^{40}$ we see that the arithmetic on the elliptic curve is faster in any case. However, if we assume that a small element $\eta \in \mathbf{F}_p$ that is not a third power exists, then the operations in the trace-zero variety are faster than for the genus two curve for double-and-add and NAF. Note that the relative advantage decreases. This is clear as the costs for the doublings remain constant and the density decreases

Table 6.6: Experiment-Based Comparison, in Multiplications in $\mathbf{F}_p$

	double-and-add	NAF
Elliptic Curve	$545 \log_2 p$	$487 \log_2 p$
Genus 2 Curve	$810 \log_2 p$	$723 \log_2 p$
Trace-Zero Group	$709 \log_2 p$	$625 \log_2 p$
no small η	$927 \log_2 p$	$851 \log_2 p$

All entries are rounded to nearest integer.

from 1/2 to 1/3 in the genus two curve whereas in G we can only achieve to lower it from 3/4 to 11/18. If no small η is avaliable then computing an m-fold in G is slower than in the other groups, but choosing G we do not loose much compared to a genus two curve.

To conclude one can say that the trace zero variety can be chosen for an efficient cryptosystem and as long as we have an appropriate η the computation of m-folds is even faster than on a genus two curve over a prime field and we have the second advantage over the genus two curve that we can compute the group order and still the resulting variety is defined over a prime field.

6.5 Example

In this section we provide a curve for which the group G is suitable for cryptographic applications.

We are very thankful to Weng for computing the following example via the CM-construction for hyperelliptic curves studied in her thesis [76]. It is not hard to compute further examples by simply invoking her algorithm until a curve is found such that the class number for $C/\mathbf{F}_{p^3}$ contains a large prime factor.

We start from the CM field defined by adjoining the roots of $z^4 + 14z^2 + 5$ to $\mathbf{Q}$. This leads to the curve
$\tilde{C} : y^2 = x'^5 + 7962401853847x'^4 + 6699639715934x'^3 + 42066039120411x'^2 + 49281149108367x' + 51518968113431.$
We consider the curve over the finite field with $p = 75013447438681$ elements, where the class group is of size 5627016660495156428378904916. Note that $p \equiv 7 \bmod 9$, and that $2^{(p-1)/3} = 49604531110780$. Therefore 2 is not a third power in $\mathbf{F}_p$ and we can construct the extension field $\mathbf{F}_{p^3}$ by $y^3 - 2$, i.e. we are in the case where the field arithmetic is fast. To fit into our scheme of defining equations we make a change of variables and obtain

$$C : y^2 = x^5 + 34672227040499x^3 + 73462645749327x^2 + 2792938982291x + 22543037864275.$$

Over $\mathbf{F}_{p^3}$ we have

$$\begin{aligned}|\mathrm{Pic}^0(C/\mathbf{F}_{p^3})| &= 178170069884878082099774294777122888103489172517617130201225512393497836950134832436\\ &= 5627016660495156428378904916 \cdot 31663327236212551408173507207346298370655198947919293721,\end{aligned}$$

hence the class number for the ground field times a prime with 184 binary digits.

The characteristic polynomial of the Frobenius endomorphism is
$T^4 - 8480356T^3 + 138416435415946T^2 - 636140739067303050436T + 56270172966357570792550197 61.$

Therefore
$\mathbf{r} = \min\{562701729663569057927217 6232, 5627017296635618662811123459\}$
$= 5627017296635618662811123459$, hence there are $\mathbf{r}^2 \sim 2^{184}$ different elements obtainable by the strategy described above, which means that $\mathbf{r}^2 \sim |G|$.

Chapter 7

Conclusion

In this chapter we investigate to what extend the results presented in this thesis generalize and show how to prevent certain attacks that use informations leaking from the implementation, e. g. power attacks. Finally we give an outlook on what could be done as well and consider some prerequisites the finite field has to satisfy.

7.1 Generalizations and Practical Considerations

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 [27] and Harasawa and Susuki [28].

To set up a system one needs a divisor class of full order l which usually is equivalent to requiring this divisor to be in the trace zero subgroup. 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 [33], interpreting $P - \infty$ 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.
Like in the elliptic curve case one need not store both components of the divisor class – the first polynomial and appropriately chosen bits to remember the second coordinates of the points involved suffice.

7.2 Side-Channel Attacks

Some devices leak information on the binary representation of the key, as the power consumption for or the time to perform an addition is different from that of a doubling. This

allows the attacker to obtain the private key when he can observe the deciphering.
In most of the schemes presented here, doublings are replaced by applications of the Frobenius endomorphism which are almost for free. It has to be studied experimentally how this effects the power consumption, but probably the complexity of the Frobenius endomorphism is not negligible enough such that one can find out how many times it was applied until the next table look-up and addition. However, as there are $q^g - 1$ nonzero coefficients the key-space is not reduced too much from the knowledge of some bits to be zero as long as the density is not too low and there are enough nonzero coefficients to avoid brute force search. To the possible use of the attack of Nguyen and Shparlinski the same remarks as in Section 5.9 apply.

Like for the use of binary expansions we can introduce dummy-operations and perform a table look-up and an addition (with an unused variable) each time the coefficient is zero to disguise the structure of the representation of the multiplier. However, this leads to a density of 1 and therefore to a much worse complexity. If the attacker can observe the address of the precomputed values than we even need to compute the respective multiple of the point like in Section 5.8. Assume now that the attacker does not have such a direct access. However it is possible that he can observe whether the element to be added is negated. This is very probable in characteristic two where we compute $[u, -v-h]$, where $-v-h$ is reduced modulo u and h can be of the same degree as u. Then we need to store the elements $D(-i)$ as well in Algorithm 5.19. In this case we can avoid introducing an unused variable by the following adaption of Hasan [30]: Using $\tau^n - 1 = 0$ in the subgroup under consideration we reduce the length of the expansion to n allowing larger coefficients. For large n the coefficients will all be of size less than $q^g - 1$. Put $r_{\min} < 0$ the minimal and $r_{\max}$ the maximal coefficient of this enlarged set of coefficients. Then for all coefficients r_i, $0 \le i \le n-1$ of the expansion $r_i - r_{\min} + 1$ is an integer > 0. We precompute the multiples $D(1), \dots, D(r_{\max} - r_{\min} + 1)$ in advance. Then $\sum_{i=0}^{n-1}(r_i - r_{\min} + 1)\sigma^i(D)$ still computes mD as $(-r_{\min} + 1)(\sigma^n - 1)/(\sigma - 1)(D) = 0$. But now we perform a used table-look-up and an addition for each of the n coefficients. However, the density is 1 and this trick simply avoids some bookkeeping.

Furthermore one can make use of the strategy of Giessmann and Löwe [24]. For the expansion they use a nonadjacent form with base 2 and process two consequent bits per time. This means that they consider 00, 01, 0-1, 10, and -10 as coefficients. For each double-bit they perform 2 doublings and one addition – which is not used only in the case of the double-bit 00. Thus compared with the NAF they started with, they have the same number of doublings but for every two coefficients they perform an addition instead of only for one third of the coefficients. This leads to a density of 1/2 which is much better compared to 1 obtained above using the obvious method and does not introduce a larger complexity except for a bit of bookkeeping.
We can make use of the same method when we use the reduced density version of Section 5.5 and we lose even less as the density is increased only from $(q^g - 1)/(2q^g - 1)$ to 1/2. If we use the τ-adic windowing method then this generalizes directly. Otherwise when we use an enlarged set of integer coefficients we do not have the non-adjacency property but only that g of any $2g$ coefficients are zero. In principle the same method works when we consider $2g$ coefficients per time but it involves more intermediate variables. Thus using the lower density version applies only for large enough devices, this time not only for storing the fixed multiples but also to store variables in the computations.

In the trace-zero subgroup the situation is a bit different. If we take the double-and-add version then in 3 of 4 cases we add a class and in 2 of 4 cases we also perform g further multiplications in the ground field to compute the needed power of the Frobenius endomorphism. Thus it might be possible to dramatically reduce the search-space from the leaked information. To avoid the second distinguishing property and to speed up the computations we can store $\sigma(2^j D)$ and $-\sigma^2(2^j D)$ along with the precomputed $2^j D$. If one uses the system several times with the same D this is advantageous anyway if enough storage is available. In any case we do not lose too much inserting dummy operations as we increase the density from 3/4 to 1. Making use of the NAF version provides the same problems depending on how much the attacker can observe.

We now deal with the more sophisticated *differential attacks*.
This kind of attacks applies if the leaked information is disguised by random noise or is even hidden by inserting the dummy-operations referred to above, hence, to those cases where one cannot read off the expansion directly. We assume that the attacker has access to a device that computes m-times the input and tries to extract information on m using side-channel information such as power consumption, time to perform the operation etc. This means that he can observe the input of the device and some characteristic values during the computation. The method is best described using an example. Assume that the device computes mD for some group element D using the binary representation of m. Let λ be the length of the representation. Then the algorithm first doubles D and then adds D in case of $r_{\lambda-2} = 1$. Then it computes two times the output of the previous step, i.e. either $4D$ or $6D$ depending on $r_{\lambda-2}$. Now assume that there is a difference in the representations of $2D$ and $3D$ that influences the performance of the doubling step; this is not too unlikely to happen, it might be the binary representation of one coordinate for example. The respective multiples can be computed on an additional device to find out how they differ in their representation. Depending on the side-channel information observed during the computation in the device under attack he now knows which intermediate result was taken and can thus recover $r_{\lambda-2}$ – at least if enough instances can be observed. Note that this attack is still possible when we introduce not used operations as proposed before.
In more generality, assume that the attacker knows the highest coefficients $r_{\lambda-1}, r_{\lambda-2}, \ldots, r_{j+1}$ of the used expansion of the multiplier m, in case of the double-and-add method these are the bits and for Koblitz curves these are the coefficients of the τ-adic expansion. Then he guesses a value for the next coefficient r_j, chooses t random elements of the group $D_1, \ldots, D_t$ and computes $E_k = \sum_{i=j}^{\lambda-1} r_i \mathbf{b}^{i-j}(D_k)$ by an additional device, where $\mathbf{b}$ is the base used for the expansion, i.e. 2 for the double-and-add method and σ for the τ-adic method. The elements $D_1, \ldots, D_t$ are supposed to be the observed cyphertexts the device decrypts. We do not assume that the attacker can influence the choice of these elements. According to the output of his device he groups the D_k into two sets $\mathcal{S}_{\texttt{true}}$ and $\mathcal{S}_{\texttt{false}}$; this two-valued function might for example be the value of a bit of E_k – this depends on the information obtainable from the leakage and the representation of E_k. Let $C(k)$ denote the side-channel information associated to the computation of mD_k. If the guess for r_j was incorrect then the difference

$$\langle C(k) \rangle_{\substack{1 \le k \le t \\ D_k \in \mathcal{S}_{\texttt{true}}}} - \langle C(k) \rangle_{\substack{1 \le k \le t \\ D_k \in \mathcal{S}_{\texttt{false}}}}$$

is approximately zero, as then the partition was at random. By $\langle . \rangle$ we denote the mean value.

For a correct guess the difference is strictly different from 0. Once r_j is known the same steps are performed to extract the next coefficient. Note that for this attack to apply the attacker must be able to observe several times the computation of a fixed multiple of changing elements.

To avoid such attacks one can insert randomness in the computation of m-times the input. In [6] Coron generalizes the differential power attack (DPA) to elliptic curves and proposes countermeasures. He suggests to add a random multiple of the group order to the multiplier m before computing mD. For the double-and-add method this leads to much longer expansions, hence to a worse running time. Using this literally in our case of Koblitz curves does not help at all. Note that we reduce modulo $(\tau^n - 1)/(\tau - 1)$ and that the group order is always a multiple of this in $\mathbf{Z}[\tau]$ (at least when it is almost prime as we suppose). This means that m plus any multiple of the group order is always reduced to the same element in $\mathbf{Z}[\tau]$. This holds for all hyperelliptic curves independent of the genus.

Hasan [30] deals especially with elliptic Koblitz curves over $\mathbf{F}_2$. As Solinas [68] showed the τ-adic expansions are of length at most n. Since we have that $(\tau^n - 1) = 0$ in the group we consider we can rotate the expansion using $r_{n-1}\tau^{n-1} + r_{n-2}\tau^{n-2} + \cdots + r_1\tau + r_0 = \tau^k(r_{k-1}\tau^{n-1} + r_{k-2}\tau^{n-2} + \cdots + r_{k+1}\tau + r_k)$. He also investigates key masking and inserting redundant symbols to protect the curves, but this leads to more kinds of operations the computing device has to perform.

A different approach is given by Joye and Tymen [32] also for elliptic Koblitz curves. Instead of reducing m modulo $\tau^n - 1$ before computing the expansion, they reduce it modulo $\rho(\tau^n - 1)$, where ρ is a random element of $\mathbf{Z}[\tau]$ of bounded norm. If for the complex norm N we have $\log_2 \mathrm{N}(\rho) \sim 40$ then the expansion will be of length 200 instead of 160 which does not seem to be too bad as the expansion is still of density 1/3 when they use a NAF. Besides one does not need to introduce further routines except for choosing a random ρ as only reduction modulo an element of $\mathbf{Z}[\tau]$ and the algorithm to compute the expansion are needed.
We think that it is even better to first compute $m \bmod (\tau^n - 1)/(\tau - 1)$ as before and then to add a random multiple $\alpha(\tau^n - 1)/(\tau - 1)$, where α is of norm less than $\mathrm{N}(\rho)$. The result is similar to what is obtained above and m is equally hidden in the full length of the element to expand. The important advantage is that we can make use of the precomputed values for $(\tau^n - 1)/(\tau - 1)$ and $(\tau - 1)/(\tau^n - 1)$ in $\mathbf{Z}[\tau]$ and only need to compute the product $\alpha(\tau^n - 1)/(\tau - 1)$ in $\mathbf{Z}[\tau]$ additionally. Using this for ρ like above also results in expansions of length 200 but the computation of the expansion is faster.

In the case of higher genus curves we can use the same approach, except that finding elements of bounded norm is not as immediate as for the elliptic case due to the structure of the norm (see Section 5.3 for details). However, slightly reducing the space for these random elements α we can choose those where the coefficients $\alpha = c_0 + \cdots + c_{2g-1}\tau^{2g-1}$ satisfy $(\sum_{j=0}^{2g-1} |c_j|\sqrt{q}^j)^2 \leq 2^{L-2}/(\sqrt{q} - 1)^2$; this means that we can choose all c_i at random under the condition that $|c_j| \leq 2^{(L+2)/2}/(q^g - 1)$, where L is the chosen parameter to guarantee enough security. The expansions will be longer by $+L$. If we use a new random α each time the algorithm is invoked the information of the expansion of the multiplier should be well hidden.

7.3 Outlook

When choosing a Koblitz 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 leading to more fields with such an efficient arithmetic was recently investigated by Nöcker [53].
It is a topic of current research to find optimal choices for pairs of curves and finite fields. For hardware implementations it is also useful to work over fields of characteristic 2.

For using the trace zero subgroup about half of the primes are suitable as characteristic as we impose $p \equiv 1 \bmod 3$. And a large proportion (about two thirds) should have a small element η that is not a third power. Furthermore the arithmetic in the ground field $\mathbf{F}_p$ depends heavily on the binary representation of p and its length in relation to the word size. Also here one should find especially efficient pairs of curves and ground fields.

For the alternative set-up for Koblitz curves we did not succeed in finding requirements on the length and the coefficients of the expansions that guarantee that no collisions occur. Here it might help to consider vanishing sums of roots of unity to derive further conditions. Probably the size of the coefficients should depend on the coefficients of the characteristic polynomial of the Frobenius endomorphism like in Theorem 6.2.

Although we proved the finiteness of the τ-adic expansions, the bounds proved on the length for arbitrary curves are weaker than the experiments suggest. We succeeded in finding a way to determine the maximal length for a given curve and motivated that the bounds from the experiments are likely to hold by considering genus two curves. Getting more restrictive bounds on the length and on the size of the coefficients would nicely round off this work.

Finally it would be nice to find shorter representations of the elements in the trace zero subgroup and to find addition formulae to perform the group operations using only this restricted set of variables. However, in the present state solving only the first task does not look too promising. If one considers the elliptic curve case and hopes for analogous results, switching from the representation using fewer variables to that of the usual group would imply factoring a polynomial of degree at least 5, which is possible, but also takes time and requires further tasks to be performed by the perhaps restricted device.

Bibliography

[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] G. Blady, Die Weil-Restriktion in der Kryptographie, *Diploma Thesis*, Universität Gesamthochschule Essen (2001).

[3] D. Boneh, R. Venkatesan, Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes, in: *Proceedings of Crypto '96* Lecture Notes in Computer Science **1109**, (Springer 1996), **129-142**.

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

[5] D. Cantor, On the analogue of the division polynomials for hyperelliptic curves, *Journal für die reine und angewandte Mathematik* **447** (1994), 91-145.

[6] J.-S. Coron, Resistance against differential power analysis for elliptic curve cryptosystems, in: *Cryptographic Hardware and Embedded Systems CHES 1999* Lecture Notes in Computer Science **1717**, (Springer 1999), **392-302**.

[7] C. Diem, A Study on Theoretical and Practical Aspects of Weil-Restriction of Varieties, *Ph.D. Thesis*, Universität Gesamthochschule Essen (2001).

[8] C. Diem, N. Naumann, On the Structure of Weil-Restriction of Abelian Varieties, (2001), to appear.

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

[10] 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.

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

[12] 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.

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

[14] 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.

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

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

[17] S. Galbraith, Weil Descent of Jacobians, to appear.

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

[19] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*, (Cambridge University Press 1999).

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

[21] 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.

[22] 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.

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

[24] E.-G. Giessmann, Ein schneller Algorithmus zur Punktevervielfachung, der gegen Seitenkanalattacken resistent ist, talk at *Workshop über Theoretische und praktische Aspekte von Kryptographie mit Elliptischen Kurven*, Berlin, 11.-12.06.2001.

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

[26] 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).

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

[28] 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.

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

[30] M. A. Hasan, Power Analysis Attacks and Algorithmic Approaches to their Countermeasures for Koblitz Curve Cryptosystems, in: *Cryptographic Hardware and Embedded Systems CHES 2000* Lecture Notes in Computer Science **1965**, (Springer 2000), 93-108.

[31] N. A. Howgrave-Graham, N. P. Smart, Lattice attacks on digital signature schemes, *Designs, Codes and Cryptography* **23** (2001), 283-290.

[32] M. Joye, C. Tymen, Protections against Differential Analysis for Elliptic Curve Cryptography – An Algebraic Approach, in: *Cryptographic Hardware and Embedded Systems CHES 2001* Lecture Notes in Computer Science **2162**, (Springer 2001), to appear.

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

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

[35] 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.

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

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

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

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

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

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

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

[43] 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.

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

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

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

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

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

[49] 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.

[50] D. Mumford, *Tata Lectures on Theta II*, (Birkhäuser 1984).

[51] N. Naumann, Weil-Restriktion abelscher Varietäten, *Diploma Thesis*, Universität Gesamthochschule Essen (1999).

[52] P. Q. Nguyen, I. E. Shparlinski, The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces, to appear.

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

[54] 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.

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

[56] 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.

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

[58] J. M. Pollard, Monte Carlo methods for index computation (mod p), *Mathematics of Computation* **32** (1978), 918-924.

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

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

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

[62] 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.

[63] 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.

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

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

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

[67] 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.

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

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

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

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

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

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

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

[75] 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.

[76] A. Weng, Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation, *Ph.D. Thesis*, Universität Gesamthochschule Essen (2001).