Constructive and Computational Aspects of Cryptographic Pairings

Michael Naehrig

Constructive and Computational Aspects of Cryptographic Pairings

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de
Technische Universiteit Eindhoven, op gezag van de
Rector Magnificus, prof.dr.ir. C.J. van Duijn, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op donderdag 7 mei 2009 om 16.00 uur

door

Michael Naehrig

geboren te Stolberg (Rhld.), Duitsland

Dit proefschrift is goedgekeurd door de promotor:

prof.dr. T. Lange

CIP-DATA LIBRARY TECHNISCHE UNIVERSITEIT EINDHOVEN

Naehrig, Michael

Constructive and Computational Aspects of Cryptographic Pairings /
door Michael Naehrig. –
Eindhoven: Technische Universiteit Eindhoven, 2009
Proefschrift. – ISBN 978-90-386-1731-2
NUR 919
Subject heading: Cryptology
2000 Mathematics Subject Classification: 94A60, 11G20, 14H45, 14H52, 14Q05

Printed by Printservice Technische Universiteit Eindhoven
Cover design by Verspaget & Bruinink, Nuenen

Für Lukas und Julius

Promotor:

prof.dr. T. Lange

Commissie:

prof.dr.dr.h.c. G. Frey (Universität Duisburg-Essen)
prof.dr. M. Scott (Dublin City University)
prof.dr.ir. H.C.A. van Tilborg
prof.dr. A. Blokhuis
prof.dr. D.J. Bernstein (University of Illinois at Chicago)
prof.dr. P.S.L.M. Barreto (Universidade de São Paulo)

Alles, was man tun muss, ist,
die richtige Taste zum richtigen
Zeitpunkt zu treffen.

Johann Sebastian Bach

Thanks

This dissertation would not exist without the help, encouragement, motivation, and company of many people.
I owe much to my supervisor, Tanja Lange. I thank her for her support; for all the efforts she made, even in those years, when I was not her PhD student; for taking care of so many things; and for being a really good supervisor.
Another important person, who deserves my sincere thanks is Paulo S.L.M. Barreto. Paulo was the one who initiated my interests in pairings. His encouragement and never-ending curiosity is a great source of motivation. It was a pleasure for me to work with him. My short visit to São Paulo was a pleasant and important experience. I highly appreciate Paulo's friendship.
I am also indebted to Gerhard Frey, who was always open to answer questions and comment on problems. I thank him for his patience, friendliness, help, and hospitality.
I express my gratitude to Gerhard Frey, Michael Scott, Henk van Tilborg, Aart Blokhuis, Dan Bernstein, and Paulo Barreto for agreeing to join my PhD committee, and for reading the manuscript and giving valuable comments.
Furthermore, I thank Laura Hitt O'Connor for scientific and general discussions. I have profited also from encouraging conversations with Steven Galbraith. I thank Paulo Barreto, Peter Schwabe, Laura Hitt O'Connor, Gary McGuire, Marco Streng, Christophe Arène, Tanja Lange, and Christophe Ritzenthaler for their fruitful collaboration.
Many thanks go to the people in the coding and cryptology group at TU/e, especially to Henk and Anita for providing a nice working atmosphere, and to the PhD students, with which I had the pleasure to share a really big office: Christiane, Jing, José, Peter, Peter, Peter, Reza, and Sebastiaan. I also appreciate the company of the PhD students from the fridge: Antonino, Bruno, Gaëtan, Daniel, Mayla, and Relinde.
I thank Peter Schwabe and Peter Birkner for proofreading and pointing out mistakes and inconsistencies in earlier versions of this dissertation. Peter Schwabe is always a great help in choosing the right band for our weekly motto.
Let me also mention Matilde Getz, Detlef, Gernot, Tobias, Daniel, Georg, Alex, Wolfgang, and Melli, some of my former colleagues in Aachen. I am grateful for their company in the last years.
I am very happy to have shared many great musical experiences with all the nice

people from the choir of the Aachener Bachverein.
I also apologize to many friends for not being very communicative in the last months and thank them for understanding my full schedule.
Vielen Dank an Simone und Andi für sehr willkommene Teepausen, die mich kurzzeitig von der Arbeit ablenken konnten.
Ein besonderer Dank gilt meiner Familie: meinen Eltern, meinen Schwiegereltern, Großeltern und meinem Bruder für ihre Unterstützung und ihre Zuversicht.
I need to thank Lukas and Julius for reminding me so many times of the important values in life. Finally, I deeply thank my wife Natalie. There are no words to express my gratitude for her enormous support and her love.

Contents

Introduction **1**

1 Preliminaries **5**
1.1 Curves . . . 5
1.1.1 Affine and projective curves . . . 5
1.1.2 Singular points and tangent lines . . . 9
1.1.3 Intersection numbers and Bézout's Theorem . . . 11
1.1.4 Functions, morphisms, and twists . . . 13
1.1.5 Divisors, the Picard group and the genus . . . 16
1.1.6 Elliptic curves . . . 17
1.1.7 Edwards curves and twisted Edwards curves . . . 26
1.1.8 Hyperelliptic curves . . . 28
1.2 Pairings . . . 31
1.2.1 The Tate-Lichtenbaum pairing . . . 32
1.2.2 The Weil pairing . . . 35
1.2.3 Pairing computation on elliptic curves . . . 35
1.3 Constructing pairing-friendly curves . . . 41
1.3.1 The CM method for elliptic curves . . . 43
1.3.2 Elliptic curves with small embedding degree . . . 45

2 BN curves **47**
2.1 Construction . . . 47
2.1.1 Distribution of BN prime pairs . . . 49
2.1.2 Choosing a generator point . . . 50
2.2 Properties . . . 52
2.2.1 Automorphisms . . . 53
2.2.2 Twists and point representation . . . 54
2.2.3 Field extensions . . . 55
2.2.4 Efficient endomorphisms . . . 56
2.2.5 Point compression . . . 59
2.3 Pairing computation . . . 61
2.3.1 Tate and twisted ate pairings . . . 63
2.3.2 ate and optimal pairings . . . 64

2.3.3 Pairing compression . . . 65
2.4 Construction revisited . . . 66
2.4.1 Prime pairs and primitive roots . . . 67
2.4.2 Curve, twist, and automorphisms . . . 68
2.4.3 Finite fields and twist isomorphism . . . 68
2.5 Examples . . . 69

3 Compressed pairing computation **71**
3.1 Preliminaries on tori . . . 72
3.2 Even embedding degree . . . 73
3.3 Curves with a sextic twist . . . 76
3.4 Implementation . . . 83

4 Pairings on Edwards curves **85**
4.1 Lines and conics . . . 86
4.2 Geometric interpretation of the group law . . . 90
4.3 Explicit formulas for Miller functions . . . 98
4.3.1 Addition . . . 99
4.3.2 Doubling . . . 100
4.3.3 Miller loop . . . 101
4.3.4 Comparison . . . 101

5 Constructing curves of genus 2 with p-rank 1 **103**
5.1 Abelian varieties with complex multiplication . . . 103
5.2 A CM construction for genus-2 curves with p-rank 1 . . . 107
5.2.1 Genus-2 curves with p-rank 1 . . . 107
5.2.2 The CM method for genus 2 . . . 109
5.2.3 Algorithms . . . 112
5.2.4 Examples . . . 114
5.3 Prescribed embedding degree in genus 2 . . . 115
5.4 Prescribed embedding degree for p-rank 1 . . . 116

A Compressed torus arithmetic **119**
A.1 Verification of formulas . . . 119
A.2 Pseudo code . . . 122

Bibliography **125**

Index **135**

Summary **139**

Curriculum vitae **141**

Introduction

In 1976, Diffie and Hellman published their groundbreaking paper *New Directions in Cryptography* [DH76], in which they introduced the concept of public-key cryptography. By then, the conventional cryptosystems were built on *symmetric* techniques, where a common secret key is used to encrypt data sent from one party to another. In contrast to that, Diffie and Hellman proposed *asymmetric* methods: A user A provides a public key, with which other users encrypt messages destined for A. The user A holds a corresponding secret key, only known to A, with which A can decrypt those messages. This solves the problem of securely distributing keys over insecure channels that always occurs in symmetric, secret-key systems. While symmetric methods are still the most efficient choice for encrypting data, asymmetric techniques provide key agreement, digital signatures, and authentication.

The security of cryptosystems as proposed by Diffie and Hellman relies on the existence of one-way functions. Evaluating such functions is easy, while inverting is infeasible. Exponentiation of integers modulo a prime number q is the most important example in [DH76]. Cryptosystems based on this function rely on the intractability of the *discrete logarithm problem* in the multiplicative group of a finite field $\mathbb{F}_q$ for sufficiently large primes q. The discrete logarithm problem (DLP) is defined for any group G as follows: Given $a, y \in G$, find an integer x with $y = a^x$ if it exists. For an abelian group, this problem is often formulated additively: Given $P, Q \in G$ with $Q = [x]P$ being the x-fold sum of P, find x. If the DLP is hard to solve in a group G, then G can be used for realizing public-key protocols as indicated by Diffie and Hellman.

It was suggested independently by Miller [Mil86b] and Koblitz [Kob87] to use the group of rational points on an elliptic curve defined over a finite field. Later, Koblitz [Kob89] also proposed the Picard group of a hyperelliptic curve over a finite field. Since then, cryptosystems based on elliptic and hyperelliptic curves and algorithms to solve the DLP in the corresponding groups have been studied thoroughly, and have been widely used. In practice, one takes subgroups of prime order. The size of such groups must be large enough such that with all known algorithms the DLP in the group is infeasible to solve. With respect to the best known algorithms, the DLP on a curve group is harder than in a finite-field group of the same size. Hence curve groups have the advantage that the same security level can be achieved with smaller parameters.

Pairings in cryptography

The group of points on an elliptic curve or the Picard group of a hyperelliptic curve is equipped with additional structure. With the help of such curves, it is possible to define pairings. For two additive groups G_1 and G_2 and a multiplicative group G_3, a *pairing* is a bilinear, non-degenerate map

$$e : G_1 \times G_2 \to G_3.$$

The first example of a pairing used in cryptography was the Weil pairing on an elliptic curve E over a finite field $\mathbb{F}_q$. For a prime r different from the characteristic of $\mathbb{F}_q$, the *Weil pairing* is a map $W_r : E[r] \times E[r] \to \mu_r$. The group $E[r]$ is the group of r-torsion points on E, and μ_r is the group of rth roots of unity, which is contained in an extension of $\mathbb{F}_q$. The degree k of the minimal extension $\mathbb{F}_{q^k} \supseteq \mathbb{F}_q$ that contains μ_r is called the *embedding degree of E with respect to r*. The first appearance of the Weil pairing in cryptography was of a destructive nature. Menezes, Okamoto, and Vanstone [MOV93] applied the Weil pairing for attacking the *elliptic-curve discrete logarithm problem (ECDLP)*. They showed that for an r-torsion point $P \in E[r]$, the Weil pairing yields a group isomorphism $\psi : \langle P \rangle \to \mu_r \subseteq \mathbb{F}_{q^k}^*$ from the cyclic group $\langle P \rangle$ of order r generated by P to the group of rth roots of unity, which lies in $\mathbb{F}_{q^k}$. Instead of solving the ECDLP given by $Q = [x]P$, one can solve the DLP in $\mathbb{F}_{q^k}^*$ given by $\psi(Q) = \psi(P)^x$. If k is small, this reduction provides a way of solving the ECDLP more easily because of the subexponential attacks on the DLP in finite fields. Elliptic curves which have a small embedding degree should therefore be avoided for conventional curve-based cryptography. Frey and Rück [FR94] generalized this to a reduction of the DLP in the Picard group of an arbitrary projective, irreducible, non-singular curve by using another pairing, the *Tate-Lichtenbaum pairing*, an explicit version of the *Tate pairing*. First constructive applications of pairings arose in 2000 as key agreement protocols with new features. Joux [Jou00] proposed a one-round, tripartite key agreement protocol, and Sakai, Ohgishi, and Kasahara [SOK00] showed how to realize identity-based non-interactive key agreement. In 2001, Boneh and Franklin [BF01, BF03] solved a long-standing open problem by proposing a practical way to realize identity-based encryption with pairings. These papers initialized a variety of constructive applications in *pairing-based cryptography*. Paterson [Pat05] gives a survey of such applications.
Most of the pairings used in practice are variants of the Tate pairing on elliptic curves, such as the ate pairing or the twisted ate pairing [HSV06]. Many improvements [MKHO07, ZZH08, LLP08] have led to the notion of optimal pairings introduced by Vercauteren [Ver08] and the framework of pairing lattices, under which Heß [Heß08] subsumes all variants of the Tate pairing.
For all applications, the choice of curve parameters is crucial. It is important that in all three groups G_1, G_2, and G_3, the DLP is infeasible, i. e. the subgroups of prime order r must be large enough. The embedding degree then determines the size of q^k and thus the difficulty of the DLP in $\mathbb{F}_{q^k}^*$. Computation of pairings is done with

variants of Miller's algorithm [Mil86a]. It comprises arithmetic on the elliptic curve or in the Picard group, respectively, and arithmetic in $\mathbb{F}_{q^k}^*$. If the embedding degree is too large, the pairing can not be computed efficiently.
Under these conditions, curves for pairing applications should be chosen to be as economical as possible, i. e. the prime divisor r of the group order should be as large as possible in relation to the full group size. The relative size of r compared to the group order is expressed by the ρ-value $\rho = g\log(q)/\log(r)$, where g is the genus of the curve. The optimal ρ-value is 1, which means that the Picard group over $\mathbb{F}_q$ has prime order r. Since for randomly chosen curves and large primes r the embedding degree is of the size of r which is much too large in general [BK98, LMS04], it is necessary to systematically construct *pairing-friendly curves*.
To improve the efficiency of practical applications of pairings in cryptography, it is required to solve two closely related problems:

- Construct pairing-friendly curves with a small embedding degree and small ρ-value.
- Improve the efficiency and flexibility of algorithms to compute pairings.

These problems suggest the distinction between constructive and computational aspects. This work contributes to the solution of both problems.

Overview

Chapter 1 provides the foundations for the remaining chapters. We define Picard groups (Jacobian varieties, respectively) of elliptic and hyperelliptic curves, which are the groups that are used for cryptographic applications. For that, we discuss affine and projective curves, their properties such as irreducibility and non-singularity, maps between them, their function fields, and divisors. In order to give a geometric interpretation of the group law on elliptic curves in Weierstraß form and Edwards curves as well as to deduce functions for pairing computation, we introduce intersection multiplicities and state Bézout's Theorem. In this work, we mainly consider Weierstraß curves, Edwards curves, and hyperelliptic curves.
We introduce the Tate-Lichtenbaum pairing and the Weil pairing on the Jacobian of a hyperelliptic curve and deduce practical relevant variants of the Tate pairing. Detailed discussions are given for pairings on elliptic curves, including the description of Miller's algorithm and formulas for line functions. We illustrate the use of twists for a more efficient representation of curve points.
Finally, we describe conditions for pairing-friendly curves, and with a focus on elliptic curves, we describe methods for their construction. This includes an overview of the complex multiplication (CM) method to construct elliptic curves with a given number of rational points.
In Chapter 2, we describe a parametrized family of pairing-friendly elliptic curves with embedding degree 12 and prime order (ρ-value 1). The results in this chapter

are based on joint work with Barreto [BN06]. After discussing existence and a construction method, we consider properties of these curves that can be used to improve pairing computation, e. g. the existence of a twist of degree 6, the use of efficient endomorphisms, and the possibilities for point compression and pairing-value compression. We show how to compute all parameters needed for implementing pairings on such curves, and give examples of curves with different bit sizes corresponding to different levels of security.

Compressed pairing computation is the topic of Chapter 3. This chapter is based on joint work with Barreto and Schwabe [NBS08]. Pairing values are elements of algebraic tori. This fact leads to a compressed representation for pairing values and the possibility to implicitly carry out computations on the compressed values. We define compressed pairings and describe a way for their computation by including the compression into the Miller loop. The method can be applied for elliptic curves with even embedding degree, giving a compression of pairing values to one half of their original length. For the special case that 6 divides the embedding degree, the compression factor is one third. In particular, this method works for the curves introduced in Chapter 2, and can be implemented without using any finite field inversions. We determine explicit formulas for the evaluation of line functions and torus arithmetic. Timing results for a C-implementation of the proposed compressed pairings are given and are compared to conventional pairings.

Chapter 4 is dedicated to pairing computation on Edwards curves. The contents of this chapter result from joint work with Arène, Lange, and Ritzenthaler. We give a geometric interpretation of the group law on a twisted Edwards curve. In contrast to the group law on a Weierstraß curve, not only lines are involved, but also conic sections. We deduce the necessary curves of degree 1 and 2, and describe a variant of Miller's algorithm that uses functions arising from these lines and conics. This shows that pairings can be computed directly on the Edwards curve, without transforming back to Weierstraß form. Explicit formulas for the addition and doubling steps in Miller's algorithm are given. The formulas are more efficient than previously proposed formulas for pairings on Edwards curves and are competitive with formulas for pairing computation on Weierstraß curves.

In Chapter 5, we propose algorithms to construct genus-2 curves with p-rank 1 using the complex multiplication method. The chapter contains joint work with Hitt O'Connor, McGuire, and Streng [HMNS08]. First, we give theoretical foundations on abelian varieties and complex multiplication (CM). After that, we discuss genus-2 curves with p-rank 1 and the CM method in genus 2. The proposed algorithms can be used to construct curves defined over a field $\mathbb{F}_{p^2}$ that have a prime number of $\mathbb{F}_{p^2}$-rational points on their Jacobian. Examples with different bit sizes of the group order are given. Finally, we propose an algorithm for the construction of p-rank 1 curves of genus 2 with a small embedding degree.

Chapter 1

Preliminaries

In this chapter, we provide definitions and fundamental results for the subsequent chapters. We discuss the necessary background for curves in Section 1.1. In Section 1.2, we define pairings, and explain how they can be computed. Section 1.3 gives a brief introduction to the problem of constructing pairing-friendly curves along with algorithms to solve it, mainly for elliptic curves. The theoretical background for Chapter 5 is not given here. Instead, fundamentals on abelian varieties and complex multiplication can be found in Section 5.1, since they are not required in Chapters 2, 3, and 4.

1.1 Curves

In this section, we give a brief introduction to plane curves. We define affine and projective curves, discuss general concepts and properties, and then move to elliptic and hyperelliptic curves. There are almost no proofs in this section since we just gather results that are necessary for the following chapters. Details and proofs can be found in the following references: For a general treatise on algebraic geometry, we refer to Hartshorne's book [Har77]. The more specific theory focusing on algebraic curves is presented by Fulton [Ful69]. Lorenzini [Lor96] gives a detailed introduction to plane curves in the context of arithmetic geometry. For results on function fields and a view on curves from that perspective, we point at Stichtenoth [Sti93]. Many facts about curves and in particular elliptic curves can be found in Silverman's book [Sil86]. An overview of the background on curves required for cryptography is given in [FL05a]. We follow parts of these books in this chapter.

1.1.1 Affine and projective curves

Let $\mathbb{F}$ be a perfect field, and let $\overline{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$. For a positive integer n, we define the *affine n-space* $\mathbb{A}^n(\overline{\mathbb{F}})$ to be the n-fold Cartesian product $\mathbb{A}^n(\overline{\mathbb{F}}) := \overline{\mathbb{F}}^n$. The space $\mathbb{A}^1(\overline{\mathbb{F}}) = \overline{\mathbb{F}}$ is called *affine line*, and $\mathbb{A}^2(\overline{\mathbb{F}}) = \overline{\mathbb{F}} \times \overline{\mathbb{F}}$ is called *affine plane*. For any field $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$, we call $\mathbb{A}^n(\tilde{\mathbb{F}}) = \tilde{\mathbb{F}}^n \subseteq \mathbb{A}^n(\overline{\mathbb{F}})$ the *set of $\tilde{\mathbb{F}}$-rational points*

in $\mathbb{A}^n(\overline{\mathbb{F}})$. Given a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ in n variables, we can evaluate f at a point $P = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n(\overline{\mathbb{F}})$ as $f(P) = f(a_1, a_2, \ldots, a_n) \in \overline{\mathbb{F}}$.

Definition 1.1. Let $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a polynomial in n variables. Define an algebraic set C_f by

$$C_f := \{P \in \mathbb{A}^n(\overline{\mathbb{F}}) \mid f(P) = 0\}. \tag{1.1}$$

For any algebraic field extension $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$, the set

$$C_f(\tilde{\mathbb{F}}) = \{P \in C_f \mid P \in \mathbb{A}^n(\tilde{\mathbb{F}})\}$$

of points with coordinates in $\tilde{\mathbb{F}}$ is called the *set of* $\tilde{\mathbb{F}}$*-rational points in* C_f.

In this thesis, we mainly consider sets $C_f \subseteq \mathbb{A}^2(\overline{\mathbb{F}})$. We then usually write the polynomial ring in two variables over $\mathbb{F}$ as $\mathbb{F}[x, y]$.

Definition 1.2. Let $f \in \mathbb{F}[x, y]$ be a polynomial in two variables. The algebraic set C_f is called an *affine plane curve*. The *degree* of C_f is defined as the degree of f.

Example 1.3. An *affine plane line* is an affine plane curve of degree 1. It is given by a polynomial $l = c_x x + c_y y + c_1 \in \mathbb{F}[x, y]$ of degree 1, i. e. $(c_x, c_y) \neq (0, 0)$. Note that a line is uniquely determined by two different points. We call an affine plane curve of degree 2 an *affine plane conic*. It is given by a polynomial $f_C = c_{x^2}x^2 + c_{y^2}y^2 + c_{xy}xy + c_x x + c_y y + c_1 \in \mathbb{F}[x, y]$ of degree 2, i. e. $(c_{x^2}, c_{y^2}, c_{xy}) \neq (0, 0, 0)$. An affine plane curve of degree 3 is called an *affine plane cubic*, and an affine plane curve of degree 4 is called an *affine plane quartic*.

Let $P = (a_1, a_2, \ldots, a_{n+1}) \in \mathbb{A}^{n+1}(\overline{\mathbb{F}})$ be a point in the affine $(n+1)$-space. Suppose $P \neq (0, \ldots, 0)$. Then P defines a unique line that passes through P and the origin $(0, \ldots, 0)$. We identify all non-zero points on this line, i. e. we define an equivalence relation $\sim$ on $\mathbb{A}^{n+1}(\overline{\mathbb{F}}) \setminus \{(0, \ldots, 0)\}$ as follows: We say that $P = (a_1, a_2, \ldots, a_{n+1})$ and $Q = (b_1, b_2, \ldots, b_{n+1})$ are equivalent, i. e. $P \sim Q$, if there exists $\lambda \in \overline{\mathbb{F}}^*$ with

$$(a_1, a_2, \ldots, a_{n+1}) = \lambda(b_1, b_2, \ldots, b_{n+1}) = (\lambda b_1, \lambda b_2, \ldots, \lambda b_{n+1}).$$

We denote the equivalence class with respect to $\sim$ that contains P by

$$P^{\sim} := (a_1 : a_2 : \cdots : a_{n+1}) := \{Q \in \mathbb{A}^{n+1}(\overline{\mathbb{F}}) \mid Q \sim P\}.$$

The set $P^{\sim}$ contains all points on the above mentioned line through P and $(0, \ldots, 0)$, except for the point $(0, \ldots, 0)$ itself. We define the *projective n-space* $\mathbb{P}^n(\overline{\mathbb{F}})$ to be the set of all such equivalence classes,

$$\mathbb{P}^n(\overline{\mathbb{F}}) := \{P^{\sim} \mid (0, \ldots, 0) \neq P \in \mathbb{A}^{n+1}(\overline{\mathbb{F}})\}.$$

The set $\mathbb{P}^1(\overline{\mathbb{F}})$ is called *projective line*, and the set $\mathbb{P}^2(\overline{\mathbb{F}})$ is called *projective plane*. An equivalence class $P^\sim$ is called a *projective point*. The set of $\tilde{\mathbb{F}}$-rational points in $\mathbb{P}^n(\overline{\mathbb{F}})$ for $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$ is defined as

$$\mathbb{P}^n(\tilde{\mathbb{F}}) := \{P^\sim = (a_1 : a_2 : \cdots : a_{n+1}) \mid \exists\, \lambda \in \overline{\mathbb{F}}^* \text{ with } \lambda a_i \in \tilde{\mathbb{F}} \text{ for all } i\} \subseteq \mathbb{P}^n(\overline{\mathbb{F}}).$$

The affine n-space $\mathbb{A}^n(\overline{\mathbb{F}})$ can be embedded into the projective n-space by identifying $(a_1, a_2, \ldots, a_n) \in \mathbb{A}^n(\overline{\mathbb{F}})$ with the point $(a_1 : a_2 : \cdots : a_n : 1) \in \mathbb{P}^n(\overline{\mathbb{F}})$.

Lemma 1.4. *Let* $U_{n+1} := \{(a_1 : a_2 : \cdots : a_{n+1}) \in \mathbb{P}^n(\overline{\mathbb{F}}) \mid a_{n+1} \neq 0\} \subseteq \mathbb{P}^n(\overline{\mathbb{F}})$. *Then the map*

$$\begin{aligned} \varphi_{n+1} : U_{n+1} &\to \mathbb{A}^n(\overline{\mathbb{F}}), \\ (a_1 : a_2 : \cdots : a_{n+1}) &\mapsto \left(\frac{a_1}{a_{n+1}}, \frac{a_2}{a_{n+1}}, \ldots, \frac{a_n}{a_{n+1}}\right) \end{aligned}$$

is a bijection.

Proof. This is [Har77, Proposition I.2.2]. □

The inverse map φ_{n+1}^{-1} is given by $(a_1, a_2, \ldots, a_n) \mapsto (a_1 : a_2 : \cdots : a_n : 1)$. From now on, we understand $\mathbb{A}^n(\overline{\mathbb{F}})$ as a subset of $\mathbb{P}^n(\overline{\mathbb{F}})$. When speaking of points in $\mathbb{P}^n(\overline{\mathbb{F}})$, we abuse notation and denote the class $P^\sim$ by P as well. We have chosen one special embedding of the affine space into the projective space by choosing U_{n+1}, i. e. fixing the last coordinate to be different from 0. Of course, we could also take each of the other coordinates, and get in this way $n+1$ different sets U_i, $1 \leq i \leq n+1$, with corresponding embeddings of the affine space into $\mathbb{P}^n(\overline{\mathbb{F}})$ (see [Har77, Section I.2]). The sets U_i cover all of $\mathbb{P}^n(\overline{\mathbb{F}})$.
To define a projective curve, we need to explain what it means that a projective point is a zero of a polynomial. A polynomial $f \in \mathbb{F}[x_1, \ldots, x_{n+1}]$ may have a zero at one representative of a projective point, while it might be different from zero at another representative. Therefore, we consider *homogeneous polynomials*. The monomials of a homogeneous polynomial all have the same degree. Thus $f(\lambda a_1, \lambda a_2, \ldots, \lambda a_{n+1}) = \lambda^d f(a_1, a_2, \ldots, a_{n+1})$ for a homogeneous polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_{n+1}]$ of degree d. This shows that for homogeneous polynomials either all representatives of a projective point are a zero or none.
From now on, we write homogeneous polynomials with capital letters. Also the variables for homogeneous polynomials are written with capital letters to distinguish between the affine and the projective case.

Definition 1.5. Let $F \in \mathbb{F}[X_1, X_2, \ldots, X_{n+1}]$ be a homogeneous polynomial in $n+1$ variables. Define a projective algebraic set

$$C_F := \{P \in \mathbb{P}^n(\overline{\mathbb{F}}) \mid F(P) = 0\}. \tag{1.2}$$

For any field $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$, the set

$$C_F(\tilde{\mathbb{F}}) := \{P \in C_F \mid P \in \mathbb{P}^n(\tilde{\mathbb{F}})\}$$

of points in the projective space over $\tilde{\mathbb{F}}$ is called the *set of $\tilde{\mathbb{F}}$-rational points in C_F*.

As above for affine algebraic sets, we choose different notation for the variables when defining projective algebraic sets $C_F \subseteq \mathbb{P}^2(\overline{\mathbb{F}})$.

Definition 1.6. Let $F \in \mathbb{F}[X, Y, Z]$ be a homogeneous polynomial in three variables. The projective algebraic set C_F is called a *projective plane curve*. Its *degree* is defined as the degree of the polynomial F.

Example 1.7. We use the same terminology as for affine curves. A *projective plane line* is a projective plane curve of degree 1. A plane line is given by a polynomial $L = c_X X + c_Y Y + c_Z Z$, where at least one of the coefficients c_X, c_Y, c_Z is different from 0. A *projective plane conic* is a projective plane curve of degree 2. It is given by a polynomial

$$F_C = c_{X^2} X^2 + c_{Y^2} Y^2 + c_{Z^2} Z^2 + c_{XY} XY + c_{XZ} XZ + c_{YZ} YZ$$

with at least one of the coefficients $c_{X^2}, c_{Y^2}, c_{Z^2}, c_{XY}, c_{XZ}, c_{YZ}$ being different from 0. Projective plane curves of degree 3 and degree 4 are called *projective plane cubics* and *projective plane quartics*, respectively.

Let $F \in \mathbb{F}[X_1, X_2, \ldots, X_{n+1}]$ be a homogeneous polynomial. Define the *dehomogenization F_* of F* as

$$F_*(x_1, x_2, \ldots, x_n) := F(x_1, x_2, \ldots, x_n, 1) \in \mathbb{F}[x_1, x_2, \ldots, x_n].$$

And vice versa, for a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ of degree d, we define the *homogenization of f* as

$$f^*(X_1, X_2, \ldots, X_{n+1}) := X_{n+1}^d f(X_1/X_{n+1}, X_2/X_{n+1}, \ldots, X_n/X_{n+1}),$$

a polynomial in $\mathbb{F}[X_1, X_2, \ldots, X_{n+1}]$. Note that $(f^*)_* = f$ for all $f \in \mathbb{F}[x_1, \ldots, x_n]$. If $X_{n+1} \nmid F$, then $(F_*)^* = F$. By means of homogenization and dehomogenization and the map φ_3, we may associate to every affine plane curve a corresponding projective plane curve and to every projective plane curve a special affine plane curve. Any projective curve C_F contains the affine curve C_{F_*}. The points that only lie in C_F and not in C_{F_*}, i. e. the points of form $(a_1 : a_2 : 0)$, are called *points at infinity*.

Remark 1.8. Throughout this work, we use the well-known notation $C_f : f = 0$ and $C_F : F = 0$ for plane curves.

Curves as defined here are special *algebraic sets* (see [Har77, Sections I.1 and I.2] and [Ful69, Chapters 1 and 4]). An algebraic set is the set of common zeros of a collection of polynomials. Algebraic sets form the closed sets of a topology on affine and projective n-space, the *Zariski topology* [Har77, Sections I.1 and I.2]. Affine and projective spaces are thus equipped with the structure of a topological space, and we can define the notion of *irreducibility* as follows: A nonempty subset X of a topological space is called *irreducible*, if it can not be expressed as the union of two proper subsets, each one of which is closed in X [Har77, Definition in Section I.1]. For an algebraic set, this means that it can not be expressed as the union of two non-trivial algebraic subsets.
The Zariski topology depends on the base field, over which the algebraic set is defined. An algebraic set that is irreducible over $\mathbb{F}$ might become reducible over an extension field. If it stays irreducible when considered over any algebraic extension of $\mathbb{F}$, i. e. it stays irreducible over $\overline{\mathbb{F}}$, we call it *absolutely irreducible*.

Definition 1.9. A curve over $\mathbb{F}$ is called *absolutely irreducible* if it can not be expressed as the union of two distinct nontrivial algebraic subsets over $\overline{\mathbb{F}}$.

For a plane curve, we can determine irreducibility by considering the associated polynomial. A polynomial over $\mathbb{F}$ is called *absolutely irreducible* if it is irreducible as a polynomial over $\overline{\mathbb{F}}$.

Lemma 1.10. *An affine plane curve C_f (or a projective plane curve C_F, respectively) is absolutely irreducible, if f (or F, respectively) is absolutely irreducible.*

Proof. This is Example 4.15 (ii) from [FL05a]. □

Any algebraic set can be written uniquely as a union of distinct irreducible algebraic sets, each one of which is not contained in another (see [Har77, Proposition I.1.5] and [Ful69, Chapter 1, Theorem 2 and Chapter 4, Section 2]). These algebraic sets are called the *irreducible components* of the algebraic set. For an affine plane curve C_f over $\overline{\mathbb{F}}$, the factorization of f displays the decomposition into irreducible components [Ful69, Chapter 1, Section 6, Corollary 3]. The homogenizations of the irreducible components are the irreducible components of the corresponding projective curve C_{f^*} [Ful69, Chapter 4, Section 3, Proposition 3].

1.1.2 Singular points and tangent lines

From now on, we restrict ourselves to plane curves. This means that curves are given by a polynomial $f \in \mathbb{F}[x, y]$ or by a homogeneous polynomial $F \in \mathbb{F}[X, Y, Z]$.

Definition 1.11. Let C_f be an affine curve with $f \in \mathbb{F}[x, y]$. A point $P \in C_f$ is called *singular* if both partial derivatives of f vanish at P, i. e. $(\partial f/\partial x)(P) = 0 = (\partial f/\partial y)(P)$.

Definition 1.12. Let C_F be a projective curve and $F \in \mathbb{F}[X, Y, Z]$. A point $P \in C_F$ is called *singular* if all three partial derivatives of F vanish at P, i. e. $(\partial F/\partial X)(P) = (\partial F/\partial Y)(P) = (\partial F/\partial Z)(P) = 0$.

Let C be an affine or a projective curve. If $P \in C$ is a singular point, C is called *singular at* P. Otherwise, it is called *nonsingular at* P, and the point P is called *nonsingular*. If there are no singular points on C, it is called *nonsingular*.

Remark 1.13. The definition of a singular point on a projective curve as in Definition 1.12 is the same as Definition 3.9 in Chapter VI of [Lor96]. Usually, a point on a projective curve is said to be singular if the corresponding affine point in a suitable dehomogenization is singular. The following lemma states that these definitions are equivalent.

Lemma 1.14. *Let $P = (X_P : Y_P : Z_P) \in C_F$ be a point on the projective curve C_F, which lies in U_3, i. e. $Z_P \neq 0$ (see Lemma 1.4). Then P is singular if and only if the point $(X_P/Z_P, Y_P/Z_P)$ is singular on C_{F_*}.*

Proof. This is Lemma 3.10 from Chapter VI of [Lor96]. □

Remark 1.15. In his book, Fulton uses the terminology *simple point* for a nonsingular point [Ful69, Chapter 3, Section 1]. The notion *simple* can be explained as follows: To each point $P \in C_F$ a *multiplicity* $m_P(C_F)$ is assigned. The multiplicity of a projective point P on a projective curve C_F is defined as the multiplicity of the corresponding affine point P_* on the affine curve C_{F_*}. Dehomogenization is done with respect to a nonzero coordinate of P.
Let C_f be an irreducible affine curve. Transform the curve by shifting the coordinates of P to $(0, 0)$. The multiplicity of P on C_f is defined to be the minimal degree of all monomials in the resulting curve polynomial. For details, see [Ful69]. A point $P \in C_F$ is nonsingular if and only if $m_P(C_F) = 1$.

If we have a nonsingular point on a curve, there is a unique tangent line to the curve in that point. It is given by the partial derivatives of the defining polynomial as follows:

Definition 1.16. Let C_f be an affine curve, $f \in \mathbb{F}[x, y]$, and $P = (x_P, y_P) \in C_f$ a nonsingular point. The line

$$t_{f,P} : \frac{\partial f}{\partial x}(P)(x - x_P) + \frac{\partial f}{\partial y}(P)(y - y_P) = 0$$

is called the *tangent line to* C_f *at* P.

Definition 1.17. Let C_F be a projective curve, $F \in \mathbb{F}[X, Y, Z]$, and $P \in C_F$ a nonsingular point. The line

$$T_{F,P} : \frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0$$

is called the *tangent line to* C_F *at* P.

Remark 1.18. Note that the defining polynomials of the tangents in the previous definitions have degree 1 since P is nonsingular; in particular, they are not 0. The defining polynomial for the projective tangent line depends on the representative of the point P, but since the partial derivatives are homogeneous polynomials of degree one less than F, the tangent line is uniquely determined [Lor96, Section VI.7].
One might expect the projective tangent line at $P = (X_P : Y_P : Z_P)$ to be defined as

$$T_{F,P} : \frac{\partial F}{\partial X}(P)(X - X_P) + \frac{\partial F}{\partial Y}(P)(Y - Y_P) + \frac{\partial F}{\partial Z}(P)(Z - Z_P) = 0.$$

Since $\frac{\partial F}{\partial X}X + \frac{\partial F}{\partial Y}Y + \frac{\partial F}{\partial Z}Z = \deg(F)F$ as polynomials, we get $\frac{\partial F}{\partial X}(P)X_P + \frac{\partial F}{\partial Y}(P)Y_P + \frac{\partial F}{\partial Z}(P)Z_P = 0$, and both definitions of the tangent line are equal.

Let $P = (x_P, y_P) \in C_f$ be nonsingular. Then from Lemma 1.14 it follows that $P^* := \varphi_3^{-1}(P) = (x_P : y_P : 1)$ is a nonsingular point on C_{f^*} and the tangent line T_{f^*,P^*} is given by the homogenization of $t_{f,P}$ [Lor96, Section VI.7].

1.1.3 Intersection numbers and Bézout's Theorem

We abbreviate $\mathbb{A}^2 := \mathbb{A}^2(\overline{\mathbb{F}})$, and let $\overline{\mathbb{F}}(\mathbb{A}^2) := \overline{\mathbb{F}}(x, y) := \mathrm{Quot}(\overline{\mathbb{F}}[x, y])$ be the *rational function field* in two variables. Its elements are *rational functions* on $\mathbb{A}^2$, i. e. fractions of polynomials in $\overline{\mathbb{F}}[x, y]$. For a point $P \in \mathbb{A}^2$, we define

$$\mathcal{O}_P(\mathbb{A}^2) := \{g/h \in \overline{\mathbb{F}}(\mathbb{A}^2) \mid h(P) \neq 0\}.$$

The subring $\mathcal{O}_P(\mathbb{A}^2) \subseteq \overline{\mathbb{F}}(\mathbb{A}^2)$ is a local ring with maximal ideal

$$\mathcal{M}_P(\mathbb{A}^2) := \{g/h \in \mathcal{O}_P(\mathbb{A}^2) \mid g(P) = 0\}$$

(see [Sti93, Appendix B.1]). Let $f, g \in \mathbb{F}[x, y]$, then $f, g \in \mathcal{O}_P(\mathbb{A}^2)$. Let (f, g) denote the ideal in $\mathcal{O}_P(\mathbb{A}^2)$ generated by f and g. Then $\mathcal{O}_P(\mathbb{A}^2)/(f, g)$ is an $\overline{\mathbb{F}}$-vector space. Let $\mathbb{P}^2 := \mathbb{P}^2(\overline{\mathbb{F}})$. Similarly, we define the *rational function field*

$$\overline{\mathbb{F}}(\mathbb{P}^2) := \{G/H \mid G, H \in \overline{\mathbb{F}}[X, Y, Z] \text{ homogen.}, H \neq 0, \deg(G) = \deg(H)\} \cup \{0\},$$

as the field of homogeneous rational functions, i. e. fractions of homogeneous polynomials of the same degree. For a point $P \in \mathbb{P}^2$, we define

$$\mathcal{O}_P(\mathbb{P}^2) := \{G/H \in \overline{\mathbb{F}}(\mathbb{P}^2) \mid H(P) \neq 0\}.$$

The ring $\mathcal{O}_P(\mathbb{P}^2)$ is a local ring with maximal ideal

$$\mathcal{M}_P(\mathbb{P}^2) := \{G/H \in \mathcal{O}_P(\mathbb{P}^2) \mid G(P) = 0\}$$

(see [Sti93, Appendix B.2]). Note that $\overline{\mathbb{F}}(\mathbb{P}^2)$ is $\overline{\mathbb{F}}$-isomorphic to $\overline{\mathbb{F}}(\mathbb{A}^2)$ [Sti93, Appendix B.3], and hence also the local rings at P and $\varphi_3(P)$ are isomorphic for $P \in U_3$. We map a homogeneous polynomial $F \in \mathbb{F}[X, Y, Z]$ of degree d into $\mathcal{O}_P(\mathbb{P}^2)$ by

choosing a projective line L, not passing through P, and setting $F_\times := F/L^d$. If $P \in U_3$, i. e. it is a point with a nonzero Z-coordinate, we can choose $L = Z$, and $F_\times$ is the usual dehomogenization F_*. Let $F, G \in \mathbb{F}[X, Y, Z]$ be homogeneous, then $F_\times, G_\times \in \mathcal{O}_P(\mathbb{P}^2)$. If $(F_\times, G_\times)$ denotes the ideal generated by $F_\times$ and $G_\times$, the ring $\mathcal{O}_P(\mathbb{P}^2)/(F_\times, G_\times)$ is an $\overline{\mathbb{F}}$-vector space.

Definition 1.19. Let $f, g \in \mathbb{F}[x, y]$ and $P \in \mathbb{A}^2(\overline{\mathbb{F}})$. The *intersection number of C_f and C_g at P* is defined as

$$I(P, C_f \cap C_g) := \dim_{\overline{\mathbb{F}}}(\mathcal{O}_P(\mathbb{A}^2)/(f, g)),$$

where (f, g) is the ideal in $\mathcal{O}_P(\mathbb{A}^2)$ generated by f and g.
Let $F, G \in \mathbb{F}[X, Y, Z]$ be two homogeneous polynomials and $P \in \mathbb{P}^2(\overline{\mathbb{F}})$. The *intersection number of C_F and C_G at P* is defined as

$$I(P, C_F \cap C_G) := \dim_{\overline{\mathbb{F}}}(\mathcal{O}_P(\mathbb{P}^2)/(F_\times, G_\times)),$$

where $(F_\times, G_\times)$ is the ideal in $\mathcal{O}_P(\mathbb{P}^2)$ generated by $F_\times$ and $G_\times$.

It is clear from the definition that for a projective point $P \in U_3$, it holds $I(P, C_F \cap C_G) = I(\varphi_3(P), C_{F_*} \cap C_{G_*})$. The intersection number is the unique integer that satisfies the seven properties given in [Ful69, Chapter 3, Section 3]. We only list a selection of those properties, which are important for further considerations.

Lemma 1.20. *The intersection number defined in Definition 1.19 satisfies the following properties: (We use the notation of the affine case.)*

(a) $I(P, C_f \cap C_g) \in \mathbb{N}_0$ for any f, g, and P such that C_f and C_g intersect properly at P, i. e. they have no common component which passes through P. If the curves do not intersect properly at P, $I(P, C_f \cap C_g) = \infty$.

(b) $I(P, C_f \cap C_g) = 0$ if and only if $P \notin C_f \cap C_g$. The intersection number only depends on the components of f and g that pass through P.

(c) $I(P, C_f \cap C_g) \geq m_P(C_f)m_P(C_g)$, with equality if and only if C_f and C_g have no tangent lines in common at P. In particular, if P is a nonsingular point on both C_f and C_g, then $I(P, C_f \cap C_g) = 1$ if and only if C_f and C_g have no tangent lines in common at P. See Remark 1.15 for the definition of $m_P(C_f)$.

Proof. See Theorem 3 in Chapter 3, Section 3 of [Ful69]. □

The above properties suffice to understand the simple cases we consider in this work. Next we state Bézout's Theorem, which tells us how many intersection points two projective curves of given degrees have.

Theorem 1.21 (Bézout's Theorem)**.** *Let $F, G \in \mathbb{F}[X, Y, Z]$ be two homogeneous polynomials of degree d and e, respectively, such that the curves C_F and C_G have no component in common. Then*

$$\sum_{P \in C_F \cap C_G} I(P, C_F \cap C_G) = d \cdot e.$$

Proof. This is the main theorem in [Ful69, Chapter 5, Section 3] or [Har77, Corollary I.7.8]. □

Bézout's Theorem shows that two projective curves of degree d and e that are sufficiently different intersect at exactly $d \cdot e$ points when counting multiplicities in the right way.

1.1.4 Functions, morphisms, and twists

We have already seen examples of function fields, namely the rational function fields corresponding to the affine space and to the projective space. Now we are going to associate a function field to every absolutely irreducible curve. We follow [Sti93, Appendix B].
Let C_f be an absolutely irreducible, affine curve with absolutely irreducible defining polynomial $f \in \mathbb{F}[x, y]$. Let $(f) \subseteq \overline{\mathbb{F}}[x, y]$ be the ideal in $\overline{\mathbb{F}}[x, y]$ generated by f. Then (f) is a prime ideal and the ring

$$\overline{\mathbb{F}}[C_f] := \overline{\mathbb{F}}[x, y]/(f)$$

is an integral domain. It is called the *coordinate ring of C_f*.

Definition 1.22. The quotient field $\overline{\mathbb{F}}(C_f) := \mathrm{Quot}(\overline{\mathbb{F}}(C_f))$ is called the *function field of C_f*.

Elements of the function field are called *rational functions*, and are fractions of polynomials modulo the curve equation. Let $\mathcal{G}_{\overline{\mathbb{F}}/\mathbb{F}}$ be the Galois group of $\overline{\mathbb{F}}/\mathbb{F}$. The action of $\mathcal{G}_{\overline{\mathbb{F}}/\mathbb{F}}$ on $\overline{\mathbb{F}}$ can be extended to affine space, polynomial rings, and thus to coordinate rings and function fields.
We define $\mathbb{F}[C_f]$, the *coordinate ring of C_f over $\mathbb{F}$*, and $\mathbb{F}(C_f)$, the *function field of C_f over $\mathbb{F}$*, as the subsets of $\overline{\mathbb{F}}[C_f]$ and $\overline{\mathbb{F}}(C_f)$, respectively, that are fixed under the action of $\mathcal{G}_{\overline{\mathbb{F}}/\mathbb{F}}$. The field $\mathbb{F}$ is contained in $\mathbb{F}(C_f)$, and C_f is absolutely irreducible if and only if $\mathbb{F}$ is algebraically closed in $\mathbb{F}(C_f)$ [Sti93, Corollary III.6.7].
The elements in $\overline{\mathbb{F}}(C_f)$ define functions on C_f since polynomials in $\overline{\mathbb{F}}[x, y]$ are maps $\mathbb{A}^2(\overline{\mathbb{F}}) \to \overline{\mathbb{F}}$. For the projective space, the situation is different since polynomials in $\overline{\mathbb{F}}[X, Y, Z]$ yield different values when evaluated at different representatives of a projective point.
Let C_F be an absolutely irreducible, projective curve with an absolutely irreducible and homogeneous defining polynomial $F \in \mathbb{F}[X, Y, Z]$. Denote by (F) the *homogeneous ideal* in $\overline{\mathbb{F}}[X, Y, Z]$ which is generated by F. As in the affine case, define

the *homogeneous coordinate ring of* C_F by $\overline{\mathbb{F}}_{\text{hom}}[C_F] := \overline{\mathbb{F}}[X,Y,Z]/(F)$. It is an integral domain, and we denote its quotient field by $\overline{\mathbb{F}}_{\text{hom}}(C_F) := \text{Quot}(\overline{\mathbb{F}}_{\text{hom}}[C_F])$. An element $g \in \overline{\mathbb{F}}_{\text{hom}}[C_F]$ is called a *form* if there exists a homogeneous polynomial G such that $g = G + (F)$.

Definition 1.23. The *function field of* C_F is the subfield of $\overline{\mathbb{F}}_{\text{hom}}(C_F)$ given by $\overline{\mathbb{F}}(C_F) := \{g/h \mid g,h \in \overline{\mathbb{F}}_{\text{hom}}[C_F] \text{ are forms of the same degree and } h \neq 0\} \cup \{0\}$.

The function field $\mathbb{F}(C_F)$ over $\mathbb{F}$ is defined as the fixed field under the action of the Galois group $\mathcal{G}_{\overline{\mathbb{F}}/\mathbb{F}}$ on $\overline{\mathbb{F}}(C_F)$. The elements of $\overline{\mathbb{F}}(C_F)$ define functions on C_F since they are represented as quotients of forms of the same degree. Therefore, the value of such an element is independent of the chosen representative of the projective point. The map $\varphi_3 : U_3 \to \mathbb{A}^2(\overline{\mathbb{F}}), P = (X_P : Y_P : Z_P) \mapsto (X_P/Z_P, Y_P/Z_P)$ induces an $\overline{\mathbb{F}}$-isomorphism

$$(\varphi_3^{-1})^* : \overline{\mathbb{F}}(C_F) \to \overline{\mathbb{F}}(C_{F_*}).$$

Thus the function field of a projective curve is isomorphic to the function field of the affine curve given by the dehomogenization (see [Lor96, Proposition VI.8.5] and [Sti93, Appendix B.3]).
The localization of the coordinate ring at a point P is a subring of $\overline{\mathbb{F}}(C_F)$ given by

$$\mathcal{O}_P(C_F) := \{g/h \in \overline{\mathbb{F}}(C_F) \mid h(P) \neq 0\}.$$

It is a local ring with maximal ideal

$$\mathcal{M}_P(C_F) := \{g/h \in \mathcal{O}_P(C_F) \mid g(P) = 0\}$$

[Sti93, Appendix B.2]. If P is nonsingular (i. e. simple, see Remark 1.15), $\mathcal{O}_P(C_F)$ is a discrete valuation ring [Sil86, Proposition II.1.1]. In this case, we can define a valuation on $\mathcal{O}_P(C_F)$.

Definition 1.24. Let $P \in C_F$ be a nonsingular point. The *valuation on* $\mathcal{O}_P(C_F)$, defined by

$$\begin{aligned} \text{ord}_P : \mathcal{O}_P(C_F) &\to \mathbb{N}_0 \cup \{\infty\}, \\ \phi &\mapsto \max\{m \in \mathbb{Z} \mid \phi \in \mathcal{M}_P(C_F)^m\} \end{aligned}$$

is called the *order of* ϕ *at* P.

The order function is extended to the whole function field by defining

$$\text{ord}_P : \overline{\mathbb{F}}(C_F) \to \mathbb{Z} \cup \{\infty\},\ \phi = f/g \mapsto \text{ord}_P(f) - \text{ord}_P(g).$$

An element $t \in \overline{\mathbb{F}}(C_F)$ with $\text{ord}_P(t) = 1$ is called a *uniformizing parameter for* C_F *at* P.
Since algebraic sets are defined by polynomials, the natural maps between them are also given by polynomials. In terms of the Zariski topology, we consider maps

which are continuous with respect to that topology. A *morphism of affine curves* is a map $\varphi : C_f \to C_g$ given by a pair (φ_x, φ_y) of polynomials in $\overline{\mathbb{F}}[x, y]$ that maps a point $P \in C_f$ to the point $(\varphi_x(P), \varphi_y(P)) \in C_g$. If $\varphi_x, \varphi_y \in \mathbb{F}[x, y]$, we say that φ is defined over $\mathbb{F}$. Any morphism between curves induces an $\overline{\mathbb{F}}$-algebra morphism $\varphi^* : \overline{\mathbb{F}}[C_g] \to \overline{\mathbb{F}}[C_f]$ between the coordinate rings. By [FL05a, Remark 4.37], φ^* is injective if and only if φ is surjective, and if φ^* is surjective, then φ is injective. The map φ is an *isomorphism* if there exists an inverse map that is a morphism. This is equivalent to φ^* being an $\overline{\mathbb{F}}$-algebra isomorphism [FL05a, Definition 4.38].
From now on, we only consider irreducible projective curves, always keeping in mind that we have the affine part given by dehomogenization. Let C_F, C_G be absolutely irreducible, projective plane curves defined over $\mathbb{F}$. In our description of morphisms, we follow [Sil86, §I.3].
A *rational map from C_F to C_G* is a map $\phi : C_F \to C_G$ given by a triple (ϕ_X, ϕ_Y, ϕ_Z) with $\phi_X, \phi_Y, \phi_Z \in \overline{\mathbb{F}}(C_F)$ such that for every point $P \in C_F$ at which ϕ_X, ϕ_Y, ϕ_Z are defined, $\phi(P) = (\phi_X(P) : \phi_Y(P) : \phi_Z(P)) \in C_G$. We say that ϕ is *defined over* $\mathbb{F}$ if there exists $\lambda \in \overline{\mathbb{F}}^*$ such that $\lambda\phi_X, \lambda\phi_Y, \lambda\phi_Z \in \mathbb{F}(C_F)$.

Definition 1.25. Two curves C_F and C_G are called *birationally equivalent* if there exist rational maps $\phi : C_F \to C_G$ and $\psi : C_G \to C_F$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identities on C_F and C_G, respectively. In that case, ϕ is called a *birational map*.

A rational map $\phi : C_F \to C_G$ is called *regular at $P \in C_F$* if there exists a function $g \in \overline{\mathbb{F}}(C_F)$ such that $g\phi_X, g\phi_Y, g\phi_Z$ are all defined at P and at least one of $g\phi_X(P), g\phi_Y(P), g\phi_Z(P)$ is different from 0.

Definition 1.26. A *morphism between C_F and C_G* is a rational map $\phi : C_F \to C_G$ that is regular at every point $P \in C_F$. The map ϕ is called an *isomorphism* if there exists a morphism $\psi : C_G \to C_F$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identities on C_F and C_G, respectively. Let $\mathrm{Mor}(C_F, C_G)$ be the set of morphisms from C_F to C_G and $\mathrm{Isom}(C_F, C_G)$ be its subset of isomorphisms. The sets of morphisms and isomorphisms that are defined over $\tilde{\mathbb{F}}$ for $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$ are denoted by $\mathrm{Mor}_{\tilde{\mathbb{F}}}(C_F, C_G)$ and $\mathrm{Isom}_{\tilde{\mathbb{F}}}(C_F, C_G)$, respectively. The curves C_F and C_G are called *isomorphic over* $\tilde{\mathbb{F}}$ or *$\tilde{\mathbb{F}}$-isomorphic* if there exists an isomorphism defined over $\tilde{\mathbb{F}}$.

Remark 1.27. Let $\phi : C_F \to C_G$ be a rational map between the projective, nonsingular, absolutely irreducible curves C_F and C_G, then ϕ is a morphism [Sil86, Proposition II.2.1]. If $\phi : C_F \to C_G$ is a morphism, then ϕ is either constant or surjective [Sil86, Theorem II.2.3]. By composition, ϕ induces an injection of function fields $\phi^* : \overline{\mathbb{F}}(C_G) \to \overline{\mathbb{F}}(C_F),\ f \mapsto f \circ \phi$ [Sil86, Theorem II.2.4]. The extension degree $[\overline{\mathbb{F}}(C_F) : \phi^*(\overline{\mathbb{F}}(C_G))]$ is called the *degree of ϕ*.

Definition 1.28. Let C be a projective, nonsingular curve defined over $\mathbb{F}$. A nonsingular curve C' defined over $\mathbb{F}$ is called a *twist of C* if C' is isomorphic to C over $\overline{\mathbb{F}}$. This means that the set $\mathrm{Isom}(C, C')$ is not empty. We denote by $\mathrm{Twist}(C/\mathbb{F})$ the set of $\mathbb{F}$-isomorphism classes of curves that are twists of C and defined over $\mathbb{F}$.

If $C'/\mathbb{F}$ is a twist of $C/\mathbb{F}$, there exists an isomorphism $\psi \in \mathrm{Isom}(C, C')$ and a finite field extension $\tilde{\mathbb{F}} \supseteq \mathbb{F}$ such that ψ is defined over $\tilde{\mathbb{F}}$.

Definition 1.29. Let $C/\mathbb{F}$ be a projective curve and $C'/\mathbb{F}$ a twist of C. The minimal extension degree d for which there exists an isomorphism $\psi \in \mathrm{Isom}(C, C')$ that is defined over $\tilde{\mathbb{F}}$ with $[\tilde{\mathbb{F}} : \mathbb{F}] = d$ is called the *degree of the twist* C'. A twist of degree 2 is called a *quadratic twist*, one of degree 3 a *cubic twist* and so on.

Remark 1.30. The set $\mathrm{Twist}(C/\mathbb{F})$ is determined by the Galois group $\mathcal{G}_{\overline{\mathbb{F}}/\mathbb{F}}$ and the group $\mathrm{Isom}(C)$ of isomorphisms of C to itself. For details, we refer to [Sil86, §X.2].

1.1.5 Divisors, the Picard group and the genus

In this subsection, we define the *Picard group* $\mathrm{Pic}^0_{\mathbb{F}}(C)$. This group is used in curve-based cryptographic applications for realizing discrete-logarithm-based protocols. In its description we follow [Sil86, §II.3] and [FL05a, Section 4.4].
Let $C/\mathbb{F}$ be an absolutely irreducible, nonsingular, projective curve defined over $\mathbb{F}$ with $C : F(X, Y, Z) = 0$. The *divisor group* $\mathrm{Div}(C)$ is the free abelian group generated by the points of C. An element $D \in \mathrm{Div}(C)$ is written as a formal sum $D = \sum_{P \in C} n_P(P)$, where $n_P \in \mathbb{Z}$ for all P and $n_P = 0$ for all but finitely many P. Any such D is called a *divisor of* C. The integer $\deg(D) := \sum_{P \in C} n_P$ is called the *degree of the divisor* D. The set of all points P for which $n_P \neq 0$ is called the *support of* D. The subgroup of $\mathrm{Div}(C)$ containing all *divisors of degree* 0 is denoted by $\mathrm{Div}^0(C) := \{D \in \mathrm{Div}(C) \mid \deg(D) = 0\}$. Since the Galois group $\mathcal{G}_{\overline{\mathbb{F}}/\mathbb{F}}$ acts on the points of C, it also acts on divisors. A divisor that is fixed under that action is said to be *defined over* $\mathbb{F}$ and is called an $\mathbb{F}$-*rational divisor*. The subgroups of $\mathrm{Div}(C)$ and $\mathrm{Div}^0(C)$ of divisors defined over $\mathbb{F}$ are denoted by $\mathrm{Div}_{\mathbb{F}}(C)$ and $\mathrm{Div}^0_{\mathbb{F}}(C)$, respectively.
With a nonzero element ϕ of the function field $\overline{\mathbb{F}}(C)$ we associate a divisor $\mathrm{div}(f) := \sum_{P \in C} \mathrm{ord}_P(\phi)(P)$. A divisor $D \in \mathrm{Div}(C)$ is called *principal* if there exists a function $\phi \in \overline{\mathbb{F}}(C)^*$ with $D = \mathrm{div}(\phi)$. We denote the set of all principal divisors by $\mathrm{Princ}(C)$. The degree of a principal divisor is 0 [Sil86, Proposition II.3.1]. Note that $\mathrm{Princ}(C) \subseteq \mathrm{Div}^0(C)$ is a subgroup of $\mathrm{Div}^0(C)$.

Definition 1.31. The *divisor class group of degree* 0 *on* C, also called the *Picard group of* C, is defined as

$$\mathrm{Pic}^0(C) := \mathrm{Div}^0(C)/\mathrm{Princ}(C).$$

The subgroup of $\mathrm{Pic}^0(C)$ fixed by the Galois group $\mathcal{G}_{\overline{\mathbb{F}}/\mathbb{F}}$ is the group of divisor classes *defined over* $\mathbb{F}$ and is denoted by $\mathrm{Pic}^0_{\mathbb{F}}(C)$.

Remark 1.32. There exists a nonsingular, absolutely irreducible, projective variety J_C defined over $\mathbb{F}$ such that $J_C(\tilde{\mathbb{F}})$ is isomorphic to $\mathrm{Pic}^0_{\tilde{\mathbb{F}}}(C)$ for all intermediate fields $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$. The variety J_C is called the *Jacobian variety of* C. It has the structure

of a group, and the group law can be described by a morphism $J_C \times J_C \to J_C$. Thus it is an *algebraic group*. A projective, algebraic group is called an *abelian variety*. More details can be found in [FL05a, Section 4.4.4]. We return to abelian varieties in Chapter 5.

We conclude this subsection by introducing the genus of a curve. This notion occurs in the important theorem of Riemann-Roch, which we state in the simplified version as in [FL05a, Theorem 4.106].
But before doing so, we need to define a partial order on $\mathrm{Div}(C)$ as follows: A divisor $D = \sum_{P \in C} n_P(P)$ is called *positive (or effective)* if $n_P \geq 0$ for all $P \in C$. We write $D \geq 0$ in that case. Let $D_1, D_2 \in \mathrm{Div}(C)$. Then we write $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$. This notation is very useful for describing zeros and poles of a function. For example, the inequality $\mathrm{div}(\phi) \geq (P) - 5(Q)$ implies that the function ϕ has a zero of order at least 1 at P and a pole of order at most 5 at Q. The inequality $\mathrm{div}(\phi) \geq -2(P)$ means that ϕ has a pole of order at most 2 at P. Let $D \in \mathrm{Div}(C)$ be a divisor of C. Define

$$\mathcal{L}(D) := \{\phi \in \overline{\mathbb{F}}(C)^* \mid \mathrm{div}(\phi) \geq -D\} \cup \{0\}.$$

The set $\mathcal{L}(D)$ is a finite dimensional $\overline{\mathbb{F}}$-vector space [Sti93, Lemmas I.4.6 and Proposition I.4.9]. We denote its dimension by $\ell(D) := \dim_{\overline{\mathbb{F}}}(\mathcal{L}(D))$.

Theorem 1.33 (Riemann-Roch)**.** *Let $C/\mathbb{F}$ be an absolutely irreducible, nonsingular curve over $\mathbb{F}$. Then there exists an integer $g \geq 0$ such that for every divisor $D \in \mathrm{Div}(C)$*

$$\ell(D) \geq \deg(D) - g + 1.$$

If $D \in \mathrm{Div}(C)$ and $\deg(D) \geq 2g - 2$, then $\ell(D) = \deg(D) - g + 1$.

Proof. See [FL05a, Theorem 4.106]; or [Sti93, Theorem I.5.15], [Sil86, Theorem II.5.4], and [Har77, Theorem IV.1.3] for the full version of the theorem. □

Definition 1.34. The number g in Theorem 1.33 is called the *genus* of C.

1.1.6 Elliptic curves

This subsection is dedicated to elliptic curves. We summarize results that we need in the following chapters. In large parts we follow [Sil86]. In this subsection, let $\mathbb{F}$ be a perfect field.

Definition 1.35. An *elliptic curve over* $\mathbb{F}$ is a nonsingular, absolutely irreducible, projective curve E of genus 1 defined over $\mathbb{F}$ together with an $\mathbb{F}$-rational point $\mathcal{O} \in E(\mathbb{F})$.

Using the Riemann-Roch Theorem 1.33, it can be shown that each such curve is isomorphic to a plane curve given by a special equation, called *Weierstraß equation*. In fact, the plane curves over $\mathbb{F}$ given by Weierstraß equations are exactly the elliptic curves over $\mathbb{F}$.

Proposition 1.36. *Let $E/\mathbb{F}$ be an elliptic curve defined over $\mathbb{F}$. Then E is isomorphic over $\mathbb{F}$ to a curve C given by a* Weierstraß equation

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.3}$$

with coefficients $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$. The corresponding isomorphism maps the point $\mathcal{O}$ to $(0:1:0)$. Conversely, every nonsingular cubic given by a Weierstraß equation (1.3) is an elliptic curve defined over $\mathbb{F}$. We can take $\mathcal{O} = (0:1:0)$.

Proof. This is part of [Sil86, Proposition III.3.1]. □

Although an elliptic curve is a projective curve, we often write the corresponding affine equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.4}$$

It can be seen easily by considering the homogenized curve equation that $(0:1:0)$ is the only point at infinity on E. Because of Proposition 1.36, we fix the point $\mathcal{O} := (0:1:0)$.
If $\mathrm{char}(\mathbb{F}) \neq 2$, we may use the transformation $(x, y) \mapsto (x', y') = (x, y + \frac{1}{2}(a_1x + a_3))$, and after substituting (x, y) for (x', y') again, we obtain the curve

$$E' : y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$. The above transformation is an $\mathbb{F}$-isomorphism $E \to E'$ [FL05a, Section 4.4.2.a]. Assuming additionally that $\mathrm{char}(\mathbb{F}) \notin \{2, 3\}$, we further carry out the isomorphism $(x, y) \mapsto (x', y') = (x + \frac{b_2}{12}, y)$. This yields the curve

$$E'' : y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864},$$

where $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. Furthermore, define $b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 = \frac{1}{4}(b_2b_6 - b_4^2)$, as well as

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \quad \text{and } j := \frac{c_4^3}{\Delta}.$$

The quantity Δ is called the *discriminant of E*, while j is called the *j-invariant of E*. We also use the notation $j(E) := j$.
The curve E'' is isomorphic to E. Thus if $\mathrm{char}(\mathbb{F}) \notin \{2, 3\}$, we may assume that E is given by a *short Weierstraß equation*

$$E : y^2 = x^3 + ax + b, \ a, b \in \mathbb{F}. \tag{1.5}$$

In that case, the discriminant and j-invariant can be computed as

$$\Delta = -16(4a^3 + 27b^2) \quad \text{and } j = -1728\frac{(4a)^3}{\Delta}.$$

When starting with a curve equation (1.4), the discriminant determines whether this equation defines a nonsingular curve or not. The curve E is nonsingular if and only if $\Delta \neq 0$ [Sil86, Proposition III.1.4(a)]. The j-invariant determines the isomorphism class of an elliptic curve, since two elliptic curves are isomorphic over $\overline{\mathbb{F}}$ if and only if they have the same j-invariant [Sil86, Proposition III.1.4(b)].

Example 1.37. Let $\mathrm{char}(\mathbb{F}) \notin \{2,3\}$ and $f = y^2 - x^3 - b$ for $0 \neq b \in \mathbb{F}$. We consider the curve $E = C_f : y^2 = x^3 + b$ over $\mathbb{F}$. We compute $\Delta = -16 \cdot 27b^2$. This is nonzero as all factors are nonzero in $\mathbb{F}$ and thus E is nonsingular and describes an elliptic curve. The j-invariant is $j = 0$. Hence all curves $E : y^2 = x^3 + b$ for $b \neq 0$ are elliptic curves. Each two of them are isomorphic over $\overline{\mathbb{F}}$ because they have the same j-invariant.

Proposition 1.38. *For every $j_0 \in \overline{\mathbb{F}}$, there exists an elliptic curve E defined over $\mathbb{F}(j_0)$ with j-invariant $j(E) = j_0$. If $\mathrm{char}(\mathbb{F}) \notin \{2,3\}$, the curve E can be given by the following short Weierstraß equations:*

(a) If $j_0 = 0$, then $E : y^2 = x^3 + b$, for any $0 \neq b \in \overline{\mathbb{F}}$.

(b) If $j_0 = 1728$, then $E : y^2 = x^3 + ax$, for any $0 \neq a \in \overline{\mathbb{F}}$.

(c) If $j_0 \neq 0, 1728$, then $E : y^2 = x^3 - \frac{27j_0}{4(j_0-1728)}x - \frac{27j_0}{4(j_0-1728)}$.

Proof. The first statement is [Sil86, Proposition III.1.4(c)]. It can be checked easily that for $\mathrm{char}(\mathbb{F}) \notin \{2,3\}$ the given curves have the claimed j-invariant. Notice that the discriminant is non-zero in all three cases. □

Of course, if $\mathrm{char}(\mathbb{F}) \in \{2,3\}$, the curves can be given as well [Sil86, Proof of Proposition III.1.4(c)]. We now turn to Picard groups of elliptic curves.

Proposition 1.39. *Let E be an elliptic curve. For every divisor $D \in \mathrm{Div}^0(E)$, there exists a unique point $P \in E$ such that $D \sim (P) - (\mathcal{O})$. Denote this point by $\sigma(D)$. Then it follows for all $D_1, D_2 \in \mathrm{Div}^0(E)$ that $\sigma(D_1) = \sigma(D_2)$ if and only if $D_1 \sim D_2$. The map σ is surjective and thus induces a bijection of sets*

$$\sigma : \mathrm{Pic}^0(E) \to E.$$

Proof. This is [Sil86, Proposition III.3.4]. □

Since $\mathrm{Pic}^0(E)$ carries the structure of an abelian group, the bijection from the previous proposition induces a group structure on E. The sets $\mathrm{Pic}^0(E)$ and E are then isomorphic as groups. Choosing a Weierstraß equation for E, the group law on E can be given by formulas involving the point coordinates. We give the formulas in the case $\mathrm{char}(\mathbb{F}) \notin \{2,3\}$ for a short Weierstraß equation.

Lemma 1.40. *Let $\mathrm{char}(\mathbb{F}) \notin \{2,3\}$, and let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}$. The commutative group law induced by σ from Proposition 1.39 is given as follows: (We denote the group law by $+$ as addition.)*

(a) *For all $P \in E$, it holds $P + \mathcal{O} = P$, i. e. $\mathcal{O}$ is the neutral element.*

(b) *If $P = (x_1, y_1)$, then $(x_1, y_1) + (x_1, -y_1) = \mathcal{O}$, i. e. the additive inverse (or negative) of P is $-P = (x_1, -y_1)$.*

(c) *Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ with $P_1 \neq -P_2$. Define*

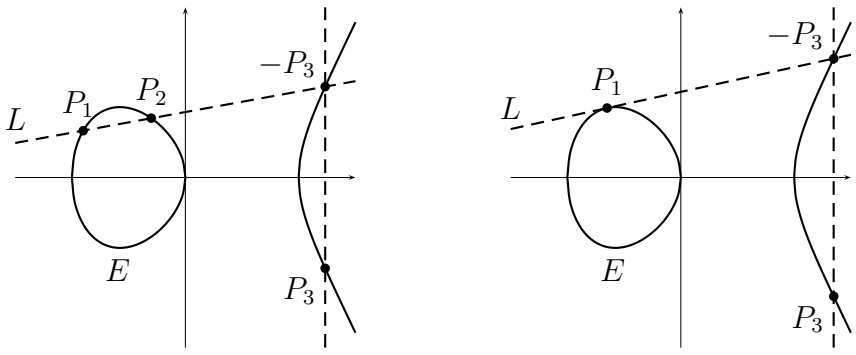
$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P_1 \neq P_2, \\ (3x_1^2 + a)/(2y_1) & \text{if } P_1 = P_2. \end{cases}$$

The point $P_3 = P_1 + P_2$ is given by $P_3 = (x_3, y_3)$ with

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1. \end{aligned}$$

Proof. Combine [Sil86, Proposition III.3.4(e)] and [Sil86, Algorithm III.2.3] or see [FL05a, Section 4.4.5]. □

Remark 1.41. The group law on an elliptic curve E has a geometric interpretation, from which the above formulas can be derived. To add two points P_1 and P_2, one takes the line L passing through them. If the points are equal, take the tangent to E in P_1. From Bézout's Theorem 1.21, we know that L intersects with E in a third point. The reflection of this third intersection point about the x-axis is the sum P_3. Figure 1.1 shows the geometric interpretation of the group law on the curve $E : y^2 = x^3 - x$ over $\mathbb{R}$. In Figure 1.1(a), the point P_1 has x-coordinate $x_1 = -0.9$ and P_2 has $x_2 = -0.3$; in Figure 1.1(b), P_1 has x-coordinate $x_1 = -0.65$.



(a) Addition (b) Doubling

Figure 1.1: Addition and doubling on $E : y^2 = x^3 - x$ over $\mathbb{R}$.

Next we consider morphisms between elliptic curves that are compatible with the group law. Let E_1, E_2 be two elliptic curves. We denote the neutral elements in E_1 and E_2 by $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively. A morphism $\varphi : E_1 \to E_2$ with $\varphi(\mathcal{O}_1) = \mathcal{O}_2$ is called an *isogeny*. If there is an isogeny between E_1 and E_2, the curves are called

isogenous. It turns out that all isogenies are group homomorphisms, which is shown in [Sil86, Theorem III.4.8]. We denote by $\mathrm{Hom}(E_1, E_2)$ the set of all isogenies from E_1 to E_2, i. e. the set of all morphisms that are group homomorphisms. The subset of all isogenies defined over $\mathbb{F}$ is denoted by $\mathrm{Hom}_{\mathbb{F}}(E_1, E_2)$.

Remark 1.42. Since we are mainly interested in the group structure of E, all morphisms of elliptic curves that occur in the following shall be group homomorphisms. In particular, when we speak of isomorphisms, we mean group isomorphisms.

The set $\mathrm{Hom}(E_1, E_2)$ is an abelian group, since E_2 is an abelian group, which means that the sum of two isogenies can be defined pointwise. If $E_1 = E_2$, the composition of isogenies turns $\mathrm{Hom}(E_1, E_1)$ into a ring.

Definition 1.43. The *endomorphism ring* $\mathrm{End}(E)$ of an elliptic curve E is defined as $\mathrm{End}(E) := \mathrm{Hom}(E, E)$. The invertible elements in $\mathrm{End}(E)$ are called *automorphisms*, and the set of all automorphisms is denoted by $\mathrm{Aut}(E)$. It is a group with respect to composition. The sets of endomorphisms and automorphisms that are defined over $\mathbb{F}$ are denoted by $\mathrm{End}_{\mathbb{F}}(E)$ and $\mathrm{Aut}_{\mathbb{F}}(E)$, respectively.

Example 1.44. For $m \in \mathbb{Z}$ define the *multiplication-by-m map* $[m] : E \to E$ on an elliptic curve $E/\mathbb{F}$ as follows: Let $P \in E$ be an arbitrary point. If $m = 0$, then $[m]P := \mathcal{O}$. If $m > 0$, then $[m]P := P + P + \cdots + P$ is the m-fold sum of P with itself. Finally, if $m \in \mathbb{Z}$, $m < 0$, then define $[m]P := -[-m]P$. The map $[m]$ is an endomorphism over $\mathbb{F}$, i. e. $[m] \in \mathrm{End}_{\mathbb{F}}(E)$.

Definition 1.45. For $0 \neq m \in \mathbb{Z}$, the kernel of the multiplication-by-m map is denoted by $E[m] := \ker([m]) = \{P \in E \mid [m]P = \mathcal{O}\}$. It is called the *$m$-torsion subgroup of E*. Elements of $E[m]$ are called *m-torsion points*. The set of $\mathbb{F}$-rational m-torsion points is denoted by $E(\mathbb{F})[m]$.

Lemma 1.46. *Let E be an elliptic curve over $\mathbb{F}$ and $0 \neq m \in \mathbb{Z}$. Suppose that $\mathrm{char}(\mathbb{F}) = 0$ or that m is prime to $\mathrm{char}(\mathbb{F})$. Then,*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},$$

in particular, if $m > 0$ is a prime, then $E[m]$ is a 2-dimensional $\mathbb{F}_m$-vector space.

Proof. See [Sil86, Corollary III.6.4]. □

The endomorphism ring of an elliptic curve is a domain of characteristic 0 [Sil86, Proposition III.4.2(c)]. Since all the maps $[m]$ are in $\mathrm{End}(E)$ for all $m \in \mathbb{Z}$, the ring $\mathbb{Z}$ can be embedded into $\mathrm{End}(E)$. Therefore, the endomorphism ring always contains a copy of $\mathbb{Z}$.

Theorem 1.47. *Let E be an elliptic curve. Then the ring $\mathrm{End}(E)$ is isomorphic either to $\mathbb{Z}$, to an order in a quadratic imaginary field, or to an order in a quaternion algebra.*

Proof. This statement is [Sil86, Corollary III.9.4]. □

Definition 1.48. If the endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E is isomorphic to an order in a quadratic imaginary field, we say that E has *complex multiplication (CM)*.

In contrast to endomorphisms, the automorphisms of E are rather rare. Over fields of characteristic different from 2 or 3, the automorphism group is a cyclic group of order 2, 4, or 6.

Theorem 1.49. *Let* $\mathrm{char}(\mathbb{F}) \notin \{2,3\}$*, and let* E *be an elliptic curve over* $\mathbb{F}$*. Then,*

$$\mathrm{Aut}(E) \cong \mu_n,$$

where μ_n *is the group of* n*th roots of unity with* $n = 2$ *if* $j(E) \notin \{0, 1728\}$*,* $n = 4$ *if* $j(E) = 1728$*, and* $n = 6$ *if* $j(E) = 0$*.*

Proof. This is [Sil86, Corollary III.10.2]. □

An automorphism of E always has the form $(x, y) \mapsto (u^2x, u^3y)$ for some $u \in \overline{\mathbb{F}}^*$. This means that $au^{-4} = a$ and $bu^{-6} = b$. Depending on whether a or b are 0 or not, this explains the above theorem.
We next describe the twists of E more closely. According to our convention that an isomorphism is a group isomorphism (see Remark 1.42), we only consider twists given by isomorphisms $\varphi : E_1 \to E_2$ with $\varphi(\mathcal{O}_1) = \mathcal{O}_2$, i. e. φ is an isogeny. The set of $\mathbb{F}$-isomorphism classes of these twists is denoted by $\mathrm{Twist}((E, \mathcal{O})/\mathbb{F})$. Such twists are related to the automorphism group of E (see Definition 1.28 and [Sil86, §X.5]).

Proposition 1.50. *Let* E *be an elliptic curve defined over the field* $\mathbb{F}$ *with* $\mathrm{char}(\mathbb{F}) \notin \{2,3\}$*. Let* E *be given by an equation* $E : y^2 = x^3 + ax + b$*. Let* $\delta = 2$ *if* $j(E) \notin \{0, 1728\}$*,* $\delta = 4$ *if* $j(E) = 1728$ *and* $\delta = 6$ *if* $j(E) = 0$*.*
There is a bijection $\mathbb{F}^*/(\mathbb{F}^*)^\delta \to \mathrm{Twist}((E, \mathcal{O})/\mathbb{F})$*. For* $\xi \in \mathbb{F}^*$ *the twist* E_ξ*, corresponding to* $\xi \mod (\mathbb{F}^*)^\delta$ *has the equation*

$$\begin{aligned}
&E_\xi : y^2 = x^3 + \xi^{-2}ax + \xi^{-3}b && \text{if } j(E) \notin \{0, 1728\} && (\delta = 2),\\
&E_\xi : y^2 = x^3 + \xi^{-1}ax && \text{if } j(E) = 1728 && (\delta = 4),\\
&E_\xi : y^2 = x^3 + \xi^{-1}b && \text{if } j(E) = 0 && (\delta = 6).
\end{aligned}$$

Proof. This is [Sil86, Proposition X.5.4] with ξ replaced by ξ^{-1}. This can be done, since ξ_1 and ξ_2 are in the same class modulo $(\mathbb{F}^*)^\delta$ if and only if ξ_1^{-1} and ξ_2^{-1} are. □

Remark 1.51. The corresponding isomorphism $\sigma_\xi : E_\xi \to E$ is given by

$$\begin{aligned}
&(x_1, y_1) \mapsto (\xi x_1, \xi^{3/2} y_1) && \text{if } j(E) \notin \{0, 1728\} && (\delta = 2),\\
&(x_1, y_1) \mapsto (\xi^{1/2} x_1, \xi^{3/4} y_1) && \text{if } j(E) = 1728 && (\delta = 4),\\
&(x_1, y_1) \mapsto (\xi^{1/3} x_1, \xi^{1/2} y_1) && \text{if } j(E) = 0 && (\delta = 6).
\end{aligned}$$

Recall Definition 1.29 for the degree of a twist. The maximal degrees that can occur are given by δ. The following table lists the degree d of the twist depending on $j(E)$ and ξ:

$j(E)$	δ	ξ	d
$\notin \{0, 1728\}$	2	$\in (\mathbb{F}^*)^2$	1
		$\notin (\mathbb{F}^*)^2$	2
1728	4	$\in (\mathbb{F}^*)^4$	1
		$\in (\mathbb{F}^*)^2, \notin (\mathbb{F}^*)^4$	2
		$\notin (\mathbb{F}^*)^2$	4
0	6	$\in (\mathbb{F}^*)^6$	1
		$\in (\mathbb{F}^*)^3, \notin (\mathbb{F}^*)^2$	2
		$\in (\mathbb{F}^*)^2, \notin (\mathbb{F}^*)^3$	3
		$\notin (\mathbb{F}^*)^2, \notin (\mathbb{F}^*)^3$	6

For all the cases with $d = 1$ we can take $\xi_1 := \xi^{1/\delta} \in \mathbb{F}^*$ and get an isomorphism $E_{\xi_1^\delta} \to E,\ (x, y) \mapsto (\xi_1^2 x, \xi_1^3 y)$. In the same way, all the cases with $d = 2$ can be treated like the cases with $j(E) \notin \{0, 1728\}$ by taking a $(\delta/2)$th root of ξ.

From now on, we consider elliptic curves over a finite field. We fix $\mathbb{F} = \mathbb{F}_q$, a field of order q. Let $p = \mathrm{char}(\mathbb{F}_q)$ be the characteristic of $\mathbb{F}_q$. Since there are only finitely many elements that can occur as coordinates of $\mathbb{F}_q$-rational points, the set $E(\mathbb{F}_q)$ is finite. Hasse's Theorem gives bounds for its cardinality.

Theorem 1.52 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve defined over $\mathbb{F}_q$. Then*

$$\#E(\mathbb{F}_q) = q + 1 - t, \ \textit{where } |t| \leq 2\sqrt{q}. \tag{1.6}$$

Proof. This is [Sil86, Theorem V.1.1]. □

The number t from the previous theorem is called the *trace of the Frobenius endomorphism of E over $\mathbb{F}_q$*. This terminology is justified in the following example. Note that the q-power Frobenius automorphism on a finite field extension $\mathbb{F}_{q^k}/\mathbb{F}_q$ generates the Galois group $\mathcal{G}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ for any $k \in \mathbb{N}$. As already mentioned in Subsection 1.1.4, the action of any field automorphism in $\mathcal{G}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$ extends to points on the elliptic curve $E/\mathbb{F}_q$. Extending the Frobenius automorphism in this way results in an $\mathbb{F}_q$-endomorphism of E:

Example 1.53. If E is an elliptic curve defined over $\mathbb{F}_q$, the map

$$\phi_q : E \to E,\ (x_1, y_1) \mapsto (x_1^q, y_1^q)$$

is an endomorphism of E, called the *Frobenius endomorphism*. Since the qth power map is the identity on $\mathbb{F}_q$, the set of points fixed by ϕ_q is the group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on E. The endomorphism ϕ_q satisfies $\phi_q^2 - [t] \circ \phi_q + [q] = 0$, see [Sch85, p. 485]. Therefore, we call $\chi_q := T^2 - tT + q \in \mathbb{Z}[T]$ the *characteristic polynomial of ϕ_q*.

Deuring [Deu41] describes the endomorphism ring of an elliptic curve over a finite field. It can not be isomorphic to $\mathbb{Z}$, since it always contains ϕ_q. Therefore, it is isomorphic to an order in a quaternion algebra or to an order in a quadratic imaginary field, see Theorem 1.47. The following theorem relates the structure of $\mathrm{End}(E)$ with that of $E[p]$.

Theorem 1.54. *Let E be an elliptic curve defined over $\mathbb{F}_q$. The following statements are equivalent:*

(a) The endomorphism ring $\mathrm{End}(E)$ is non-commutative.

(b) The ring $\mathrm{End}(E)$ is an order in a quaternion algebra.

(c) The p-torsion subgroup is $E[p] = \{\mathcal{O}\}$.

(d) The trace of Frobenius t is divisible by p, i. e. $p \mid t$.

If the above conditions do not hold, then $E[p] \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. The theorem follows from [Sil86, Theorem V.3.1] with [Wat69, Theorem 4.1 and the definition before] or [Sil86, Exercise 5.10] concerning condition (d). □

Definition 1.55. An elliptic curve $E/\mathbb{F}_q$ is called *supersingular* if one of the conditions in Theorem 1.54 holds. Otherwise, the curve is called *ordinary*.

Returning to Hasse's Theorem, the question arises whether for any number t with $|t| \leq 2\sqrt{q}$ there exists an elliptic curve with $q + 1 - t$ rational points. For most of such numbers t this is true. There are only a few exceptions (see [Wat69, Theorem 4.1] and [Sch87, Theorem 4.2 and Theorem 4.6]). In the following lemma, we only state the case that we need later.

Lemma 1.56. *Let $t \in \mathbb{Z}$ with $|t| \leq 2\sqrt{q}$ and $p \nmid t$. Then there exists an ordinary elliptic curve E defined over $\mathbb{F}_q$, such that $\#E(\mathbb{F}_q) = q + 1 - t$. In particular, if $q = p$ is prime, then for every $t \neq 0$ with $|t| \leq 2\sqrt{p}$ there exists an ordinary elliptic curve over $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p + 1 - t$.*

Proof. This result follows immediately from [Wat69, Theorem 4.1]. □

Consider the twists of an elliptic curve over a finite field $\mathbb{F}_q$ as described in Proposition 1.50 and Remark 1.51. The number of $\mathbb{F}_q$-rational points on the twist can be given in terms of the trace t of the original curve E and the order q of the field. Heß, Smart, and Vercauteren [HSV06] determine the possible group orders of the twists of an ordinary elliptic curve over a finite field, which we give in the following proposition. Note that $\#E(\mathbb{F}_{q^d}) = \#E'(\mathbb{F}_{q^d})$ for a twist of degree d.

Proposition 1.57. *Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$, and let $\#E(\mathbb{F}_q) = q + 1 - t$. Let E' be a twist of E of degree d. The possible group orders of $E'(\mathbb{F}_q)$ are given as follows:*

d	$\#E'(\mathbb{F}_q)$
2	$q+1+t$
3	$q+1-(3v-t)/2$ *with* $t^2-4q=-3v^2$ $q+1-(-3v-t)/2$ *with* $t^2-4q=-3v^2$
4	$q+1-v$ *with* $t^2-4q=-v^2$ $q+1+v$ *with* $t^2-4q=-v^2$
6	$q+1-(3v+t)/2$ *with* $t^2-4q=-3v^2$ $q+1-(-3v+t)/2$ *with* $t^2-4q=-3v^2$

Proof. This is [HSV06, Proposition 8]. □

The groups of points on elliptic curves used in cryptography are cyclic groups of a large prime order. Let E be an elliptic curve defined over $\mathbb{F}_q$ with $n := \#E(\mathbb{F}_q)$. Let $r \neq p$ be a prime dividing n.

Definition 1.58. The *embedding degree of E with respect to r* is the smallest integer k such that $r \mid (q^k - 1)$.

If $r \nmid (q-1)$, the embedding degree determines the smallest extension of $\mathbb{F}_q$ over which all r-torsion points of E are defined.

Theorem 1.59. *Let $E/\mathbb{F}_q$ be an elliptic curve, $n = \#E(\mathbb{F}_q)$, r a prime with $r \mid n$ and $r \nmid (q-1)$. Then $E[r] \subseteq E(\mathbb{F}_{q^k})$ if and only if $r \mid (q^k - 1)$.*

Proof. See [BK98, Theorem 1]. □

Let $k > 1$ be the embedding degree of E with respect to r. Since $r \mid n$, we know that there are r-torsion points defined over $\mathbb{F}_q$. Let ϕ_q be the q-power Frobenius endomorphism as in Example 1.53. Since an r-torsion point is again mapped to an r-torsion point by ϕ_q, its restriction to $E[r]$ is a group endomorphism.

Lemma 1.60. *Let $E/\mathbb{F}_q$ be an elliptic curve, $r \neq p$ a prime with $r \mid \#E(\mathbb{F}_q)$, $k > 1$ the embedding degree of E with respect to r, and ϕ_q the q-power Frobenius endomorphism.*
Then $E[r]$ is a 2-dimensional vector space over $\mathbb{F}_r$. The restriction of ϕ_q to $E[r]$, $\phi_q : E[r] \to E[r]$ is a bijective linear map, which has the two eigenvalues $\lambda_1 = 1$ and $\lambda_2 = q$. We have the following vector space decomposition into eigenspaces:

$$E[r] = (\ker(\phi_q - [1]) \cap E[r]) \oplus (\ker(\phi_q - [q]) \cap E[r]).$$

It is $\ker(\phi_q - [1]) \cap E[r] = E(\mathbb{F}_q)[r]$ *and* $\ker(\phi_q - [q]) \cap E[r] \subseteq E(\mathbb{F}_{q^k})[r]$.

Proof. It is clear that $E[r]$ is a 2-dimensional $\mathbb{F}_r$-vector space (see Lemma 1.46). It can be seen easily that ϕ_q is injective and thus bijective on $E[r]$. There are r-torsion points in $E(\mathbb{F}_q)$, because $r \mid \#E(\mathbb{F}_q)$. Points defined over $\mathbb{F}_q$ are fixed under ϕ_q and so 1 is an eigenvalue of ϕ_q, and the corresponding eigenspace is $\ker(\phi_q - [1]) \cap E[r] = E(\mathbb{F}_q)[r]$. The characteristic polynomial of the vector space homomorphism ϕ_q is

the polynomial χ_q from Example 1.53. From $r \mid q+1-t = \chi_q(1)$, it can also be seen that $(T-1) \mid \chi_q$ modulo r. Over $\mathbb{F}_r$, the polynomial $\chi_q = T^2 - tT + q$ splits as $(T-1)(T-q) \in \mathbb{F}_r[T]$, showing that the other eigenvalue of ϕ_q on $E[r]$ is q. Thus $E[r]$ is the direct sum of the eigenspaces. The statement $\ker(\phi_q - [q]) \cap E[r] \subseteq E(\mathbb{F}_{q^k})[r]$ follows from $r \mid n$ and $k > 1$. □

1.1.7 Edwards curves and twisted Edwards curves

In this subsection, we briefly describe Edwards curves and twisted Edwards curves. Edwards curves were introduced as a new normal form for elliptic curves by Edwards in 2007 [Edw07]. Their importance for cryptography was shown by Bernstein and Lange [BL07].
Let $\mathbb{F}$ be a field of characteristic different from 2. An *Edwards curve over* $\mathbb{F}$ is a curve

$$E_d : x^2 + y^2 = 1 + dx^2y^2, \ d \in \mathbb{F} \setminus \{0, 1\}. \tag{1.7}$$

A group law on E_d can be defined as follows: The sum of two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ in $E_d(\mathbb{F})$ is given by

$$P_1 + P_2 = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right). \tag{1.8}$$

The neutral element with respect to this addition is $(0, 1)$. The point $(0, -1)$ has order 2 and the points $(1, 0)$ and $(-1, 0)$ have order 4. The above group law has the advantage that it is complete for certain values of d, i. e. there are no exceptional cases, the formulas work for any pair of input points. Theorem 3.3 in [BL07] shows that this is the case if d is not a square in $\mathbb{F}$.
Bernstein, Birkner, Joye, Lange, and Peters generalize the concept of Edwards curves and introduce *twisted Edwards curves* in [BBJ+08].

Definition 1.61. Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) \neq 2$. A *twisted Edwards curve over* $\mathbb{F}$ is a curve

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2, \ a, d \in \mathbb{F}^*, \ d \neq a. \tag{1.9}$$

Remark 1.62. In fact, a twisted Edwards curve is a quadratic twist of an Edwards curve. The curve $E_{a,d}$ is a quadratic twist of the curve $E_{1,d/a}$, see [BBJ+08, Section 2]. Note that for $a = 1$, the curve $E_{a,d} = E_{1,d}$ is an *Edwards curve* E_d as defined before.

The fact that many elliptic curves are birationally equivalent to twisted Edwards curves can be used to represent elliptic curves by Edwards curves or twisted Edwards curves. The following theorem shows that an elliptic curve E over $\mathbb{F}$ which has a point of order 4 is birationally equivalent to an Edwards curve E_d.

Theorem 1.63. *Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) \neq 2$. Let E be an elliptic curve over $\mathbb{F}$ that has a point of order 4. Then there exists $d \in \mathbb{F} \setminus \{0, 1\}$ such that the curve $E_d : x^2 + y^2 = 1 + dx^2y^2$ is birationally equivalent to E over $\mathbb{F}$.*

Proof. This is Theorem 3.3 in [BBJ+08]. □

The algorithm of how to determine the curve E_d from a given elliptic curve E is described in the proof of [BBJ+08, Theorem 3.3]. Moreover, the group law on the elliptic curve E corresponds to the group law on the Edwards curve under the birational equivalence. Theorem 3.2 in [BL07] shows that two corresponding points add to the corresponding point of the sum.
As a generalization of Edwards curves, twisted Edwards curves naturally cover a larger set of elliptic curves that can be represented. The set of twisted Edwards curves covers all elliptic curves that can be transformed into a Montgomery curve.

Definition 1.64. Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) \neq 2$. Let $A \in \mathbb{F} \setminus \{-2, 2\}$ and $B \in \mathbb{F}^*$. A curve

$$E^M_{A,B} : By^2 = x^3 + Ax^2 + x$$

is called a *Montgomery curve*.

Details on Montgomery curves can be found in [DL05a, Section 13.2.3].

Theorem 1.65. *Every twisted Edwards curve over $\mathbb{F}$ is birationally equivalent over $\mathbb{F}$ to a Montgomery curve, and conversely, every Montgomery curve over $\mathbb{F}$ is birationally equivalent over $\mathbb{F}$ to a twisted Edwards curve.*

Proof. This is proved as Theorem 3.2 in [BBJ+08]. □

The specific transformations are given in the proof of [BBJ+08, Theorem 3.2]. Over a finite field $\mathbb{F}_q$, many Montgomery curves are even birationally equivalent to an Edwards curve. This is the case if $q \equiv 3 \pmod 4$ [BBJ+08, Theorem 3.4].
The group law on a twisted Edwards curve is very similar to that on an Edwards curve. For $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E_{a,d}(\mathbb{F})$ the sum of the two points is given by

$$P_1 + P_2 = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right). \tag{1.10}$$

If a is a square in $\mathbb{F}$, $E_{a,d}$ is $\mathbb{F}$-isomorphic to $E_{1,d/a}$ under the isomorphism $(x, y) \mapsto (\sqrt{a}x, y)$ that fixes the neutral element $(0, 1)$. Therefore, the above formulas are complete on $E_{a,d}(\mathbb{F})$ if a is a square in $\mathbb{F}$ and d is a nonsquare in $\mathbb{F}$ (see also [BBJ+08, Section 6]).
For the remainder of this subsection, we consider a twisted Edwards curve in its projective form

$$E_{a,d} : (aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2.$$

The point $\mathcal{O} := (0 : 1 : 1)$ is the neutral element of the addition, and the point $\mathcal{O}' := (0 : -1 : 1)$ has order 2. The points $(1/\sqrt{a} : 0 : 1)$ and $(-1/\sqrt{a} : 0 : 1)$ both have order 4. All affine points are nonsingular, but there are two singular points at infinity.

Lemma 1.66. *Let $E_{a,d}$ be a twisted Edwards curve over $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2$. The points $\Omega_1 := (1:0:0)$ and $\Omega_2 := (0:1:0)$ are the only points at infinity on $E_{a,d}$. Both points are singular, and their multiplicities are $m_{\Omega_1}(E_{a,d}) = 2 = m_{\Omega_2}(E_{a,d})$.*

Proof. Let $f = (aX^2 + Y^2)Z^2 - Z^4 - dX^2Y^2$ be the polynomial defining $E_{a,d}$. A point $P = (X_P : Y_P : 0) \in E_{a,d}$ must satisfy $dX_P^2Y_P^2 = 0$. Since $d \neq 0$, the only two possible points with Z-coordinate equal to 0 are $\Omega_2 = (1:0:0)$ and $\Omega_2 = (0:1:0)$. We compute the partial derivatives

$$\frac{\partial f}{\partial X} = 2X(aZ^2 - dY^2), \quad \frac{\partial f}{\partial Y} = 2Y(Z^2 - dX^2), \quad \frac{\partial f}{\partial Z} = 2Z(aX^2 + Y^2 - 2Z^2),$$

and see that they all vanish at Ω_1 and Ω_2. According to Definition 1.12, both points are singular. To show that the multiplicity of each point is 2, we follow Remark 1.15. Dehomogenize f with respect to the first coordinate such that Ω_1 corresponds to the affine point $(0,0)$ on the affine curve given by the polynomial $az^2 + y^2z^2 - z^4 - dy^2$. The lowest-degree monomials az^2 and $-dy^2$ have degree 2, which means that $m_{\Omega_1}(E_{a,d}) = 2$. The point Ω_2 is handled similarly. □

1.1.8 Hyperelliptic curves

In this section, we give a basic introduction to hyperelliptic curves, mainly to introduce notation for hyperelliptic curves of genus 2. Let $\mathbb{F}$ be a perfect field.

Definition 1.67. A nonsingular projective curve $C/\mathbb{F}$ of genus g is called a *hyperelliptic curve of genus g* if its function field $\mathbb{F}(C)$ is a separable extension of degree 2 of the rational function field $\mathbb{F}(x)$, i. e. $[\mathbb{F}(C) : \mathbb{F}(x)] = 2$.

With the help of the Riemann-Roch Theorem 1.33, it can be shown that a hyperelliptic curve of genus g can be given by a nonsingular plane affine curve (see Section 4.4.2.b in [FL05a]). For the purpose of this work, it suffices to characterize hyperelliptic curves by their affine plane parts as given in the following proposition.

Proposition 1.68. *The function field of a hyperelliptic curve of genus g over $\mathbb{F}$ is the function field of a nonsingular, plane, affine curve given by*

$$C : y^2 + h(x)y = f(x),$$

where $h(x), f(x) \in \mathbb{F}[x]$, $\deg(f) \in \{2g+1, 2g+2\}$, $\deg(h) \leq g+1$.

Proof. This follows from Theorem 4.122 in [FL05a]. □

A *Weierstraß point* on C is a fixed point under the hyperelliptic involution induced by the nontrivial automorphism of the field extension $\mathbb{F}(C)/\mathbb{F}(x)$. For details, see [FL05a, Section 4.4.2.b]. If there exists an $\mathbb{F}$-rational Weierstraß point, the curve is birationally equivalent to one of the form

$$C : y^2 + h(x)y = f(x),$$

where $h(x), f(x) \in \mathbb{F}[x]$, $\deg(f) = 2g+1$, $\deg(h) \leq g$. The homogenization of any such curve has a singular point at infinity.

Remark 1.69. If $\deg(f) = 2g+1$ and $\mathrm{char}(\mathbb{F}) \neq 2$, the equation can be transformed by completing the square to achieve $h(x) = 0$ [FL05a, p.74]. If we have a curve given by an equation $y^2 = f(x)$, a point $P = (x_P, y_P)$ being singular means that $y_P = 0$ and x_P is a double root of $f(x)$. Therefore, a hyperelliptic curve over a field of characteristic different from 2 can be given as $C : y^2 = f(x)$ such that f has only simple roots in $\overline{\mathbb{F}}[x]$.

With the above definition of hyperelliptic curves we may subsume elliptic curves as hyperelliptic curves of genus 1. But if $g > 1$, the points on C do not form a group anymore. Therefore, we use the Picard group $\mathrm{Pic}^0(C)$, or in other words, the Jacobian variety J_C for cryptographic applications (see Definition 1.31 and Remark 1.32). The following theorem gives a nice representation for elements of $\mathrm{Pic}^0(C)$, from which their field of definition can be read off.

Theorem 1.70 (Mumford representation)**.** *Let $C : y^2 + h(x)y = f(x)$ be a hyperelliptic curve of genus g with $h, f \in \mathbb{F}[x]$, $\deg(f) = 2g + 1$, $\deg(h) \leq g$. Let $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$. Each nontrivial group element in $\mathrm{Pic}^0_{\tilde{\mathbb{F}}}(C)$ can be represented by a unique pair of polynomials $(u(x), v(x))$, $u, v \in \tilde{\mathbb{F}}[x]$, where*

(a) the polynomial u is monic,

(b) $\deg(v) < \deg(u) \leq g$,

(c) $u \mid (v^2 + vh - f)$.

Proof. See [FL05a, Theorem 4.145]. □

Remark 1.71. Arithmetic in the group $\mathrm{Pic}^0_{\tilde{\mathbb{F}}}(C)$ with elements in Mumford representation can be done with *Cantor's algorithm*, see [Can87] or [DL05b, Algorithm 14.7]. The Mumford representation in the previous theorem shows that the Picard group $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ of a hyperelliptic curve C over a finite field $\mathbb{F}_q$ is finite.

From now on, we identify the Jacobian variety J_C (see Remark 1.32) with $\mathrm{Pic}^0(C)$. For the sake of brevity, we use the notation J_C, always keeping in mind that for us, elements of J_C are divisor classes. We denote the class of a divisor D by $\overline{D}$. It has already been mentioned that J_C is an abelian variety (see Remark 1.32). An *endomorphism of J_C* is a morphism of abelian varieties $J_C \to J_C$, i. e. a morphism of varieties that additionally is a group homomorphism (see [FL05a, Section 4.3.3]). In particular, it fixes the neutral element of J_C. We denote the set of all endomorphisms of J_C by $\mathrm{End}(J_C)$. The set of all endomorphisms defined over a field $\tilde{\mathbb{F}}$ with $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$ is denoted by $\mathrm{End}_{\tilde{\mathbb{F}}}(J_C)$.

Example 1.72. An important endomorphism of J_C is the multiplication-by-m map $[m] : J_C \to J_C$ for $m \in \mathbb{Z}$. An element $\overline{D} \in J_C$ is mapped to $[m]\overline{D}$, which is defined as the m-fold sum of $\overline{D}$, understanding $m = 0$ and negative m as usual (compare with Example 1.44). The kernel of $[m]$ is denoted by

$$J_C[m] := \{\overline{D} \in J_C \mid [m]\overline{D} = \overline{0}\},$$

where $\overline{0}$ is the class of the zero-divisor $D = 0$. The set $J_C[m]$ is called the *subgroup of m-torsion points on J_C*. For any $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$, the subset of $\tilde{\mathbb{F}}$-rational divisor classes in $J_C[m]$ is denoted by $J_C(\tilde{\mathbb{F}})[m]$.

The previous example shows that there is an embedding $\mathbb{Z} \to \mathrm{End}_{\mathbb{F}}(J_C)$. Next we state the generalization of Lemma 1.46.

Theorem 1.73. *Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}$ and let J_C be its Jacobian variety. Let $0 \neq m \in \mathbb{Z}$. If $\mathrm{char}(\mathbb{F}) = 0$ or if m is prime to $\mathrm{char}(\mathbb{F})$, then*

$$J_C[m] \cong (\mathbb{Z}/m\mathbb{Z})^{2g}.$$

If $\mathrm{char}(\mathbb{F}) = p > 0$, then $J_C[p^e] \cong (\mathbb{Z}/p^e\mathbb{Z})^s$, where $0 \leq s \leq g$ for all $e \geq 1$.

Proof. This is [DL05b, Theorem 14.11]. □

Definition 1.74. The number s in Theorem 1.73 is called the *p-rank of C over $\mathbb{F}$*.

For the remainder of this section, we consider hyperelliptic curves C over finite fields $\mathbb{F} = \mathbb{F}_q$.

Definition 1.75. If the p-rank of C is equal to g, then J_C is called *ordinary*. The Jacobian J_C is called *supersingular* if it is the product of supersingular elliptic curves. The curve C is called ordinary or supersingular if J_C is ordinary or supersingular, respectively.

Remark 1.76. An elliptic curve is supersingular if and only if it has p-rank 0. For curves of genus larger than 1, we have that if C is supersingular, then it has p-rank 0. The converse only holds for $g \leq 2$ [FL05a, Remark 4.75].

If we extend the q-power Frobenius automorphism of $\overline{\mathbb{F}_q}$ to points on C, to divisors, and finally to divisor classes, we obtain an endomorphism $\phi_q : J_C \to J_C$, called the *Frobenius endomorphism on J_C*. When using the Mumford representation, the endomorphism is carried out by applying the q-power map to the coefficients of the polynomials u and v.

Theorem 1.77. *The endomorphism ϕ_q satisfies a* characteristic polynomial *of degree $2g$ given by*

$$\chi_q(T) = T^{2g} + a_1 T^{2g-1} + \cdots + a_g T^g + \cdots + a_1 q^{g-1} T + q^g \in \mathbb{Z}[T].$$

Let $\alpha_i \in \mathbb{C}$ be the roots of χ_q over $\mathbb{C}$, i. e.

$$\chi_q(T) = \prod_{i=1}^{2g} (T - \alpha_i).$$

Then the following statements hold:

(a) *The numbers* α_i *satisfy* $|\alpha_i| = \sqrt{q}$ *for all* $1 \leq i \leq 2g$. *There exists an ordering of the* α_i *with* $\overline{\alpha_{i+g}} = \alpha_i$, *i. e.* $\alpha_i \alpha_{i+g} = q$ *for all* $1 \leq i \leq g$.

(b) *For any positive integer* k, *it holds*

$$\#C(\mathbb{F}_{q^k}) = q^k + 1 - \sum_{i=1}^{2g} \alpha_i^k, \quad \#J_C(\mathbb{F}_{q^k}) = \prod_{i=1}^{2g} (1 - \alpha_i^k),$$

as well as $|\#C(\mathbb{F}_{q^k}) - (q^k + 1)| \leq g\lfloor 2q^{k/2} \rfloor$. *In particular,* $\#J_C(\mathbb{F}_q) = \chi_q(1)$.

Proof. See Theorem 14.16 and Theorem 14.17 in [DL05b]. □

Example 1.78. Let C be a hyperelliptic curve of genus 2 over the finite field $\mathbb{F}_q$. The characteristic polynomial of the Frobenius endomorphism on J_C is

$$\chi_q(T) = T^4 + a_1 T^3 + a_2 T^2 + a_1 q T + q^2$$

with $a_1, a_2 \in \mathbb{Z}$. The equations in Theorem 1.77 lead to a relation between the coefficients a_1, a_2 and $n_k := \#C(\mathbb{F}_{q^k})$, $k \in \{1, 2\}$.
We have $\chi_q = T^4 - \sum_{i=1}^4 \alpha_i T^3 + \sum_{i<j} \alpha_i \alpha_j T^2 - q \sum_{i=1}^4 \alpha_i T + q^2$. It follows that $a_1 = -(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)$ and thus $n_1 = q + 1 + a_1$. Computing a_1^2 shows that $n_2 = q^2 + 1 + 2a_2 - a_1^2$. Knowing a_1 and a_2, it is possible to compute n_1 and n_2 and vice versa. From the inequality in part (b) of the previous theorem, it follows $|a_1| \leq 2\lfloor 2\sqrt{q} \rfloor$ and $-2q \leq a_2 \leq 10q$. More accurate are the following bounds depending on a_1 (see [Rüc90, Theorem 1.1]):

$$2|a_1|\sqrt{q} - 2q \leq a_2 \leq \frac{a_1^2}{4} + 2q.$$

The techniques from the example can be applied for arbitrary genus g. Thus the order of the Jacobian $J_C(\mathbb{F}_q)$ can be computed from the number of $\mathbb{F}_{q^k}$-rational points on C for $1 \leq k \leq g$. Knowing the coefficients of the characteristic polynomial of the Frobenius endomorphism means knowing $\#C(\mathbb{F}_{q^k})$ for $1 \leq k \leq g$.

1.2 Pairings

In this section, we define pairings and introduce the Tate-Lichtenbaum pairing and the Weil pairing on the Jacobian of a hyperelliptic curve. In the case of elliptic curves, we describe the details of pairing computation for different variants of pairings.
Pairings used in cryptography are efficiently computable bilinear maps on torsion subgroups of the Jacobian variety of a hyperelliptic curve that map into the multiplicative group of a finite field. We call such a map a *cryptographic pairing*. In contrast to the mathematical concept of a pairing, this additionally includes the existence of algorithms for efficient pairing computation.

Definition 1.79. Let G_1, G_2 be finite abelian groups written additively, and let G_3 be a multiplicatively written finite abelian group. A *cryptographic pairing* is a map

$$e : G_1 \times G_2 \to G_3$$

that satisfies the following properties:

(a) It is *non-degenerate*, i. e. for all $0 \neq P \in G_1$ there is a $Q \in G_2$ with $e(P, Q) \neq 1$, and for all $0 \neq Q \in G_2$ there is a $P \in G_1$ with $e(P, Q) \neq 1$.

(b) It is *bilinear*, i. e. for $P_1, P_2 \in G_1$ and $Q_1, Q_2 \in G_2$ we have

$$\begin{aligned} e(P_1 + P_2, Q_1) &= e(P_1, Q_1)e(P_2, Q_1), \\ e(P_1, Q_1 + Q_2) &= e(P_1, Q_1)e(P_1, Q_2). \end{aligned}$$

(c) It is efficiently computable.

An important property that is used in most applications, and that follows immediately from bilinearity is $e([a]P, [b]Q) = e(P, Q)^{ab} = e([b]P, [a]Q)$ for all $a, b \in \mathbb{Z}$ and for all $P \in G_1$ and $Q \in G_2$.
The first applications in cryptography used the Weil pairing. Menezes, Okamoto, and Vanstone [MOV93] describe a way of reducing the discrete logarithm problem (DLP) on a supersingular elliptic curve to a DLP in the multiplicative group of a finite field. They construct a group isomorphism from the Weil pairing. Frey and Rück [FR94] use a map deduced from the Tate pairing for a more general reduction of the DLP in a torsion subgroup of the Jacobian of a curve. First constructive applications were the identity-based non-interactive key agreement of Sakai, Ohgishi, and Kasahara [SOK00], Joux's tripartite one-round key agreement [Jou00], the identity-based encryption scheme by Boneh and Franklin [BF01, BF03], and the short signature scheme by Boneh, Lynn, and Shacham [BLS04b]. Currently, most cryptographic pairings are variants of the Tate pairing.

1.2.1 The Tate-Lichtenbaum pairing

The Tate pairing can be defined on an arbitrary abelian variety. It induces a pairing on the r-torsion subgroup of the abelian variety for a prime r. A brief overview of the definition of the Tate pairing can be found in [DF05a, Sections 6.2 and 6.3]. Lichtenbaum describes a version of the Tate pairing which can be computed very efficiently (see [DF05a, Corollary 6.17]). Since we are interested in practical implementations, we restrict ourselves to discussing the Tate-Lichtenbaum pairing [DF05a, Definition 6.15]. We also refer to it simply as the Tate pairing, knowing that we use Lichtenbaum's approach.
Let C be a hyperelliptic curve of genus g defined over a finite field $\mathbb{F}_q$ of characteristic p. Let J_C be the Jacobian variety of C. Note that we regard elements of J_C as divisor classes represented by a divisor of degree 0. Let $n = \#J_C(\mathbb{F}_q)$ and $r > 5$ be a prime

different from p with $r \mid n$. The embedding degree can be defined as for elliptic curves (Definition 1.58).

Definition 1.80. The smallest integer k with $r \mid (q^k - 1)$ is called the *embedding degree of C with respect to r*.

Remark 1.81. The embedding degree as defined in the previous definition is a function of r and q and actually does not depend on the curve itself. Nevertheless, we attach it to the curve C if the prime r divides $\#J_C(\mathbb{F}_q)$.
If k is the smallest integer with $r \mid (q^k - 1)$, then the order of q modulo r is k. Furthermore, the smallest field extension of $\mathbb{F}_q$ that contains the group μ_r of all rth roots of unity is $\mathbb{F}_{q^k}$. This does not mean that $\mathbb{F}_{q^k}$ is the smallest extension of $\mathbb{F}_p$ that contains μ_r. As shown by Hitt [Hit07], this observation may have an influence on the security of pairing-based cryptosystems.

Definition 1.82. Let C be a hyperelliptic curve of genus g over the finite field $\mathbb{F}_q$ of characteristic p, and let $r \neq p$ be a prime dividing $\#J_C(\mathbb{F}_q)$. Let k be the embedding degree of C with respect to r. The *Tate-Lichtenbaum pairing* (or simply *Tate pairing*) is a map

$$T_r : J_C(\mathbb{F}_{q^k})[r] \times J_C(\mathbb{F}_{q^k})/[r]J_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$$

defined as follows: Let $P \in J_C(\mathbb{F}_{q^k})[r]$ be an $\mathbb{F}_{q^k}$-rational divisor class of order dividing r represented by a divisor D_P, and let $Q \in J_C(\mathbb{F}_{q^k})$ be an $\mathbb{F}_{q^k}$-rational divisor class represented by a divisor D_Q such that its support is disjoint from the support of D_P. Let $f_{r,P} \in \overline{\mathbb{F}_{q^k}}(C)$ be a function on C with $\operatorname{div}(f_{r,P}) = rD_P$. Then

$$T_r(P, Q + [r]J_C(\mathbb{F}_{q^k})) = f_{r,P}(D_Q)(\mathbb{F}_{q^k}^*)^r.$$

The evaluation of $f_{r,P}$ at a divisor $D = \sum_{R \in C} n_R(R)$ is given as

$$f_{r,P}(D) = \prod_{R \in C} f_{r,P}(R)^{n_R}.$$

Proposition 1.83. *The Tate pairing as defined in Definition 1.82 is well defined, bilinear, non-degenerate, and can be computed in $O(\log_2(r))$ operations in $\mathbb{F}_{q^k}^*$.*

Proof. This is Proposition 2.3 in [FR94] and [DF05a, Theorem 6.15 and Corollary 6.17]. □

For a suitable curve, the Tate pairing is hence a cryptographic pairing in the sense of Definition 1.79. The following lemma gives a simple statement from elementary group theory that can be used to represent the group $J_C(\mathbb{F}_{q^k})/[r]J_C(\mathbb{F}_{q^k})$ with points in $J_C(\mathbb{F}_{q^k})[r]$.

Lemma 1.84. *Let G be a finite abelian group written additively, and let r be a prime dividing $|G|$. Let $G[r]$ be the subgroup of all points of order dividing r and rG the set of all r-fold sums of elements in G. If there is no element of order r^2 in G, then $G[r] \cong G/rG$.*

Proof. We show that the map $G[r] \to G/rG, g \mapsto g + rG$ is a group isomorphism. It is clear that it is a group homomorphism. Suppose $g_1 + rG = g_2 + rG$ for $g_1, g_2 \in G[r]$. Then it follows that $g_1 - g_2 \in rG$, i. e. $g_1 - g_2 = rg$ for some $g \in G$. Since $g_1, g_2 \in G[r]$, we have $0 = rg_1 - rg_2 = r^2 g$. As there is no element of order r^2 by assumption, we have $rg = 0$ and thus $g_1 = g_2$. Therefore, the above map is injective. Consider the group homomorphism $G \to rG, g \mapsto rg$. The kernel of this map is $G[r]$ and it follows $G/G[r] \cong rG$. Hence $|G| = |G[r]| \cdot |rG|$. This proves the lemma. □

Corollary 1.85. *If there are no points of order r^2 in $J_C(\mathbb{F}_{q^k})$, we have*

$$J_C(\mathbb{F}_{q^k})[r] \cong J_C(\mathbb{F}_{q^k})/[r]J_C(\mathbb{F}_{q^k}),$$

i. e. we can choose the r-torsion points as representatives of the classes on the right hand side.

Remark 1.86. Since $r \mid \#J_C(\mathbb{F}_q)$, there are r-torsion points in $\#J_C(\mathbb{F}_q)$, and we may restrict the first argument to be taken from this set. Thus we can also define the Tate pairing as a map

$$T_r : J_C(\mathbb{F}_q)[r] \times J_C(\mathbb{F}_{q^k})/[r]J_C(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r.$$

From now on, we assume that $J_C(\mathbb{F}_{q^k})$ does not contain any point of order r^2. In this case, by Corollary 1.85, the Tate pairing can be given as a map

$$T_r : J_C(\mathbb{F}_q)[r] \times J_C(\mathbb{F}_{q^k})[r] \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r.$$

Nevertheless, we keep in mind that we can take any other representative in $J_C(\mathbb{F}_{q^k})$ of a class for the second argument.
Values of the Tate pairing are classes in $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$. By applying the multiplicative version of Lemma 1.84, we see that $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \cong \mu_r$, the subgroup of rth roots of unity in $\mathbb{F}_{q^k}^*$. The isomorphism is made explicit by computing

$$\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \to \mu_r,\ a(\mathbb{F}_{q^k}^*)^r \mapsto a^{(q^k-1)/r}.$$

This map is called the *final exponentiation*.

Taking into account all the modifications made in the previous remark, we can define a version of the Tate pairing suitable for practical implementations (compare with the description in [DF05b, Section 16.1.1]).

Definition 1.87. The *reduced Tate pairing* is the map

$$\begin{aligned} e_r : J_C(\mathbb{F}_q)[r] \times J_C(\mathbb{F}_{q^k})[r] &\to \mu_r \subseteq \mathbb{F}_{q^k}^*, \\ (P, Q) &\mapsto T_r(P, Q)^{(q^k-1)/r} = f_{r,P}(D_Q)^{(q^k-1)/r}, \end{aligned}$$

induced by the Tate pairing.

1.2.2 The Weil pairing

Early applications in cryptography used the Weil pairing on supersingular elliptic curves (see [MOV93] or [BF03]). Here, we define the Weil pairing for arbitrary hyperelliptic curves. Let the assumptions be as in the previous subsection. In particular, let k be the embedding degree of C with respect to r.

Definition 1.88. The *Weil pairing* is defined as

$$\begin{aligned} W_r : J_C[r] \times J_C[r] &\to \mu_r \subseteq \mathbb{F}_{q^k}^*, \\ (P, Q) &\mapsto \frac{f_{r,P}(D_Q)}{f_{r,Q}(D_P)}. \end{aligned}$$

The functions and divisors are defined as in the definition of the Tate-Lichtenbaum pairing in Definition 1.82.

Note that there is no need for a final exponentiation. The pairing value itself is an rth root of unity.

Remark 1.89. Rubin and Silverberg [RS08, Theorem 3.1] show that the q-eigenspace $U = J_C[r] \cap \ker(\phi_q - [q])$ of the Frobenius endomorphism ϕ_q on $J_C[r]$ is contained in $J_C(\mathbb{F}_{q^k})$, and that the Weil pairing induces a non-degenerate pairing $J_C(\mathbb{F}_q)[r] \times U \to \mu_r$. For practical applications, one may therefore restrict the Weil pairing to these groups.

Remark 1.90. Both the Weil and the reduced Tate pairing map into the group μ_r of rth roots of unity. As already mentioned, in some cases, if q is not a prime, it might happen that this group lies in an extension of $\mathbb{F}_p$ that is a proper subfield of $\mathbb{F}_{q^k}$ but not an extension of $\mathbb{F}_q$. Then the discrete logarithm problem in μ_r is easier to solve than that in $\mathbb{F}_{q^k}$. For details, we refer to Hitt's paper [Hit07].

We have introduced the Tate pairing and the Weil pairing. We proceed with a more detailed description of pairing computation on elliptic curves. But before doing so, we shall note that pairings can only be computed efficiently if the embedding degree of the underlying curve is small enough, since computations in the field $\mathbb{F}_{q^k}^*$ must be performed. Such curves are rare and need to be constructed. We return to this problem in Section 1.3.

1.2.3 Pairing computation on elliptic curves

In [Mil86a], Miller gives an algorithm to compute the Weil pairing on elliptic curves. A more detailed description of this algorithm, which is known as *Miller's algorithm*, is presented in [Mil04]. It explains an efficient way to compute the functions $f_{r,P}(D_Q)$ used in the Weil and Tate pairings.
Let E be an elliptic curve over the finite field $\mathbb{F}_q$ of characteristic $p > 3$ given by a short Weierstraß equation $E : y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}_q$. Let $r \neq p$ be a prime such that $r \mid n = \#E(\mathbb{F}_q)$, and let $k > 1$ be the embedding degree of E with respect to r.

Theorem 1.91. *Let $D = \sum_{P\in E} n_P(P) \in \mathrm{Div}(E)$. Then D is a principal divisor if and only if $\deg(D) = 0$ and $\sum_{P\in E}[n_P]P = 0$, where the latter sum describes addition on E.*

Proof. This is Corollary III.3.5 in [Sil86] or Theorem 1 in [Mil04]. □

We use Proposition 1.39 to replace divisor classes by points, and find the reduced Tate pairing to be the map

$$\begin{aligned} e_r = E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})[r] &\to \mu_r \subseteq \mathbb{F}_{q^k}^*, \\ (P, Q) &\mapsto f_{r,P}(D_Q)^{(q^k-1)/r}. \end{aligned}$$

When computing $f_{r,P}(Q)$, i. e. when rD_P is supposed to be the divisor of the function $f_{r,P}$, we can choose $D_P = (P) - (\mathcal{O})$, see Proposition 1.39. The divisor $D_Q \sim (Q) - (\mathcal{O})$ needs to have a support disjoint from $\{\mathcal{O}, P\}$. To achieve that, one may choose a suitable point $S \in E(\mathbb{F}_{q^k})$ and represent D_Q as $(Q + S) - (S)$.
The Weil pairing is the map

$$\begin{aligned} W_r = E[r] \times E[r] &\to \mu_r \subseteq \mathbb{F}_{q^k}^*. \\ (P, Q) &\mapsto f_{r,P}(D_Q)/f_{r,Q}(D_P). \end{aligned}$$

For the computation of $f_{r,Q}(P)$, we can take $D_Q = (Q) - (\mathcal{O})$ and need to choose a suitable point R such that $D_P = (P + R) - (R)$ has support disjoint from $\{\mathcal{O}, Q\}$. In the following, we describe how to compute the functions $f_{r,P}$ and $f_{r,Q}$. Since both computations are totally analogous, we choose notation for $f_{r,P}$, but allow $P \in E(\mathbb{F}_{q^k})$. We need to compute the function $f_{r,P}$ having divisor $\mathrm{div}(f_{r,P}) = r(P) - r(\mathcal{O})$. Theorem 1.91 shows that for $m \in \mathbb{Z}$ the divisor $m(P) - ([m]P) - (m - 1)(\mathcal{O})$ is principal, such that there exists a function $f_{m,P} \in \overline{\mathbb{F}_q}(E)$ with $\mathrm{div}(f_{m,P}) = m(P) - ([m]P) - (m - 1)(\mathcal{O})$. Since P is an r-torsion point, we see that $\mathrm{div}(f_{r,P}) = r(P) - r(\mathcal{O})$, and $f_{r,P}$ is actually a function we are looking for, which justifies our notation.

Definition 1.92. Given $m \in \mathbb{Z}$ and $P \in E(\mathbb{F}_{q^k})[r]$, a function $f_{m,P} \in \overline{\mathbb{F}_{q^k}}(E)$ with divisor $\mathrm{div}(f_{m,P}) = m(P) - ([m]P) - (m - 1)(\mathcal{O})$ is called a *Miller function*.

The computation of $f_{r,P}$ makes use of the lines arising when two points on the curve are added. The following three lemmas discuss divisors of functions related to these lines, give their defining polynomials, and fix notation for later use.

Lemma 1.93. *Let $P_1, P_2 \in E$. Let l_{P_1,P_2} be the homogeneous polynomial defining the line through P_1 and P_2, being the tangent to the curve in P_1 if $P_1 = P_2$. The function $L_{P_1,P_2} = l_{P_1,P_2}(X, Y, Z)/Z$ has the divisor*

$$\mathrm{div}(L_{P_1,P_2}) = (P_1) + (P_2) + (-(P_1 + P_2)) - 3(\mathcal{O}).$$

Proof. See [Mil04, Proposition 2]. □

Next we give affine polynomials for the lines occurring in the previous lemma. Compare these to the formulas of the addition law described in Lemma 1.40.

Lemma 1.94. *Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2), Q = (x_Q, y_Q) \in E$. For $P_1 \neq -P_2$ define*

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P_1 \neq P_2, \\ (3x_1^2 + a)/(2y_1) & \text{if } P_1 = P_2. \end{cases}$$

Then the dehomogenization $(l_{P_1,P_2})_*$ of l_{P_1,P_2} evaluated at Q is given by

$$(l_{P_1,P_2})_*(Q) = \lambda(x_Q - x_1) + (y_1 - y_Q).$$

If $P_1 = -P_2$, then $(l_{P_1,P_2})_*(Q) = x_Q - x_1$.

Proof. This follows from the formulas for the elliptic-curve group law (Lemma 1.40) and their geometric interpretation (Remark 1.41). □

Lemma 1.95. *Let $P_1, P_2 \in E$. The function $g_{P_1,P_2} := L_{P_1,P_2}/L_{P_1+P_2,-(P_1+P_2)}$ has the divisor*

$$\operatorname{div}(g_{P_1,P_2}) = (P_1) + (P_2) - (P_1 + P_2) - (\mathcal{O}).$$

Proof. The result follows easily from Lemma 1.93. □

The function from the previous lemma can be used to compute Miller functions recursively as shown in the next lemma.

Lemma 1.96 (Miller's formula)**.** *The Miller functions $f_{m,P}$ can be chosen such that $f_{1,P} = 1$ and such that for $m_1, m_2 \in \mathbb{Z}$, it holds*

$$f_{m_1+m_2,P} = f_{m_1,P} f_{m_2,P} g_{[m_1]P,[m_2]P}, \tag{1.11}$$

$$f_{m_1 m_2,P} = f_{m_1,P}^{m_2} f_{m_2,[m_1]P} = f_{m_2,P}^{m_1} f_{m_1,[m_2]P}. \tag{1.12}$$

Proof. See Lemma 2 in [Mil04] and Lemma IX.17 in [Gal05]. □

Remark 1.97. We state some special cases of the formulas from the previous lemma. Let $m \in \mathbb{Z}$, then

(a) $f_{m+1,P} = f_{m,P} g_{[m]P,P}$,

(b) $f_{2m,P} = f_{m,P}^2 g_{[m]P,[m]P}$,

(c) $f_{-m,P} = (f_{m,P} g_{[m]P,-[m]P})^{-1}$.

Note that $f_{0,P} = 1$ for all $P \in E$ and $g_{P_1,P_2} = 1$ if P_1 or P_2 equals the point at infinity $\mathcal{O}$. These formulas show that any function $f_{m,P}$ can be computed recursively as a product of line functions. The functions are defined over the field of definition of P.

Miller's algorithm uses these formulas along a scalar multiplication to compute $[r]P$. Its general form works for the Weil pairing, as well as the Tate pairing. We state the algorithm in the case of the Tate pairing to be able to include several simplifications, some of which benefit from the final exponentiation. For example, the evaluation of $f_{r,P}$ at the divisor D_Q can be replaced by the evaluation at the point Q.

Lemma 1.98. *Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$, $Q \notin E(\mathbb{F}_q)$, then the reduced Tate pairing can be computed as $e_r(P,Q) = f_{r,P}(Q)^{(q^k-1)/r}$.*

Proof. This is [BLS04a, Theorem 1]. □

Algorithm 1.1 can be used to compute $f_{r,P}(Q)$ for $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$ up to irrelevant factors lying in a proper subfield of $\mathbb{F}_{q^k}$. Since $k > 1$, these factors are mapped to 1 by the final exponentiation.

Input: $P \in E(\mathbb{F}_q)[r]$, $Q \in E(\mathbb{F}_{q^k})[r]$, $r = (r_l, \ldots, r_0)_2$.
Output: $f_{r,P}(Q)$ as representative of the class $f_{r,P}(Q)(\mathbb{F}_{q^k}^*)^r$.
1: $R \leftarrow P$, $f \leftarrow 1$
2: **for** $(i \leftarrow l-1;\ i \geq 0;\ i--)$ **do**
3: $\quad f \leftarrow f^2 \cdot g_{R,R}(Q)$
4: $\quad R \leftarrow [2]R$
5: $\quad$ **if** $(r_i = 1)$ **then**
6: $\quad\quad f \leftarrow f \cdot g_{R,P}(Q)$
7: $\quad\quad R \leftarrow R + P$
8: $\quad$ **end if**
9: **end for**
10: **return** f

Algorithm 1.1: Miller's algorithm for elliptic curves

Remark 1.99. Note that the functions $g_{R,R}$ and $g_{R,P}$ in steps 3 and 6 of Algorithm 1.1 are fractions and that the inversions in each step of the loop can be postponed until the end of the loop by keeping track of numerator and denominator separately.
To complete the pairing computation, the final exponentiation has to be applied to the result of Miller's algorithm. For this, one uses fast exponentiation methods in the finite field $\mathbb{F}_{q^k}$ (see [Doc05a] and [Doc05b]). It can be accelerated by using actions of the q-power map on $\mathbb{F}_{q^k}^*$ [GS08]. For recent improvement on the final exponentiation, see [SBC+08].

In practice, the Tate pairing is computed as

$$e_r : G_1 \times G_2 \to G_3 = \mu_r \subseteq \mathbb{F}_{q^k}^*,$$

with

$$\begin{aligned} G_1 &= E[r] \cap \ker(\phi_q - [1]) = E(\mathbb{F}_q)[r], \\ G_2 &= E[r] \cap \ker(\phi_q - [q]) \subseteq E(\mathbb{F}_{q^k})[r]. \end{aligned}$$

For the second pairing argument, one must assure that it has a non-trivial component in the second eigenspace of the Frobenius, since choosing both points from the first results in a trivial pairing value.
If the embedding degree is even, there are further improvements of Miller's algorithm by exploiting twists of E to represent the points in G_2.

Proposition 1.100. *Let $\delta = 2$ if $j(E) \notin \{0, 1728\}$, $\delta = 4$ if $j(E) = 1728$, and $\delta = 6$ if $j(E) = 0$. If $\delta \mid k$, there exists a unique twist E' of E of degree δ with $r \mid \#E'(\mathbb{F}_{q^{k/\delta}})$.*

Proof. This is a consequence of the discussion in Section IV.C of [HSV06]. See in particular the last paragraph of that section. □

Lemma 1.101. *Let E' be the twist from Proposition 1.100, and let $\sigma_\xi : E' \to E$ be the corresponding isomorphism given by $\xi \in \mathbb{F}_{q^{k/\delta}}$ as in Remark 1.51. The restriction of σ_ξ to $E'(\mathbb{F}_{q^{k/\delta}})[r]$ is a group isomorphism*

$$\sigma_\xi : E'(\mathbb{F}_{q^{k/\delta}})[r] \to G_2$$

of cyclic groups of order r. If $Q \in G_2$, then its x-coordinate lies in a proper subfield of $\mathbb{F}_{q^k}$.

Proof. Since σ_ξ is a group homomorphism $E' \to E$, it maps points of order r to points of order dividing r. Since it is nontrivial on $E'(\mathbb{F}_{q^{k/\delta}})[r]$ and r is prime, the image of $E'(\mathbb{F}_{q^{k/\delta}})[r]$ is a cyclic group of order r contained in $E(\mathbb{F}_{q^k})[r]$. It is shown in [HSV06, Section V] that $\sigma_\xi(E'(\mathbb{F}_{q^{k/\delta}})[r])$ is stable under ϕ_q and therefore must be G_2 since it is not contained in G_1, and these are the only eigenspaces of ϕ_q. Therefore, σ_ξ is a group isomorphism $E'(\mathbb{F}_{q^{k/\delta}})[r] \to G_2$. The statement about the x-coordinates follows from the form of σ_ξ given in Remark 1.51. Note that $\delta \neq 3$. □

The previous lemma shows that we can define a pairing $G_1 \times E'(\mathbb{F}_{q^{k/\delta}})[r] \to G_3$ by simply mapping points from $E'(\mathbb{F}_{q^{k/\delta}})[r]$ to G_2 via σ_ξ and then computing the Tate pairing.

Definition 1.102. Define $G_2' := E'(\mathbb{F}_{q^{k/\delta}})[r]$. The pairing

$$e_r' : G_1 \times G_2' \to G_3, \ (P, Q') \mapsto e_r(P, \sigma_\xi(Q'))$$

is called the *twisted Tate pairing*.

If k is even, there is always the possibility to use a quadratic twist, i. e. a twist of degree 2. In this case, the x-coordinates of all points in G_2 and G_2' lie in a proper subfield of $\mathbb{F}_{q^k}$. The denominators of the functions $g_{R,R}$ or $g_{R,P}$ in Miller's algorithm are polynomials defining vertical lines, and thus are of the form $x - x_{[2]R}$ or $x - x_{R+P}$. Since the points R and P are defined over $\mathbb{F}_q$, the values $g_{R,R}(Q)$ and $g_{R,P}(Q)$ lie in a proper subfield of $\mathbb{F}_{q^k}$. Therefore, the final exponentiation maps them to 1.

Proposition 1.103. *Let k be even. Then the denominators of the functions $g_{R,R}$ and $g_{R,P}$ in Steps 3 and 6 of Miller's algorithm can be discarded without changing the value of the reduced Tate pairing.*

Proof. See Theorem 3 in [BLS04a]. □

We conclude this section by giving a brief overview of other variants of the Tate pairing which can be computed with a shorter loop in Miller's algorithm.

Remark 1.104 (ate pairing)**.** Heß, Smart, and Vercauteren introduce the *ate pairing* in [HSV06]. The map

$$\begin{aligned} a_{t-1} : G_2 \times G_1 &\to G_3, \\ (Q, P) &\mapsto f_{t-1,Q}(P)^{(q^k-1)/r} \end{aligned}$$

defines a non-degenerate bilinear pairing [HSV06, Theorem 1], called the *ate pairing*. Note that for the ate pairing the first argument is defined over $\mathbb{F}_{q^k}$ and thus curve arithmetic is more costly than for the Tate pairing. But the loop length in Miller's algorithm, which is given by the bit length of $t - 1$, may be much shorter.

Remark 1.105 (Twisted ate pairing or Eta pairing)**.** The *Eta pairing* has first been introduced by Barreto, Galbraith, Ó hÉigeartaigh, and Scott in [BGOS07] on Jacobians of supersingular curves in small characteristic. Heß, Smart, and Vercauteren generalize the idea to ordinary curves in large characteristic and call the resulting pairing the *twisted ate pairing* [HSV06]. Let $d \mid k$ such that the curve E has a twist of degree d. Define $e := k/d$. As for the ate pairing, we set $\lambda_e := (t-1)^e \mod r$. The map

$$\begin{aligned} \eta_{\lambda_e} : G_1 \times G_2 &\to G_3, \\ (P, Q) &\mapsto f_{\lambda_e,P}(Q)^{(q^k-1)/r} \end{aligned}$$

defines a bilinear, non-degenerate pairing [HSV06, Lemma 11] called the *twisted ate pairing*. It has the advantage of a shorter loop while curve arithmetic can be done over $\mathbb{F}_q$. But the loop length is in general larger than for the ate pairing.

There are so-called optimized and generalized versions of the ate and twisted ate pairing that can be computed with even shorter loop length. The parameters $t - 1$ and $(t-1)^e$ can be replaced by any of their powers modulo r. Naturally one chooses the power with the smallest bit length [ZZH08]. They can also be replaced with

other integers $S \equiv q \pmod{r}$ to obtain a shorter loop length [MKHO07]. Another approach is given in [LLP08].
Vercauteren introduces optimal pairings discussing a lower bound on the length of the loop in Miller's algorithm and giving pairing functions which are optimal in that sense [Ver08]. All the previous pairing functions are subsumed under the framework of pairing lattices that Heß proposes in [Heß08].

1.3 Constructing pairing-friendly curves

Let $\mathbb{F}_q$ be a finite field of characteristic p. Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$, and let J_C be its Jacobian variety. We denote by n the order of $J_C(\mathbb{F}_q)$. We recall Definition 1.80 of the embedding degree: For a prime divisor r of n, $r \neq p$, the *embedding degree of C with respect to r* is defined as the minimal integer k with $r \mid (q^k - 1)$.

Definition 1.106. Let $C/\mathbb{F}_q$ be a hyperelliptic curve of genus g and r the largest prime divisor of $n = \#J_C(\mathbb{F}_q)$. The parameter

$$\rho := g \log(q) / \log(r) \geq 1$$

is called the *ρ-value of C*.

A pairing-based cryptosystem is only secure if the prime r is large enough such that the discrete logarithm problems (DLP) in the subgroups of $J_C(\mathbb{F}_{q^k})$ of order r are infeasible, and such that the DLP in the multiplicative group $\mathbb{F}_{q^k}^*$ is infeasible. For a fixed size of r, the size of q^k depends on the embedding degree k and the ρ-value. The goal is to choose a curve with ρ as small as possible and an embedding degree that is small, but large enough to guarantee the DLP in $\mathbb{F}_{q^k}$ to be infeasible.
The embedding degree k has several interpretations, as was already indicated in Remark 1.81. The following lemma adds another very simple, but important observation.

Lemma 1.107. *Assume that $k \in \mathbb{N}$ with $r \nmid k$. The embedding degree of $C/\mathbb{F}_q$ with respect to the prime r is k if and only if $r \mid \Phi_k(q)$, where Φ_k is the kth cyclotomic polynomial.*

Proof. The number k is the embedding degree with respect to r if and only if q has order k in $\mathbb{F}_r$, i. e. q is a primitive kth root of unity in $\mathbb{F}_r$ (see Remark 1.81). This is equivalent to q being a root of Φ_k over $\mathbb{F}_r$ [LN97, Definition 2.44]. □

In light of Theorem 1.77, we reformulate the conditions for a curve to have embedding degree k in the following lemma.

Lemma 1.108. *Let $C/\mathbb{F}_q$ be a hyperelliptic curve, and let J_C be its Jacobian. Let r be a prime number and $k \in \mathbb{N}$ with $r \nmid k$. Then k is the embedding degree of C with respect to r if and only if the following conditions hold:*

$$\chi_q(1) \equiv 0 \pmod{r}, \tag{1.13}$$
$$\Phi_k(q) \equiv 0 \pmod{r}, \tag{1.14}$$

where χ_q is the characteristic polynomial of the Frobenius endomorphism as in Theorem 1.77, and Φ_k is the kth cyclotomic polynomial.

Proof. This is an easy consequence of Lemma 1.107 and the definition of the embedding degree. □

One approach to finding q and r that satisfy equation (1.14) is to parametrize them as polynomials $q(l)$ and $r(l)$ over $\mathbb{Z}$ such that the condition is fulfilled in $\mathbb{Z}[l]$. The following lemma by Galbraith, McKee, and Valença provides a way of finding suitable polynomials.

Lemma 1.109. *Let $q(l) \in \mathbb{Q}[l]$ be a quadratic polynomial and ζ_k a primitive kth root of unity in $\mathbb{C}$. Then*

$$\Phi_k(q(l)) = n_1(l)n_2(l)$$

for irreducible polynomials $n_1(l), n_2(l) \in \mathbb{Q}[l]$ of degree $\varphi(k)$ if and only if the equation

$$q(z) = \zeta_k$$

has a solution in $\mathbb{Q}(\zeta_k)$. Otherwise, $\Phi_k(q(l))$ is irreducible of degree $\varphi(k)$.

Proof. This is [GMV07, Lemma 5.1]. □

It is unlikely for a randomly chosen curve to have a small embedding degree and a good ρ-value (see the discussion in [DF05a, Section 6.4.2]). For elliptic curves, this is shown by Balasubramanian and Koblitz [BK98]. The probability that an elliptic curve over a prime field $\mathbb{F}_p$ with a prime number of $\mathbb{F}_p$-rational points has an embedding degree less than $(\log_2 p)^2$ is very small [BK98, Theorem 2]. Luca, Mireles, and Shparlinski extend this result and make similar conclusions in more general cases [LMS04]. This means that pairing-friendly curves are rare and need to be constructed.
A successful approach is to fix a number k and to first find the following parameters: a prime power q and a potential group order n having a large prime divisor r such that the conditions (1.13) and (1.14) are satisfied. Then one uses the complex multiplication (CM) method to construct a hyperelliptic curve over $\mathbb{F}_q$ with n rational points on its Jacobian. The following subsection briefly explains the CM method for elliptic curves.

1.3.1 The CM method for elliptic curves

The CM method for elliptic curves has been introduced by Atkin and Morain [AM93] for elliptic curve primality proving. We recall Definition 1.48: An elliptic curve E has complex multiplication (CM) if its endomorphism ring $\mathrm{End}(E)$ is isomorphic to an order in a quadratic imaginary field K. Note that an elliptic curve E over $\mathbb{C}$ has either $\mathrm{End}(E) \cong \mathbb{Z}$ or $\mathrm{End}(E) \cong \mathcal{R}$ for an order $\mathcal{R}$ in a quadratic imaginary number field. Thus a curve over $\mathbb{C}$ has complex multiplication if its endomorphism ring $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$.
To describe the CM method, we need to introduce lattices. A *lattice in* $\mathbb{C}$ is a discrete additive subgroup $\Lambda \subseteq \mathbb{C}$ that contains an $\mathbb{R}$-basis of $\mathbb{C}$. We start with an elliptic curve $E/\mathbb{C}$. From Corollary VI.5.1.1 in [Sil86], we know that there exists a lattice Λ for which there is a group isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. Without loss of generality we may assume that there exists a $\tau \in \mathbb{C}$ with positive imaginary part (i. e. it lies in the upper half plane) and $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ [FL05c, Corollary 5.36]. This means that to every elliptic curve over $\mathbb{C}$, we can associate a number $\tau \in \mathbb{C}$ with $\mathrm{Im}(\tau) > 0$ and a lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. Two elliptic curves E and E' over $\mathbb{C}$ with corresponding lattices Λ and Λ' are isogenous if and only if there exists an $\alpha \in \mathbb{C}^*$ with $\alpha\Lambda \subseteq \Lambda'$. They are isogenous and isomorphic if and only if there exists an $\alpha \in \mathbb{C}^*$ with $\alpha\Lambda = \Lambda'$ [Sil86, Theorem VI.4.1 and Corollary VI.4.1.1]. This gives a new interpretation of the endomorphism ring of E as

$$\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}.$$

If E has complex multiplication, then $\mathrm{End}(E)$ is in fact isomorphic to an order $\mathcal{R}$ in $\mathbb{Q}(\tau)$ [FL05c, Theorem 5.47]. Vice versa, one may start with an imaginary quadratic field K, an order $\mathcal{R}$ in K, and an ideal Λ of $\mathcal{R}$. The ideal Λ is a lattice in $\mathbb{C}$ and there exists an elliptic curve $E/\mathbb{C}$ with $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ and $\mathrm{End}(E) \cong \mathcal{R}$ [FL05c, Proposition 5.46].
We fix the order $\mathcal{R}$ to be the maximal order, i. e. the ring of integers $\mathcal{O}_K$ in K. Every ideal in $\mathcal{O}_K$ is a lattice and thus leads to an elliptic curve. It follows from [Sil86, Corollary VI.4.1.1] that ideals lying in the same ideal class lead to isomorphic elliptic curves. Furthermore, it can be shown that there is a bijection between the ideal class group and the set of isomorphism classes of elliptic curves over $\mathbb{C}$ with endomorphism ring $\mathcal{O}_K$ [Sil86, Proposition C.11.1]. Thus the class number h_K of K is equal to the number of isomorphism classes of such curves. For the definition of the class group and class number, see [IR90, §12.2] or [Lor96, Chapter V].

Theorem 1.110. *Let $E/\mathbb{C}$ be an elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}_K$, the ring of integers in an imaginary quadratic field K. The j-invariant $j(E)$ is an algebraic integer over $\mathbb{Q}$. There are only finitely many isomorphism classes of elliptic curves with endomorphism ring isomorphic to $\mathcal{O}_K$. The corresponding j-invariants are exactly the roots of the minimal polynomial of $j(E)$ over $\mathbb{Q}$.*

Proof. These results are given in [FL05c, Theorem 5.47 and Corollary 5.48] and [Sil86, Corollary C.11.1.1]. □

Definition 1.111. The minimal polynomial of $j(E)$ from Theorem 1.110 is called the *Hilbert class polynomial of* K, denoted by H_K.

Note that $H_K(x) \in \mathbb{Z}[x]$ since $j(E)$ is an algebraic integer and that its degree is equal to the class number h_K. For methods to compute the class number and the Hilbert class polynomial for a given quadratic field, see [Coh93, Section 5.3 and Section 7.6] or [FL05b, Section 18.1.3]. The computation of the Hilbert class polynomial can only be done efficiently if the discriminant of K is small enough. For the current state of the art of class polynomial computation see Sutherland's homepage[1].

Example 1.112. The class number of $K = \mathbb{Q}(\sqrt{-3})$ is $h_K = 1$, and its Hilbert class polynomial is $H_K(x) = x$. Thus all elliptic curves over $\mathbb{C}$ with endomorphism ring isomorphic to $\mathcal{O}_K$ are isomorphic and have j-invariant 0. One example is the curve $E : y^2 = x^3 + 1$. Compare this with Example 1.37.

The CM method constructs an ordinary elliptic curve $\bar{E}/\mathbb{F}_p$ for a prime p by reducing a curve $E/\mathbb{C}$ modulo a prime ideal lying over $p\mathcal{O}_K$. Deuring's lifting Theorem states that any ordinary elliptic curve over $\mathbb{F}_p$ can be obtained by reduction of a curve over a number field [Lan87, Theorem 14 in Chapter 13]. To obtain an ordinary curve, the prime p needs to split in the field K.

Theorem 1.113. *Let $E/\mathbb{C}$ be an elliptic curve with CM by $\mathcal{O}_K$ for an imaginary quadratic field K. Let $p \nmid \Delta(E)$ be a prime which splits completely in O_K, i. e. there exist prime ideals $\mathfrak{p}_1 \neq \mathfrak{p}_2$ with $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$. Then the reduction $\bar{E}$ of E modulo $\mathfrak{p}_1$ is an ordinary curve defined over $\mathbb{F}_p$, and* $\mathrm{End}(E) \cong \mathrm{End}(\bar{E})$.

Proof. See Theorem 12 in Chapter 13 of [Lan87]. □

Since the endomorphism ring is not changed by the reduction, we are able to choose an endomorphism ring for $\bar{E}$ that has an element π of norm p and trace $t = \pi + \bar{\pi}$ such that $p+1-t$ is the desired number of $\mathbb{F}_p$-rational points on $\bar{E}$, see Theorem 1.52. This means that the element π corresponds to the Frobenius endomorphism on the curve $\bar{E}$. The j-invariant of such a curve can be found by reducing the Hilbert class polynomial modulo p as is shown in the following theorem.

Theorem 1.114. *Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field, i. e. $D < 0$, and let H_K be its Hilbert class polynomial. Let p be a prime. The prime p is a norm in K, i. e. there exists $\pi = u + v\sqrt{D} \in \mathcal{O}_K$ with $p = \pi\bar{\pi} = u^2 - Dv^2$, if and only if the reduction of H_K modulo p has only simple roots all of which lie in $\mathbb{F}_p$.*

Proof. This is part of [AM93, Theorem 3.2]. □

Since the j-invariant of an elliptic curve only determines the curve up to isomorphism, the curve with the desired group order may be a twist of the curve we have constructed. The twist with the correct group order can be found easily.

[1] `http://www-math.mit.edu/~drew/`

Summarizing, we get the following method: Suppose, we have a quadratic imaginary number field $K = \mathbb{Q}(\sqrt{D})$ with Hilbert class polynomial H_K and a prime p that satisfies $p = \pi\bar{\pi}$ in $\mathcal{O}_K$ and $n = p + 1 - t$, $t = \pi + \bar{\pi}$. Let $H_{K,p}$ be the reduction of H_K modulo p. Then $H_{K,p}$ has only simple roots in $\mathbb{F}_p$. Let j_0 be one of its roots. We can construct an elliptic curve $\bar{E}$ over $\mathbb{F}_p$ with j-invariant j_0 by Proposition 1.38, and one of the twists of $\bar{E}$ has n points. The equation $p = \pi\bar{\pi}$ is often called the *CM norm equation*. The element π can be written as $\frac{1}{2}(t + v\sqrt{D})$ and the norm equation becomes

$$p = \frac{1}{4}(t^2 - Dv^2) \text{ or } t^2 - 4p = Dv^2. \tag{1.15}$$

Hilbert class polynomials over $\mathbb{C}$ can be precomputed. Their computation is not considered part of the CM algorithm [FL05b, Remark 18.1].

1.3.2 Elliptic curves with small embedding degree

Supersingular elliptic curves have embedding degree at most 6 [MOV93]. Therefore they are natural candidates for the use in pairing-based cryptographic protocols. But since higher security demands need higher embedding degrees, ordinary elliptic curves are the more flexible choice.
Let $E/\mathbb{F}_q$ be an elliptic curve and r a prime dividing $\#E(\mathbb{F}_q)$. The conditions from Lemma 1.108 translate into the following:

$$q + 1 - t \equiv 0 \pmod{r}, \tag{1.16}$$
$$\Phi_k(q) \equiv 0 \pmod{r}, \tag{1.17}$$

where t is the trace of the Frobenius endomorphism, in particular $|t| \leq 2\sqrt{q}$.

Example 1.115 (MNT curves)**.** Miyaji, Nakabayashi, and Takano [MNT01] introduce the first parametrized families that yield ordinary elliptic curves with embedding degree $k \in \{3, 4, 6\}$. The curves have ρ-value 1. The families are given by parametrizations for p and t as polynomials in $\mathbb{Z}[l]$ with $n(l) = p(l) + 1 - t(l)$ and

$$n(l) \mid \Phi_k(p(l)).$$

To find an MNT curve, one chooses polynomials as in the table below for the embedding degree of choice.

k	$p(l)$	$t(l)$
3	$12l^2 - 1$	$-1 \pm 6l$
4	$l^2 + l + 1$	$-l$ or $l + 1$
6	$4l^2 + 1$	$1 \pm 2l$

Curves can be constructed using the CM method by first solving the corresponding norm equation for a given CM discriminant (see Section 1.3.1). Any solution which

leads to n and p prime gives a curve $E/\mathbb{F}_p$ with $n = \#E(\mathbb{F}_p)$ and the chosen embedding degree. The idea to parametrize the prime p and the group order n leads to other families, e. g. the family of curves described in Chapter 2, which were found by exploiting the following simple observation.

Remark 1.116. Equation (1.16) implies that $q \equiv t - 1 \pmod{r}$, and thus for any polynomial $f \in \mathbb{Z}[x]$ it holds that $f(q) \equiv f(t-1) \pmod{r}$. In particular, Equation (1.17) can be replaced by $\Phi_k(t-1) \equiv 0 \pmod{r}$.

Example 1.117 (Freeman curves)**.** The family found by Freeman [Fre06] consists of curves with embedding degree $k = 10$ over a prime field and ρ-value 1. It is given via the parametrization

$$\begin{aligned} n(l) &= 25l^4 + 25l^3 + 15l^2 + 5l + 1, \\ p(l) &= 25l^4 + 25l^3 + 25l^2 + 10l + 3, \end{aligned}$$

which has been found by using the embedding degree condition of the form in Remark 1.116 and one of the quadratic families in [GMV07]. To get a curve in that family for a group order n and a prime p given by the above polynomials, one needs to carry out the CM construction just as for MNT curves.

The families in the previous two examples and the family we turn to in Chapter 2 yield the only known construction methods for elliptic curves of prime order (ρ-value equal to 1) and small embedding degree. There are construction methods for all other embedding degrees, but the resulting curves have composite group order, i. e. a ρ-value larger than 1.
A survey on pairing-friendly elliptic curves is given by Freeman, Scott, and Teske [FST06]. The paper reflects the current state-of-the-art. For every embedding degree up to $k = 50$, they list the best known construction with respect to the ρ-value. They also provide suggestions for curves with certain properties, for example having large degree twists, which leads to more efficient implementations at the cost of less flexibility in choosing curves.

Chapter 2

BN curves

In this chapter, we study pairing-friendly elliptic curves defined over a prime field $\mathbb{F}_p$ such that the group of $\mathbb{F}_p$-rational points on the curve has prime order n, and the curve has embedding degree $k = 12$ with respect to n. The results in this chapter are based on joint work with Barreto [BN06]. Others started calling curves belonging to that family *BN curves*; we follow this notation here.
In Section 2.1, we show how the family is given by a polynomial parametrization for the primes p and n. We deduce the parametrization and show how curves are obtained from it. Also, heuristic evidence is given that a curve E with a prescribed size of the primes p and n can be found quickly. Furthermore, we discuss the choice of a generator for $E(\mathbb{F}_p)$. Section 2.2 addresses properties of the proposed family of curves. We describe the automorphisms on a BN curve, prove the existence of a twist of degree 6, and propose a representation of extensions of $\mathbb{F}_p$ corresponding to the chosen twist. Furthermore, we discuss efficient endomorphisms as well as possibilities to compress points on the curve and its twist. In Section 2.3, we discuss pairing computation on BN curves, give the line functions involved in Miller's algorithm for different pairings, and show how to compress pairing values in a way that is consistent with the point compression described in Section 2.2. Section 2.4 is devoted to gathering the ingredients for generating all the required parameters needed to implement pairings on BN curves. Finally, we provide examples of BN curves for different security levels in Section 2.5.

2.1 Construction

The main observation that leads to the construction of BN curves is Lemma 2.1, which is the special case $k = 12$ of Lemma 6.1 in the paper of Galbraith, McKee, and Valença [GMV07] (see also Lemma 1.109).

Lemma 2.1. *Let Φ_{12} be the 12th cyclotomic polynomial. Then*

$$\Phi_{12}(6l^2) = n(l)n(-l), \tag{2.1}$$

where $n(l) = 36l^4 + 36l^3 + 18l^2 + 6l + 1$.

Proof. See Lemma 6.1 in [GMV07] and the examples for $k = 12$. □

Galbraith, McKee, and Valença give a criterion to determine which quadratic polynomials $q(l)$ lead to the splitting of $\Phi_k(q(l))$. Their intention was to construct pairing-friendly genus-2 curves. For such curves the quadratic polynomial q must be able to take the value of a prime power when evaluated at an integer. This can not be satisfied for the polynomial $q(l) = 6l^2$.
We apply their results to elliptic curves and use the simple observation from Remark 1.116 that $n = p + 1 - t$ implies $p \equiv t - 1 \pmod{n}$ when E is an elliptic curve defined over $\mathbb{F}_p$, $n = \#E(\mathbb{F}_p)$ is the number of $\mathbb{F}_p$-rational points on E, and t is the trace of the Frobenius endomorphism over $\mathbb{F}_p$. It follows that $\Phi_k(p) \equiv \Phi_k(t-1) \pmod{n}$ for any $k \in \mathbb{N}$. This leads to the parameters of a family of elliptic curves as described in the following theorem.

Theorem 2.2. *Let $u \in \mathbb{Z}$ be an integer such that*

$$p = p(u) = 36u^4 + 36u^3 + 24u^2 + 6u + 1, \tag{2.2}$$
$$n = n(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1 \tag{2.3}$$

are prime numbers. Then there exists an ordinary elliptic curve E defined over $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = n$. The embedding degree of E with respect to n is $k = 12$, and the curve can be given by the equation

$$E : y^2 = x^3 + b, \ b \in \mathbb{F}_p. \tag{2.4}$$

The trace of the Frobenius endomorphism over $\mathbb{F}_p$ is given by $t = t(u) = 6u^2 + 1$.

Proof. From the parametrizations for p and n, we obtain $t - 1 = p - n = 6u^2$. From Lemma 2.1 we see that n divides $\Phi_{12}(t-1)$ and thus also $\Phi_{12}(p)$, which means that p and n satisfy the embedding degree condition (1.17) for $k = 12$. Therefore, a potential curve over $\mathbb{F}_p$ with n rational points has embedding degree 12.
The number t satisfies $|t| \leq 2\sqrt{p}$ because

$$t^2 - 4p = -3(6u^2 + 4u + 1)^2 \tag{2.5}$$

is negative. Since t is not divisible by p, a theorem by Waterhouse [Wat69, Theorem 4.1] (see Lemma 1.56) shows that there exists an ordinary elliptic curve E defined over $\mathbb{F}_p$ such that the trace of the Frobenius endomorphism is equal to t, i. e. $n = \#E(\mathbb{F}_p)$.
We may construct a curve E with the above properties that has complex multiplication by the ring of integers $\mathcal{O}_K$ of the quadratic CM field $K = \mathbb{Q}(\sqrt{t^2 - 4p}) = \mathbb{Q}(\sqrt{-3})$ (see Section 1.3.1). Example 1.112 shows that K has class number 1 and its Hilbert class polynomial is $H_K(x) = x$. The j-invariant of this curve is thus $j = 0$. The relations between the j-invariant and the coefficients a, b show that $a = 0$ (see Proposition 1.38). This proves the theorem. □

A curve $E : y^2 = x^3 + b$ over a field of characteristic larger than 3 is nonsingular if and only if $b \neq 0$ (Example 1.37). For a fixed prime $p > 3$, all curves $E : y^2 = x^3 + b$ for $b \in \mathbb{F}_p^*$ are twists of each other. We know from Proposition 1.50 that in the case $j = 0$ there are six different twists. In order to construct a curve as in Theorem 2.2, we only need to run through different values for b, i. e. run through different twists, and check for the right group order. Assuming that we choose b at random from $\mathbb{F}_p^*$, we expect to do six checks on average to find the twist with the correct number of points.

Corollary 2.3. *Under the assumptions of Theorem 2.2, a curve with the correct group order can be found after on average six tries of random choices for the parameter $b \in \mathbb{F}_p^*$.*

Thus once we have the primes p and n as in Theorem 2.2, it is fairly easy to actually find a curve with the given property. What remains to be examined, is the question how easy it is to find suitable pairs of primes (p, n).

Definition 2.4. A pair (p, n) of prime numbers is called a *BN prime pair* if there exists an integer $u \in \mathbb{Z}$ with $p = p(u)$ and $n = n(u)$, where $p(u)$ and $n(u)$ are given by the polynomials in (2.2) and (2.3).

2.1.1 Distribution of BN prime pairs

A conjecture by Bateman and Horn [BH62] allows us to estimate the number of BN prime pairs which are produced when letting the parameter u run through a given range. We adapt the conjecture to our purposes as follows:

Conjecture 2.5. For large $N \in \mathbb{N}$, we heuristically expect the number of positive integers u with $1 \leq u \leq N$ for which (2.2) and (2.3) provide a BN prime pair $(p, n) = (p(u), n(u))$ to be

$$Q(N) = \frac{C}{16} \int_2^N \frac{1}{(\log u)^2} du. \tag{2.6}$$

The constant C is given as

$$C = \prod_q \left[\left(1 - \frac{1}{q}\right)^{-2} \left(1 - \frac{w(q)}{q}\right) \right], \tag{2.7}$$

where the product is taken over all primes q, and where $w(q)$ denotes the number of solutions of $p(x)n(x) \equiv 0 \pmod{q}$.

Assuming that Conjecture 2.5 is true, we are now able to estimate the probability $\mathfrak{p}_I$ to find a BN prime pair when the parameter u is taken uniformly at random from a certain interval $I = [u_1, u_2] \subset \mathbb{N}$. Define $Q(I) = Q(u_2) - Q(u_1 - 1)$, then $\mathfrak{p}_I = Q(I)/(u_2 - u_1 + 1)$.

u_1	$u_2 - u_1 + 1$	$R(I)$	$\lfloor Q(I) \rfloor$	$r_I \cdot 10^2$	bits
1	72621324	250565	277429	0.34503	≤ 109
448869734239	4008033	5794	6142	0.14456	160
114911668072285	9977856	9952	10501	0.09974	192
29417389567148395	13774482	10011	10567	0.07268	224
7530851732698370160	17949966	10097	10481	0.05625	256
1927898043575355590045	22521445	9961	10343	0.04423	288
4935418991552967689868804	27819263	10127	10311	0.03640	320
1263467261837559799486438 11	34034872	10109	10394	0.02970	352
323447619030415308755258630 96	40428318	10048	10349	0.02485	384
828025904717863190414492371 9775	47727580	9975	10388	0.02090	416
211974631607772976746111263540 0325	55123647	9927	10327	0.01801	448
542655056915898820470044848710404692	63634474	9933	10368	0.01561	480
138919694570470098040331481257823718878	71157457	10048	10176	0.01412	512

Table 2.1: The number $R(I)$ of all BN prime pairs $(p(u), n(u))$ where $u \in I = [u_1, u_2]$, the estimate $Q(I)$ for $R(I)$ from Conjecture 2.5, and the ratio $r_I = R(I)/(u_2 - u_1 + 1)$. The last column gives the bit size of the primes p and n.

We have computed all BN prime pairs arising when u lies in the intervals shown in Table 2.1. We denote the number of actually existing pairs in I by $R(I)$. To compare this number with the conjectured number of pairs, we approximated the constant C from Conjecture 2.5 by computing the product over the first primes up to 81824487889, and obtained $C \approx 17.65105$. The integral has been computed numerically. The values for $Q(I)$ given in the table are rounded down. Instead of $\mathfrak{p}_I$ we give the ratio $r_I = R(I)/(u_2 - u_1 + 1)$ of the actual number of prime pairs to the number of all possible values for u, i. e. the length of I.
From the heuristic results of Table 2.1, we may conclude that it is not too difficult to find a BN prime pair of a certain bit size. One just chooses a set of numbers from which values for the parameter u are taken randomly, until both $p(u)$ and $n(u)$ are prime. The set can be chosen to guarantee that p and n have a desired bit size. Also a sequential search quickly finds BN prime pairs. This approach is taken in Algorithm 2.1 below.

2.1.2 Choosing a generator point

Along with the curve, we need a generator of the group of $\mathbb{F}_p$-rational points to carry out cryptographic protocols. Since the group has prime order, we may take any $\mathbb{F}_p$-rational point $P \neq \mathcal{O}$ on the curve. To favor efficient implementation, one might be interested in the coefficients of this generator point to be as simple as possible, e. g. one of them being equal to 1. The choice of the generator should be included into the curve construction algorithm. During construction, it is anyway required to choose a point on the curve for checking the curve order. The following remark discusses the choice of a point coordinate on a curve of the form $E : y^2 = x^3 + b$ without taking into account the choice of the correct twist.

Remark 2.6. Let $p \in \mathbb{N}$ be a prime.
(a) Let $x_0 \in \mathbb{F}_p$. Then $b \in \mathbb{F}_p^*$ can be chosen such that $x_0^3 + b$ is a square in $\mathbb{F}_p$. In this case, let $y_0 \in \mathbb{F}_p$ be a square root of $x_0^3 + b$. Then $P = (x_0, y_0)$ is an affine point on the curve $E : y^2 = x^3 + b$; in particular, it is not equal to $\mathcal{O}$. As half of the elements in $\mathbb{F}_p^*$ are squares, there is a chance of $1/2$ to obtain a square $x_0^3 + b$ when randomly choosing b from $\mathbb{F}_p^*$.
(b) Let $y_0 \in \mathbb{F}_p$. We may similarly choose $b \in \mathbb{F}_p^*$, such that $y_0^2 - b$ is a cube in $\mathbb{F}_p$. Let x_0 be one of its cube roots. Then as above, $P = (x_0, y_0)$ is a point on $E : y^2 = x^3 + b$. The chance of finding a cube $y_0^2 - b$ is at least $1/3$ because at least one third of the elements of $\mathbb{F}_p$ are cubes, depending on whether $p \equiv 1 \pmod 3$ or not.

When choosing the generator point in advance, it must be noted that neither of the coordinates can be equal to 0, as the following lemma shows.

Lemma 2.7. *Let $E : y^2 = x^3 + b$ be a BN curve defined over $\mathbb{F}_p$. Then b is neither a square nor a cube in $\mathbb{F}_p$. In particular, it is not a 6th power. If $P = (x_0, y_0) \in E(\mathbb{F}_p)$, then $x_0 \neq 0$ and $y_0 \neq 0$.*

Proof. Assume that b is a cube. Then there exists a cube root $x_b \in \mathbb{F}_p$ of b and the point $P = (-x_b, 0)$ is a point of order 2 in $E(\mathbb{F}_p)$, which is a contradiction since $n = \#E(\mathbb{F}_p)$ is an odd prime. Next assume that b is a square. Then there exists a square root $y_b \in \mathbb{F}_p$ of b and the point $\tilde{P} = (0, y_b)$ is in $E(\mathbb{F}_p)$. We compute $[2]\tilde{P}$ using the formulas in Lemma 1.40 to see that $[2]\tilde{P} = -\tilde{P}$, i. e. $\tilde{P}$ is a point of order 3, again a contradiction since $3 \nmid n$. Now if $P = (x_0, y_0) \in E(\mathbb{F}_p)$, the above proof also shows that $x_0 \neq 0$ and $y_0 \neq 0$. □

Computer experiments show that heuristically the condition $x_0 y_0 \neq 0$ is the only restriction when choosing the coordinates for a generator point. We have the following conjecture about the expected number of choices for the curve parameter $b \in \mathbb{F}_p^*$ that is needed until a suitable curve with a given generator is found.

Conjecture 2.8. Let (p, n) be a BN prime pair, and let $x_0 \in \mathbb{F}_p^*$ ($y_0 \in \mathbb{F}_p^*$, respectively). Then on average we expect 12 (18, respectively) random choices for $b \in \mathbb{F}_p^*$ until the curve $E : y^2 = x^3 + b$ has order n and a generator with x-coordinate x_0 (y-coordinate y_0, respectively).

Algorithm 2.1 is an algorithm for constructing BN curves. It gives a curve which has a generator with x-coordinate equal to 1. For an implementation of pairings on BN curves, more parameters are required such as a representation for the finite field extension $\mathbb{F}_{p^{12}}$ and points on the curve $E(\mathbb{F}_{p^{12}})$ for the second pairing argument. These issues and the construction of parameters to exploit the properties and techniques explained in Sections 2.2 and 2.3 are addressed in Section 2.4.

Input: The approximate bit length m of the curve order.
Output: Parameters p, n, b, y_0 such that the curve $y^2 = x^3 + b$ has order n over $\mathbb{F}_p$, the point $P = (1, y_0)$ is a generator of the curve, and n has at least m bits.

Let $\tilde{p} = 36l^4 + 36l^3 + 24l^2 + 6l + 1$, $\tilde{n} = \tilde{p} - 6l^2 \in \mathbb{Z}[l]$.
Compute the smallest $u \approx 2^{m/4}$ such that $\lceil \log_2 \tilde{n}(-u) \rceil = m$.
loop
    Compute $t \leftarrow 6u^2 + 1$,
    compute $p \leftarrow \tilde{p}(-u)$ and $n \leftarrow p + 1 - t$.
    if p and n are prime **then**
        exit loop
    end if
    Compute $p \leftarrow \tilde{p}(u)$, and $n \leftarrow p + 1 - t$.
    if p and n are prime **then**
        exit loop
    end if
    Increase $u \leftarrow u + 1$.
end loop
repeat
    repeat
        Choose $b \in \mathbb{F}_p^*$ at random
    until $b + 1$ is a quadratic residue mod p.
    Compute y_0 such that $y_0^2 = b + 1 \bmod p$,
    and set $P \leftarrow (1, y_0)$.
until $nP = \mathcal{O}$.
return p, n, b, y_0.

Algorithm 2.1: Constructing a BN curve

2.2 Properties

In this section, let $(p, n) \in \mathbb{Z}^2$ be a BN prime pair, and let $E/\mathbb{F}_p$ be a BN curve, i. e. $E : y^2 = x^3 + b$, $b \in \mathbb{F}_p^*$, $n = \#E(\mathbb{F}_p)$, and E has embedding degree $k = 12$ with respect to n. Recall that the j-invariant of E is $j(E) = 0$. We briefly recapitulate all parameters obtained so far as polynomials in u (see Theorem 2.2). The definition of v is given implicitly in (2.5) by $t^2 - 4p = -3v^2$:

$$\begin{aligned} p &= 36u^4 + 36u^3 + 24u^2 + 6u + 1, \\ n &= 36u^4 + 36u^3 + 18u^2 + 6u + 1, \\ t &= 6u^2 + 1, \\ v &= 6u^2 + 4u + 1. \end{aligned}$$

Next we collect properties of the curve E in view of efficient pairing computation, before we describe pairing computation on E in the next section. First we consider endomorphisms on a BN curve. The endomorphism ring $\mathrm{End}(E)$ of a BN curve is

by construction isomorphic to the maximal order $\mathcal{O}_K$ in the quadratic CM field $K = \mathbb{Q}(\sqrt{-3})$. It is $\mathcal{O}_K = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ [IR90, Proposition 13.1.1]. We have $\mathrm{End}^0(E) := \mathbb{Q} \otimes \mathrm{End}(E) = \mathbb{Q}(\sqrt{-3})$. Let

$$\phi_p : E \to E,\ (x, y) \mapsto (x^p, y^p)$$

be the p-power Frobenius endomorphism. Its characteristic polynomial is $\chi_p = T^2 - tT + p \in \mathbb{Z}[T]$. Thus ϕ_p can be identified with the element $\pi = \frac{1}{2}(t + \sqrt{-3}v)$ of norm p in $\mathcal{O}_K$. We have $K = \mathbb{Q}(\pi)$ and $\mathbb{Z}[\pi] \subset \mathcal{O}_K$.
The group $\mathrm{Aut}(E)$ of automorphisms of E is the subset of $\mathrm{End}(E)$ containing the invertible endomorphisms, i. e. the units of $\mathrm{End}(E)$. The group $\mathrm{Aut}(E)$ will be discussed in the following section.

2.2.1 Automorphisms

In this short subsection, we describe all automorphisms of a BN curve in terms of the parameter u. In a slightly more general setting, we first summarize what is known about automorphisms of curves with j-invariant 0.

Lemma 2.9. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p, and let $j(E) = 0$. We fix $\zeta_6 \in \overline{\mathbb{F}_q}$, a primitive 6th root of unity, and set $\zeta_3 = \zeta_6^2$. Then the automorphism group $\mathrm{Aut}(E)$ is a cyclic group of order 6. It is generated by*

$$\sigma_6 : E \to E,\ (x, y) \mapsto (\zeta_6^2 x, \zeta_6^3 y) = (\zeta_3 x, -y).$$

If $q \equiv 1 \pmod 6$, then all automorphisms are defined over $\mathbb{F}_q$, i. e. $\mathrm{Aut}_{\mathbb{F}_q}(E) = \mathrm{Aut}(E)$.

Proof. The lemma follows from Theorem III.10.1, Corollary III.10.2 in [Sil86], and the fact that $\zeta_6 \in \mathbb{F}_q$ if $q \equiv 1 \pmod 6$. □

Now let E be a BN curve as at the beginning of this section. Since a primitive 6th root of unity in $\mathbb{F}_p$ can be computed in terms of a polynomial in u similar to the primes p and n, the automorphisms are defined over $\mathbb{F}_p$, and can be described in terms of u as well.

Lemma 2.10. *Let $u \in \mathbb{Z}$ be such that $p = p(u)$ given by (2.2) is prime. Then the primitive 6th roots of unity in $\mathbb{F}_p$ are given by*

$$\zeta_6 = 18u^3 + 18u^2 + 9u + 2 \mod p, \tag{2.8}$$
$$\zeta_6^5 = -18u^3 - 18u^2 - 9u - 1 \mod p. \tag{2.9}$$

Proof. We set $\zeta(l) = 18l^3 + 18l^2 + 9l + 2$. Evaluating the 6th cyclotomic polynomial $\Phi_6(x) = x^2 - x + 1$ at $\zeta(l)$, we see that it splits in $\mathbb{Z}[l]$ as

$$\Phi_6(\zeta(l)) = 3(3l^2 + 3l + 1)(36l^4 + 36l^3 + 24l + 6l + 1).$$

Therefore, $\tilde{p}(l) = 36l^4 + 36l^3 + 24l^2 + 6l + 1$ is a divisor. It follows that $\zeta(l)$ is a 6th root of unity in $\mathbb{Z}[l]/(\tilde{p}(l))$. Evaluating at u, we see that $\Phi_6(\zeta_6) \equiv 0 \pmod{p}$, and thus ζ_6 is a primitive 6th root of unity in $\mathbb{F}_p$. The second primitive root can be computed from $\zeta(l)^5 = -\zeta(l) + 1 \mod \tilde{p}(l)$. □

Remark 2.11. Note that the two preceding lemmas describe the automorphism group for any curve E defined over a field $\mathbb{F}_q$ of characteristic p where p is a prime of the form (2.2) and the j-invariant of E is $j(E) = 0$. They hold especially for the sextic twist of the BN curve $E : y^2 = x^3 + b$. We study such twists in the next subsection.

2.2.2 Twists and point representation

The property we address in this subsection is the existence of a twist of degree 6, which helps to represent the second pairing argument more efficiently. This point is usually taken from the p-eigenspace of the Frobenius endomorphism on the n-torsion subgroup. It is a point defined over the field $\mathbb{F}_{p^{12}}$ (see Subsection 1.2.3).

Lemma 2.12. *Let $E/\mathbb{F}_p$ be a BN curve. The curve E has a twist $E'/\mathbb{F}_{p^2}$ of degree $d = 6$ with the following properties: The order $\#E'(\mathbb{F}_{p^2})$ is divisible by n; the twist can be represented by the equation*

$$E' : y^2 = x^3 + b/\xi, \tag{2.10}$$

where $\xi \in \mathbb{F}_{p^2} \setminus \left((\mathbb{F}_{p^2})^2 \cup (\mathbb{F}_{p^2})^3\right)$; the corresponding isomorphism $\psi \in \mathrm{Hom}(E', E)$ is given by

$$\psi : E' \to E,\ (x', y') \mapsto (\xi^{1/3}x', \xi^{1/2}y'). \tag{2.11}$$

Furthermore, a point $Q' \in E'(\mathbb{F}_{p^2})$ of order n is mapped via ψ into the p-eigenspace of the Frobenius endomorphism ϕ_p, i. e. $\phi_p(\psi(Q')) = [p]\psi(Q')$.

Proof. The lemma follows from Proposition 1.100 and Lemma 1.101. For the curve equation and the isomorphism, see also Proposition 1.50 and Remark 1.51. The fact, that ξ is neither a square nor a cube follows from the minimality of the degree $d = 6$. □

Remark 2.13. We compute the group order of the twist E' explicitly: First determine $n_2 = \#E(\mathbb{F}_{p^2})$. We know that $p = \pi\overline{\pi}$ with $\pi = \frac{1}{2}(t + v\sqrt{-3}) \in \mathbb{Q}(\sqrt{-3})$, where $v = 6u^2 + 4u + 1$ (see (2.5)). The group order n_2 is

$$n_2 = p^2 + 1 - (\pi^2 + \overline{\pi}^2),$$

which is equal to $(p + 1 + t) \cdot n$. We set $t_2 = \pi^2 + \overline{\pi}^2 = \frac{1}{2}(t^2 - 3v^2)$, compute $t_2^2 - 4p^2 = -3t^2v^2$, and let $v_2 = tv$. Application of Proposition 1.57 yields that one of the two possible group orders for the twist is

$$p^2 + 1 - \frac{1}{2}(3v_2 + t_2) = (p - 1 + t) \cdot n.$$

Theorem 9 in [HSV06] implies that only one of the two twists over $\mathbb{F}_{p^2}$ of degree 6 can have order divisible by n (see also Proposition 1.57). Hence the order of $E'(\mathbb{F}_{p^2})$ is $(p-1+t)n$.

We fix the following notation for the rest of this chapter. As in Subsection 1.2.3 we define

$$G_1 := \ker(\phi_p - [1]) = E(\mathbb{F}_p),\ G_2 := E[n] \cap \ker(\phi_p - [p]) \subseteq E(\mathbb{F}_{p^{12}})[n]. \tag{2.12}$$

Pairings on BN curves are usually defined on $G_1 \times G_2$ or $G_2 \times G_1$ (see Section 1.2.3). Lemma 2.12 shows that we can represent the group G_2 by the $\mathbb{F}_{p^2}$-rational points of order n on the twist E'. Elliptic curve operations that need to be done in G_2 may as well be done on the twist. Only for pairing computation we apply the map ψ to move into G_2 (see Definition 1.102 for the concept of a twisted pairing). Points on the twist can be represented with only one sixth of the space which is required for an arbitrary point on $E(\mathbb{F}_{p^{12}})$ (see also [HSV06, Section V.]).
We define G_2' to be the group of $\mathbb{F}_{p^2}$-rational n-torsion points on the twist E',

$$G_2' := E'(\mathbb{F}_{p^2})[n]. \tag{2.13}$$

A twisted pairing on a BN curve is then defined on $G_1 \times G_2'$ or $G_2' \times G_1$. The restriction $\psi|_{G_2'}$ of the isomorphism ψ to G_2', which we also call ψ, is a group isomorphism

$$\psi : G_2' \to G_2.$$

The three groups G_1, G_2, and G_2' are all cyclic groups of prime order n. Note that G_2' is cyclic because the whole n-torsion is only defined over $\mathbb{F}_{p^{12}}$ and not over $\mathbb{F}_{p^2}$ (see Theorem 1.59).

2.2.3 Field extensions

Since the twist E' from the previous section is defined over $\mathbb{F}_{p^2}$, it appears natural to construct the finite field $\mathbb{F}_{p^{12}}$ as an extension of $\mathbb{F}_{p^2}$.

Lemma 2.14. *Let q be a prime power, $q \equiv 1 \pmod 6$, and $\xi \in \mathbb{F}_q \setminus \left((\mathbb{F}_q)^2 \cup (\mathbb{F}_q)^3\right)$. Then the polynomials $x^2 - \xi$, $x^3 - \xi$, and $x^6 - \xi \in \mathbb{F}_q[x]$ are irreducible over $\mathbb{F}_q$.*

Proof. The polynomial $x^2 - \xi$ is irreducible since otherwise, a square root of ξ would exist. Similarly, $x^3 - \xi$ is irreducible. For the same reasons, $x^6 - \xi$ can not have a linear factor. From $q \equiv 1 \pmod 6$, we know that $\mathbb{F}_q$ contains all 6th roots of unity. Let $\zeta_6 \in \mathbb{F}_q$ be a primitive 6th root of unity. Let ω be a root of $x^6 - \xi$ lying in some extension of $\mathbb{F}_q$. The elements $\zeta_6^i\omega$, $0 \le i \le 5$, are exactly the roots of $x^6 - \xi$, and we may write $x^6 - \xi = \prod_{i=0}^{5}(x - \zeta_6^i\omega)$. Assume $x^6 - \xi$ has a quadratic factor over $\mathbb{F}_q$. Then its constant term is the product of two of the above roots, say $\zeta_6^i\omega$ and $\zeta_6^j\omega$. Since $\zeta_6 \in \mathbb{F}_q$, it follows from $\zeta_6^{i+j}\omega^2 \in \mathbb{F}_q$ that $\omega^2 \in \mathbb{F}_q$. This is a contradiction, since $(\omega^2)^3 = \xi$ implies that ξ is a cube in $\mathbb{F}_q$. A similar argument shows that $x^6 - \xi$ does not have a factor of degree 3. Altogether, this shows that the polynomial is irreducible. □

Let E be a BN curve, and let E' be its sextic twist by $\xi \in \mathbb{F}_{p^2}$ as in Lemma 2.12. Let $\omega \in \mathbb{F}_{p^{12}}$ be a root of the irreducible polynomial $x^6 - \xi$, i. e. $\omega^6 = \xi$. This means that we can construct $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(\omega^3)$, $\mathbb{F}_{p^6} = \mathbb{F}_{p^2}(\omega^2)$, and $\mathbb{F}_{p^{12}} = \mathbb{F}_{p^2}(\omega)$. The curve isomorphism ψ may now be written as

$$\psi : \ E' \to E, \ (x', y') \mapsto (\omega^2 x', \omega^3 y').$$

Remark 2.15. We see, that the x-coordinates of points in the image of ψ (i. e. in G_2) all lie in $\mathbb{F}_{p^6}$, and their y-coordinates all lie in $\mathbb{F}_{p^4}$.

The p^2-power Frobenius automorphism of the field $\mathbb{F}_{p^{12}}$ applied to ω gives $\omega^{p^2} = -\zeta_3\omega$ for a primitive 3rd root of unity ζ_3, and hence we have $(\omega^3)^{p^2} = -\omega^3$ and $(\omega^2)^{p^2} = \zeta_3^2\omega^2$. These identities will be useful later.
Furthermore, we fix notation for constructing the field $\mathbb{F}_{p^2}$. Let $\mu \in \mathbb{F}_p \setminus (\mathbb{F}_p)^2$, then $x^2 - \mu$ is irreducible over $\mathbb{F}_p$. Let $\nu \in \mathbb{F}_{p^2}$ be a root of $x^2 - \mu$, i. e. $\nu^2 = \mu$, $\nu^p = -\nu$. Then we may write $\mathbb{F}_{p^2} = \mathbb{F}_p(\nu)$.

2.2.4 Efficient endomorphisms

Gallant, Lambert, and Vanstone show in [GLV01] how endomorphisms on an elliptic curve can be exploited to speed up elliptic-curve scalar multiplication. An *efficient endomorphism* is an endomorphism of the curve which can be computed with very little effort, e. g. with just one field multiplication, and thus provides very fast computation of certain scalar multiples of elliptic-curve points. An endomorphism φ that is non-trivial on a cyclic prime-order subgroup of $E(\mathbb{F}_p)$ is a group automorphism on this subgroup. Thus for a point $P \in E(\mathbb{F}_p)$, there exists a suitable $s \in \mathbb{Z}$ with $\varphi(P) = [s]P$.
Recently, Galbraith and Scott applied the method of Gallant, Lambert, and Vanstone for exponentiation in groups arising in pairing-based cryptography [GS08], e. g. for BN curves. In particular, this method may be applied to the group $G_1 = E(\mathbb{F}_p)$ and the group G_2' on the twist $E'(\mathbb{F}_{p^2})$. For details, we refer to [GS08]. In this subsection, we will state efficient endomorphisms on BN curves and show which multiples can be computed easily. As usual, we give the relevant parameters as polynomials in u.
A prominent example of an efficient endomorphism is of course the p-power Frobenius endomorphism ϕ_p. It is trivial on G_1, but on its second eigenspace G_2, the eigenvalue is p. For every point $Q \in G_2$, it holds that $\phi_p(Q) = [p]Q$. Let $\rho_{12} := t - 1$, and note that ρ_{12} is a primitive 12th root of unity modulo n because it is a root of $\Phi_{12}(x)$. Since $\rho_{12} = t - 1 \equiv p \pmod{n}$, this means that the Frobenius provides a quick way of computing $[\rho_{12}^i]Q$ for all $i \in \{0, 1, \ldots, 11\}$. The following lemma gives parametrizations for all 12th roots of unity modulo n.

Lemma 2.16. *Let n be a prime given by (2.3), and let $\rho_{12} = 6u^2$. Then the 12th roots of unity in $\mathbb{F}_n$ are given by the powers of ρ_{12}. They can be described in terms*

of the parameter u as follows:

$$\begin{aligned}
\rho_{12} &= 6u^2, \\
\rho_{12}^2 &= -36u^3 - 18u^2 - 6u - 1 \mod n, \\
\rho_{12}^3 &= -36u^3 - 24u^2 - 12u - 3 \mod n, \\
\rho_{12}^4 &= -36u^3 - 18u^2 - 6u - 2 \mod n, \\
\rho_{12}^5 &= -36u^3 - 30u^2 - 12u - 3 \mod n, \\
\rho_{12}^6 &= -1 \mod n, \\
\rho_{12}^7 &= -6u^2 \mod n, \\
\rho_{12}^8 &= 36u^3 + 18u^2 + 6u + 1 \mod n, \\
\rho_{12}^9 &= 36u^3 + 24u^2 + 12u + 3 \mod n, \\
\rho_{12}^{10} &= 36u^3 + 18u^2 + 6u + 2 \mod n, \\
\rho_{12}^{11} &= 36u^3 + 30u^2 + 12u + 3 \mod n.
\end{aligned}$$

Proof. The powers can be computed as polynomials in u modulo the polynomial $n(u)$. □

Lemma 2.17. *Let E be a BN curve, $Q = (x_Q, y_Q) \in G_2$, and let $\phi_p \in \mathrm{End}(E)$ be the p-power Frobenius endomorphism. Then for all $i \geq 0$ we have*

$$\phi_p^i(Q) = (x_Q^{p^i}, y_Q^{p^i}) = [\rho_{12}^i]Q. \tag{2.14}$$

Proof. See Lemma 1.60 for the eigenspaces of ϕ_p. □

Another source for efficient endomorphisms is the automorphism group $\mathrm{Aut}(E)$. We have seen in Subsection 2.2.1 that for BN curves the automorphisms are defined over $\mathbb{F}_p$, thus they commute with the Frobenius ϕ_p. The restriction of each automorphism to $E(\mathbb{F}_p)$ therefore gives a group automorphism of $E(\mathbb{F}_p)$.

Lemma 2.18. *Let E be a BN curve, and $\sigma_6 \in \mathrm{Aut}(E)$ be the automorphism of order 6 from Lemma 2.9. Then the restriction $\sigma_6|_{G_1}$ is a group automorphism of $G_1 = E(\mathbb{F}_p)$, and it holds*

$$\begin{aligned}
\sigma_6|_{G_1} : \ G_1 &\to G_1, \\
P = (x_P, y_P) &\mapsto (\zeta_3 x_P, -y_P) = [\rho_6]P,
\end{aligned}$$

where ζ_3 is the 3rd root of unity in $\mathbb{F}_p$ from Lemma 2.9, and $\rho_6 \in \mathbb{Z}$ is a primitive 6th root of unity modulo n, i. e. $\rho_6 = -36u^3 - 18u^2 - 6u - 1 \mod n$ or $\rho_6 = 36u^3 + 18u^2 + 6u + 2 \mod n$.

Proof. Since σ_6 is defined over $\mathbb{F}_p$, it maps into $E(\mathbb{F}_p)$. The latter group is cyclic of prime order n, and σ_6 is nontrivial, which means that $\sigma_6|_{G_1}$ is a group automorphism and the image of a point P must be a multiple $[\rho]P$ of P. Now σ_6 has order 6. It follows

$$P = \sigma_6^6(P) = [\rho^6]P$$

for all $P \in E(\mathbb{F}_p)$, and so $\rho^6 \equiv 1 \pmod{n}$, i. e. ρ is a 6th root of unity modulo n. Since σ_6 has order 6, so has ρ. Lemma 2.16 gives the parametrizations for the two primitive 6th roots of unity in $\mathbb{F}_n$. □

Remark 2.19. The automorphisms commute with the multiplication-by-n map $[n]$; thus the restriction $\sigma_6|_{G_2}$ is a group automorphism of G_2. Therefore, the previous lemma holds for the group G_2 as well. The automorphisms act as scalar multiplications by 6th roots of unity. Combining this with Lemma 2.17 shows that the automorphisms coincide on G_2 with the even powers of the Frobenius endomorphism.

We now turn to efficiently computable endomorphisms on the twist E' of Lemma 2.12. The automorphism group can be used on the subgroup G_2' of points of order n in $E'(\mathbb{F}_{p^2})$ just as for the curve E itself (see Lemma 2.18 and Remark 2.11). In general, given an endomorphism $\varphi \in \mathrm{End}(E)$, we obtain an endomorphism $\varphi^\psi \in \mathrm{End}(E')$ on the twist by applying the map

$$\mathrm{End}(E) \to \mathrm{End}(E'),\ \varphi \mapsto \varphi^\psi := \psi^{-1}\varphi\psi, \tag{2.15}$$

depicted in the following diagram:

$$\begin{array}{ccc} E' & \xrightarrow{\varphi^\psi} & E' \\ \downarrow{\scriptstyle \psi} & & \uparrow{\scriptstyle \psi^{-1}} \\ E & \xrightarrow{\varphi} & E \end{array}$$

The isomorphism $\psi : E' \to E$ is defined in (2.11) in Lemma 2.12. Applying the above map to the group $\mathrm{Aut}(E)$ gives $\mathrm{Aut}(E')$. The image of the generator σ_6 is $\sigma_6' \in \mathrm{Aut}(E')$, where $\sigma_6'(x', y') = (\zeta_3 x', -y')$ uses the same cube root of unity ζ_3 as σ_6. We have

$$\sigma_6' = \sigma_6^\psi = \psi^{-1}\sigma_6\psi. \tag{2.16}$$

Thus the automorphisms do not provide any new efficient endomorphisms on the twist E'. Next we will take powers of the Frobenius and apply (2.15). As on G_2 (see Remark 2.19), the even powers of ϕ_p lead to automorphisms again.

Lemma 2.20. *Let E be a BN curve, and let E' and ψ be as in Lemma 2.12. Let $\phi_p \in \mathrm{End}(E)$ be the p-power Frobenius endomorphism. Denote by $\phi_{p^2} := \phi_p^2$ the square of ϕ_p. Then*

$$\{(\phi_{p^2}^i)^\psi \mid 0 \le i \le 5\} = \mathrm{Aut}(E').$$

Proof. Since $(\omega^3)^{p^2} = -\omega^3$ and $(\omega^2)^{p^2} = \zeta_3\omega^2$ for a primitive 3rd root of unity ζ_3, we obtain

$$\phi_{p^2}^\psi(x', y') = \psi^{-1}\phi_{p^2}\psi(x', y') = (\omega^{-2}(\omega^2 x')^{p^2}, \omega^{-3}(\omega^3 y')^{p^2}) = (\zeta_3 x', -y'),$$

which means that $\phi_{p^2}^\psi$ is a generator of the automorphism group $\mathrm{Aut}(E')$. The lemma follows from $(\phi_p^i)^\psi = \psi^{-1}\phi_p^i\psi = (\psi^{-1}\phi_p\psi)^i = (\phi_p^\psi)^i$. □

In contrast to its square, the p-power Frobenius itself gives a new endomorphism $\eta = \phi_p^\psi = \psi^{-1}\phi_p\psi$. It satisfies the 12th cyclotomic polynomial $\eta^4 - \eta^2 + 1 = 0$ (see also [GS08]).

Lemma 2.21. *Let E be a BN curve, and let E' and ψ be as in Lemma 2.12. Let $\phi_p \in \mathrm{End}(E)$ be the p-power Frobenius endomorphism. Let $\eta = \phi_p^\psi = \psi^{-1}\phi_p\psi \in \mathrm{End}(E')$ and let $Q' \in G_2'$ be a point of order n on the twist E'. Then for all $i \geq 0$, we have*

$$\eta^i(Q') = [\rho_{12}^i]Q'.$$

Proof. This follows directly from Lemma 2.17. □

2.2.5 Point compression

It is possible to compress points on an elliptic curve, e. g. to save bandwidth when storing or transmitting such points. The usual technique is to keep only the x-coordinate of the point and a single bit to distinguish between the at most two possible y-coordinates. See [DL05a, Section 13.2.5, p. 288] for details. If the y-coordinate needs to be determined, a square root has to be computed.
We aim at compressing n-torsion points on the sextic twist, i. e. points $Q' = (x', y') \in G_2'$. Instead of compressing to x', we discard x' and keep y' as the compressed representation of Q'. To be able to decompress, we need to keep two bits to distinguish between the at most three possible points with the given y-coordinate. Keeping only the y-coordinate means that we identify the three points (x', y'), $(\zeta_3 x', y')$, and $(\zeta_3^2 x', y')$, which all share the same y-coordinate, while their x-coordinates differ by the primitive 3rd roots of unity ζ_3 and ζ_3^2. We may describe such a set of points in terms of the automorphism group $\mathcal{G}' := \mathrm{Aut}(E')$ of E'.
The group $\mathcal{G}'$ acts on the group G_2'. We consider $\mathcal{H}' = \langle(\sigma_6')^2\rangle$, the subgroup of order 3 of the automorphism group $\mathcal{G}'$ and its action on G_2'. Lemma 2.9 shows that for a point $Q' = (x', y') \neq \mathcal{O}$, the orbit $\mathcal{H}'Q' = \mathcal{H}'(x', y')$ consists exactly of all points in G_2' that share the same y-coordinate. The orbit containing the point $\mathcal{O}$ is just the set $\{\mathcal{O}\}$. For the same reasons as for the original curve E, there are no points with a coordinate being 0 in the prime order group G_2' (see Lemma 2.7). Therefore, for a point $Q' = (x', y') \neq \mathcal{O}$, the orbit

$$\mathcal{H}'Q' = \mathcal{H}'(x', y') = \{(x', y'), (\zeta_3 x', y'), (\zeta_3^2 x', y')\}$$

has cardinality 3. We denote by $\mathrm{Orb}_{\mathcal{H}'}(G_2')$ the set of orbits of $\mathcal{H}'$ on G_2'.
The following Lemma summarizes that we can represent orbits under the action of $\mathcal{H}'$ by one element in $\mathbb{F}_{p^2}$, namely by the y-coordinate of the points contained in the orbit. We define

$$G_{2,y}' = \{y' \in \mathbb{F}_{p^2} \mid \exists\ x' \in \mathbb{F}_{p^2} \text{ such that } (x', y') \in G_2'\}$$

to be the set of possible y-coordinates of points in G_2'.

Lemma 2.22. *Let E be a BN curve, and let E' be its twist of degree 6. Then with notation as above, the map*

$$\begin{aligned} G'_{2,y} &\to \mathrm{Orb}_{\mathcal{H}'}(G'_2) \setminus \{\{\mathcal{O}\}\}, \\ y' &\mapsto \mathcal{H}'(x', y') \end{aligned}$$

is bijective.

Proof. The map is injective since different y-coordinates are mapped to different orbits. It is surjective, since each orbit different from $\{\mathcal{O}\}$ contains a point with some y-coordinate from $G'_{2,y}$. □

Of course, we may also consider the action of the whole group $\mathcal{G}'$ on G'_2. For a nonzero point, the orbit becomes

$$\mathcal{G}'(x', y') = \{(x', y'), (\zeta_3 x', -y'), (\zeta_3^2 x', y'), (x', -y'), (\zeta_3 x', y'), (\zeta_3^2 x', -y')\}.$$

Such an orbit can be represented by one bit less since we may forget about the sign of y' and just identify all points that have y-coordinate equal to y' or $-y'$. We denote by $\mathrm{Orb}_{\mathcal{G}'}(G'_2)$ the set of orbits of $\mathcal{G}'$ on G'_2. Let $y' = y'_0 + y'_1\nu \in \mathbb{F}_{p^2}$ with $y'_0, y'_1 \in \mathbb{F}_p$. Define $\tilde{y}' := y'$ if the integer in $[0, p-1]$ representing y'_0 is even, and $\tilde{y}' := -y'$ if it is odd. Then if $\tilde{y}' = \tilde{y}'_0 + \tilde{y}'_1\nu$, the least significant bit of $\tilde{y}'_0$ is always 0 and can be omitted. Let

$$G'_{2,\tilde{y}} = \{\tilde{y}' \mid \exists\ x' \in \mathbb{F}_{p^2},\ \text{such that } (x', y') \in G'_2\}$$

be the set of all elements $\tilde{y}'$ for all y-coordinates of points in G'_2. It can be easily seen, that the following lemma is true.

Lemma 2.23. *Let E be a BN curve and E' its twist of degree 6. Then the map*

$$\begin{aligned} G'_{2,\tilde{y}} &\to \mathrm{Orb}_{\mathcal{G}'}(G'_2) \setminus \{\{\mathcal{O}\}\}, \\ \tilde{y}' &\mapsto \mathcal{G}'(x', y') \end{aligned}$$

is well-defined and bijective.

The orbit structure is carried over to G_2 when mapped via ψ, which is stated explicitly in the following remark.

Remark 2.24. It follows from (2.16) that $\psi\sigma'_6 = \sigma_6\psi$. If we denote by $\mathcal{G} := \mathrm{Aut}(E)$ the automorphism group of E and by $\mathcal{H} := \langle\sigma_6^2\rangle$ its subgroup of order 3, we get the following identities. For $Q' \in G'_2$,

$$\psi(\mathcal{G}'Q') = \mathcal{G}\psi(Q') \text{ and } \psi(\mathcal{H}'Q') = \mathcal{H}\psi(Q'),$$

i. e. an orbit of points in G'_2 is mapped to the corresponding orbit of points in G_2, and thus $\psi(\mathrm{Orb}_{\mathcal{G}'}(G'_2)) = \mathrm{Orb}_{\mathcal{G}}(G_2)$, $\psi(\mathrm{Orb}_{\mathcal{H}'}(G'_2)) = \mathrm{Orb}_{\mathcal{H}}(G_2)$.

Remark 2.25. From Remark 2.19 we see that the orbits in G_2 under $\mathcal{G}$ and $\mathcal{H}$ consist of even p-power multiples of one point. The orbits of a point $Q \in G_2$ are

$$\mathcal{G}Q = \{Q, [p^2]Q, [p^4]Q, [p^6]Q, [p^8]Q, [p^{10}]Q\}$$

and

$$\mathcal{H}Q = \{Q, [p^4]Q, [p^8]Q\},$$

respectively.

We have seen that we can compress points by identifying points in the orbits of the automorphism group. We only need to keep part of the y-coordinate of one of the points and a few additional bits to distinguish between at most six possible points in the orbit. We will see in the next section how this can be used together with the compression of pairing values.
If a point needs to be reconstructed, i. e. decompressed, the x-coordinate corresponding to a point in G_1, G_2, or G_2' with a given y-coordinate is needed. We may obtain it by simply computing a cube root of $y^2 - b$ or $y'^2 - b/\xi$. We now briefly discuss how to efficiently compute cube roots in fields occurring for BN curves.
Each prime number of form (2.2), i. e. $p(u) = 36u^4+36u^3+24u^2+6u+1$, is congruent to $6u^2 + 6u + 1 \pmod 9$ and hence $p(u) \equiv 1 \pmod 9$ if $u \equiv 0 \pmod 3$ or $u \equiv 2 \pmod 3$, and $p(u) \equiv 4 \pmod 9$ if $u \equiv 1 \pmod 3$.

Lemma 2.26. *Let q be a prime power such that $q \equiv 4 \pmod 9$, i. e. $2q + 1 \equiv 0 \pmod 9$. Let $a \in \mathbb{F}_q^*$ be a cube. Then a cube root $r \in \mathbb{F}_q^*$ of a is given by $r = a^{(2q+1)/9}$.*

Proof. Since a is a cube, $a^{(q-1)/3} = 1$. It is $r^3 = a^{(2q+1)/3} = aa^{(2q-2)/3} = a$. □

Computing cube roots modulo $p \equiv 4 \pmod 9$ only takes one exponentiation. For recovering the x-coordinate of points in $E'(\mathbb{F}_{p^2})$ given only their y-coordinate, one needs to compute a cube root in $\mathbb{F}_{p^2}^*$, and for $p \equiv 4 \pmod 9$ we have $p^2 \equiv 7 \pmod 9$.

Lemma 2.27. *Let q be a prime power such that $q \equiv 7 \pmod 9$. Let $a \in \mathbb{F}_q^*$ be a cube. Then a cube root $r \in \mathbb{F}_q^*$ is given by $r = a^{(q+2)/9}$.*

Proof. Since a is a cube, $a^{(q-1)/3} = 1$. It is $r^3 = a^{(q+2)/3} = aa^{(q-1)/3} = a$. □

Again, the computation of a cube root only takes one exponentiation. When applying both lemmas, one must check that the result is correct, i. e. that $r^3 = a$, if it is not known, whether u is a cube.

2.3 Pairing computation

In this section, we discuss different pairings on BN curves and elaborate on how they can be computed. First of all, we recall the notation fixed in the previous sections.

Throughout the section let (p, n) be a BN prime pair, and let $E : y^2 = x^3 + b$ be a BN curve over $\mathbb{F}_p$. Let $E' : y^2 = x^3 + b/\xi$ be the twist of degree 6 as in Lemma 2.12, which is defined over $\mathbb{F}_{p^2}$, and $\xi \in \mathbb{F}_{p^2}$ is neither a square nor a cube. We take $\mathbb{F}_{p^2} = \mathbb{F}_p(\nu)$, where ν is a root of the irreducible polynomial $x^2 - \mu \in \mathbb{F}_p[x]$. The embedding degree of E with respect to n is $k = 12$, and thus pairings map into $\mathbb{F}_{p^{12}}$. This field is represented as $\mathbb{F}_{p^{12}} = \mathbb{F}_{p^2}(\omega)$, where ω is a root of the irreducible polynomial $x^6 - \xi \in \mathbb{F}_{p^2}[x]$. The intermediate fields $\mathbb{F}_{p^4}$ and $\mathbb{F}_{p^6}$ can then be given as $\mathbb{F}_{p^6} = \mathbb{F}_{p^2}(\omega^2)$ and $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(\omega^3)$, see Section 2.2.3. We define $\varsigma := \omega^3$ and $\tau := \omega^2$, i. e. $\mathbb{F}_{p^6} = \mathbb{F}_{p^2}(\tau)$, $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}(\varsigma)$, and $\mathbb{F}_{p^{12}} = \mathbb{F}_{p^4}(\tau) = \mathbb{F}_{p^6}(\varsigma)$.
We now assemble the groups that are involved in the pairing computation. The first of those is the group $E(\mathbb{F}_p)$, which is the 1-eigenspace of the p-power Frobenius endomorphism $\phi_p \in \mathrm{End}(E)$,

$$G_1 = E(\mathbb{F}_p) = \ker(\phi_p - [1]). \tag{2.17}$$

The second group is the p-eigenspace of the Frobenius on $E[n]$, which consists of points defined over $\mathbb{F}_{p^{12}}$,

$$G_2 = E[n] \cap \ker(\phi_p - [p]) \subseteq E(\mathbb{F}_{p^{12}})[n]. \tag{2.18}$$

We have seen that we can represent the points in G_2 by points in the group

$$G_2' = E'(\mathbb{F}_{p^2})[n], \tag{2.19}$$

and then, if needed, map to G_2 via

$$\psi : G_2' \to G_2,\ (x', y') \mapsto (\omega^2 x', \omega^3 y') = (\tau x', \varsigma y').$$

This map is needed when a pairing is actually computed. Other operations, like for example the elliptic curve arithmetic during Miller's algorithm for the ate pairing, should be done in G_2'. When curve arithmetic in G_2 is required in a protocol, it can be replaced by arithmetic in G_2'. The following remark shows that computing the map ψ from G_2' to G_2 is almost for free.

Remark 2.28. In the chosen setting of finite fields, the computation of $\psi(Q') = \psi(x', y')$ does not require any finite field arithmetic. An element $\alpha \in \mathbb{F}_{p^{12}}$ can be written as

$$\alpha = \alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3 + \alpha_4\omega^4 + \alpha_5\omega^5,$$

with coefficients $\alpha_i \in \mathbb{F}_{p^2}$. It is uniquely determined by $(\alpha_0, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$, its coefficient vector. The element $\omega^2 x'$ has just one coefficient different from 0, i. e. it is given by the vector $(0, 0, x', 0, 0, 0)$. The second coordinate, $\omega^3 y'$, is given by $(0, 0, 0, y', 0, 0)$. In particular, no field multiplications are needed at all.

Since $\psi : G_2' \to G_2$ is a group isomorphism, every point in G_2 is of the form $(\tau x', \varsigma y')$. Note that both coordinates lie in proper subfields of $\mathbb{F}_{p^{12}}$ (see Remark 2.15). This

makes the evaluation of line functions easier, as we are able to do computations in subfields of $\mathbb{F}_{p^{12}}$.
Finally, the third group that occurs is the group $\mu_n \subseteq \mathbb{F}_{p^{12}}^*$ of nth roots of unity, into which the pairing maps:

$$G_3 = \mu_n \subseteq \mathbb{F}_{p^{12}}^*. \tag{2.20}$$

All the groups G_1, G_2, G_2', and G_3 are cyclic groups of order n. If needed, one can use point compression techniques on the groups G_1, G_2, and G_2' as proposed in Subsection 2.2.5. To speed up elliptic-curve scalar multiplication, the methods discussed in Subsection 2.2.4 may be applied.
We now turn towards pairing computation. An essential part of Miller's algorithm (see Algorithm 1.1) is the evaluation of the line functions $l_{U,V}$ for two points $U = (x_U, y_U)$ and $V = (x_V, y_V)$ lying in either of the groups G_1, G_2, or G_2'. If $U \neq -V$, the function $l_{U,V}$ is given by

$$l_{U,V}(x, y) = \lambda(x - x_U) + (y_U - y),$$

where λ is the slope of the line through U and V, being tangent to the curve, if $U = V$ (see Lemma 1.94).
The pairing functions that we consider in the sequel are either maps

$$G_1 \times G_2 \to G_3 \text{ or } G_2 \times G_1 \to G_3.$$

Line function computation and evaluation are different in both cases, since $U, V \in G_1$ in the first case and $U, V \in G_2$ in the second case. Thus point coordinates lie in different fields. The point Q, at which the line functions are evaluated, lies in the other group, and also has different fields of definition in the different cases. We address each case in one of the following two subsections.
The final exponentiation has to be carried out after the Miller function computation in either case. For BN curves, the exponent is $(p^{12}-1)/n$. It can be split up, and the exponentiation can be carried out by some applications of the finite field Frobenius automorphism and a remaining part, done in a multi-exponentiation. For details, we refer to the paper of Devegili, Scott, and Dahab [DSD07]. Recently, Scott et. al. [SBC+08] have been able to further improve the final exponentiation.

2.3.1 Tate and twisted ate pairings

For the Tate and the twisted ate pairing (see Section 1.2), we compute a function

$$e : G_1 \times G_2' \to G_3,\ (P, Q') \mapsto f_{m,P}(\psi(Q'))^{\frac{p^{12}-1}{n}}.$$

Here $m = n$ if the Tate pairing is computed and $m = \rho_{12}^2 \mod n$ if e is the twisted ate pairing. The best choice for this setting of groups is the generalized twisted ate pairing proposed by Zhao, Zhang, and Huang in [ZZH08]. Depending on the sign of the parameter u, we can always choose $m \in \{\rho_{12}^2 \mod n, \rho_{12}^{10} \mod n\}$, i. e.

$$m \in \{-36u^3 - 18u^2 - 6u - 1, 36u^3 + 18u^2 + 6u + 2\},$$

such that the bitsize of m is 3/4 that of n.
We now give the line functions that occur in Miller's algorithm for points in affine representation. Remember that an element α of $\mathbb{F}_{p^{12}}$ can be represented as

$$\begin{aligned}\alpha &= \alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3 + \alpha_4\omega^4 + \alpha_5\omega^5 \\ &= \alpha_0 + \alpha_1\omega + \alpha_2\tau + \alpha_3\varsigma + \alpha_4\omega\varsigma + \alpha_5\varsigma\tau.\end{aligned}$$

We state the evaluated line functions in this representation.

Lemma 2.29. *Let $U, V \in G_1$, $U = (x_U, y_U), V = (x_V, y_V)$, i. e. $x_U, y_U, x_V, y_V \in \mathbb{F}_p$, and $Q' = (x_{Q'}, y_{Q'}) \in G_2'$, i. e. $x_{Q'}, y_{Q'} \in \mathbb{F}_{p^2}$. Then the line function $l_{U,V}(\psi(Q'))$ can be computed as follows.*

(a) If $U \neq \pm V$, then $\lambda = (y_V - y_U)/(x_V - x_U)$. If $U = V$, then $\lambda = (3x_U^2)/(2y_U)$. In both cases,

$$l_{U,V}(\psi(Q')) = (y_U - \lambda x_U) + \lambda x_{Q'}\tau - y_{Q'}\varsigma.$$

(b) If $U = -V$, then

$$l_{U,-U}(\psi(Q')) = -x_U + x_{Q'}\tau.$$

Proof. This follows easily from Lemma 1.94. □

Note that due to the representation of G_2 as the image of G_2', the computation of line functions involves only the computation of $\lambda \in \mathbb{F}_p$ and the multiplications $\lambda x_U \in \mathbb{F}_p$ and $\lambda x_{Q'}$, where only $x_{Q'} \in \mathbb{F}_{p^2}$.
To avoid inversions, one usually represents U, V in projective coordinates. The formulas in this case can be easily deduced from the above and are given in [DSD07].

2.3.2 ate and optimal pairings

The ate pairing on a BN curve is computed as

$$e : G_2' \times G_1 \to G_3,\ (Q', P) \mapsto f_{t-1,\psi(Q')}(P)^{\frac{p^{12}-1}{n}}.$$

In contrast to pairings from the previous subsection, the curve arithmetic in Miller's algorithm must now be done in G_2'. Line function coefficients are computed from the coordinates of $Q' \in G_2'$, while they are evaluated at a point $P \in G_1$ defined over the base field.

Lemma 2.30. *Let $U, V \in G_2$ and define U' and V' by $U = \psi(U') = (\tau x_{U'}, \varsigma y_{U'})$ and $V = \psi(V') = (\tau x_{V'}, \varsigma y_{V'})$. If $U \neq -V$, the slope λ of the line passing through U and V (being tangent to the curve E if $U = V$) is given by*

$$\lambda = \omega\lambda',$$

where λ' is the slope of the line through U' and V' (being tangent to the curve if $U' = V'$).

Proof. Let $U \neq V$, then

$$\lambda = \frac{y_V - y_U}{x_V - x_U} = \frac{\varsigma(y_{V'} - y_{U'})}{\tau(x_{V'} - x_{U'})} = \omega \frac{y_{V'} - y_{U'}}{x_{V'} - x_{U'}} = \omega\lambda'.$$

Now, let $U = V$, then

$$\lambda = \frac{3x_U^2}{2y_U} = \frac{\tau^2(3x_{U'}^2)}{\varsigma(2y_{U'})} = \omega \frac{3x_{U'}^2}{2y_{U'}} = \omega\lambda'.$$

□

Once more, computations with points in G_2 can be replaced by corresponding computations with points in G_2'. We proceed by giving the line functions.

Lemma 2.31. *Let $U', V' \in G_2'$, $U' = (x_{U'}, y_{U'}), V' = (x_{V'}, y_{V'})$, i. e. $x_{U'}, y_{U'}$, $x_{V'}, y_{V'} \in \mathbb{F}_{p^2}$, and $P = (x_P, y_P) \in G_1$, i. e. $x_P, y_P \in \mathbb{F}_p$. Then the line function $l_{\psi(U'),\psi(V')}(P)$ evaluated at P can be computed as follows:*

(a) If $U' \neq \pm V'$, let $\lambda' = (y_{V'} - y_{U'})/(x_{V'} - x_{U'})$. If $U' = V'$, let $\lambda' = (3x_{U'}^2)/(2y_{U'})$. In both cases,

$$l_{\psi(U'),\psi(V')}(P) = -y_P + \lambda' x_P \omega + (y_{U'} - \lambda' x_{U'})\varsigma.$$

(b) If $U' = -V'$, then

$$l_{\psi(U'),-\psi(U')}(P) = x_P - x_{U'}\tau.$$

Proof. Case (b) is trivial. For case (a), compute $\lambda(x_P - x_{\psi(U')}) + (y_{\psi(U')} - y_P) = \lambda'\omega(x_P - x_{U'}\tau) + (y_{U'}\varsigma - y_P)$. □

Compared to Lemma 2.29, more computations in $\mathbb{F}_{p^2}$ must be made. We have the computation of λ' and the multiplications $\lambda' x_P$, where only $\lambda' \in \mathbb{F}_{p^2}$ and $\lambda' x_{U'} \in \mathbb{F}_{p^2}$. These formulas have been proposed in [DSD07] already.
The shortest loop length for a pairing based on the ate pairing can be achieved by using so called optimal pairings as introduced by Vercauteren in [Ver08]. The loop length for the Miller function is $m = 6u + 2$ in this case. But note that then the function $(P, Q') \to (f_{m,\psi(Q')}(P))^{\frac{p^{12}-1}{n}}$ is not bilinear, and that it needs to be adjusted by some line-function factors.

2.3.3 Pairing compression

In [SB04], Scott and Barreto suggest to compress pairing values by computing a finite field trace. Implicit exponentiation of compressed values can be done as in the XTR public key system [LV00]. Following the ideas in [LV00] and [SB04], we can compress pairing values to 1/3 of their length by computing their $\mathbb{F}_{p^4}$-trace. Pairing values are then represented by one $\mathbb{F}_{p^4}$-element, and can be implicitly exponentiated.

Compression in such a way is consistent with point compression in G_2'. All points with the same y-coordinate, i. e. all points that lie in the same orbit under the subgroup $\mathcal{H}'$ of the automorphism group $\mathrm{Aut}(E')$ (see Subsection 2.2.5) are mapped to the same value.

Proposition 2.32. *Let $e_1 : G_1 \times G_2' \to G_3$ and $e_2 : G_2' \times G_1 \to G_3$ be bilinear pairings. Let $P \in G_1$ and $Q' = (x', y') \in G_2'$. Then for all points $R' \in G_2'$ with y-coordinate equal to y', it holds:*

$$\mathrm{tr}_{\mathbb{F}_{p^4}}(e_1(P, Q')) = \mathrm{tr}_{\mathbb{F}_{p^4}}(e_1(P, R')) \text{ and } \mathrm{tr}_{\mathbb{F}_{p^4}}(e_2(Q', P)) = \mathrm{tr}_{\mathbb{F}_{p^4}}(e_2(R', P)),$$

where $\mathrm{tr}_{\mathbb{F}_{p^4}} : \mathbb{F}_{p^{12}} \to \mathbb{F}_{p^4}, \alpha \mapsto \alpha + \alpha^{p^4} + \alpha^{p^8}$ is the $\mathbb{F}_{p^4}$-trace.

Proof. It follows from Lemma 2.22 that the set of all points with the same y-coordinate y' is exactly the orbit $\mathcal{H}'Q'$. Remark 2.24 then shows that this orbit is bijectively mapped to the orbit $\mathcal{H}\psi(Q')$ in G_2. By Remark 2.25, we see that this orbit is exactly $\{Q, [p^4]Q, [p^8]Q\}$, where $Q = \psi(Q')$. Let $e_0 = e_1(P, Q')$. Then the pairing values of the other two points with y-coordinate y' are $e_0^{p^4}$ and $e_0^{p^8}$, respectively. Thus the traces of all three values are equal to $\mathrm{tr}_{\mathbb{F}_{p^4}}(e_0)$. The same holds for the pairing $e_2(Q', P)$ with groups interchanged. □

Similarly, if we compress points in G_2' to one bit less, i. e. if we identify all points with their y-coordinates being equal up to sign, we can do the corresponding sixfold compression of pairing values by computing the $\mathbb{F}_{p^2}$-trace.

Proposition 2.33. *Let $e_1 : G_1 \times G_2' \to G_3$ and $e_2 : G_2' \times G_1 \to G_3$ be bilinear pairings. Let $P \in G_1$ and $Q' = (x', y') \in G_2'$. Then for all points $R' \in G_2'$ that have a y-coordinate equal to y' or $-y'$, it holds:*

$$\mathrm{tr}_{\mathbb{F}_{p^2}}(e_1(P, Q')) = \mathrm{tr}_{\mathbb{F}_{p^2}}(e_1(P, R')) \text{ and } \mathrm{tr}_{\mathbb{F}_{p^2}}(e_2(Q', P)) = \mathrm{tr}_{\mathbb{F}_{p^2}}(e_2(R', P)),$$

where $\mathrm{tr}_{\mathbb{F}_{p^2}} : \mathbb{F}_{p^{12}} \to \mathbb{F}_{p^2}, \alpha \mapsto \alpha + \alpha^{p^2} + \alpha^{p^4} + \alpha^{p^6} + \alpha^{p^8} + \alpha^{p^{10}}$ is the $\mathbb{F}_{p^2}$-trace.

Proof. The proposition follows in the same way as Proposition 2.32 from Lemma 2.23 and Remarks 2.24 and 2.25. □

The approach to compress pairing values by computing traces is not suitable for implicit multiplication of compressed values. This problem can be solved by a compression technique that exploits the fact that pairing values lie in algebraic tori, certain subgroups of $\mathbb{F}_{p^{12}}^*$. We discuss this approach in Chapter 3.

2.4 Construction revisited

In this section, we return to the construction of BN curves. In contrast to Section 2.1, we summarize in one place, how to get all the parameters needed for implementing

pairings on BN curves, including generator points, field extensions, the primitive roots of unity needed for the use of efficient endomorphisms, and the automorphism groups. We use the following polynomial parametrizations:

$$\begin{aligned} p &= 36u^4 + 36u^3 + 24u^2 + 6u + 1, \\ n &= 36u^4 + 36u^3 + 18u^2 + 6u + 1, \\ t &= 6u^2 + 1. \end{aligned}$$

2.4.1 Prime pairs and primitive roots

Algorithm 2.2 is a randomized algorithm to find a BN prime pair. Note that the set I in Step 1 might not contain any u leading to a BN prime pair, in which case the loop would not terminate. We therefore assume, that the algorithm is only applied for large enough values of m, such that I is not empty and large enough to provide a prime pair. Our heuristic results in Subsection 2.1.1 imply that this is always the case for $m > 32$. The notation $u \in_R I$ in Step 3 indicates that u is chosen at random from the set I.

Input: A desired bitsize m for the group order n.
Output: A parameter $u \in \mathbb{Z}$ such that p and n are prime and have m bits, and the corresponding BN prime pair (p, n).
1: Find the largest set $I \subset \mathbb{Z}$, such that p and n have m bits for all $u \in I$.
2: **repeat**
3: Select $u \in_R I$,
4: compute $p \leftarrow 36u^4 + 36u^3 + 24u^2 + 6u + 1$,
5: compute $t \leftarrow 6u^2 + 1$ and $n \leftarrow p + 1 - t$.
6: **until** p and n are prime.
7: **return** $u, (p, n)$.

Algorithm 2.2: Finding a BN prime pair

Let $\mu \in \mathbb{F}_p$ be a non-square. To construct $\mathbb{F}_{p^2}$ use $\mathbb{F}_{p^2} = \mathbb{F}_p(\nu)$, where $\nu^2 = \mu$. From the parameter u, we can compute the 6th roots of unity in $\mathbb{F}_p$ as

$$\begin{aligned} \zeta_6 &= 18u^3 + 18u^2 + 9u + 2 \mod p, \\ \zeta_6^2 &= 18u^3 + 18u^2 + 9u + 1 \mod p, \\ \zeta_6^3 &= -1 \mod p, \\ \zeta_6^4 &= -18u^3 - 18u^2 - 9u - 2 \mod p, \\ \zeta_6^5 &= -18u^3 - 18u^2 - 9u - 1 \mod p, \end{aligned}$$

and the 12th roots of unity in $\mathbb{F}_n$ as

$$\begin{aligned}
\rho_{12} &= 6u^2, \\
\rho_{12}^2 &= -36u^3 - 18u^2 - 6u - 1 \mod n, \\
\rho_{12}^3 &= -36u^3 - 24u^2 - 12u - 3 \mod n, \\
\rho_{12}^4 &= -36u^3 - 18u^2 - 6u - 2 \mod n, \\
\rho_{12}^5 &= -36u^3 - 30u^2 - 12u - 3 \mod n, \\
\rho_{12}^6 &= -1 \mod n, \\
\rho_{12}^7 &= -6u^2 \mod n, \\
\rho_{12}^8 &= 36u^3 + 18u^2 + 6u + 1 \mod n, \\
\rho_{12}^9 &= 36u^3 + 24u^2 + 12u + 3 \mod n, \\
\rho_{12}^{10} &= 36u^3 + 18u^2 + 6u + 2 \mod n, \\
\rho_{12}^{11} &= 36u^3 + 30u^2 + 12u + 3 \mod n.
\end{aligned}$$

Note that $\rho_{12} = t - 1$. Define $\zeta_3 := \zeta_6^2$, a primitive 3rd root of unity modulo p, and define $\rho_6 := \rho_{12}^2$, a primitive 6th root of unity modulo n.

2.4.2 Curve, twist, and automorphisms

On input of a BN prime pair (p, n), Algorithm 2.3 constructs a BN curve over $\mathbb{F}_p$ with $n = \#E(\mathbb{F}_p)$ and a degree 6 twist E' of E over $\mathbb{F}_{p^2}$ such that n divides $\#E'(\mathbb{F}_{p^2})$. It further gives generators P and Q' for the groups $G_1 = E(\mathbb{F}_p)$ and $G_2' = E'(\mathbb{F}_{p^2})[n]$. As discussed in Subsection 2.1.2, the random choice of P in Step 4 may be replaced by the choice with a certain given x-coordinate or y-coordinate.
The 3rd root of unity ζ_3 from the previous subsection defines a generator σ_6 of the automorphism group $\mathrm{Aut}(E)$ by

$$\sigma_6 : E \to E,\ (x, y) \mapsto (\zeta_3 x, -y)$$

and a generator σ_6' of $\mathrm{Aut}(E')$ by

$$\sigma_6' : E' \to E',\ (x', y') \mapsto (\zeta_3 x', -y').$$

Then it holds $\sigma_6(P) = [\rho_6]P$ or $\sigma_6(P) = [\rho_6^5]P$. Which one is correct, can be checked easily. Similarly, we can test whether $\sigma_6'(Q') = [\rho_6]Q'$ or $\sigma_6(Q') = [\rho_6^5]Q'$.

2.4.3 Finite fields and twist isomorphism

Finally, we can construct the finite fields $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, and $\mathbb{F}_{p^{12}}$ as extensions of $\mathbb{F}_{p^2}$ using the element $\xi \in \mathbb{F}_{p^2} \setminus \left((\mathbb{F}_{p^2})^2 \cup (\mathbb{F}_{p^2})^3\right)$ that defines the twist E' (see Lemma 2.14 and Algorithm 2.3). As indicated in Subsection 2.2.3, we can choose $\omega \in \mathbb{F}_{p^{12}}$ with

Input: A BN prime pair (p, n) and $\mathbb{F}_{p^2} = \mathbb{F}_p(\nu)$.
Output: A parameter $b \in \mathbb{F}_p$, such that $n = \#E(\mathbb{F}_p)$ for $E : y^2 = x^3 + b$, a parameter $\xi \in \mathbb{F}_{p^2}$, such that $n \mid \#E'(\mathbb{F}_{p^2})$ for $E' : y^2 = x^3 + b/\xi$, and generators P for $E(\mathbb{F}_p)$ and Q' for $E'(\mathbb{F}_{p^2})[n]$.

1: **repeat**
2: Select $b \in_R \mathbb{F}_p \setminus ((\mathbb{F}_p)^2 \cup (\mathbb{F}_p)^3)$,
3: define $E : y^2 = x^3 + b$,
4: select $P \in_R E(\mathbb{F}_p) \setminus \{\mathcal{O}\}$.
5: **until** $[n]P = \mathcal{O}$.
6: Compute $h \leftarrow p - 1 + t$.
7: Select $\xi \in \mathbb{F}_{p^2} \setminus \left((\mathbb{F}_{p^2})^2 \cup (\mathbb{F}_{p^2})^3\right)$,
8: define $E' : y'^2 = x'^3 + b/\xi$.
9: **repeat**
10: Select $R' \in_R E'(\mathbb{F}_{p^2})$,
11: compute $Q' \leftarrow [h]R'$,
12: **until** $Q' \neq \mathcal{O}$.
13: **if** $[n]Q' \neq \mathcal{O}$ **then**
14: Set $\xi \leftarrow \xi^5$ and go to Step 8.
15: **end if**
16: **return** b, ξ, P, Q'.

Algorithm 2.3: Constructing a BN curve and its twist

$\omega^6 = \xi$ and define $\tau := \omega^2$ and $\varsigma := \omega^3$. Then the fields can be represented as

$$\begin{aligned} \mathbb{F}_{p^{12}} &= \mathbb{F}_{p^2}(\omega), \\ \mathbb{F}_{p^6} &= \mathbb{F}_{p^2}(\tau), \\ \mathbb{F}_{p^4} &= \mathbb{F}_{p^2}(\varsigma). \end{aligned}$$

The isomorphism ψ, mapping from the twist E' to E, is given as

$$\psi : E' \to E,\ (x', y') \mapsto (\tau x', \varsigma y').$$

2.5 Examples

All of the following curves have an equation $E : y^2 = x^3 + 3$ over $\mathbb{F}_p$ with a group of $\mathbb{F}_p$-rational points of prime order n and the trace of the Frobenius endomorphism equal to t. A sample generator for any of them is $P = (1, 2) \in E(\mathbb{F}_p)$. In all cases, we choose $p \equiv 3 \pmod 4$ and $p \equiv 4 \pmod 9$ to simplify the computation of square and cube roots, and the bitlengths of p and n are equal. The field $\mathbb{F}_{p^2}$ is represented as $\mathbb{F}_p(i)$, where $i^2 = -1$. The sextic twist for all examples has the form $E'(\mathbb{F}_{p^2}) : y^2 = x^3 + 3/\xi$, where $1/\xi = -8 + 8i$. Furthermore, we provide a primitive 6th root of unity ζ_6 modulo p, and a 12th root of unity ρ_{12} modulo n can be simply obtained as $t - 1$. A generator for the group $E'(\mathbb{F}_{p^2})[n]$ is given as $Q' = (x_{Q'}, y_{Q'})$.

160-bit groupsize

$$
\begin{aligned}
p &= 1461501624496790265145448589920785493717258890819\\
n &= 1461501624496790265145447380994971188499300027613\\
t &= 120892581430521795886320 7\\
u &= 448873741399\\
\zeta_6 &= 162796516002667448021219974392045779 3\\
x_{Q'} &= 3494285672289083136047523889540911039212100713 09i\\
&\quad +8218299599350494814906130554498550701224932392 44\\
y_{Q'} &= 8712026738052474350720494170493867247460630869 07i\\
&\quad +1239146125490754416389195992354273864776961399618
\end{aligned}
$$

192-bit groupsize

$$
\begin{aligned}
p &= 627710171953126940051704371006089286231860471313967450 9723\\
n &= 627710171953126940051704370998166469990440174416003655 6389\\
t &= 7922816241420296897963795 3335\\
u &= -114911677977917\\
\zeta_6 &= 627710171953124208779378534130251503165855423100490099 2640\\
x_{Q'} &= 589078237886627886412000379109769546321621676110465892923i\\
&\quad +4140652997028575876232653427843338644184272370846988816508\\
y_{Q'} &= 311062608876303269865181467343517033259193924511652798681 8i\\
&\quad +3761433986678713844778960232477894755556338428328701225 51
\end{aligned}
$$

224-bit groupsize

$$
\begin{aligned}
p &= 269599466671492057583834697369216954350157367352611551414234174239 23\\
n &= 269599466671492057583834697369216902427188782005715310297492359969 09\\
t &= 5192296858534689624111674181427015\\
u &= -29417389580922737\\
\zeta_6 &= 269599466671492053001520112149729998822144981770797475001551175483 80\\
x_{Q'} &= 123260399683748282141489315304767407528172316015091598062886238406 58i\\
&\quad +1554435382870902038741677368895545680515306578904763540520449157250 3\\
y_{Q'} &= 133882702550329848592897982160900244870254150800820798892943000593 12i\\
&\quad +3178522513471092300347338705055807506872703350697542114351541449187
\end{aligned}
$$

256-bit groupsize

$$
\begin{aligned}
p &= 115792089237314936872688561244471742058375878355761205198700409522629664518163\\
n &= 115792089237314936872688561244471742058035595988840268584488757999429535617037\\
t &= 340282366920936614211651523200128901127\\
u &= -7530851732716300289\\
\zeta_6 &= 115792089237314936865000713086853723961501417581576165808556977265798185842700\\
x_{Q'} &= 486374312833233451088493857489118467886330493150493717511206975056499463383 69i\\
&\quad +762234086972264187987456430936054828901398125130840779326705471533866549847 03\\
y_{Q'} &= 126147823422008541096079568410263045450953560075366003851539029734295257585 72i\\
&\quad +112103232229758856060671276297199689204345964658951607162631544293223609182175
\end{aligned}
$$

Chapter 3

Compressed pairing computation

In this chapter we discuss a method to compute pairings in compressed form. This method has been proposed in joint work with Barreto and Schwabe in [NBS08]. For an elliptic curve $E/\mathbb{F}_q$ with embedding degree k with respect to some prime divisor r of $\#E(\mathbb{F}_q)$, pairing values are rth roots of unity. Thus they lie in algebraic tori, certain subgroups of $\mathbb{F}_{q^k}^*$. Torus elements α are characterized by having relative norm 1, i. e. $N_{\mathbb{F}_{q^k}/\tilde{\mathbb{F}}}(\alpha) = 1$, for certain subfields $\tilde{\mathbb{F}} \subseteq \mathbb{F}_{q^k}$. These conditions allow to represent a torus element with less coefficients than a general element of $\mathbb{F}_{q^k}$ needs. Techniques based on algebraic tori are already used in the public-key systems LUC proposed by Smith and Lennon [SL93], the system by Gong and Harn [GH99, GHW01], and XTR by Lenstra and Verheul [LV00]. Rubin and Silverberg [RS03] describe a framework for torus-based cryptography.
The compression of pairing values is addressed by Scott and Barreto [SB04]. They use finite field traces of pairing values to represent them by elements in a smaller field. This approach is useful for implicit exponentiation, and they propose to do part of the final exponentiation in compressed form. But implicit multiplication of general compressed values can not be done easily. We have discussed trace-based compression techniques for BN curves in Subsection 2.3.3 of Chapter 2.
Granger, Page, and Stam [GPS06] propose to use torus-based compression techniques for pairing-based cryptography. They have shown how a pairing value in a field extension $\mathbb{F}_{q^6}$ can be compressed to an element in $\mathbb{F}_{q^3}$ plus one bit. We note that the technique of compression that we use here has already been explained in [GPS06] for supersingular curves in characteristic 3. Granger, Page, and Stam mention that the technique works also for curves over large characteristic fields, but they do not give the details. We show how to use the compression in this case. As a new contribution, we include the compression to inside the Miller loop, and show how to work with compressed representation.
In Section 3.1, we define algebraic tori and discuss basic properties. We introduce compressed pairing computation on elliptic curves with an even embedding degree in Section 3.2. The method is discussed in more detail for curves that have a twist of degree 6 and embedding degree divisible by 6 in Section 3.3. In this case, we give

explicit formulas for compressed pairing computation.

3.1 Preliminaries on tori

Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_{q^l} \supseteq \mathbb{F}_q$ a field extension. Then the *norm* of an element $\alpha \in \mathbb{F}_{q^l}$ with respect to $\mathbb{F}_q$ is defined as the product of all conjugates of α over $\mathbb{F}_q$, namely

$$N_{\mathbb{F}_{q^l}/\mathbb{F}_q}(\alpha) = \alpha\alpha^q \cdots \alpha^{q^{l-1}} = \alpha^{1+q+\cdots+q^{l-1}} = \alpha^{(q^l-1)/(q-1)}.$$

Definition 3.1. For a positive integer l, the *torus of degree l over $\mathbb{F}_q$* is defined as

$$T_l(\mathbb{F}_q) = \bigcap_{\mathbb{F}_q \subseteq \tilde{\mathbb{F}} \subsetneq \mathbb{F}_{q^l}} \ker(N_{\mathbb{F}_{q^l}/\tilde{\mathbb{F}}}). \tag{3.1}$$

If $\mathbb{F}_q \subseteq \tilde{\mathbb{F}} \subsetneq \mathbb{F}_{q^l}$, then $\tilde{\mathbb{F}} = \mathbb{F}_{q^d}$, where $d \mid l, d \neq l$; so the relative norm is given as

$$N_{\mathbb{F}_{q^l}/\mathbb{F}_{q^d}}(\alpha) = \alpha^{(q^l-1)/(q^d-1)}.$$

It follows that

$$T_l(\mathbb{F}_q) = \{\alpha \in \mathbb{F}_{q^l} \mid \alpha^{(q^l-1)/(q^d-1)} = 1,\ d \mid l, d \neq l\}.$$

Since the norm map is multiplicative, the set $T_l(\mathbb{F}_q)$ is a subgroup of $\mathbb{F}_{q^l}^*$.

Lemma 3.2. *The set $T_l(\mathbb{F}_q)$ is the unique subgroup of the cyclic group $\mathbb{F}_{q^l}^*$ of order $\Phi_l(q)$, where Φ_l is the lth cyclotomic polynomial.*

Proof. This is [RS03, Lemma 7]. □

From the definition of cyclotomic polynomials [LN97, Definition 2.44 and Theorem 2.45], we know that for $p \nmid l$

$$X^l - 1 = \prod_{d \mid l} \Phi_d(X) = \Phi_l(X) \prod_{d \mid l, d \neq l} \Phi_d(X).$$

Define

$$\Psi_l(X) := \prod_{d \mid l, d \neq l} \Phi_d(X) = (X^l - 1)/\Phi_l(X).$$

Lemma 3.3. *Let $\alpha \in \mathbb{F}_{q^l}^*$. Then $\alpha^{\Psi_l(q)} \in T_l(\mathbb{F}_q)$.*

Proof. Let $\beta = \alpha^{\Psi_l(q)}$. Then $\beta^{\Phi_l(q)} = \alpha^{q^l-1} = 1$, thus β has order dividing $\Phi_l(q)$. Since $\mathbb{F}_{q^l}^*$ and $T_l(\mathbb{F}_q)$ are finite cyclic groups, and $T_l(\mathbb{F}_q)$ is the unique subgroup of order $\Phi_l(q)$, β lies in $T_l(\mathbb{F}_q)$. □

Lemma 3.4. *For each divisor $d \mid l$ of l, it holds $T_l(\mathbb{F}_q) \subseteq T_{l/d}(\mathbb{F}_{q^d})$.*

Proof. Let $\beta \in T_l(\mathbb{F}_q)$. Then $N_{\mathbb{F}_{q^l}/\mathbb{F}_{q^e}}(\beta) = 1$ for all $e \mid l, e \neq l$. In particular, the norm is 1 for all such e with $d \mid e$, hence $\beta \in T_{l/d}(\mathbb{F}_{q^d})$. □

Combining the above two lemmas shows that the element α raised to the power $\Psi_l(q)$ is an element of each torus $T_{l/d}(\mathbb{F}_{q^d})$ for all divisors $d \mid l$, $d \neq l$.

Remark 3.5. Let E be an elliptic curve defined over $\mathbb{F}_q$ and r a prime with $r \mid \#E(\mathbb{F}_q)$. Let k be the embedding degree of E with respect to r. By Lemma 1.107, we have that $r \mid \Phi_k(q)$. Hence, the exponent of the final exponentiation can be split up as

$$\frac{q^k - 1}{r} = \Psi_k(q)\frac{\Phi_k(q)}{r}.$$

Therefore, a pairing value computed from the reduced Tate pairing or any other pairing variant that includes the final exponentiation (see Section 1.2.3) lies in the torus $T_k(\mathbb{F}_q)$. By the preceding lemmas, it also lies in each torus $T_{k/d}(\mathbb{F}_{q^d})$ for $d \mid k$, $d \neq k$.

3.2 Even embedding degree

Let k be even, and let $p \geq 5$ be a prime. In this section, let $q = p^{k/2}$ and thus $\mathbb{F}_q = \mathbb{F}_{p^{k/2}}$ so that $\mathbb{F}_{q^2} = \mathbb{F}_{p^k}$. Choose $\xi \in \mathbb{F}_q$ to be a nonsquare. Then the polynomial $x^2 - \xi \in \mathbb{F}_q[x]$ is irreducible, and we represent $\mathbb{F}_{q^2} = \mathbb{F}_q(\sigma)$, where σ is a root of $x^2 - \xi$. We exploit properties of the torus $T_2(\mathbb{F}_q)$ in this section. We have

$$T_2(\mathbb{F}_q) = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^{q+1} = 1\} = \{a_0 + a_1\sigma \in \mathbb{F}_{q^2} \mid a_0^2 - a_1^2\xi = 1\}.$$

If $a_1 = 0$, then $a_0 \in \{1, -1\}$. Therefore, 1 and -1 are the only elements from $\mathbb{F}_q$ that lie in $T_2(\mathbb{F}_q)$.

Proposition 3.6. *Each element $1 \neq \alpha \in T_2(\mathbb{F}_q)$ has a unique representation as*

$$\alpha = \frac{a - \sigma}{a + \sigma}$$

for some element $a \in \mathbb{F}_q$. Vice versa, every fraction of this form is an element of $T_2(\mathbb{F}_q)$. If $\alpha = a_0 + a_1\sigma$ with $a_1 \neq 0$, a can be computed as $a = -(1 + a_0)/a_1$. The map

$$\theta : T_2(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q),\ \alpha \mapsto (X_\alpha : Y_\alpha) := \begin{cases} (-(1+a_0)/a_1 : 1) & \text{if } a_1 \neq 0, \\ (0:1) & \text{if } a_1 = 0, a_0 = -1, \\ (1:0) & \text{if } a_1 = 0, a_0 = 1 \end{cases}$$

is a bijection.

Proof. This follows from [RS03, Section 5.2]. □

Remark 3.7. The map θ from the previous proposition can be given as $\theta(\alpha) = (-(1+a_0) : a_1)$ for $\alpha = a_0 + a_1\sigma \neq -1$. The definition in Proposition 3.6 uses as representative for a projective point $\theta(\alpha)$ the corresponding affine point if $\alpha \neq 1$, and uses the point at infinity $(1:0)$ for $\alpha = 1$. This emphasizes that we can represent a torus element $\alpha \in T_2(\mathbb{F}_q)$ by $\theta(\alpha)$ which can be given by one element in $\mathbb{F}_q$ and an additional bit to distinguish the neutral element $1 \in T_2(\mathbb{F}_q)$. Hence we consider θ as a compression function.

We wish to multiply elements in $T_2(\mathbb{F}_q)$ implicitly with their compressed values. The next lemma shows how to compute the compressed value of the product of two torus elements from the compressed values of the single elements.

Lemma 3.8. *Let $\alpha, \beta \in T_2(\mathbb{F}_q)$. If $X_\alpha = -X_\beta$, then $\theta(\alpha\beta) = (1:0)$; if $Y_\alpha = 0$, then $\theta(\alpha\beta) = \theta(\beta)$; and if $Y_\beta = 0$, then $\theta(\alpha\beta) = \theta(\alpha)$. Otherwise,*

$$\theta(\alpha\beta) = ((X_\alpha X_\beta + \xi)/(X_\alpha + X_\beta) : 1), \tag{3.2}$$

where $\xi = \sigma^2$.

Proof. If either $Y_\alpha = 0$ or $Y_\beta = 0$, i. e. $\alpha = 1$ or $\beta = 1$, the result is the other value. If $X_\alpha = -X_\beta$, we have that $(X_\alpha - \sigma)/(X_\alpha + \sigma) = (X_\beta + \sigma)/(X_\beta - \sigma)$ is the inverse of $(X_\beta - \sigma)/(X_\beta + \sigma)$, and their product is 1.
For all other cases, the product is

$$\frac{X_\alpha - \sigma}{X_\alpha + \sigma} \cdot \frac{X_\beta - \sigma}{X_\beta + \sigma} = \frac{X_{\alpha\beta} - \sigma}{X_{\alpha\beta} + \sigma}$$

with $X_{\alpha\beta} = (X_\alpha X_\beta + \xi)/(X_\alpha + X_\beta)$. □

Remark 3.9. Let $\alpha \in T_2(\mathbb{F}_q) \setminus \{1, -1\}$. Then $X_\alpha \neq 0$, and the compressed value of α^2 is $\theta(\alpha^2) = (X_\alpha/2 + \xi/(2X_\alpha) : 1)$. It follows from

$$\alpha^{-1} = \left(\frac{X_\alpha - \sigma}{X_\alpha + \sigma}\right)^{-1} = \frac{X_\alpha + \sigma}{X_\alpha - \sigma} = \frac{-X_\alpha - \sigma}{-X_\alpha + \sigma} \tag{3.3}$$

that $\theta(\alpha^{-1}) = (-X_\alpha : 1)$. Hence inversion of compressed torus elements does not need inversions in a finite field. Instead, it only requires negation of a finite field element.
The multiplication by -1 is implicitly given as $\theta(-\alpha) = \xi/X_\alpha$ because

$$-\frac{X_\alpha - \sigma}{X_\alpha + \sigma} = \frac{\sigma^2 - X_\alpha\sigma}{\sigma^2 + X_\alpha\sigma} = \frac{\xi - X_\alpha\sigma}{\xi + X_\alpha\sigma} = \frac{\xi/X_\alpha - \sigma}{\xi/X_\alpha + \sigma}.$$

We define a multiplication "$\star$" on $\mathbb{P}^1(\mathbb{F}_q)$ by $(X_\alpha : Y_\alpha) \star (X_\beta : Y_\beta) := \theta(\alpha\beta)$. Then $(\mathbb{P}^1(\mathbb{F}_q), \star)$ is a multiplicative group, which is isomorphic to the group $T_2(\mathbb{F}_q)$ with usual multiplication inherited from $\mathbb{F}_{q^2}^*$.

Granger, Page, and Stam [GPS06] suggest to use the above described compression on pairing values after the final exponentiation, and carry out any arithmetic that has to be done with pairing values in the compressed representation. We propose to use part of the final exponentiation to do the compression. Computing the torus representation of the $(q-1)$th power of an element in $\mathbb{F}_{q^2}^*$ can be done in one field inversion in $\mathbb{F}_q$.

Lemma 3.10. *Let $\alpha = a_0 + a_1\sigma \in \mathbb{F}_{q^2}^*$. Then α^{q-1} is an element of the torus $T_2(\mathbb{F}_q)$ and*

$$\theta(\alpha^{q-1}) = \begin{cases} (a_0/a_1 : 1) & \text{if } a_1 \neq 0 \ (\alpha \notin \mathbb{F}_q), \\ (1:0) & \text{if } a_1 = 0 \ (\alpha \in \mathbb{F}_q). \end{cases}$$

Proof. First let $\alpha \in \mathbb{F}_q$, i. e. $a_1 = 0$. Then $\alpha^{q-1} = 1$ and $\theta(\alpha^{q-1}) = (1:0)$. Suppose now that $\alpha \notin \mathbb{F}_q$ and hence $a_1 \neq 0$. Applying the q-power Frobenius automorphism on $\mathbb{F}_{q^2}$ to σ gives $\sigma^q = -\sigma$. We raise α to the power of $q-1$ and obtain

$$\alpha^{q-1} = (a_0 + a_1\sigma)^{q-1} = \frac{(a_0 + a_1\sigma)^q}{a_0 + a_1\sigma} = \frac{a_0 - a_1\sigma}{a_0 + a_1\sigma}.$$

Since $a_1 \neq 0$, we can proceed further by dividing in numerator and denominator by a_1, which gives

$$(a_0 + a_1\sigma)^{q-1} = \frac{a_0/a_1 - \sigma}{a_0/a_1 + \sigma}. \tag{3.4}$$

Proposition 3.6 shows that $\alpha^{q-1} \in T_2(\mathbb{F}_q)$ and that $\theta(\alpha^{q-1}) = (a_0/a_1 : 1)$. □

Let E be an elliptic curve over $\mathbb{F}_p$, and let k be the embedding degree of E with respect to a prime r. The group of rth roots of unity μ_r is contained in $\mathbb{F}_{q^2}^* = \mathbb{F}_{p^k}^*$. Recall from Section 1.2.1 that the final exponentiation is the map

$$\mathbb{F}_{q^2}^*/(\mathbb{F}_{q^2}^*)^r \to \mu_r \subseteq \mathbb{F}_{q^2}^*, \ \alpha(\mathbb{F}_{q^2}^*)^r \mapsto \alpha^{(q^2-1)/r}.$$

We may write the exponent as

$$\frac{q^2-1}{r} = (q-1)\frac{q+1}{r}.$$

Suppose that we carry out the final exponentiation in two steps. First we compute α^{q-1}, and in a second step raise the result to the power $(q+1)/r$. After the first step, the result lies in $T_2(\mathbb{F}_q)$ by Lemma 3.10. Its compressed representation can be computed with just one field inversion. One can do the compression to a torus representation inside the Miller loop with this first step. This means that the remaining part of the exponentiation has to be done with the implicit torus arithmetic described in Lemma 3.8.

Definition 3.11. Let e_r be the reduced Tate pairing on E as in Section 1.2.3. We call the map

$$\begin{aligned} \tau_{r,T_2} : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})[r] &\to \mathbb{P}^1(\mathbb{F}_{p^{k/2}}), \\ (P,Q) &\mapsto \theta(e_r(P,Q)) = \theta(f_{r,P}(Q)^{(q^k-1)/r}) \end{aligned}$$

the *T_2-compressed Tate pairing.*

Corollary 3.12. *Let $P \in E(\mathbb{F}_p)[r]$ and $Q \in E(\mathbb{F}_{p^k})[r]$ with $Q \notin \langle P \rangle$. Let $f = f_{r,P}(Q) = f_0 + f_1\sigma$ be the value of the Miller function represented as an element of $\mathbb{F}_{p^k} = \mathbb{F}_{q^2}$ over $\mathbb{F}_q$. The T_2-compressed Tate pairing can be computed as*

$$\tau_{r,T_2}(P,Q) = (f_0/f_1 : 1)^{(p^{k/2}+1)/r},$$

where the exponentiation is done with respect to the multiplication $\star$ in $\mathbb{P}^1(\mathbb{F}_{p^{k/2}})$.

Proof. This is a simple consequence of Lemma 3.10 and the discussion before Definition 3.11. Note that $f \notin \mathbb{F}_q$ since $Q \notin \langle P \rangle$ and thus $\theta(f^{q-1}) = (f_0/f_1 : 1)$. □

3.3 Curves with a sextic twist

In this section, let p be a prime with $p \equiv 1 \pmod 3$, and let E be an elliptic curve over $\mathbb{F}_p$ with j-invariant $j(E) = 0$, i. e. $E : y^2 = x^3 + b$, $b \in \mathbb{F}_p$. Let r be a prime divisor of $n = \#E(\mathbb{F}_p)$, and let k be the embedding degree of E with respect to r. We assume in this section that k is divisible by 6, i. e. $k = 6m$ for $m \in \mathbb{N}$. We set $q := p^{k/6} = p^m$. Then $\mathbb{F}_q = \mathbb{F}_{p^m}$ and $\mathbb{F}_{q^6} = \mathbb{F}_{p^k}$.
It follows from Proposition 1.100 that there exists a twist E' of degree 6 over $\mathbb{F}_q$ with $r \mid \#E'(\mathbb{F}_q)$. We can choose $\xi \in \mathbb{F}_q^*$ such that the twist with the correct order is given by $E' : y^2 = x^3 + \xi^{-1}b$. Note that in this case, ξ is neither a square nor a cube in $\mathbb{F}_q$. An $\mathbb{F}_{q^6}$-isomorphism is given by

$$\psi : E' \to E, \ (x', y') \mapsto (\xi^{1/3}x', \xi^{1/2}y'). \tag{3.5}$$

The field extensions of $\mathbb{F}_q$ contained in $\mathbb{F}_{q^6}$ can be represented as $\mathbb{F}_{q^2} = \mathbb{F}_q(\xi^{1/2})$ and $\mathbb{F}_{q^3} = \mathbb{F}_q(\xi^{1/3})$, respectively. We aim at computing the twisted Tate pairing as introduced in Definition 1.102 in a compressed form, and recall its definition:

$$e'_r : G_1 \times G'_2 \to G_3, \ (P, Q') \mapsto e_r(P, \psi(Q')),$$

where $G_1 = E(\mathbb{F}_p)[r]$ and $G'_2 := E'(\mathbb{F}_q)[r]$. Miller functions are products of the line functions discussed in Lemma 1.93. We evaluate all functions at affine points, and thus a line function is equal to the defining polynomial $l_{U,V}$ of the corresponding line through the points U and V. In Miller's algorithm (see Section 1.2.3), the line function is evaluated at a point $Q \in E(\mathbb{F}_{q^6})[r]$, i. e. one computes $l_{U,V}(Q)$.

When computing the twisted Tate pairing, the points U and V are in $E(\mathbb{F}_p)$ and $Q = \psi(Q')$ for a point $Q' \in E'(\mathbb{F}_q)$. Let $U = (x_U, y_U)$, $V = (x_V, y_V)$, and $Q' = (x_{Q'}, y_{Q'})$. Hence $Q = (x_Q, y_Q) = (\tau x_{Q'}, \sigma y_{Q'})$, where $\sigma = \xi^{1/2} \in \mathbb{F}_{q^2}$ and $\tau = \xi^{1/3} \in \mathbb{F}_{q^3}$. Notice that $\sigma^q = -\sigma$ since $X^2 - \xi = (X - \sigma)(X + \sigma)$ and that $\mathbb{F}_{q^6} = \mathbb{F}_{q^3}(\sigma)$. Similarly, since

$$X^3 - \xi = (X - \tau)(X - \zeta\tau)(X - \zeta^2\tau)$$

for a primitive 3rd root of unity ζ, which lies in $\mathbb{F}_p$ since $p \equiv 1 \pmod 3$, we have $\tau^q = \zeta\tau$. For $U \neq -V$, the line function is

$$l_{U,V}(Q) = \lambda(x_Q - x_U) + (y_U - y_Q),$$

where λ is the slope of the line through U and V, i.e. $\lambda = (y_V - y_U)/(x_V - x_U)$ if $U \neq \pm V$ and $\lambda = (3x_U^2)/(2y_U)$ if $U = V$, respectively. In the case $U = -V$, the value of the line function is $l_{U,-U}(Q) = x_Q - x_U$, which is contained in $\mathbb{F}_{q^3}$. Such factors can be omitted in Miller's algorithm since they are mapped to 1 by the final exponentiation (see discussion before Proposition 1.103).

Lemma 3.13. *For $U \neq -V$ and $Q = \psi(Q')$ with $Q' \in E'(\mathbb{F}_q)$ of order r, we have*

$$\theta(l_{U,V}(Q)^{q^3-1}) = ((\lambda x_U - y_U - \lambda x_{Q'}\tau)/y_{Q'} : 1) \in \mathbb{P}^1(\mathbb{F}_{q^3}),$$

where θ is the function described in Proposition 3.6 (see also Remark 3.7).

Proof. We evaluate the line function at Q and obtain

$$\begin{aligned} l_{U,V}(Q) &= \lambda(\tau x_{Q'} - x_U) + (y_U - \sigma y_{Q'}) \\ &= (y_U - \lambda x_U + \lambda x_{Q'}\tau) - y_{Q'}\sigma. \end{aligned}$$

The coordinate $y_{Q'}$ is not zero since the point Q' has order r and $r > 2$. □

Remark 3.14. Although $(\lambda x_U - y_U - \lambda x_{Q'}\tau)/y_{Q'}$ is an element of $\mathbb{F}_{q^3}$, it could be computed with just 4 multiplications in $\mathbb{F}_q$ as $y_{Q'}^{-1} \cdot (\lambda \cdot x_U - y_U) - (y_{Q'}^{-1} \cdot \lambda \cdot x_{Q'})\tau$. Note that λ as well as the coordinates of all involved points are elements of $\mathbb{F}_q$. The inversion $y_{Q'}^{-1}$ can be done as a precomputation because Q' is fixed in the Miller loop. But we use a more efficient way, merging the computation with the subsequent multiplication.

Lemma 3.13 can be used to compute the compressed values of line functions arising in the Miller loop. For computing the T_2-compressed Tate pairing, we can thus do the first step of the final exponentiation—raising to the $(q^3 - 1)$th power—with the line functions and then compute the Miller loop with respect to the multiplication $\star$ in $\mathbb{P}^1(\mathbb{F}_{q^3})$. Of course, this can only be done since Miller functions are computed as products of line functions.
In Miller's algorithm, we need to carry out squarings and multiplications. Squarings are done with general elements in $\mathbb{P}^1(\mathbb{F}_{q^3})$. Multiplications always have a factor coming from a line function as in Lemma 3.13.

Lemma 3.15. *Let $\alpha \in T_2(\mathbb{F}_{q^3})$ with $\theta(\alpha) = (X_\alpha : 1)$ and $\beta = l_{U,V}(Q)^{q^3-1}$ as in Lemma 3.13. Define $\rho := \lambda x_U - y_U - \lambda x_{Q'}\tau \in \mathbb{F}_{q^3}$. Then it holds*

$$\theta(\alpha\beta) = \left(\frac{X_\alpha \rho + \xi y_{Q'}}{X_\alpha y_{Q'} + \rho} : 1\right).$$

Proof. This is an easy application of Lemma 3.8. □

There is no need to invert $y_{Q'}$ to compute $\theta(l_{U,V}(Q)^{q^3-1})$. Instead, we directly compute the product representative $\theta(\alpha\beta)$ as in the previous lemma.
For the assumptions in this section, the exponent of the final exponentiation is $(q^6-1)/r$, which we rewrite as

$$\frac{q^6-1}{r} = (q^3-1)(q+1)\frac{q^2-q+1}{r}.$$

It is $\Psi_6(q) = (q^3-1)(q+1)$. Instead of only computing $l_{U,V}(Q)^{q^3-1}$, we can compute $l_{U,V}(Q)^{\Psi_6(q)}$, and obtain an element in $T_6(\mathbb{F}_q)$ by Lemma 3.3. It is

$$T_6(\mathbb{F}_q) = \{\alpha \in \mathbb{F}_{q^6} \mid \alpha^{q^3+1} = 1 \text{ and } \alpha^{q^4+q^2+1} = 1\}.$$

Note that by the transitivity of the norm, the condition $N_{\mathbb{F}_{q^6}/\mathbb{F}_q}(\alpha) = 1$ follows from

$$N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(\alpha) = \alpha^{q^3+1} = 1.$$

This equality also implies

$$N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\alpha) = \alpha^{q^4+q^2+1} = \alpha^{q^2-q+1} = 1.$$

It is clear that $-1 \notin T_6(\mathbb{F}_q)$. By exploiting the norm conditions, it can be shown that 1 is the only element in $T_6(\mathbb{F}_q)$ that lies in a proper subfield of $\mathbb{F}_{q^6}$. Furthermore, it is clear that $T_6(\mathbb{F}_q) \subseteq T_2(\mathbb{F}_{q^3})$ (see Lemma 3.4). We next describe a compression technique that has also been demonstrated similarly by Granger, Page, and Stam [GPS06, Section 3.4].

Proposition 3.16. *Let $\alpha \in T_6(\mathbb{F}_q) \subseteq T_2(\mathbb{F}_{q^3})$. Let $\theta(\alpha) = (X_\alpha : Y_\alpha) \in \mathbb{P}^1(\mathbb{F}_{q^3})$, and if $Y_\alpha = 1$, let $X_\alpha = b_0 + b_1\tau + b_2\tau^2$ with $b_0, b_1, b_2 \in \mathbb{F}_q$. Define*

$$M_6 := \{(a_0, a_1) \in \mathbb{A}^2(\mathbb{F}_q) \mid a_1 \neq 0\} \cup \{(1,0)\}.$$

The map

$$\theta_6 : T_6(\mathbb{F}_q) \to M_6,\ \alpha \mapsto \begin{cases} (b_0, b_1) & \text{if } \alpha \neq 1, \\ (1,0) & \text{if } \alpha = 1 \end{cases}$$

is a bijection.

Proof. Let first α be such that $Y_\alpha = 1$, i. e. $\alpha = (X_\alpha - \sigma)/(X_\alpha + \sigma)$. We have $N_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\alpha) = 1$, i. e.

$$\left(\frac{X_\alpha - \sigma}{X_\alpha + \sigma}\right)^{q^2-q+1} = 1,$$

which is equivalent to $(X_\alpha - \sigma)^{q^2-q+1} = (X_\alpha + \sigma)^{q^2-q+1}$. We use the fact that $\tau^q = \zeta^2\tau$ for ζ a primitive third root of unity which lies in $\mathbb{F}_q$ since $q \equiv 1 \pmod 3$. An explicit computation of $(X_\alpha \pm \sigma)^{q^2-q+1}$ and simplification of the equation $(X_\alpha - \sigma)^{q^2-q+1} = (X_\alpha + \sigma)^{q^2-q+1}$ yields the relation $-3b_1b_2\xi + \xi + 3b_0^2 = 0$. If $b_1 \neq 0$, this equation can be used to recover b_2 from b_0 and b_1 as

$$b_2 = \frac{3b_0^2 + \xi}{3b_1\xi}. \tag{3.6}$$

If $b_1 = 0$, we have $\xi = -3b_0^2$. Since $p \equiv 1 \pmod 3$, -3 is a square modulo p and thus ξ is a square which is not true. Therefore, b_1 can not be 0. We may thus use $(1, 0)$ to represent $1 \in T_6(\mathbb{F}_q)$.
Summarizing, we see that since $T_6(\mathbb{F}_q) \subseteq T_2(\mathbb{F}_{q^3})$, $\alpha \in T_6(\mathbb{F}_q) \setminus \{1\}$ is uniquely determined by X_α, and X_α is uniquely determined by $(b_0, b_1) \in M_6$, which completes the proof. □

Corollary 3.17. *Let $\alpha \in \mathbb{F}_{q^6}^*$. Then $\alpha^{\Psi_6(q)}$ can be uniquely represented by a pair $(a_0, a_1) \in \mathbb{A}^2(\mathbb{F}_q)$.*

Proof. This is clear with Lemma 3.3 and Proposition 3.16. □

Multiplication formulas on M_6 (see Proposition 3.16) corresponding to the usual multiplication in $T_6(\mathbb{F}_q)$ can be derived from the arithmetic on $T_2(\mathbb{F}_{q^3})$ (Lemma 3.8).

Lemma 3.18. *Let $\alpha, \beta \in T_6(\mathbb{F}_q) \setminus \{1\}$ with $\theta_6(\alpha) = (a_0, a_1)$, $\theta_6(\beta) = (b_0, b_1)$, and $(a_0, a_1) \neq (-b_0, -b_1)$. Then $\theta_6(\alpha\beta) = (c_0, c_1)$, where c_0 and c_1 are given by the following formulas:*

$$\begin{aligned}
r_0 &= a_0^2 + \tfrac{1}{3}\xi, & r_1 &= b_0^2 + \tfrac{1}{3}\xi,\\
s_0 &= \xi(a_1b_1(a_0b_0 + \xi) + a_1^2r_1 + b_1^2r_0), & s_1 &= a_1b_1\xi(a_0b_1 + a_1b_0) + r_0r_1,\\
s_2 &= a_1^2b_1^2\xi + a_0a_1r_1 + b_0b_1r_0, & t_0 &= a_1b_1\xi(a_0 + b_0),\\
t_1 &= a_1b_1\xi(a_1 + b_1), & t_2 &= b_1r_0 + a_1r_1,\\
u &= t_0^3 + t_1^3\xi + t_2^3\xi^2 - 3\xi t_0t_1t_2, & u_0 &= t_0^2 - t_1t_2\xi,\\
u_1 &= t_2^2\xi - t_0t_1, & u_2 &= t_1^2 - t_0t_2,\\
v_0 &= s_0u_0 + s_1u_2\xi + s_2u_1\xi, & v_1 &= s_0u_1 + s_1u_0 + s_2u_2\xi,\\
c_0 &= \frac{v_0}{u}, & c_1 &= \frac{v_1}{u}.
\end{aligned}$$

Furthermore, $\theta_6(\alpha^2) = (d_0, d_1)$ *with* d_0 *and* d_1 *given as follows:*

$$\begin{aligned} r_0 &= a_0^5 + \xi(a_0^3 - 2a_0^2a_1^3) + \xi^2(\tfrac{1}{3}a_0 - a_1^3), & r_1 &= a_0^5 + \xi(2a_0^3 - 2a_0^2a_1^3) + \xi^2(a_0 - 2a_1^3), \\ s_0 &= a_0(a_0r_0 + a_1^6\xi^2 + \tfrac{1}{27}\xi^3) - \tfrac{1}{3}a_1^3\xi^3, & s_1 &= a_1(a_0r_1 + a_1^6\xi^2 + \tfrac{4}{27}\xi^3), \\ s &= 2(a_0r_0 + a_1^6\xi^2 + \tfrac{1}{27}\xi^3), & d_0 &= \frac{s_0}{s},\ d_1 = \frac{s_1}{s}. \end{aligned}$$

Proof. The formulas can be derived from Lemma 3.8. We show how to verify them in Appendix A.1. □

We split up the final exponentiation into two parts again. The exponent of the first part is $\Psi_6(q)$ and that of the remaining second part is $(q^2 - q + 1)/r$. After the first part, the result lies in $T_6(\mathbb{F}_q)$.

Definition 3.19. Let e_r be the reduced Tate pairing on E. The map

$$\begin{aligned} \tau_{r,T_6} : E(\mathbb{F}_p)[r] \times E(\mathbb{F}_{p^k})[r] &\to M_6, \\ (P, Q) &\mapsto \theta_6(e_r(P, Q)) = \theta_6(f_{r,P}(Q)^{(q^k-1)/r}) \end{aligned}$$

is called the T_6*-compressed Tate pairing.*

Corollary 3.20. *Let* $P \in E(\mathbb{F}_p)[r]$ *and* $Q \in E(\mathbb{F}_{p^k})[r]$ *with* $Q \notin \langle P \rangle$*. Let* $(f_1, f_2) = \theta_6(f_{r,P}(Q)^{\Psi_6(p^m)})$*. The* T_6*-compressed Tate pairing can be computed as*

$$\tau_{r,T_6}(P, Q) = (f_1, f_2)^{(p^{2m}-p^m+1)/r},$$

where the exponentiation is done with respect to the multiplication in M_6 *given by the formulas in Lemma 3.18.*

As for the T_2-compressed pairing, we can exponentiate the line functions to the first part of the final exponentiation, and perform the Miller loop completely in compressed representation. The compressed representation of line function values can be computed directly from the coordinates of the points involved.

Proposition 3.21. *Let* $\zeta \in \mathbb{F}_p$ *be a primitive third root of unity such that* $\tau^q = \zeta\tau$*. Let* $\beta = l_{U,V}(Q)^{\Psi_6(q)}$ *with* $U \neq -V$ *and* $Q = \psi(Q')$*. If* $\beta \neq 1$*, then* $\theta_6(\beta) = (c_0, c_1) \in \mathbb{A}^2(\mathbb{F}_q)$ *with*

$$c_0 = \left(\frac{-\zeta^2}{1-\zeta}y_{Q'}^{-1}\right)(y_U - \lambda x_U),\ c_1 = \left(\frac{\zeta}{1-\zeta}y_{Q'}^{-1}\right)\lambda x_{Q'}. \tag{3.7}$$

Proof. Let $\alpha = l_{U,V}(Q)^{q^3-1}$. By assumption, we have $\alpha^{q+1} = l_{U,V}(Q)^{\Psi_6(q)} \neq 1$. Let $\theta(\alpha) = (X_\alpha : 1)$, i. e. $\alpha = l_{U,V}(Q)^{q^3-1} = \frac{X_\alpha - \sigma}{X_\alpha + \sigma}$. It is

$$\beta = \alpha^{q+1} = \left(\frac{X_\alpha - \sigma}{X_\alpha + \sigma}\right)^{q+1}.$$

We determine X_β from

$$\beta = \left(\frac{X_\alpha - \sigma}{X_\alpha + \sigma}\right)^q \cdot \frac{X_\alpha - \sigma}{X_\alpha + \sigma} = \frac{X_\alpha^q + \sigma}{X_\alpha^q - \sigma} \cdot \frac{X_\alpha - \sigma}{X_\alpha + \sigma} = \frac{-X_\alpha^q - \sigma}{-X_\alpha^q + \sigma} \cdot \frac{X_\alpha - \sigma}{X_\alpha + \sigma}.$$

Since $\beta \neq 1$, it is $X_\alpha^q \neq X_\alpha$. By applying (3.2), we get $X_\beta = (-X_\alpha^{q+1} + \xi)/(-X_\alpha^q + X_\alpha)$. Lemma 3.13 shows that $X_\alpha = (\lambda x_U - y_U - \lambda x_{Q'}\tau)/y_{Q'}$. We thus obtain

$$-X_\alpha^q = \frac{y_U - \lambda x_U + \lambda x_{Q'}\zeta\tau}{y_{Q'}}.$$

Multiplying with X_α yields

$$-X_\alpha^{q+1} = -\frac{1}{y_{Q'}^2}\Big((y_U - \lambda x_U)^2 + (1+\zeta)\lambda x_{Q'}(y_U - \lambda x_U)\tau + \lambda^2 x_{Q'}^2 \zeta\tau^2\Big).$$

For the denominator of X_β, we obtain

$$-X_\alpha^q + X_\alpha = \frac{\lambda x_{Q'}(\zeta - 1)\tau}{y_{Q'}}$$

and determine X_β as

$$\begin{aligned} X_\beta &= \frac{(1+\zeta)\lambda x_{Q'}(y_U - \lambda x_U)\xi + \lambda^2 x_{Q'}^2 \zeta\xi\tau + ((y_U - \lambda x_U)^2 - \xi y_{Q'}^2)\tau^2}{\lambda(1-\zeta)x_{Q'}y_{Q'}\xi} \\ &= \frac{1+\zeta}{1-\zeta} \cdot \frac{y_U - \lambda x_U}{y_{Q'}} + \frac{\zeta}{1-\zeta} \cdot \frac{\lambda x_{Q'}}{y_{Q'}}\tau + \frac{(y_U - \lambda x_U)^2 - \xi y_{Q'}^2}{\lambda(1-\zeta)x_{Q'}y_{Q'}\xi}\tau^2. \end{aligned}$$

Recall that $\tau^3 = \xi$. Taking c_i the coefficient at τ^i in the above expression we have the property $c_2 = (3c_0^2 + \xi)/(3c_1\xi)$, and thus c_2 can be computed from c_0 and c_1. □

Remark 3.22. The input Q is not changed in the course of Miller's algorithm. Hence, $y_{Q'}^{-1}$ can be precomputed before the loop. Note also that $-\zeta^2/(1-\zeta)y_{Q'}^{-1}$ and $\zeta/(1-\zeta)y_{Q'}^{-1}$ can be determined in a precomputation and that we do not need inversions to compute the values of the exponentiated line functions inside the Miller loop.

Multiplication in $\mathbb{A}^2(\mathbb{F}_q)$ corresponding to the multiplication in $T_6(\mathbb{F}_q)$ needs inversions as can be seen from the formulas in Lemma 3.18. One can replace inversion of an element a in $\mathbb{F}_{p^m}$ by an inversion in $\mathbb{F}_p$ and at most $\lfloor \lg m \rfloor + 1$ multiplications in $\mathbb{F}_{p^m}$ by

$$\frac{1}{a} = \frac{a^{p+p^2+\cdots+p^{m-1}}}{N_{\mathbb{F}_{p^m}/\mathbb{F}_p}(a)}.$$

The term in the numerator can be computed by addition-chain methods. For details see Section 11.3.4 in [Doc05b].

But it is possible to completely avoid inversions in Miller's algorithm by storing the denominator in a separate coordinate, or in other words, by moving to projective representation. We embed $\mathbb{A}^2(\mathbb{F}_q)$ into $\mathbb{P}^2(\mathbb{F}_q)$ as usual with the map $\varphi_3^{-1} : \mathbb{A}^2(\mathbb{F}_q) \to \mathbb{P}^2(\mathbb{F}_q)$, $(c_0, c_1) \mapsto (c_0 : c_1 : 1)$ (for notation see Subsection 1.1.1).

Definition 3.23. We define the compression function

$$\tilde{\theta}_6 : T_6(\mathbb{F}_q) \to \mathbb{P}^2(\mathbb{F}_q),\ \alpha \mapsto \varphi_3^{-1}(\theta(\alpha)).$$

The compressed line functions computed in Proposition 3.21 can be given as elements of $\mathbb{P}^2(\mathbb{F}_q)$.

Lemma 3.24. *Let assumptions be as in Proposition 3.21. Let $\mu, \nu \in \mathbb{F}_p$ be the numerator and denominator of the slope λ, i. e. $\mu = y_V - y_U, \nu = x_V - x_U$ if $U \neq \pm V$ and $\mu = 3x_U^2, \nu = 2y_U$ if $U = V$, respectively. Then $\tilde{\theta}_6(l_{U,V}(Q)^{\Psi_6(q)}) = (C_0 : C_1 : C)$, where*

$$C_0 = \left(\frac{-\zeta^2}{1-\zeta}\right)(\nu y_U - \mu x_U),\ C_1 = \left(\frac{\zeta}{1-\zeta}\right)\mu x_{Q'},\ C = \nu y_{Q'}. \tag{3.8}$$

Proof. The representation follows by multiplying with all denominators. □

When $m > 1$, we are able to compress further. The denominator C which has to be stored in a third coordinate can be replaced by a denominator which is an element in $\mathbb{F}_p$, namely the norm $N_{\mathbb{F}_{p^m}/\mathbb{F}_p}(C)$ of the previous denominator in $\mathbb{F}_q$. We only need to multiply the other two coordinates by $C^{p+p^2+\cdots+p^{m-1}}$.
The methods described make it possible to completely avoid inversions during pairing computation. Taking into account that inversion of torus elements can be done by negating the representative, we also do not need finite field inversions for the final exponentiation. Normally, an inversion is needed to efficiently implement the exponentiation by using the Frobenius automorphism.
We give an example of the squaring and multiplication formulas in $\mathbb{P}^2(\mathbb{F}_q)$ that correspond to squaring and multiplication in $T_6(\mathbb{F}_q)$ for embedding degree $k = 12$.

Example 3.25. For embedding degree 12, we have $q = p^2$. Let $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ and $i^2 = -z$ for some element $z \in \mathbb{F}_p$. Let $(A_0 : A_1 : A)$ be an element in compressed form, i.e. $A_0, A_1 \in \mathbb{F}_{p^2}$ and $A \in \mathbb{F}_p$. We can compute the square $(C_0 : C_1 : C)$ as follows:

$$\begin{aligned}
R_0 &= A_0^5 + \xi(A_0^3A^2 - 2A_0^2A_1^3) + \xi^2(\tfrac{1}{3}A_0A^4 - A_1^3A^2),\\
R_1 &= A_0^5 + 2\xi(A_0^3A^2 - A_0^2A_1^3) + \xi^2(A_0A^4 - 2A_1^3A^2),\\
S_0 &= A_0(A_0R_0 + A_1^6\xi^2 + \tfrac{1}{27}A^6\xi^3) - \tfrac{1}{3}A_1^3A^4\xi^3,\\
S_1 &= A_1(A_0R_1 + A_1^6\xi^2 + \tfrac{4}{27}A^6\xi^3),\\
S &= 2A(A_0R_0 + A_1^6\xi^2 + \tfrac{1}{27}A^6\xi^3).
\end{aligned}$$

Write $S = s_0 + is_1$ with $s_0, s_1 \in \mathbb{F}_p$. Then the square is given by

$$C_0 = S_0(s_0 - is_1),\ C_1 = S_1(s_0 - is_1),\ C = s_0^2 + zs_1^2.$$

To multiply two compressed elements $(A_0 : A_1 : A)$ and $(B_0 : B_1 : B)$ we can use the following formulas:

$$\begin{aligned}
R_0 &= A_0^2 + \tfrac{1}{3}A^2\xi,\ R_1 = B_0^2 + \tfrac{1}{3}B^2\xi,\\
S_0 &= \xi(A_1B_1(A_0B_0 + \xi AB) + A_1^2R_1 + B_1^2R_0),\\
S_1 &= A_1B_1\xi(A_0B_1 + A_1B_0) + R_0R_1,\ S_2 = A_1^2B_1^2\xi + A_0A_1R_1 + B_0B_1R_0,\\
T_0 &= A_1B_1\xi(A_0B + B_0A),\ T_1 = A_1B_1\xi(A_1B + B_1A),\ T_2 = B_1BR_0 + A_1AR_1,\\
T &= T_0^3 + T_1^3\xi + T_2^3\xi^2 - 3\xi T_0T_1T_2,\\
U_0 &= T_0^2 - T_1T_2\xi,\ U_1 = T_2^2\xi - T_0T_1,\ U_2 = T_1^2 - T_0T_2,\\
V_0 &= S_0U_0 + S_1U_2\xi + S_2U_1\xi,\ V_1 = S_0U_1 + S_1U_0 + S_2U_2\xi.
\end{aligned}$$

Write $T = t_0 + it_1$, where $t_0, t_1 \in \mathbb{F}_p$. Then the product $(C_0 : C_1 : C)$ of the two elements is given by

$$C_0 = V_0(t_0 - it_1),\ C_1 = V_1(t_0 - it_1),\ C = t_0^2 + zt_1^2.$$

These formulas are homogenized versions of the formulas given in Lemma 3.18 where the denominators are kept in an additional variable. Correctness of the formulas in this lemma can be checked with the help of Appendix A.1. The only difference is that in the end, we compute the $\mathbb{F}_p$-norm of the denominator to keep it as small as possible. We thus have to multiply the numerators with the denominator's conjugate in $\mathbb{F}_{p^2}$.
For an implementation of a pairing algorithm in compressed form without inversions, one can use (3.8) to compute the evaluated compressed line functions, and then use the above formulas for squaring and multiplication in Miller's algorithm. The remaining part of the exponent for the final exponentiation is $(p^4 - p^2 + 1)/n$. The final pairing value can be computed by use of the Frobenius automorphism and a square-and-multiply algorithm with the above squaring and multiplication formulas (see Devegili, Scott, and Dahab [DSD07]). A three-operand pseudo code for these formulas is given in Appendix A.

3.4 Implementation

In order to evaluate the performance of the compressed pairing computation, we implemented several pairing algorithms in C. For all these implementations[1] we used the BN curve $E : y^2 = x^3 + 24$ over $\mathbb{F}_p$ with parameters described in Table 3.1. This curve has also been used for the performance evaluation of pairing algorithms by Devegili, Scott, and Dahab in [DSD07]. To ease comparison with [DOSD06] and [DSD07], we implemented pairing algorithms with $\mathbb{F}_{p^{12}}$ constructed as a quadratic extension on top of a cubic extension which is again built on top of a quadratic extension, as described in [DSD07] and by Devegili, Scott, Ó hÉigeartaigh, and

[1] The code of the implementation can be found at http://www.cryptojedi.org/crypto/

p	824340166543006797212173535031900388365717818113862289211673224128190294931 83
n	824340166543006797212173535031900388362846685642966864301145100525564013737 69
bitsize	256
t	28711324708954249105281236026262811941 5
k	12
λ^c	$(t-1)^8 \mod n$

Table 3.1: Parameters of the curve used in our implementation

Dahab in [DOSD06]. For ate, generalized Eta, and Tate pairings we thus achieve similar timings as [DSD07]. We did not use windowing methods since the group order of the chosen curve is sparse. The final exponentiation for the non-compressed pairings uses the decomposition of the exponent $(p^{12}-1)/n$ into the factors (p^6-1), (p^2+1), and $(p^4-p^2+1)/n$.
In the Miller loop we entirely avoided field inversions by computing the elliptic curve operations in Jacobian coordinates (see [DL05a, Section 13.2.1.c]) and by using the compressed representation and storing denominators separately as described in Example 3.25. For multiplication and squaring of torus elements, we used the algorithms stated in Appendix A.2. Timing results are given in Table 3.2.

	Core 2 Quad Q6600
Tate	32835888
Compressed Tate	53160480
Generalized Eta	26795205
Compressed generalized Eta	42471414
ate	22861386
Optimal ate	16231797

Table 3.2: Performance measurements for different pairing variants on an Intel Core 2 Quad CPU Q6600 running at 2394 MHz using only one core. Numbers give the median of 1000 measurements for a complete pairing computation including Miller loop and final exponentiation in CPU cycles.

Chapter 4

Pairings on Edwards curves

In this chapter, we consider pairings on a twisted Edwards curve

$$E_{a,d} : Z^2(aX^2 + Y^2) = Z^4 + dX^2Y^2$$

over a finite field $\mathbb{F}_q$, where a, d are nonzero and distinct elements of $\mathbb{F}_q$. If $a = 1$, i. e. if we have a plain Edwards curve, we denote $E_{1,d}$ simply by E_d. As in Subsection 1.1.7 of Chapter 1, we denote by $\mathcal{O} = (0 : 1 : 1)$ the neutral element in $E_{a,d}(\mathbb{F}_q)$ and by $\mathcal{O}' = (0 : -1 : 1)$ its reflection across the x-axis, which is a point of order 2. The point $\mathcal{T} = (1/\sqrt{a} : 0 : 1)$ has order 4. Then $[2]\mathcal{T} = \mathcal{O}'$ and $-\mathcal{T} = [3]\mathcal{T} = (-1/\sqrt{a} : 0 : 1)$. Let the two singular points at infinity be denoted by $\Omega_1 = (1 : 0 : 0)$ and $\Omega_2 = (0 : 1 : 0)$. Let $f_{E_{a,d}} = Z^2(aX^2 + Y^2) - Z^4 - dX^2Y^2$ be the polynomial defining the curve $E_{a,d}$.

For pairing computation on Weierstraß curves, we need line functions that are evaluated in Miller's algorithm (see Subsection 1.2.3). In the case of twisted Edwards curves, the analogue procedure leads to functions arising from lines and conics. This chapter contains results from joint work with Arène, Lange, and Ritzenthaler. Section 4.1 states properties of lines and conics passing through points on twisted Edwards curves. In Section 4.2, we give a geometric interpretation of the group law on twisted Edwards curves. We show how pairings can be computed using functions coming from the lines and conics described in Section 4.1. Explicit formulas for the doubling and addition steps in Miller's algorithm are derived in Section 4.3. The formulas are significantly faster than any reported so far for Edwards curves. Let the curve be defined over $\mathbb{F}_p$, and let k be its embedding degree. Then an addition step needs $1\mathbf{M} + (k+14)\mathbf{m} + 1\mathbf{m_a}$, a doubling step costs $1\mathbf{M} + 1\mathbf{S} + (k+6)\mathbf{m} + 5\mathbf{s} + 2\mathbf{m_a}$, where one multiplication in $\mathbb{F}_{p^k}$ is denoted by $1\mathbf{M}$ and one squaring in the same field by $1\mathbf{S}$. Multiplication and squaring in the smaller field $\mathbb{F}_p$ are denoted by $1\mathbf{m}$ and $1\mathbf{s}$, respectively. Furthermore, we use $1\mathbf{m_a}$ for a multiplication with the constant a. The above costs are for both points in projective Edwards coordinates. Using mixed addition, i. e. the second point in affine coordinates, an addition step costs only $1\mathbf{M} + (k + 12)\mathbf{m} + 1\mathbf{m_a}$.

4.1 Lines and conics

Let $\mathbb{F}$ be an arbitrary field of characteristic different from 2 and $\overline{\mathbb{F}}$ an algebraic closure of $\mathbb{F}$. The points $\mathcal{O}, \mathcal{O}', \mathcal{T}, \Omega_1, \Omega_2$ are all points in the projective plane $\mathbb{P}^2(\overline{\mathbb{F}})$. We begin with projective lines in $\mathbb{P}^2(\overline{\mathbb{F}})$. A general line is of the form

$$L : c_X X + c_Y Y + c_Z Z = 0, \tag{4.1}$$

where $(c_X : c_Y : c_Z) \in \mathbb{P}^2(\overline{\mathbb{F}})$ (see Example 1.7). A line is uniquely determined by two different points. We first consider lines that pass through one of the points at infinity and an affine point P. Note that the line through Ω_1 and Ω_2 is the line at infinity $L_\infty : Z = 0$.

Lemma 4.1. *Let $P = (X_0 : Y_0 : Z_0) \in \mathbb{P}^2(\overline{\mathbb{F}})$ be an affine point, i. e. $Z_0 \neq 0$, and let $L_{1,P}$ be the projective line passing through P and Ω_1. Then $L_{1,P}$ is a horizontal line of the form*

$$L_{1,P} : Z_0 Y - Y_0 Z = 0.$$

Let $L_{2,P}$ be the line through P and Ω_2. Then $L_{2,P}$ is a vertical line

$$L_{2,P} : Z_0 X - X_0 Z = 0.$$

Proof. We use the general equation of a line (4.1). From $\Omega_1 \in L_{1,P}$, we see that $c_X = 0$, and from $P \in L_{1,P}$, it follows that $c_Z Z_0 = -c_Y Y_0$. Assume $c_Y = 0$, then $c_Z = 0$, which yields a contradiction. Therefore, we may write $L_{1,P}$ in the desired form. The equation for $L_{2,P}$ follows analogously. □

In the following, we describe a special conic which passes through both points at infinity, Ω_1 and Ω_2, the point $\mathcal{O}'$, and two arbitrary affine points P_1 and P_2 on $E_{a,d}$. A general conic can be written as

$$C : c_{X^2} X^2 + c_{Y^2} Y^2 + c_{Z^2} Z^2 + c_{XY} XY + c_{XZ} XZ + c_{YZ} YZ = 0, \tag{4.2}$$

where $(c_{X^2} : c_{Y^2} : c_{Z^2} : c_{XY} : c_{XZ} : c_{YZ}) \in \mathbb{P}^5(\overline{\mathbb{F}})$ (see Example 1.7). Let $f_C = c_{X^2} X^2 + c_{Y^2} Y^2 + c_{Z^2} Z^2 + c_{XY} XY + c_{XZ} XZ + c_{YZ} YZ$ be the polynomial of C. First we only assume that the points at infinity and $\mathcal{O}'$ are on C.

Lemma 4.2. *If a conic C passes through the points Ω_1, Ω_2, and $\mathcal{O}'$, then it has an equation of the form*

$$C : c_{Z^2}(Z^2 + YZ) + c_{XY} XY + c_{XZ} XZ = 0, \tag{4.3}$$

where $(c_{Z^2} : c_{XY} : c_{XZ}) \in \mathbb{P}^2(\overline{\mathbb{F}})$.

Proof. We evaluate f_C at the three points Ω_1, Ω_2, and $\mathcal{O}'$. The fact that Ω_1 lies on the conic implies $c_{X^2} = 0$. Similarly, $c_{Y^2} = 0$ since Ω_2 lies on C. Further, the condition $\mathcal{O}' \in C$ shows that $c_{YZ} = c_{Z^2}$. □

We have a closer look at conics C as described in the above lemma. The following lemma shows that if there is an affine singular point on C, the conic is the product of a vertical and a horizontal line.

Lemma 4.3. *Let C be a conic passing through Ω_1, Ω_2, and $\mathcal{O}'$, i. e. C is given by (4.3). Let $P = (X_1 : Y_1 : Z_1)$ be a singular point on C. Then C splits as the product of two lines that intersect in P, and one of the following cases occurs:*

(a) The conic is given by $C : X(Z_1Y - Y_1Z) = 0$ and $X_1 = 0$, i. e. P lies on the line $X = 0$. In particular, we have $c_{Z^2} = 0$, $c_{XY} = Z_1$, and $c_{XZ} = -Y_1$.

(b) The conic is given by $C : (Z_1X - X_1Z)(Y + Z) = 0$ and $Y_1 = -Z_1$, i. e. P lies on the line $Y + Z = 0$. In particular, we have $c_{Z^2} = -X_1$ and $c_{XY} = Z_1 = c_{XZ}$.

(c) The conic is given by $C : (Y_1X - X_1(Y + Z))Z = 0$ and $Z_1 = 0$, i. e. P lies on the line $Z = 0$ at infinity. In particular, we have $c_{Z^2} = -X_1$, $c_{XY} = 0$, and $c_{XZ} = Y_1$.

Proof. An irreducible conic is always nonsingular (see [Ful69, Theorem 2, p. 117]). Thus we know that f_C splits into two linear factors as

$$f_C = (a_1X + b_1Y + c_1Z)(a_2X + b_2Y + c_2Z).$$

From Bézout's Theorem (Theorem 1.21), we know that two lines have exactly one intersection point or are identical. Because there is no line passing through Ω_1, Ω_2, and $\mathcal{O}'$, there must be exactly one intersection point of the lines $a_1X+b_1Y+c_1Z = 0$ and $a_2X + b_2Y + c_2Z = 0$, which then must be equal to P since all other points are nonsingular.
We expand the product and obtain $f_C = a_1a_2X^2+b_1b_2Y^2+c_1c_2Z^2+(a_1b_2+a_2b_1)XY+(a_1c_2 + a_2c_1)XZ + (b_1c_2 + b_2c_1)YZ$. Then (4.3) implies that a_1 or a_2 is equal to 0. Without loss of generality, we assume $a_2 = 0$. Then f_C becomes $b_1b_2Y^2 + c_1c_2Z^2 + a_1b_2XY + a_1c_2XZ + (b_1c_2 + b_2c_1)YZ$.
Since the Y^2-term must vanish, either b_1 or b_2 is 0. If $b_1 = 0$, we have $f_C = c_1c_2Z^2 + a_1b_2XY + a_1c_2XZ + c_1b_2YZ$ and $c_1c_2 = c_1b_2$. If $c_1 = 0$, then a_1 must be different from 0 and we arrive at case (a). For $c_1 \neq 0$, it follows $c_2 = b_2 \neq 0$ and case (b) is valid.
Finally, if $b_2 = 0$, then $c_2 \neq 0$, and the conic is $C : c_1Z^2 + a_1XZ + b_1YZ$. It follows that $b_1 = c_1$, which yields case (c). □

We are now able to describe the conic that passes through Ω_1, Ω_2, and $\mathcal{O}'$ as well as through two affine points P_1 and P_2. If the latter points are equal, we consider intersection multiplicities of C with $E_{a,d}$, which usually means that C and $E_{a,d}$ have the same tangent at $P_1 = P_2$.

Proposition 4.4. *Let $E_{a,d}$ be a twisted Edwards curve over $\mathbb{F}$, and let $P_1 = (X_1 : Y_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : Z_2)$ be two affine, not necessarily distinct points on*

$E_{a,d}$. Let C be the conic passing through Ω_1, Ω_2, $\mathcal{O}'$, P_1, and P_2, i. e. C is given by an equation of the form (4.3). If some of the above points are equal, we count them as one point with multiplicity and consider C and $E_{a,d}$ to intersect with at least that multiplicity at the corresponding point. Then the coefficients in (4.3) are given as follows:

(a) If $P_1 \neq P_2$, $P_1 \neq \mathcal{O}'$, and $P_2 \neq \mathcal{O}'$,

$$\begin{aligned} c_{Z^2} &= X_1X_2(Y_1Z_2 - Y_2Z_1), \\ c_{XY} &= Z_1Z_2(X_1Z_2 - X_2Z_1 + X_1Y_2 - X_2Y_1), \\ c_{XZ} &= X_2Y_2Z_1^2 - X_1Y_1Z_2^2 + Y_1Y_2(X_2Z_1 - X_1Z_2). \end{aligned}$$

(b) If $P_1 \neq P_2 = \mathcal{O}'$,

$$c_{Z^2} = -X_1,\ c_{XY} = Z_1,\ c_{XZ} = Z_1.$$

(c) If $P_1 = P_2$,

$$\begin{aligned} c_{Z^2} &= X_1Z_1(Y_1 - Z_1), \\ c_{XY} &= Z_1^3 - dX_1^2Y_1, \\ c_{XZ} &= Z_1(aX_1^2 - Y_1Z_1). \end{aligned}$$

Proof. We start by proving the case $P_1 \neq P_2$ and $P_1, P_2 \notin \{\mathcal{O}, \mathcal{O}'\}$, which, together with the assumption of P_1, P_2 being affine, means that X_1, X_2, Z_1, and Z_2 are all different from 0. Since $P_1, P_2 \in C$, we obtain the two equations

$$\begin{aligned} c_{Z^2}Z_1(Z_1 + Y_1) + c_{XY}X_1Y_1 + c_{XZ}X_1Z_1 &= 0, \\ c_{Z^2}Z_2(Z_2 + Y_2) + c_{XY}X_2Y_2 + c_{XZ}X_2Z_2 &= 0. \end{aligned}$$

We may solve both for $c_{XZ} = -c_{XY}Y_i/Z_i - c_{Z^2}(Z_i/X_i + Y_i/X_i)$, $i \in \{1, 2\}$, equate them, and multiply with denominators to get

$$c_{Z^2}Z_1Z_2(Z_2X_1 - Z_1X_2 + Y_2X_1 - Y_1X_2) = c_{XY}X_1X_2(Y_1Z_2 - Y_2Z_1).$$

Thus we may choose $c_{Z^2} = X_1X_2(Y_1Z_2 - Y_2Z_1)$ and $c_{XY} = Z_1Z_2(Z_2X_1 - Z_1X_2 + Y_2X_1 - Y_1X_2)$, then compute $c_{XZ} = X_2Y_2Z_1^2 - X_1Y_1Z_2^2 + Y_1Y_2(X_2Z_1 - X_1Z_2)$, and we obtain the formulas in (a). We still need to prove that the same formulas hold if $P_1 = \mathcal{O}$ or $P_2 = \mathcal{O}$. Without loss of generality, we assume $P_2 = \mathcal{O} = (0 : 1 : 1)$. Evaluating f_C at $\mathcal{O}$ shows that $c_{Z^2} = 0$. Since $X_1 \neq 0$, the fact that $P_1 \in C$ then yields $c_{XY}Y_1 + c_{XZ}Z_1 = 0$. Thus we may choose $c_{XY} = Z_1$ and $c_{XZ} = -Y_1$. The formulas in (a) for $P_2 = \mathcal{O}$ give $c_{Z^2} = 0$, $c_{XY} = 2X_1Z_1$, and $c_{XZ} = -2X_1Y_1$. Again $X_1 \neq 0$ implies that this describes the same conic and we see that the formulas are the same in that case. It can be checked by explicit calculations that the coefficients can not all be equal to 0 at the same time. Assuming so implies that $P_1 = P_2$, which we excluded in (a). This completes the proof of part (a).

We first prove (c) for $P_1 = P_2 \notin \{\mathcal{O}, \mathcal{O}'\}$, i. e. we have that $X_1 \neq 0$. By assumption, $Z_1 \neq 0$. The conic C needs to intersect the curve $E_{a,d}$ with multiplicity 2 at P_1. Since P_1 is an affine point, we may consider the dehomogenizations

$$(f_C)_* = f_C(x, y, 1) = c_{XY}xy + c_{XZ}x + c_{Z^2}(y + 1)$$

of f_C and

$$(f_{E_{a,d}})_* = f_{E_{a,d}}(x, y, 1) = ax^2 + y^2 - 1 - dx^2y^2$$

of $f_{E_{a,d}}$ as well as the affine notation for $P_1 = (x_1, y_1)$, where $x_1 = X_1/Z_1$ and $y_1 = Y_1/Z_1$. Since P_1 does not lie on any of the lines in Lemma 4.3, it is a nonsingular point on C. Note that case (b) in Lemma 4.3 does not occur because $Y_1 = -Z_1$ only holds for $P_1 = \mathcal{O}'$, which we excluded. Thus the intersection multiplicity is larger than 1 if C and $E_{a,d}$ have equal tangents in P_1 (see Lemma 1.20 (c)). The tangent lines to C and $E_{a,d}$ in P_1 are

$$\begin{aligned} T_{C,P_1} : (c_{XY}y_1 + c_{XZ})(x - x_1) + (c_{XY}x_1 + c_{Z^2})(y - y_1) &= 0, \\ T_{E_{a,d},P_1} : \quad 2x_1(a - dy_1^2)(x - x_1) + 2y_1(1 - dx_1^2)(y - y_1) &= 0 \end{aligned}$$

(see Definition 1.16). They are equal if $(c_{XY}x_1 + c_{Z^2})2x_1(a - dy_1^2) = (c_{XY}y_1 + c_{XZ})2y_1(1 - dx_1^2)$. Using $P_1 \in C$, we express c_{XZ} by $c_{XZ} = -c_{XY}y_1 - c_{Z^2}(y_1 + 1)/x_1$. Note that $x_1 \neq 0$. We combine the last two equations, multiply by x_1, reorder, apply the Edwards curve equation, and arrive at

$$(1 + y_1)(1 - dx_1^2y_1)c_{Z^2} = -x_1(1 - y_1^2)c_{XY}.$$

Since $P_1 \neq \mathcal{O}'$, we have $y_1 \neq -1$ and we can simplify to $(1 - dx_1^2y_1)c_{Z^2} = -x_1(1 - y_1)c_{XY}$. From this, we see that we can choose $c_{Z^2} = -x_1(1 - y_1)$ and $c_{XY} = 1 - dx_1^2y_1$. We compute $c_{XZ} = ax_1^2 - y_1$ with help of the curve equation. We homogenize the formulas by setting $x_1 = X_1/Z_1$ and $y_1 = Y_1/Z_1$, multiply by Z_1^3, and obtain the formulas claimed in part (c). As for (a), we now prove that the same formulas hold if $P_1 = \mathcal{O}$. To achieve the intersection multiplicity at least 2 at $\mathcal{O}$, we may use the singular conic C being the product of the line $Y = Z$ tangent to $E_{a,d}$ in $\mathcal{O}$ and the line $X = 0$ passing through the point $\mathcal{O}'$. Thus $f_C = X(Z - Y) = XZ - XY$, so $c_{Z_2} = 0$, $c_{XY} = -1$, and $c_{XZ} = 1$. The same values arise when evaluating the formulas under (c) at $P_1 = \mathcal{O}$. Furthermore, the same formulas hold if $P_1 = \mathcal{O}'$ since intersection multiplicity 3 at $\mathcal{O}'$ is achieved by setting $f_C = X(Y + Z) = XY + XZ$. Again, not all three coefficients can be 0, because this implies $a = d$. This is a contradiction and therefore, we have proved (c).

Next we deal with the case $P_1 \neq P_2 = \mathcal{O}'$. The conic C and the curve $E_{a,d}$ must intersect in $\mathcal{O}'$ with multiplicity 2. We may use a singular conic that is the product of the line $Y + Z = 0$, which is tangent to $E_{a,d}$ in $\mathcal{O}'$, and the vertical line $Z_1X - X_1Z$ through P_1. Thus $f_C = (Z_1X - X_1Z)(Y + Z) = -X_1Z(Z + Y) + Z_1XY + Z_1XZ$ shows that $c_{Z^2} = -X_1$, $c_{XY} = Z_1 = c_{XZ}$. Therefore, (b) is correct and the proof is complete. □

Example 4.5. As an example, we consider the Edwards curve $E_{-30} : Z^2(X^2+Y^2) = Z^4-30X^2Y^2$ over the field of real numbers $\mathbb{R}$. Of course, all pictures in our examples show the affine part of the curves. In Figure 4.1(a), the conic C is shown in the case $P_1, P_2 \neq \mathcal{O}'$. The point P_1 has x-coordinate $x_1 = -0.6$ and P_2 has x-coordinate $x_2 = 0.1$. Figure 4.1(b) shows the conic C for the case $P_1 \neq P_2 = \mathcal{O}'$. The point P_1 is the same as in 4.1(a).
The case $P_1 = P_2$ is shown in Figure 4.2(a) for $P_1 \neq \mathcal{O}'$ and in Figure 4.2(b) for $P_1 = \mathcal{O}'$. In the latter case, $\mathcal{O}'$ is a triple intersection point of C and E_{-30}.

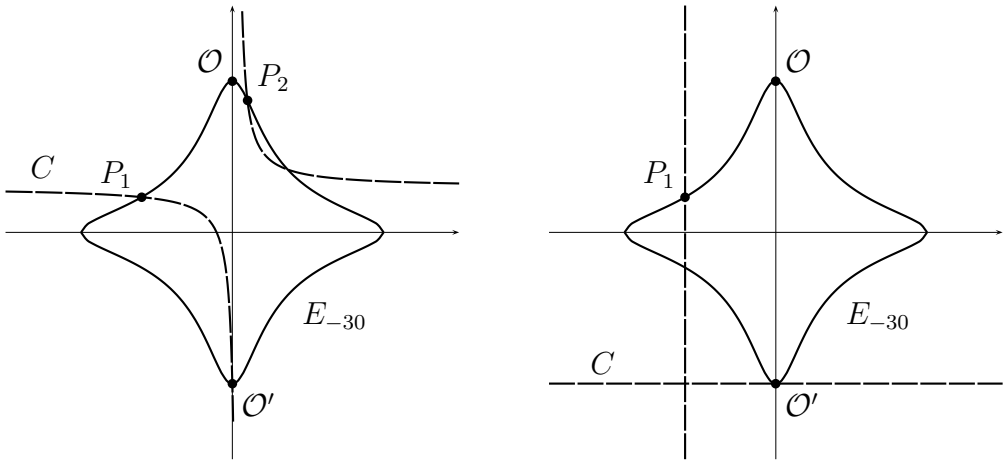
Example 4.6. In Example 4.5, the parameter d assumes a negative value. For positive values of d, the curve has a different shape. We consider $d = 2$, i. e. the curve $E_2 : Z^2(X^2 + Y^2) = Z^4 + 2X^2Y^2$. We show the respective cases in Figures 4.3 and 4.4. In Figures 4.3(a), 4.3(b), and 4.4(a), the point P_1 has x-coordinate $x_1 = -1.1$. In Figure 4.3(a), the point P_2 has x-coordinate $x_2 = 1.2$.

Example 4.7. This example covers the case $0 < d < 1$. Figure 4.5 shows the conic C on $E_{1/2} : Z^2(X^2 + Y^2) = Z^4 + \frac{1}{2}X^2Y^2$ through P_1 with x-coordinate $x_1 = -1.5$ and P_2 with x-coordinate $x_2 = 0.7$ in Figure 4.5(a). Figure 4.5(b) shows the conic that has a common tangent with $E_{1/2}$ in P_1 with x-coordinate $x_1 = -2.2$.

Remark 4.8. Note that a complete group law can be given for addition on a twisted Edwards curve $E_{a,d}$ if a is a square and d is not (see Subsection 1.1.7 in Chapter 1). In this case, the same addition formulas apply to any pair of input points, but still computation of the conic C requires case distinctions.
This can be explained as follows: First, we choose the point $\mathcal{O}'$ to always lie on the conic. It is thus clear that if one of the points P_1 or P_2 is chosen to be $\mathcal{O}'$, we need to take that into account by means of the intersection multiplicity.
Second, we have the distinction between the cases $P_1 \neq P_2$ and $P_1 = P_2$. In the first case, the conic is given by 5 different points (not lying on the same line) which may be considered as 5 points in general position in the projective plane, and finding C is independent of the curve $E_{a,d}$. Thus the conic coefficients only depend on the coefficients of P_1 and P_2. For $P_1 = P_2$, there are less than 5 different points and additional conditions due to intersection multiplicities, e. g. the conic is tangent to the curve. Therefore, the curve coefficients a and d appear in the formulas.

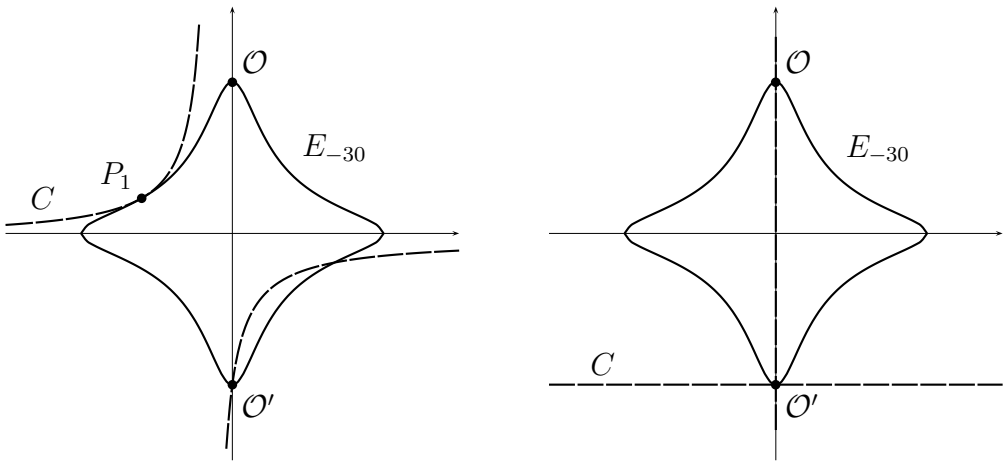
4.2 Geometric interpretation of the group law

It has been noted in Arène's master's thesis [Arè08] that the conic C described in Proposition 4.4 gives a nice geometric interpretation of the group law on an Edwards curve, similar to the chord-and-tangent method of elliptic curves in Weierstraß form. We therefore give the corresponding functions for the conic and the lines from Lemma 4.1 in the respective cases that occur in point addition.



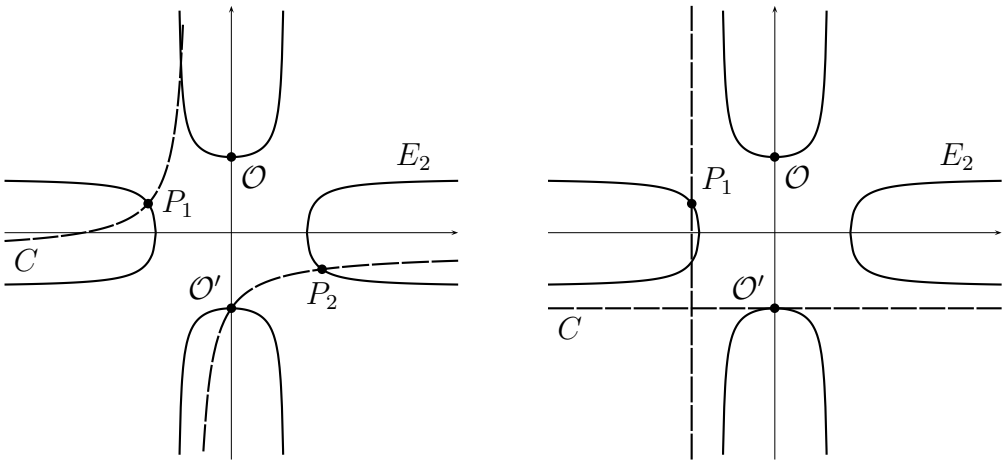
(a) $P_1 \neq P_2$, $P_1, P_2 \neq \mathcal{O}'$ (b) $P_1 \neq P_2 = \mathcal{O}'$

Figure 4.1: The conic C for $P_1 \neq P_2$ on $E_{-30} : x^2 + y^2 = 1 - 30x^2y^2$ over $\mathbb{R}$.



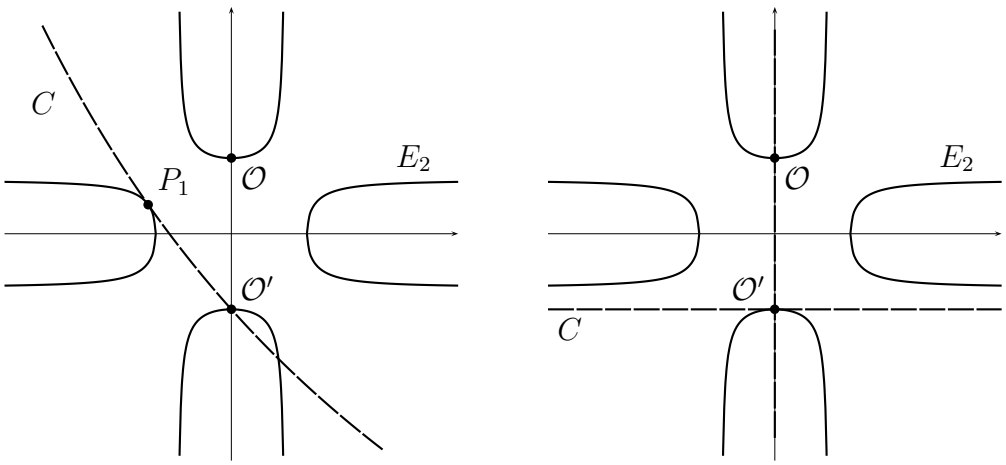
(a) $P_1 = P_2 \neq \mathcal{O}'$ (b) $P_1 = P_2 = \mathcal{O}'$

Figure 4.2: The conic C for $P_1 = P_2$ on $E_{-30} : x^2 + y^2 = 1 - 30x^2y^2$ over $\mathbb{R}$.



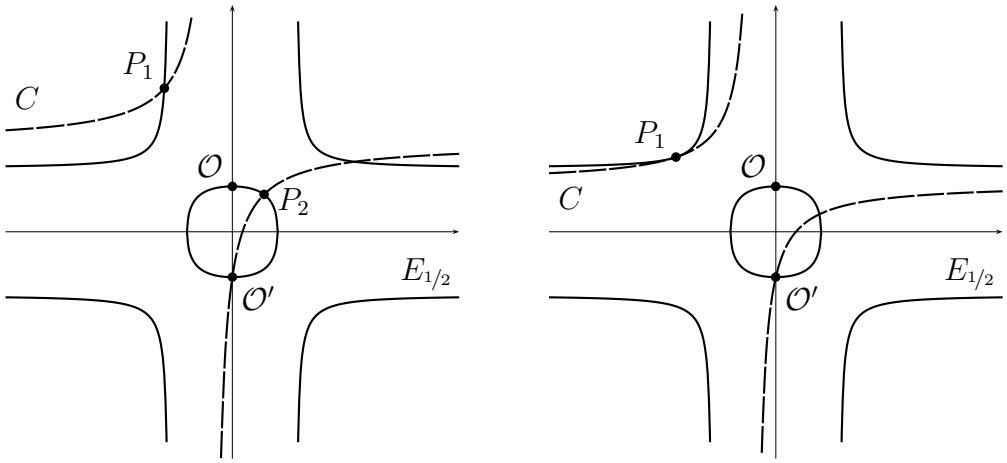
(a) $P_1 \neq P_2$, $P_1, P_2 \neq \mathcal{O}'$ (b) $P_1 \neq P_2 = \mathcal{O}'$

Figure 4.3: The conic C for $P_1 \neq P_2$ on $E_2 : x^2 + y^2 = 1 + 2x^2y^2$ over $\mathbb{R}$.



(a) $P_1 = P_2 \neq \mathcal{O}'$ (b) $P_1 = P_2 = \mathcal{O}'$

Figure 4.4: The conic C for $P_1 = P_2$ on $E_2 : x^2 + y^2 = 1 + 2x^2y^2$ over $\mathbb{R}$.



(a) $P_1 \neq P_2$, $P_1, P_2 \neq \mathcal{O}'$ (b) $P_1 = P_2 \neq \mathcal{O}'$

Figure 4.5: The conic C on $E_{1/2} : x^2 + y^2 = 1 + \frac{1}{2}x^2y^2$ over $\mathbb{R}$.

Let P_1 and P_2 be two affine $\mathbb{F}$-rational points on a twisted Edwards curve $E_{a,d}$, and let $P_3 := (X_3 : Y_3 : Z_3) = P_1 + P_2$ be their sum. Let

$$l_{1,P_3} = Z_3Y - Y_3Z,\ l_{2,\mathcal{O}} = X$$

be the polynomials of the horizontal line L_{1,P_3} and the vertical line $L_{2,\mathcal{O}}$, respectively (see Lemma 4.1). Let

$$f_C = c_{Z^2}(Z^2 + YZ) + c_{XY}XY + c_{XZ}XZ$$

be the polynomial of the conic C from Proposition 4.4. Define homogeneous functions

$$l_1 = \frac{l_{1,P_3}}{Z} = \frac{Z_3Y - Y_3Z}{Z},\ l_2 = \frac{l_{2,\mathcal{O}}}{Z} = \frac{X}{Z},$$

and

$$\phi_C = \frac{f_C}{Z^2} = \frac{c_{Z^2}(Z^2 + YZ) + c_{XY}XY + c_{XZ}XZ}{Z^2}.$$

The following lemma shows that the twisted Edwards group law indeed has a geometric interpretation involving the above functions. It gives us an important ingredient to compute Miller functions (see Lemma 1.96).

Lemma 4.9. *Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) \neq 2$. Let $a, d \in \mathbb{F}\setminus\{0\}$, $a \neq d$, and let $E_{a,d}$ be a twisted Edwards curve over $\mathbb{F}$. Let $P_1, P_2 \in E_{a,d}(\mathbb{F})$, and define $P_3 := P_1 + P_2$. Then we have*

$$\mathrm{div}\left(\frac{\phi_C}{l_1 l_2}\right) = (P_1) + (P_2) - (P_3) - (\mathcal{O}).$$

Proof. First, consider the function ϕ_C on $E_{a,d}$. By Bézout's Theorem (see Theorem 1.21), the intersection of C and $E_{a,d}$ should have eight points counting multiplicities. We note that the two points at infinity Ω_1 and Ω_2 are singular points of multiplicity 2 (Lemma 1.66). The polynomial f_C has zeros at P_1, P_2, and $\mathcal{O}'$ and zeros at Ω_1 and Ω_2, which are counted with multiplicity 2. In total, this sums up to seven points, which means that there is an eighth point Q in the intersection. The positive part of the divisor $\mathrm{div}(\phi_C)$ of ϕ_C is thus $(P_1) + (P_2) + (\mathcal{O}') + (Q) + 2(\Omega_1) + 2(\Omega_2)$. The Z^2-term in the denominator leads to ϕ_C having double poles at Ω_1 and Ω_2 and the negative part of $\mathrm{div}(\phi_C)$ being $-4(\Omega_1) - 4(\Omega_2)$. Thus the divisor of ϕ_C is

$$\mathrm{div}(\phi_C) = (P_1) + (P_2) + (\mathcal{O}') + (Q) - 2(\Omega_1) - 2(\Omega_2).$$

Let $l_Q = \frac{l_{1,Q}}{Z}$ be the function given by the horizontal line $L_{1,Q}$ through Q, and let l_2 be the function of the vertical line through $\mathcal{O}$. Then

$$\begin{aligned} \mathrm{div}(l_Q) &= (Q) + (-Q) - 2(\Omega_2), \\ \mathrm{div}(l_2) &= (\mathcal{O}) + (\mathcal{O}') - 2(\Omega_1). \end{aligned}$$

By combining the above divisors we get

$$\mathrm{div}\left(\frac{\phi_C}{l_Q l_2}\right) = (P_1) + (P_2) - (-Q) - (\mathcal{O}).$$

We now see that we have an equivalence of divisors

$$((P_1) - (\mathcal{O})) + ((P_2) - (\mathcal{O})) \sim (-Q) - (\mathcal{O}),$$

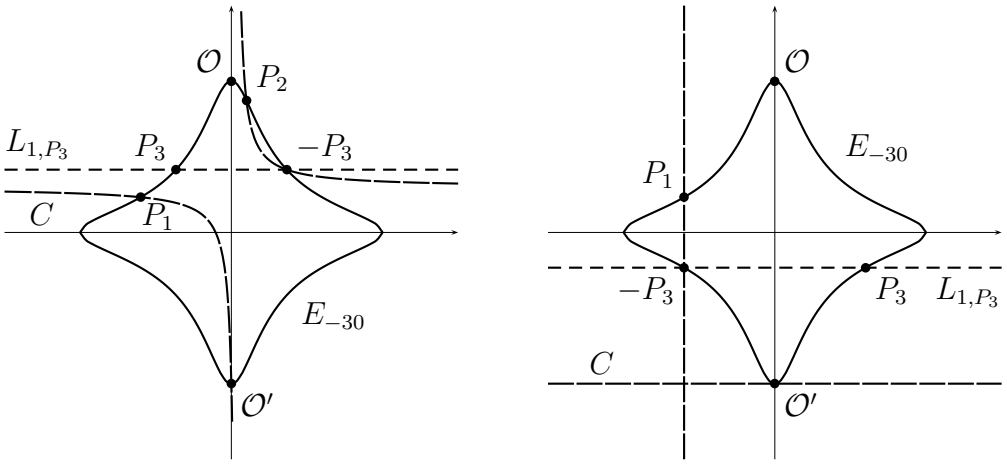
showing that $-Q$ is indeed equal to the sum $P_1 + P_2 = P_3$ (see Theorem 1.91). Thus the line l_Q is equal to l_1, and the lemma follows. □

Remark 4.10. From the proof of the previous lemma, we see that $P_1 + P_2$ is obtained as the reflection across the y-axis of the eighth intersection point of $E_{a,d}$ and the conic C passing through $\Omega_1, \Omega_2, \mathcal{O}', P_1$, and P_2.

Example 4.11. We return to the curve and points from Example 4.5. We denote by $P_3 = P_1 + P_2$ or $P_3 = [2]P_1$ the sum of P_1 and P_2 or the double of P_1, respectively. Figures 4.6 and 4.7 show the specific cases as in Example 4.5.

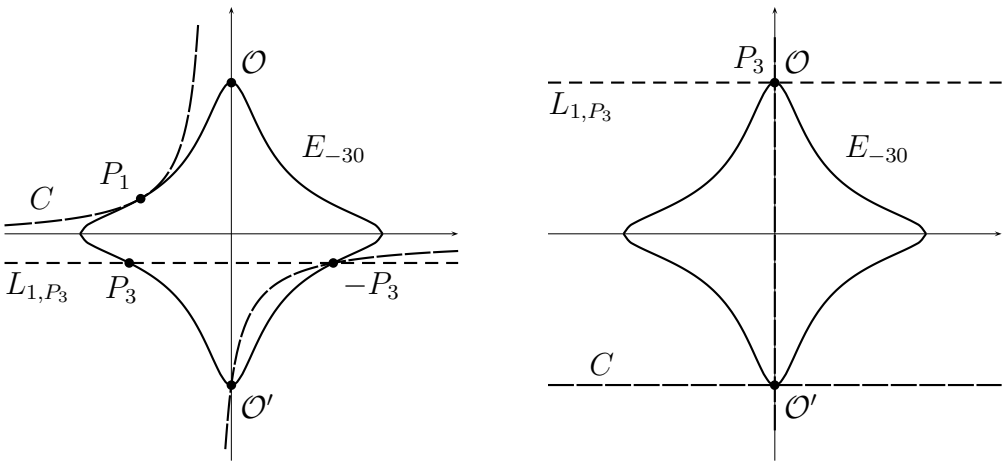
Example 4.12. This example shows the geometric interpretation of the Edwards group law with the curve and points from Example 4.6 in Figures 4.8 and 4.9. The sum of P_1 and P_2 and the double of P_1 are again denoted by P_3.

Example 4.13. This example shows the group law on the curve $E_{1/2}$ with the points from Example 4.7. Addition of two different points is depicted in Figure 4.10(a), and doubling of a point is visualized in Figure 4.10(b).



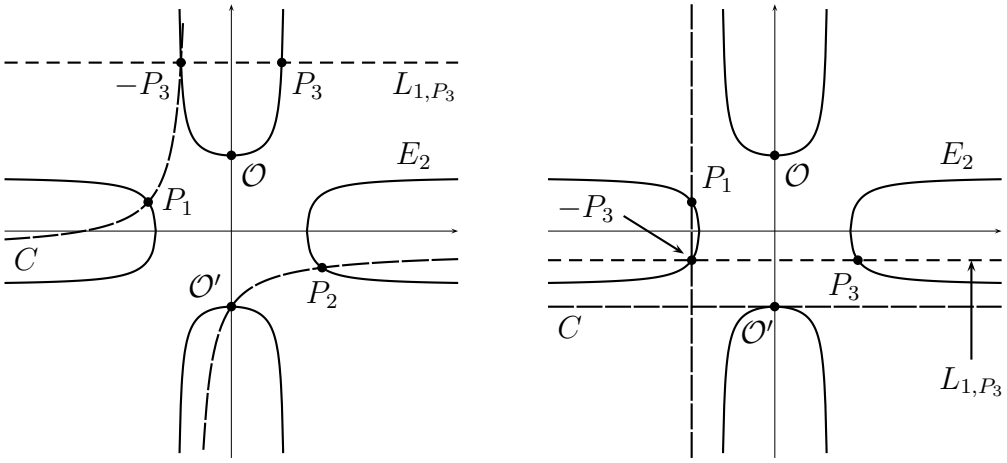
(a) $P_1 \neq P_2$, $P_1, P_2 \neq \mathcal{O}'$, $P_3 = P_1 + P_2$ (b) $P_1 \neq P_2 = \mathcal{O}'$, $P_3 = P_1 + P_2$

Figure 4.6: Geometric interpretation of the Edwards group law for $P_1 \neq P_2$ on $E_{-30} : x^2 + y^2 = 1 - 30x^2y^2$ over $\mathbb{R}$.



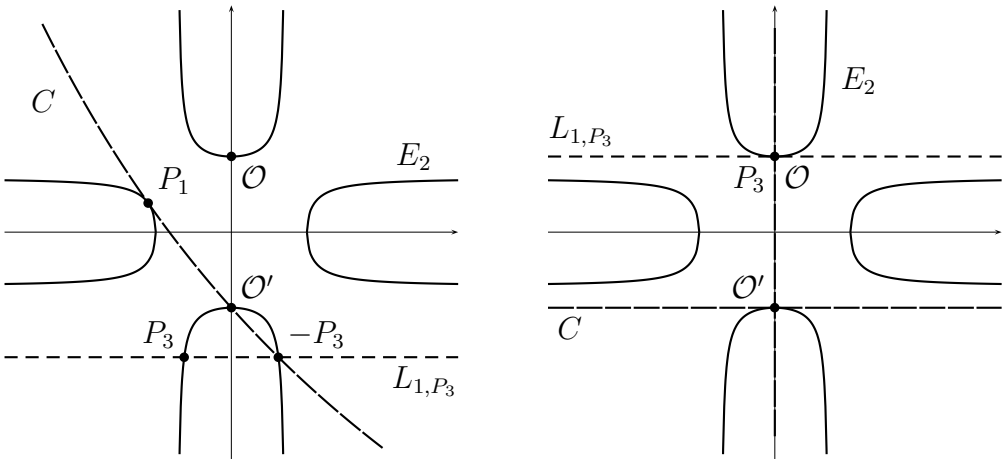
(a) $P_1 = P_2 \neq \mathcal{O}'$, $P_3 = 2P_1$ (b) $P_1 = P_2 = \mathcal{O}'$, $P_3 = 2\mathcal{O}' = \mathcal{O}$

Figure 4.7: Geometric interpretation of the Edwards group law for $P_1 = P_2$ on $E_{-30} : x^2 + y^2 = 1 - 30x^2y^2$ over $\mathbb{R}$.



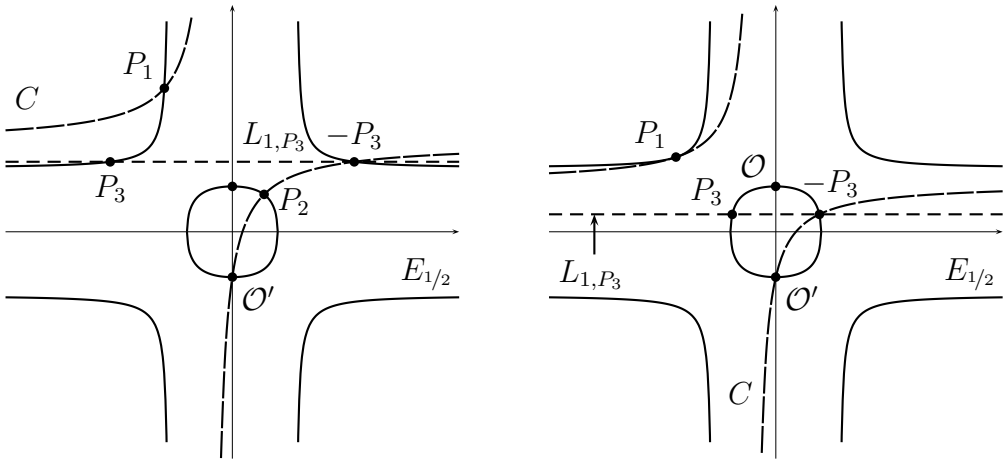
(a) $P_1 \neq P_2$, $P_1, P_2 \neq \mathcal{O}'$, $P_3 = P_1 + P_2$ (b) $P_1 \neq P_2 = \mathcal{O}'$, $P_3 = P_1 + P_2$

Figure 4.8: Geometric interpretation of the Edwards group law for $P_1 \neq P_2$ on $E_2 : x^2 + y^2 = 1 + 2x^2y^2$ over $\mathbb{R}$.



(a) $P_1 = P_2 \neq \mathcal{O}'$, $P_3 = 2P_1$ (b) $P_1 = P_2 = \mathcal{O}'$, $P_3 = 2\mathcal{O}' = \mathcal{O}$

Figure 4.9: Geometric interpretation of the Edwards group law for $P_1 = P_2$ on $E_2 : x^2 + y^2 = 1 + 2x^2y^2$ over $\mathbb{R}$.



(a) $P_1 \neq P_2$, $P_1, P_2 \neq \mathcal{O}'$, $P_3 = P_1 + P_2$ (b) $P_1 = P_2 \neq \mathcal{O}'$, $P_3 = 2P_1$

Figure 4.10: Geometric interpretation of the group law on $E_{1/2} : x^2 + y^2 = 1 + \frac{1}{2}x^2y^2$ over $\mathbb{R}$.

We now turn to Miller's formula (see Lemma 1.96). Recall that for $i \in \mathbb{Z}$ and $P \in E_{a,d}$, a Miller function is a function $f_{i,P} \in \mathbb{F}(E_{a,d})$ with divisor

$$\operatorname{div}(f_{i,P}) = i(P) - ([i]P) - (i-1)(\mathcal{O}).$$

We have the following equality of divisors relating the Miller function $f_{i+j,P}$ with $f_{i,P}$ and $f_{j,P}$ for $i, j \in \mathbb{Z}$:

$$\operatorname{div}(f_{i+j,P}) = \operatorname{div}(f_{i,P}f_{j,P}) + ([i]P) + ([j]P) - ([i+j]P) - (\mathcal{O}) \tag{4.4}$$

(see Lemma 1.95 and Lemma 1.96). The previous equality leads to an analog of Miller's formula for twisted Edwards curves.

Lemma 4.14. *Let $\mathbb{F}$ be a field with $\operatorname{char}(\mathbb{F}) \neq 2$. Let $a, d \in \mathbb{F} \setminus \{0\}$, $a \neq d$, and let $E_{a,d}$ be a twisted Edwards curve over $\mathbb{F}$. Let $P \in E_{a,d}$. Let ϕ_C and l_1, l_2 be the functions corresponding to the conic C and the lines L_1 and L_2 occurring in the addition $[i]P + [j]P = [i+j]P$ for $i, j \in \mathbb{Z}$. Then the following formula holds:*

$$f_{i+j,P} = f_{i,P}f_{j,P}\frac{\phi_C}{l_1 l_2}. \tag{4.5}$$

Proof. The lemma follows easily from (4.4) and Lemma 4.9 by setting $P_1 = [i]P$ and $P_2 = [j]P$. □

This formula may now be used in Miller's algorithm (as in Section 1.2.3) to compute pairings on twisted Edwards curves.

4.3 Explicit formulas for Miller functions

In this section we show how to use the geometric interpretation of the group law derived in Section 4.2 to compute pairings. Let $E_{a,d}$ be a twisted Edwards curve defined over a prime field $\mathbb{F}_p$. Let k be the embedding degree of $E_{a,d}$ with respect to a large prime divisor of $\#E_{a,d}(\mathbb{F}_p)$. We assume that k is even. For pairings based on the Tate pairing, we assume that the second input point Q is chosen as the image of a point on a quadratic twist as described in Section 1.2.3. Note that on twisted Edwards curves $\mathrm{E}_{a,d}$, twists affect the x-coordinate. Let $\mathbb{F}_{p^k}$ have basis $\{1, \alpha\}$ over $\mathbb{F}_{p^{k/2}}$ with $\alpha^2 = \delta \in \mathbb{F}_{p^{k/2}}$ and let $Q' = (x_0, y_0) \in \mathrm{E}_{a\delta,d\delta}(\mathbb{F}_{p^{k/2}})$ be an $\mathbb{F}_{p^{k/2}}$-rational point on the curve twisted with α. We can use $Q = (x_0\alpha, y_0)$ as the image of Q' under the twisting isomorphism. This ensures that the second argument of the pairing is on $\mathrm{E}_{a,d}(\mathbb{F}_{p^k})$ and is not defined over a smaller field.

According to Lemma 4.14 we define $g_{R,P} := \frac{\phi_C}{l_1 l_2}$ with the functions occurring in the addition of R and P. So the update in the Miller loop computes $g_{R,P}$, evaluates it at $Q = (x_0\alpha, y_0)$, and updates f as $f \leftarrow f \cdot g_{R,P}(Q)$ (addition) or as $f \leftarrow f^2 \cdot g_{R,R}(Q)$ (doubling). Given the shape of ϕ_C and the point $Q = (x_0\alpha, y_0)$, we see that we need to compute

$$\frac{\phi_C}{l_1 l_2}(x_0\alpha, y_0) = \frac{c_{Z^2}(1+y_0) + c_{XY}x_0\alpha y_0 + c_{XZ}x_0\alpha}{(Z_3y_0 - Y_3)x_0\alpha} = \frac{c_{Z^2}\frac{(1+y_0)}{x_0\delta}\alpha + c_{XY}y_0 + c_{XZ}}{Z_3y_0 - Y_3},$$

where $(X_3 : Y_3 : Z_3)$ are the coordinates of the point $R + P$ or $R + R$.

Put $\eta = \frac{(1+y_0)}{x_0\delta}$. Note that $\eta \in \mathbb{F}_{p^{k/2}}$ and that it is fixed for the whole computation, so it can be precomputed. The denominator $Z_3y_0 - Y_3$ is defined over $\mathbb{F}_{p^{k/2}}$; since it enters the function multiplicatively, the final exponentiation removes all contributions from it. We can thus avoid its computation completely, and only have to evaluate

$$c_{Z^2}\eta\alpha + c_{XY}y_0 + c_{XZ}.$$

The coefficients c_{Z^2}, c_{XY}, and c_{XZ} are defined over $\mathbb{F}_p$. Given these coefficients, the evaluation at Q can be computed in $k\mathbf{m}$ (the multiplications by η and y_0 each need $\frac{k}{2}\mathbf{m}$).

In the next sections, we give explicit formulas to efficiently compute c_{Z^2}, c_{XY}, and c_{XZ} for addition and doubling. For applications in cryptography we restrict our considerations to points in a group of prime order. Ideally, the number of points on the curve factors as $\#\mathrm{E}_{a,d}(\mathbb{F}_p) = 4n$ for a prime n, and the base point P has order n. This implies in particular that none of the additions or doublings involves Ω_1, Ω_2, or $\mathcal{O}'$. The neutral element $\mathcal{O}$ is a multiple of P, namely nP, but none of the operations in the Miller loop will have it as its input. This means that without loss of generality we can assume that none of the coordinates of the input points is 0. In fact, for this assumption we only need that P has odd order, so that the points of order 2 or 4 are not multiples of it.

4.3.1 Addition

Hisil et al. present new addition formulas for twisted Edwards curves in [HWCD08]. To save $1\mathbf{m}$ they extend the representation by a further coordinate $T_1 = X_1Y_1/Z_1$ for points $P = (X_1 : Y_1 : Z_1)$ with $Z_1 \neq 0$. In the following section, we show how to compute this value as part of the doubling step. As suggested in [HWCD08], it is only computed for the last doubling in a sequence of doublings and is not computed after an addition. Note that no addition is ever followed by another addition in the scalar multiplication. Furthermore, we assume that the base point P has odd order, so in particular, $Z_1, Z_2 \neq 0$. The sum $P_3 = (X_3 : Y_3 : Z_3)$ of two different points $P_1 = (X_1 : Y_1 : Z_1 : T_1)$ and $P_2 = (X_2 : Y_2 : Z_2 : T_2)$ in extended representation is given by

$$\begin{aligned} X_3 &= (X_1Y_2 - Y_1X_2)(T_1Z_2 + Z_1T_2), \\ Y_3 &= (aX_1X_2 + Y_1Y_2)(T_1Z_2 - Z_1T_2), \\ Z_3 &= (aX_1X_2 + Y_1Y_2)(X_1Y_2 - Y_1X_2). \end{aligned}$$

Proposition 4.4 (a) in Section 4.1 states the coefficients of the conic section for addition. We use T_1, T_2 to shorten the formulas.

$$\begin{aligned} c_{Z^2} &= X_1X_2(Y_1Z_2 - Y_2Z_1) = Z_1Z_2(T_1X_2 - X_1T_2), \\ c_{XY} &= Z_1Z_2(X_1Z_2 - Z_1X_2 + X_1Y_2 - Y_1X_2), \\ c_{XZ} &= X_2Y_2Z_1^2 - X_1Y_1Z_2^2 + Y_1Y_2(X_2Z_1 - X_1Z_2) \\ &= Z_1Z_2(Z_1T_2 - T_1Z_2 + Y_1T_2 - T_1Y_2). \end{aligned}$$

Note that all coefficients are divisible by $Z_1Z_2 \neq 0$, and so we scale the coefficients. The explicit formulas for computing $P_3 = P_1 + P_2$ and $(c_{Z^2}, c_{XY}, c_{XZ})$ are given as follows:

$$\begin{aligned} A &= X_1 \cdot X_2;\ B = Y_1 \cdot Y_2;\ C = Z_1 \cdot T_2;\ D = T_1 \cdot Z_2;\ E = D + C; \\ F &= (X_1 - Y_1) \cdot (X_2 + Y_2) + B - A;\ G = B + aA;\ H = D - C;\ I = T_1 \cdot T_2; \\ c_{Z^2} &= (T_1 - X_1) \cdot (T_2 + X_2) - I + A;\ c_{XY} = X_1 \cdot Z_2 - X_2 \cdot Z_1 + F; \\ c_{XZ} &= (Y_1 - T_1) \cdot (Y_2 + T_2) - B + I - H;\ X_3 = E \cdot F;\ Y_3 = G \cdot H;\ Z_3 = F \cdot G. \end{aligned}$$

With these formulas, P_3 and $(c_{Z^2}, c_{XY}, c_{XZ})$ can be computed in $13\mathbf{m} + 1\mathbf{m_a}$. If T_3 is desired as part of the output, it can be computed in $1\mathbf{m}$ as $T_3 = E \cdot H$. The point P_2 is not changed during pairing computation, and can be given in affine coordinates, i. e. $Z_2 = 1$. Applying mixed addition, the above costs reduce to $11\mathbf{m} + 1\mathbf{m_a}$. Note that there is no extra speed up from choosing $a = -1$ as in [HWCD08] since all subexpressions are used also in the computation of the coefficients c_{Z^2}, c_{XY}, c_{XZ}. A mixed addition step in Miller's algorithm for the Tate pairing thus costs $1\mathbf{M} + (k + 11)\mathbf{m} + 1\mathbf{m_a}$.

4.3.2 Doubling

Proposition 4.4 (c) in Section 4.1 states the coefficients of the conic section in the case of doubling. To speed up the computation, we multiply each coefficient by $2Y_1/Z_1$ (remember that f_C is unique up to scaling). Note also that $Y_1, Z_1 \neq 0$ because all points have odd order. The multiplication by Y_1/Z_1 reduces the overall degree of the equations since we can use the curve equation to simplify the formula for c_{XY}; the factor 2 is useful in obtaining an $\mathbf{s}-\mathbf{m}$ trade-off in the explicit formulas below. We obtain:

$$\begin{aligned} c_{Z^2} &= X_1(2Y_1^2 - 2Y_1Z_1), \\ c_{XY} &= 2(Y_1Z_1^3 - dX_1^2Y_1^2)/Z_1 = 2(Y_1Z_1^3 - Z_1^2(aX_1^2 + Y_1^2) + Z_1^4)/Z_1 \\ &= Z_1(2(Z_1^2 - aX_1^2 - Y_1^2) + 2Y_1Z_1), \\ c_{XZ} &= Y_1(2aX_1^2 - 2Y_1Z_1). \end{aligned}$$

Of course, we also need to compute $P_3 = [2]P_1$. We use the explicit formulas from [BBJ+08] for the doubling, and reuse subexpressions in computing the coefficients of the conic.

$$\begin{aligned} A &= X_1^2;\ B = Y_1^2;\ C = Z_1^2; D = (X_1 + Y_1)^2;\ E = (Y_1 + Z_1)^2; \\ F &= D - (A + B);\ G = E - (B + C);\ H = aA;\ I = H + B; \\ J &= C - I;\ K = J + C;\ c_{XZ} = Y_1 \cdot (2H - G);\ c_{XY} = Z_1 \cdot (2J + G); \\ c_{Z^2} &= F \cdot (Y_1 - Z_1);\ X_3 = F \cdot K;\ Y_3 = I \cdot (B - H);\ Z_3 = I \cdot K. \end{aligned}$$

These formulas compute $P_3 = (X_3 : Y_3 : Z_3)$ and $(c_{Z^2}, c_{XY}, c_{XZ})$ in $6\mathbf{m} + 5\mathbf{s} + 1\mathbf{m_a}$. If the doubling is followed by an addition, the additional coordinate $T_3 = X_3Y_3/Z_3$ needs to be computed. This is done by additionally computing $T_3 = F \cdot (B - H)$ in $1\mathbf{m}$.

If the input is given in extended form as $P_1 = (X_1 : Y_1 : Z_1 : T_1)$, we can use T_1 in the computation of the conic as

$$\begin{aligned} c_{Z^2} &= X_1(2Y_1^2 - 2Y_1Z_1) = 2Z_1Y_1(T_1 - X_1), \\ c_{XY} &= Z_1(2(Z_1^2 - aX_1^2 - Y_1^2) + 2Y_1Z_1), \\ c_{XZ} &= Y_1(2aX_1^2 - 2Y_1Z_1) = 2Z_1(aX_1T_1 - Y_1^2), \end{aligned}$$

and then scale the coefficients by $1/Z_1$. The computation of $P_3 = (X_3 : Y_3 : Z_3 : T_3)$ and $(c_{Z^2}, c_{XY}, c_{XZ})$ is then done in $6\mathbf{m} + 5\mathbf{s} + 2\mathbf{m_a}$ as

$$\begin{aligned} A &= X_1^2;\ B = Y_1^2;\ C = Z_1^2; D = (X_1 + Y_1)^2;\ E = (Y_1 + Z_1)^2; \\ F &= D - (A + B);\ G = E - (B + C);\ H = aA;\ I = H + B;\ J = C - I; \\ K &= J + C;\ c_{Z^2} = 2Y_1 \cdot (T_1 - X_1);\ c_{XY} = 2J + G;\ c_{XZ} = 2(aX_1 \cdot T_1 - B); \\ X_3 &= F \cdot K;\ Y_3 = I \cdot (B - H);\ Z_3 = I \cdot K;\ T_3 = F \cdot (B - H). \end{aligned}$$

For computing the Tate pairing this means that a doubling step costs $1\mathbf{M}+1\mathbf{S}+(k+6)\mathbf{m}+5\mathbf{s}+1\mathbf{m_a}$ in twisted Edwards coordinates and $1\mathbf{M}+1\mathbf{S}+(k+6)\mathbf{m}+5\mathbf{s}+2\mathbf{m_a}$ in extended coordinates.

4.3.3 Miller loop

Miller's algorithm loops over the bits in the representation of n. We follow Hisil et al. [HWCD08] and denote the system of projective Edwards coordinates $(X_1 : Y_1 : Z_1)$ by $\mathcal{E}$ and the extended system $(X_1 : Y_1 : Z_1 : T_1)$ by $\mathcal{E}^e$.
If the whole computation is carried out in $\mathcal{E}^e$ each addition step in the Tate pairing needs $1\mathbf{M}+(k+14)\mathbf{m}+1\mathbf{m_a}$ if both points are projective and $1\mathbf{M}+(k+12)\mathbf{m}+1\mathbf{m_a}$ if the addition is mixed. A doubling step costs $1\mathbf{M}+1\mathbf{S}+(k+6)\mathbf{m}+5\mathbf{s}+2\mathbf{m_a}$.
We can save $1\mathbf{m_a}$ per doubling by using the following idea which is already mentioned by Cohen et. al. [CMO98]. If we are faced with s consecutive doublings between additions, we execute the first $s-1$ doublings as $2\mathcal{E} \to \mathcal{E}$, do the last doubling as $2\mathcal{E} \to \mathcal{E}^e$ and then perform the addition as $\mathcal{E}^e+\mathcal{E}^e \to \mathcal{E}$. We account for the extra $\mathbf{m}$ needed in $2\mathcal{E} \to \mathcal{E}^e$ when stating the cost for addition. This way each addition step needs $1\mathbf{M}+(k+14)\mathbf{m}+1\mathbf{m_a}$ if both points are projective and $1\mathbf{M}+(k+12)\mathbf{m}+1\mathbf{m_a}$ if the addition is mixed. A doubling costs $1\mathbf{M}+1\mathbf{S}+(k+6)\mathbf{m}+5\mathbf{s}+1\mathbf{m_a}$.

4.3.4 Comparison

We compare our results with formulas in the literature, in particular, with the pairing formulas for Edwards curves due to Ionica and Joux [IJ08] and the formulas for Weierstraß curves by Chatterjee, Sarkar, and Barua [CSB05].
In [HMS09], Hankerson, Menezes, and Scott study pairing computation on BN curves [BN06]. All BN curves have the form $y^2 = x^3 + b$ and are thus more special than curves with $a_4 = -3$. In their presentation they combine the pairing computation with the extension-field arithmetic and thus the operation for the pure pairing computation is not stated explicitly but the formulas match those in [CN05].
Das and Sarkar [DS08] were the first to publish pairing formulas for Edwards curves. We do not include them in our overview in Table 4.1 since their study is specific to supersingular curves with $k = 2$.
Ionica and Joux [IJ08] proposed the thus far fastest pairing formulas for Edwards curves. Note that they actually compute the 4th power of the Tate pairing. This has almost no negative effect for usage in protocols. So we include their result as pairings on Edwards curves.
We denote Edwards coordinates by $\mathcal{E}$ and Jacobian coordinates by $\mathcal{J}$. The row "this work" in the table below reports the results of the previous section using $2\mathcal{E} \to \mathcal{E}$ for the main doublings, $2\mathcal{E} \to \mathcal{E}^e$ for the final doubling, and $\mathcal{E}^e + \mathcal{E}^e \to \mathcal{E}$ for the addition. Using only $\mathcal{E}^e$ for all operations requires $1\mathbf{m_a}$ more per doubling.
Each mADD or ADD entry has an additional $1\mathbf{M}+k\mathbf{m}$ in the operation count; each DBL entry has an additional $1\mathbf{M}+k\mathbf{m}+1\mathbf{S}$. Since this does not depend on the chosen representation, we do not report it in this overview. The symbols $\mathbf{m_{a_4}}$ and $\mathbf{m_d}$ denote multiplication by the constants a_4 and d, respectively.
This overview shows that our new formulas solidly beat any formulas published for pairing computation on Edwards curves. We point out that on Edwards curves or

	DBL	mADD	ADD
$\mathcal{J}$, [IJ08], [CSB05]	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m_{a_4}}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}, a_4 = -3$, [CSB05]	$7\mathbf{m} + 4\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}, a_4 = 0$, [CN05], [CSB05]	$6\mathbf{m} + 5\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{E}$, [IJ08]	$8\mathbf{m} + 4\mathbf{s} + 1\mathbf{m_d}$	$14\mathbf{m} + 4\mathbf{s} + 1\mathbf{m_d}$	—
$\mathcal{E}$, this work	$6\mathbf{m} + 5\mathbf{s} + 1\mathbf{m_a}$	$12\mathbf{m} + 1\mathbf{m_a}$	$14\mathbf{m} + 1\mathbf{m_a}$

Table 4.1: Overview of operation counts for doubling and addition steps

twisted Edwards curves with very small a, the multiplication costs $\mathbf{m_a}$ vanish.
The comparison with Jacobian coordinates depends on the $\mathbf{m} - \mathbf{s}$ ratio and the size of the parameters. Since both a_4 and a can be chosen to be small, multiplications by them are negligible, i.e. we assume $1\mathbf{m_{a_4}} = 1\mathbf{m_a} = 0$. The number of operations on the Edwards curve is no more than on the Weierstrass curve. For doubling, our formulas are as efficient as the most efficient ones (for BN curves) and cover more general curves. For addition, we need the same number of operations, but the formulas have no squarings. So they are slower if squarings are cheaper than multiplications. Overall, the new formulas are competitive for doubling, if not better, and slightly worse for mixed addition.
Finally, the penalty for computing full additions instead of mixed additions is significantly worse for Jacobian coordinates where an addition (without computation of the line function) costs $12\mathbf{m} + 4\mathbf{s}$ which is more than the full computation in Edwards coordinates. Therefore, Edwards curves are the clear winner if for some reason the input point is not in affine coordinates.

Chapter 5

Constructing curves of genus 2 with p-rank 1

In this chapter, we discuss the complex multiplication method for hyperelliptic curves of genus 2 and p-rank 1. For this purpose, we introduce general facts about abelian varieties and complex multiplication (CM) in Section 5.1. Section 5.2 and Section 5.4 provide results of joint work with Hitt O'Connor, McGuire, and Streng [HMNS08]. We present an algorithm for constructing hyperelliptic curves of genus 2 with p-rank 1 that are defined over $\mathbb{F}_{p^2}$. The algorithm allows the construction of curves with a prime number of $\mathbb{F}_{p^2}$-rational points on its Jacobian variety of a cryptographic relevant size. We give examples of curves constructed with the proposed algorithm. In Section 5.3 we discuss existing construction algorithms for genus-2 curves with prescribed embedding degree. Finally, in Section 5.4 we propose an algorithm to construct p-rank-1 curves of genus 2 with a prescribed embedding degree.

5.1 Abelian varieties with complex multiplication

Let $\mathbb{F}$ be a perfect field, and let $\overline{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$.

Definition 5.1. An *abelian variety* over $\mathbb{F}$ is an absolutely irreducible projective algebraic group defined over $\mathbb{F}$.

The reader is referred to [FL05a] for a brief introduction to abelian varieties in view of their application in cryptography. Mumford [Mum74] and Lang [Lan83] give an elaborate introduction, and Shimura [Shi97] treats the theory of complex multiplication on abelian varieties. In Chapter 1, we have already seen examples of abelian varieties, namely Jacobian varieties of hyperelliptic curves. In particular, an elliptic curve is an abelian variety.
Let $\mathcal{A}$ be an abelian variety over $\mathbb{F}$. For any field extension $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$, the set of $\tilde{\mathbb{F}}$-rational points on $\mathcal{A}$ is denoted by $\mathcal{A}(\tilde{\mathbb{F}})$, where $\mathcal{A} = \mathcal{A}(\overline{\mathbb{F}})$.

Definition 5.2. An abelian variety $\mathcal{A}$ over $\mathbb{F}$ is called *simple over* $\mathbb{F}$ if for all abelian varieties $\mathcal{B} \subseteq \mathcal{A}$ defined over $\mathbb{F}$ either $\mathcal{B} = 0$ or $\mathcal{B} = \mathcal{A}$. It is called *absolutely simple* if it is simple over $\overline{\mathbb{F}}$.

Let $\mathcal{A}$ and $\mathcal{B}$ be two abelian varieties over $\mathbb{F}$. A morphism $\mathcal{A} \to \mathcal{B}$ is called a *homomorphism* if it is a group homomorphism. A homomorphism φ is an *isogeny* if it is surjective and the kernel of φ is finite. The abelian varieties $\mathcal{A}$ and $\mathcal{B}$ are called *isogenous* if there exists an isogeny between them.
Any abelian variety $\mathcal{A}$ is isogenous to a product of powers of simple abelian varieties (see [Mum74, Corollary 1, p. 174] and [FL05a, Section 4.3.4], i. e. there exist a number $l \in \mathbb{N}$, simple abelian varieties $\mathcal{A}_i$, $1 \leq i \leq l$, each two of which are not isogenous to each other, and $n_i \in \mathbb{N}_0$ such that $\mathcal{A}$ is isogenous to $\mathcal{A}_1^{n_1} \times \cdots \times \mathcal{A}_l^{n_l}$. The $\mathcal{A}_i$ and the n_i are uniquely determined.
An *endomorphism* of $\mathcal{A}$ is a homomorphism $\mathcal{A} \to \mathcal{A}$ of $\mathcal{A}$ to itself. We denote the set of all endomorphisms of $\mathcal{A}$ defined over $\overline{\mathbb{F}}$ by $\mathrm{End}_{\overline{\mathbb{F}}}(\mathcal{A})$. The set $\mathrm{End}_{\overline{\mathbb{F}}}(\mathcal{A})$ with addition given by the group law on $\mathcal{A}$ and composition as multiplicative structure is a ring, the *endomorphism ring of* $\mathcal{A}$. The subring of endomorphisms defined over $\tilde{\mathbb{F}}$ for $\mathbb{F} \subseteq \tilde{\mathbb{F}} \subseteq \overline{\mathbb{F}}$ is denoted by $\mathrm{End}_{\tilde{\mathbb{F}}}(\mathcal{A})$. We define the *endomorphism algebra of* $\mathcal{A}$ *over* $\tilde{\mathbb{F}}$ by $\mathrm{End}^0_{\tilde{\mathbb{F}}}(\mathcal{A}) := \mathbb{Q} \otimes \mathrm{End}_{\tilde{\mathbb{F}}}(\mathcal{A})$. If $\mathcal{A}$ is simple over $\tilde{\mathbb{F}}$, $\mathrm{End}_{\tilde{\mathbb{F}}}(\mathcal{A})$ has no zero divisors and $\mathrm{End}^0_{\tilde{\mathbb{F}}}(\mathcal{A})$ is a division algebra [FL05a, Proposition 4.70].
Let $\mathcal{A}$ be isogenous to $\mathcal{A}_1^{n_1} \times \cdots \times \mathcal{A}_l^{n_l}$ as above, and define $D_i := \mathrm{End}^0_{\overline{\mathbb{F}}}(\mathcal{A}_i)$. Then

$$\mathrm{End}^0_{\overline{\mathbb{F}}}(\mathcal{A}) \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_l}(D_l),$$

where $M_{n_i}(D_i)$ is the matrix ring of $(n_i \times n_i)$-matrices over D_i. The structure of $\mathrm{End}^0_{\overline{\mathbb{F}}}(\mathcal{A})$ for a simple abelian variety $\mathcal{A}$ is classified in [Mum74, Section 21]. As already seen for elliptic curves and Jacobians of hyperelliptic curves, the multiplication-by-m map $[m]$ defined as usual is an endomorphism on $\mathcal{A}$ for any $m \in \mathbb{Z}$.
Let $g := \dim(\mathcal{A})$ be the dimension of $\mathcal{A}$ as a projective variety. For the definition of the dimension of a variety, see [FL05a, Definition 4.17], [Ful69, Chapter 6, Section 5], and [Har77, Section II.3]. Every endomorphism φ of $\mathcal{A}$ has a *characteristic polynomial* $f_{\varphi,\mathcal{A}} \in \mathbb{Z}[T]$, monic, of degree $2g$ such that $f_{\varphi,\mathcal{A}}(\varphi) = 0$. The constant term of $f_{\varphi,\mathcal{A}}$ is called the *norm of* φ, and the negative of the coefficient of T^{2g-1} is called the *trace of* φ [Mum74, Theorem 4 in Section 18].
For the remainder of this section, we fix $\mathbb{F}$ to be a finite field $\mathbb{F}_q$ with q elements of characteristic p. Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{F}_q$. The *set of* p*-torsion points* on $\mathcal{A}$ is the kernel of the map $[p]$, denoted by $\mathcal{A}[p]$. It is an $\mathbb{F}_p$-vector space.

Definition 5.3. The dimension $r_p(\mathcal{A}) := \dim_{\mathbb{F}_p}(\mathcal{A}[p])$ of $\mathcal{A}[p]$ as an $\mathbb{F}_p$-vector space is called the *p-rank of* $\mathcal{A}$.

It holds

$$0 \leq r_p(\mathcal{A}) \leq g$$

(see [Mum74, Proposition on p. 64]). If $r_p(\mathcal{A}) = g$, then $\mathcal{A}$ is called *ordinary*. The abelian variety $\mathcal{A}$ is called *supersingular* if it is isogenous to a product of supersingular elliptic curves. In this case, $r_p(\mathcal{A}) = 0$. If $g \leq 2$, the converse is also true, i. e. an abelian variety of dimension 1 or 2 is supersingular if and only if $r_p(\mathcal{A}) = 0$ [FL05a, Remark 4.75]. The p-rank of $\mathcal{A}$ is invariant under isogenies, and it is $r_p(\mathcal{A} \times \mathcal{B}) = r_p(\mathcal{A}) + r_p(\mathcal{B})$. Therefore, if $\mathcal{A}$ is isogenous to $\mathcal{A}_1^{n_1} \times \cdots \times \mathcal{A}_l^{n_l}$, then $r_p(\mathcal{A}) = \sum_i n_i r_p(\mathcal{A}_i)$.
The q-power Frobenius automorphism on $\overline{\mathbb{F}_q}$ extends to an endomorphism ϕ_q on $\mathcal{A}$, the *Frobenius endomorphism on* $\mathcal{A}$. We denote the characteristic polynomial of ϕ_q by $f_{\mathcal{A}} := f_{\phi_q,\mathcal{A}}$. A polynomial f is called a *q-Weil polynomial* if $f = f_{\mathcal{A}}$ for some abelian variety $\mathcal{A}$ over $\mathbb{F}_q$.

Theorem 5.4. *Let $\mathcal{A}$ and $\mathcal{B}$ be abelian varieties over $\mathbb{F}_q$, and let $f_{\mathcal{A}}$ and $f_{\mathcal{B}}$ be the characteristic polynomials of their Frobenius endomorphisms. Then the following statements are equivalent:*

(a) $\mathcal{A}$ and $\mathcal{B}$ are isogenous over $\mathbb{F}_q$.

(b) $f_{\mathcal{A}} = f_{\mathcal{B}}$.

(c) $\#\mathcal{A}(\tilde{\mathbb{F}}) = \#\mathcal{B}(\tilde{\mathbb{F}})$ for all finite extensions $\tilde{\mathbb{F}} \supseteq \mathbb{F}_q$.

Proof. This is Theorem 1(c) in [Tat66]. □

Let $\pi_{\mathcal{A}}$ be a root of the characteristic polynomial $f_{\mathcal{A}}$ of the Frobenius endomorphism. Define the number field $K = \mathbb{Q}(\pi_{\mathcal{A}})$. In the sequel, we identify ϕ_q with the algebraic integer $\pi_{\mathcal{A}}$. Weil proved the Riemann hypothesis for abelian varieties, which states that every root of $f_{\mathcal{A}}$ has absolute value $\sqrt{q}$. Or in other words: the image of $\pi_{\mathcal{A}}$ under every embedding of K into $\mathbb{C}$ has absolute value $\sqrt{q}$. An algebraic integer that satisfies this property is called a *q-Weil number*. Two q-Weil numbers π_1 and π_2 are conjugate if there exists a field isomorphism $\mathbb{Q}(\pi_1) \to \mathbb{Q}(\pi_2)$ that maps π_1 to π_2. Honda and Tate proved the following relation between q-Weil numbers and isogeny classes of abelian varieties.

Theorem 5.5. *The map $\mathcal{A} \mapsto \pi_{\mathcal{A}}$ induces a bijection between isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and conjugacy classes of q-Weil numbers.*

Proof. This is the main theorem in [Hon68] or Théorème 1(i) in [Tat71]. □

A q-Weil number thus determines a simple abelian variety that is unique up to isogeny. The following theorem relates the q-Weil number $\pi_{\mathcal{A}}$ to the endomorphism algebra of $\mathcal{A}$.

Theorem 5.6. *Let $\mathcal{A}$ be a simple abelian variety over $\mathbb{F}_q$ of dimension g. Let $f_{\mathcal{A}}$ be the characteristic polynomial of the Frobenius endomorphism $\pi_{\mathcal{A}}$ on $\mathcal{A}$. Let $K = \mathbb{Q}(\pi_{\mathcal{A}})$. Then the following statements hold:*

(a) $\mathcal{E} := \mathrm{End}^0_{\mathbb{F}_q}(\mathcal{A})$ *is a division algebra with center* K.

(b) $2g = [\mathcal{E} : K]^{1/2}[K : \mathbb{Q}]$.

(c) Let $e := [\mathcal{E} : K]^{1/2}$. *Then* $f_{\mathcal{A}}(T) = m_{\mathcal{A}}(T)^e$ *for some irreducible polynomial* $m_{\mathcal{A}}(T) \in \mathbb{Q}[T]$.

Proof. See [Tat71, Théorème 1 (ii) (2) and Remarques 2)]. □

Theorem 2 in [Tat66] states that $\mathcal{E}$ is commutative if and only if $\mathcal{E} = K$ if and only if $f_{\mathcal{A}}$ has no multiple roots, i. e. it is irreducible. In this case, $[\mathcal{E} : \mathbb{Q}] = [K : \mathbb{Q}] = 2g$.

Remark 5.7. There is a connection between the number of $\mathbb{F}_q$-rational points on $\mathcal{A}$ and the q-Weil number $\pi_{\mathcal{A}}$: The set of $\mathbb{F}_q$-rational points is equal to the kernel of $[1] - \phi_q$, hence $\#\mathcal{A}(\mathbb{F}_q) = \#\ker([1] - \phi_q)$. The cardinality of the kernel is equal to $\deg([1] - \phi_q) = f_{\mathcal{A}}(1)$ [Mum74, Theorem 4, p. 180]. We thus have

$$\#\mathcal{A}(\mathbb{F}_q) = f_{\mathcal{A}}(1).$$

Let $\mathcal{E} = K = \mathbb{Q}(\pi_{\mathcal{A}})$. If $f_{\mathcal{A}}(T) = \prod_{i=1}^{2g}(T - \alpha_i)$ is the factorization of $f_{\mathcal{A}}$ in $\mathbb{C}[x]$ with $\alpha_1 := \pi_{\mathcal{A}}$, then $f_{\mathcal{A}}(1) = \prod_i(1 - \alpha_i) = N_{K/\mathbb{Q}}(1 - \pi_A)$, the $K/\mathbb{Q}$-norm of $1 - \pi_{\mathcal{A}}$. Therefore, in this case

$$\#\mathcal{A}(\mathbb{F}_q) = N_{K/\mathbb{Q}}(1 - \pi_{\mathcal{A}})$$

(see also Theorem 1.77).

Hence we can compute the number of $\mathbb{F}_q$-rational points on $\mathcal{A}$ from a corresponding q-Weil number. By fixing a number field K of degree $2g$, we can choose a q-Weil number $\pi \in K$ such that the norm $N_{K/\mathbb{Q}}(1 - \pi)$ fulfills a given property. In certain cases, it is possible to construct a simple abelian variety $\mathcal{A}$ over $\mathbb{F}_q$ of dimension g with $\mathcal{E} = K$ and $\#\mathcal{A}(\mathbb{F}_q) = N_{K/\mathbb{Q}}(1 - \pi)$ by using the complex multiplication (CM) method. This method is briefly explained in Subsection 5.2.2 below. We conclude this section by giving some basic definitions.

Definition 5.8. A field K is called a *CM field* if it is a totally imaginary quadratic extension of a totally real algebraic number field. Let $\mathcal{O}$ be an order of K. An abelian variety $\mathcal{A}$ has *complex multiplication (CM) by* $\mathcal{O}$ if $\mathrm{End}_{\overline{\mathbb{F}}}(\mathcal{A}) \cong \mathcal{O}$; it has *CM by* K if it has CM by an order $\mathcal{O}$ of K.

Example 5.9. An elliptic curve E over a finite field $\mathbb{F}_q$ is an abelian variety. If E is ordinary, it has CM by a quadratic imaginary number field [Sil86, Theorem V.3.1(b)]. An elliptic curve defined over $\mathbb{C}$ has complex multiplication if its endomorphism ring is strictly larger than $\mathbb{Z}$ (see [Sil86, Remark II.4.3] and Section 1.3.1).

Definition 5.10. Let K be a CM field of degree $2g$. Let $\Phi := \{\varphi_1, \ldots, \varphi_g\}$ be a set of distinct embeddings of K into $\mathbb{C}$ such that no two of the φ_i are complex conjugate to each other. Then the pair (K, Φ) is called a *CM type*. A CM type

is called *primitive* if there is no proper subfield $K' \subset K$ such that for the set of restrictions $\Phi' := \{\varphi_1|_{K'}, \ldots, \varphi_g|_{K'}\}$, the pair (K', Φ') is a CM type. The *reflex field of* (K, Φ) is defined as

$$\widehat{K} := \mathbb{Q}\left(\left\{\sum_{i=1}^{g} \varphi_i(\alpha) \mid \alpha \in K\right\}\right),$$

i. e. $\widehat{K}$ is the number field generated by all elements $\sum_{i=1}^{g} \varphi_i(\alpha)$ for $\alpha \in K$. If the context is clear, we omit Φ and say that $\widehat{K}$ is the reflex field of K.

Example 5.11. (a) If a CM type (K, Φ) is primitive and K is normal over $\mathbb{Q}$, then $\widehat{K} = K$ [Shi97, Example 8.4(1)].
(b) Let K be a non-normal quartic CM field. Then the normal closure L of K has degree 2 over K, and its Galois group over $\mathbb{Q}$ is the dihedral group D_8 of order 8 [Shi97, Example 8.4(2)(C)]. In that case, the reflex field is non-normal of degree 4, contained in L, and not conjugate to K.

5.2 A CM construction for genus-2 curves with p-rank 1

The abelian varieties that we consider in this section are Jacobian varieties of hyperelliptic curves of genus 2. Note that the Jacobian variety has dimension equal to the genus of the curve [Har77, Remark IV.4.10.9]. Hence when the genus is 2, we also call the abelian variety an *abelian surface*. We recall from Theorem 1.77 and Example 1.78 that the characteristic polynomial of the Frobenius endomorphism on the Jacobian variety of a hyperelliptic curve $C/\mathbb{F}_q$ of genus 2 has the form

$$f_{J_C} = T^4 + a_1 T^3 + a_2 T^2 + a_1 q T + q^2$$

for integers a_1, a_2. If $n_k := \#C(\mathbb{F}_{q^k})$, $k \in \{1, 2\}$, then $n_1 = q + 1 + a_1$ and $n_2 = q^2 + 1 + 2a_2 - a_1^2$. In the following subsection, we discuss curves that have a Jacobian with p-rank 1.

5.2.1 Genus-2 curves with p-rank 1

In Definition 1.74, we have defined the p-rank of a hyperelliptic curve as the p-rank of its Jacobian variety. This coincides with Definition 5.3, and we may use both definitions synonymously. The following theorem summarizes the results of Rück [Rüc90] and Maisner and Nart [MN02], and gives conditions on a_1, a_2 for a hyperelliptic genus-2 curve C to have p-rank 1.

Theorem 5.12. *Let $q = p^n$ for a prime p and a positive integer n. Let $f = T^4 + a_1 T^3 + a_2 T^2 + q a_1 T + q^2 \in \mathbb{Z}[T]$, and let $\Delta = a_1^2 - 4a_2 + 8q$, $\delta = (a_2 + 2q)^2 - 4q a_1^2$. Then f is the characteristic polynomial of a simple Jacobian variety of a hyperelliptic curve of genus 2 with p-rank 1 defined over $\mathbb{F}_q$ if and only if*

(a) $|a_1| < 4\sqrt{q}$,

(b) $2|a_1|\sqrt{q} - 2q < a_2 < a_1^2/4 + 2q$,

(c) Δ *is not a square in* $\mathbb{Z}$,

(d) $\nu_p(a_1) = 0$,

(e) $\nu_p(a_2) \geq n/2$,

(f) δ *is not a square in the* p*-adic integers,*

where ν_p *denotes the* p*-adic valuation.*

Proof. Assume that the conditions (a) - (f) hold. The first three conditions are equivalent to f being an irreducible q-Weil polynomial (see [MN02, Lemma 2.1, Lemma 2.4] and [Rüc90, Lemma 3.1]). Let π be a root of f. By Theorem 5.5 there exists a simple abelian surface $\mathcal{A}$ defined over $\mathbb{F}_q$ such that π corresponds to its Frobenius endomorphism. It follows from [MN02, Theorem 2.15] that $\mathcal{A}$ is absolutely simple. Theorem 4.3 of [MN02] then implies that $\mathcal{A}$ is isogenous to the Jacobian of a hyperelliptic curve of genus 2 with characteristic polynomial f. By [MN02, Theorem 2.9], the curve C has p-rank 1.
Conversely, let f be the characteristic polynomial of a simple Jacobian of a hyperelliptic curve of genus 2 with p-rank 1. Then f has the required shape. Note that since J_C is simple, by Theorem 5.6, we have $f(T) = m(T)^e$ for some monic irreducible polynomial $m \in \mathbb{Z}[T]$. The number e must divide the p-rank of J_C [Gon98, Prop. 3.2]. Thus for a simple abelian variety with p-rank 1 the characteristic polynomial of the Frobenius endomorphism is always irreducible. This implies the first three conditions by [MN02, Lemma 2.4]. The last three conditions follow from [MN02, Theorem 2.9] because J_C has p-rank 1. □

The previous theorem states conditions for f_{J_C} which are equivalent to the curve C having p-rank 1. They connect the q-Weil number π_{J_C} and the p-rank of C.
Next we consider the endomorphism algebra to see whether the Jacobian of a curve over $\mathbb{F}_q$ with p-rank 1 can have complex multiplication. For an elliptic curve $E/\mathbb{F}_q$, Theorem 1.54 shows that, there are two cases for $\mathrm{End}^0(E) := \mathrm{End}^0_{\mathbb{F}_q}(E)$, which coincide with the two cases for the p-rank of E. Either the curve is ordinary with p-rank 1, where $\mathrm{End}^0(E)$ is a CM field of degree 2, or the curve is supersingular with p-rank 0, where $\mathrm{End}^0(E)$ is a quaternion algebra.
The following lemma shows that the endomorphism algebra $\mathrm{End}^0_{\mathbb{F}_q}(J_C)$ for a curve C with p-rank 1 is a quartic CM field if J_C is simple. In contrast to the genus-1 case, not only ordinary curves can have a CM field as their endomorphism algebra.

Lemma 5.13. *Let* J_C *be the Jacobian of a hyperelliptic genus-2 curve* C *defined over* $\mathbb{F}_q$*. Assume that* J_C *is simple. If* C *has* p*-rank* 1*, then* J_C *is absolutely simple and* $\mathrm{End}^0_{\mathbb{F}_q}(J_C) = \mathrm{End}^0_{\mathbb{F}_q}(J_C)$ *is a CM field of degree 4.*

Proof. Maisner and Nart [MN02, Corollary 2.17] show that a simple abelian surface of p-rank 1 is absolutely simple.
By Theorem 5.6, the characteristic polynomial of Frobenius is $f_{J_C} = m_{J_C}^e$ for some irreducible monic polynomial $m_{J_C} \in \mathbb{Z}[T]$. We have seen in the proof of Theorem 5.12 that $e = 1$. Furthermore, Theorem 5.6 implies that $\mathrm{End}^0_{\mathbb{F}_q}(J_C)$ is a field of degree 4. It is a CM field, since $\pm\sqrt{q}$ are no roots of f_{J_C}.
It remains to show $\mathrm{End}^0_{\mathbb{F}_q}(J_C) = \mathrm{End}^0_{\overline{\mathbb{F}_q}}(J_C)$. Let $\varphi \in \mathrm{End}^0_{\overline{\mathbb{F}_q}}(J_C)$. There exists a finite field extension $\tilde{\mathbb{F}} \supseteq \mathbb{F}_q$ such that $\varphi \in \mathrm{End}^0_{\tilde{\mathbb{F}}}(J_C)$. Since J_C is absolutely simple, it is simple over $\tilde{\mathbb{F}}$, and it has p-rank 1. With the same arguments as above, it follows from Theorem 5.6 that $\mathrm{End}^0_{\tilde{\mathbb{F}}}(J_C)$ is a field of degree 4 containing $\mathrm{End}^0_{\mathbb{F}_q}(J_C)$. Thus they are equal and $\varphi \in \mathrm{End}^0_{\mathbb{F}_q}(J_C)$. □

This lemma indicates that J_C has CM by the quartic CM field $K = \mathrm{End}^0_{\mathbb{F}_q}(J_C)$ if J_C is simple. Note that if C has p-rank 1 and J_C is not simple, then J_C is isogenous to the product of an ordinary elliptic curve and a supersingular elliptic curve. We do not consider this case in the following but restrict to curves of p-rank 1 with a simple Jacobian variety, which then is absolutely simple by Lemma 5.13.

5.2.2 The CM method for genus 2

In Subsection 1.3.1, we have seen how the CM method can be used to construct elliptic curves with CM over a finite field as the reduction of curves over $\mathbb{C}$ with CM by the same field K. In principle, this method, although in a more complicated way, can also be applied to construct hyperelliptic curves of genus 2. In this subsection, we briefly discuss the CM method for genus 2. A more detailed description can be found in [FL05b] and [FL05c].
We aim at obtaining a genus-2 curve over a finite field $\mathbb{F}_q$ of characteristic p with a given number of $\mathbb{F}_q$-rational points on the Jacobian. This means the curve corresponds to a q-Weil number π that lies in an order $\mathcal{O}$ in a given quartic CM field K (see Section 5.1). We restrict to the case that this order is the maximal order $\mathcal{O}_K$. First we need to find abelian surfaces over $\mathbb{C}$ that are suitable candidates for being reduced.
Any abelian variety of dimension g over $\mathbb{C}$ corresponds to a lattice in $\mathbb{C}^g$. For $g \in \mathbb{N}$, a *lattice* in $\mathbb{C}^g$ is a $\mathbb{Z}$-module of full rank, i. e. it contains an $\mathbb{R}$-basis of $\mathbb{C}^g$. Let $\mathcal{A}$ be an abelian variety of dimension g over $\mathbb{C}$. Then $\mathcal{A}$ is isomorphic to $\mathbb{C}^g/\Lambda$ for a lattice $\Lambda \subseteq \mathbb{C}^g$ [FL05c, Section 5.1.3]. The group $\mathbb{C}^g/\Lambda$ is called a *complex torus*. A torus is attached to an abelian variety if and only if there exists a Hermitian form $\mathscr{H}$ on $\mathbb{C}^d$, and for $\mathscr{E} = \mathrm{Im}(\mathscr{H})$, the restriction of $\mathscr{E}$ to $\Lambda \times \Lambda$ maps into $\mathbb{Z}$ [FL05c, Theorem 5.16].
We define the *dual lattice* $\hat{\Lambda}$ of a lattice Λ by

$$\hat{\Lambda} := \{x \in \mathbb{C}^g \mid \mathscr{E}(x, y) \in \mathbb{Z} \text{ for all } y \in \Lambda\}.$$

An abelian variety $\mathcal{A}$ is called *principally polarized* if $\hat{\Lambda} = \Lambda$.

Remark 5.14. The Jacobian variety of a projective irreducible nonsingular curve over $\mathbb{C}$ is a principally polarized abelian variety [FL05c, Proposition 5.24].

Vice versa, any principally polarized abelian surface $\mathcal{A}$ over $\mathbb{C}$ is the Jacobian variety of a genus-2 curve [FL05c, Section 5.1.6.a]. The candidates we are looking for are thus principally polarized abelian surfaces $\mathcal{A}$ over $\mathbb{C}$ with endomorphism ring isomorphic to $\mathcal{O}_K$ for a given quartic CM field K.
We obtain such abelian surfaces from ideals in $\mathcal{O}_K$ (compare the CM method for elliptic curves in Subsection 1.3.1). Let K be a quartic CM field, and let $(K, \Phi) = (K, \{\varphi_1, \varphi_2\})$ be a CM type. For an ideal $\mathfrak{a} \subset \mathcal{O}_K$ the set $\Phi(\mathfrak{a}) := \{(\varphi_1(\alpha), \varphi_2(\alpha))^t \mid \alpha \in \mathfrak{a}\}$ is a lattice in $\mathbb{C}^2$, and the torus $\mathbb{C}^2/\Phi(\mathfrak{a})$ is an abelian surface which has CM by $\mathcal{O}_K$, and vice versa, every abelian surface with this property can be obtained in this way up to isomorphism [FL05c, Theorem 5.58 and discussion after that]. The abelian surfaces with principal polarization are obtained by only using special ideals and assuming that the totally real quadratic subfield K_0 of K has class number 1. For details, see [FL05c, Section 5.1.6.d].
The isomorphism class of an elliptic curve is given by its j-invariant. In the genus-1 CM method, one analytically computes the Hilbert class polynomial the roots of which are the j-invariants of all isomorphism classes of elliptic curves over $\mathbb{C}$ with CM by the maximal order in a given quadratic CM field (see Subsection 1.3.1). The isomorphism class of any hyperelliptic curve C of genus 2 is uniquely determined by three invariants $(j_1, j_2, j_3) = (j_1(C), j_2(C), j_3(C))$, called the *(absolute) Igusa invariants* [Igu60]. From a triple of Igusa invariants, a corresponding curve can be constructed for example with Mestre's algorithm (see [Mes91], [Spa94], and [Wen01]).

Definition 5.15. Let s be the number of isomorphism classes of principally polarized abelian surfaces over $\mathbb{C}$ with CM by $\mathcal{O}_K$. Let $j_\ell^{(i)}$ be the ℓth Igusa invariant of a curve in the ith isomorphism class for $1 \leq i \leq s$. The three polynomials

$$H_\ell(x) = \prod_{i=1}^{s} (x - j_\ell^{(i)}), \ \ell \in \{1, 2, 3\}$$

are called the *Igusa class polynomials* of $\mathcal{O}_K$.

The Igusa class polynomials have rational coefficients, i. e. $H_\ell \in \mathbb{Q}[x]$ for $\ell \in \{1, 2, 3\}$ [FL05c, Theorem 5.64 (iii)]. The class polynomials over $\mathbb{C}$ can be computed from the list of principally polarized abelian surfaces over $\mathbb{C}$. This method is known as the complex analytic approach. It is first described by Spallek [Spa94]. Van Wamelen [vW99] computes the abelian surfaces as lattices in $\mathbb{C}^2$ and evaluates Igusa invariants via Siegel modular forms. Recently, a complete runtime analysis of the complex analytic method was given by Streng [Str08]. There are also other methods: Eisenträger and Lauter [EL04] present an algorithm for constructing genus-2 curves over finite fields that differs from the classical approach. Their method computes

the class polynomials using a Chinese Remainder Theorem method. Gaudry et. al. [GHK+05, GHK+06] use a p-adic or 2-adic lifting method. The computation of class polynomials over $\mathbb{C}$ is a precomputation and not considered part of the algorithm [FL05b, Section 18.2.2]. Class polynomials for many CM fields can be obtained from Kohel's database[1].

Next we need to reduce the abelian surfaces over $\mathbb{C}$ to obtain abelian surfaces over finite fields. This reduction can be done by reducing the Igusa invariants and the class polynomials, respectively. The Igusa invariants are algebraic numbers that lie in a class field over the reflex field $\widehat{K}$ of K [FL05c, Theorem 5.64 (i)].

Suppose we are given a prime p, a CM field K, and a principally polarized abelian variety $\mathcal{A}$ defined over $\mathbb{C}$ which has CM by $\mathcal{O}_K$. Assume that $\mathcal{A}$ is defined over a number field $L \subseteq \mathbb{C}$. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_L$ over p, and assume that p does not divide the denominator of any of the coefficients of the class polynomials H_i. Then we can reduce the H_i modulo p and obtain class polynomials over $\mathbb{F}_p$. This corresponds to reducing the Igusa invariants modulo $\mathfrak{p}$ [FL05b, Section 18.2.5.b]. The reduced invariants are roots of the reduced class polynomials and thus lie in an extension $\mathbb{F}_q \supseteq \mathbb{F}_p$. We denote the abelian surface corresponding to the reduced invariants by $\overline{\mathcal{A}}$.

It is shown in [Shi97, Proposition 12 in 11.1] that the endomorphism ring $\mathrm{End}_L(\mathcal{A})$ can be embedded into $\mathrm{End}_{\mathbb{F}_q}(\overline{\mathcal{A}})$. Therefore, if we choose a q-Weil number $\pi \in \mathcal{O}_K$, we have $\pi \in \mathrm{End}_{\mathbb{F}_q}(\overline{\mathcal{A}})$ and thus $\mathrm{End}^0_{\mathbb{F}_q}(\overline{\mathcal{A}})$ contains K.

The splitting behavior of p in K determines the p-rank of the reduction $\overline{\mathcal{A}}/\mathbb{F}_q$ of $\mathcal{A}$ modulo $\mathfrak{p}$. If $\mathcal{A} = E$ is an elliptic curve, a criterion of Deuring [Deu41] states that $\overline{E}$ is supersingular if p is either ramified or inert in K, and $\overline{E}$ is ordinary if p splits completely in K. If $\mathcal{A}$ has dimension 2, then there are more cases to consider.

For dimension 2, Goren distinguishes these cases in [Gor97] assuming p is unramified in K. If an ordinary curve shall be constructed, then p needs to split completely in K. Gaudry, Houtmann, Kohel, Ritzenthaler, and Weng in [GHK+05] extend Goren's results to the ramified case. They show that whenever K is cyclic, then the reduction of $\mathcal{A}$ is either ordinary or supersingular, but if K is non-normal, then it is possible for $\overline{\mathcal{A}}$ to have p-rank 1. If K is normal, non-cyclic, then $\overline{\mathcal{A}}$ is not absolutely simple. As simple p-rank-1 varieties are absolutely simple, we restrict to the case that K is non-normal. The part of the results of [Gor97] and [GHK+05] that applies to p-rank 1 is as follows:

Lemma 5.16. *Let K be a quartic CM field, and let C be a curve of genus 2 over a number field $L \supseteq K$ with endomorphism ring $\mathcal{O}_K$. Let p be a prime number, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_L$ lying over p. The reduction $\overline{C}$ of C modulo $\mathfrak{p}$ is a genus-2 curve with p-rank 1 if and only if (p) decomposes in $\mathcal{O}_K$ as $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ or $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$. In this case, $J_{\overline{C}}$ is absolutely simple.*

Proof. This is [GHK+05, Theorem 3.5 (3)]. □

[1] http://echidna.maths.usyd.edu.au/echidna/dbs/index.html

Thus when looking for curves of p-rank 1, we require that (p) splits as $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ or $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$.
Summarizing, the genus-2 CM method is as follows: Suppose as input we are given a quartic CM field K, a prime p, and a q-Weil number π, i. e. $\pi\bar{\pi} = q$, where q is a power of p. Obtain the Igusa class polynomials H_1, H_2, H_3 for K from a database or in a precomputation with the above mentioned methods. As for the genus-1 CM method, the discriminant of K needs to be small enough such that the H_i can be computed.
Reduce the Igusa class polynomials modulo p and compute all possible triples $(j_1, j_2, j_3) \in \mathbb{F}_q^3$ from the roots of $H_1 \bmod p$, $H_2 \bmod p$, and $H_3 \bmod p$. If s is the degree of the class polynomials, we obtain at most s^3 triples $(j_1, j_2, j_3) \in \mathbb{F}_q^3$. But not all of them are triples of invariants. If Mestre's algorithm is used, it must be applied to all triples. If a useful triple is chosen, the curve obtained from it may still be a twist of the curve that yields the correct group order. The correct triples and twists, if they exist, can be selected by probabilistic checking of the order of J_C, which is $N_{K/\mathbb{Q}}(1-\pi)$ for the correct curve C (see Section 5.1). Gaudry et. al. [GHK+05] propose to replace $H_2(x)$ and $H_3(x)$ by two other polynomials in such a way that they directly only yield the correct n triples (j_1, j_2, j_3). For details, see [GHK+05, Section 4].

5.2.3 Algorithms

In this subsection, we present two algorithms to construct hyperelliptic curves of genus 2 with p-rank 1. Algorithms 5.1 and 5.2 construct a curve C defined over $\mathbb{F}_{p^2}$ such that $\#J_C(\mathbb{F}_{p^2})$ is a prime of a given bitsize. The algorithms require as input a quartic CM field K and a desired bitsize for the group order.
Both algorithms apply the prime decomposition $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. The following remark shows that the other case is not useful for constructing curves for cryptography since the choices for p are very limited:

Remark 5.17. Let p be a prime that decomposes in $\mathcal{O}_K$ as $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$. Then p has ramification index 2 at $\mathfrak{p}_3$, thus p is a ramified prime. Therefore, p divides the discriminant of the CM field K. When we fix K in advance, this means that p is an element of a small finite set of primes.

The two algorithms differ as follows: Algorithm 5.1 chooses a prime p of suitable size until the splitting behavior in $\mathcal{O}_K$, the ring of integers in K, is $(p) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ (see Lemma 5.16). From the prime decomposition of p, the corresponding p^2-Weil number π is defined as $\pi = \alpha\overline{\alpha}^{-1}p$, if $\mathfrak{p}_1 = (\alpha)$ is a principal ideal generated by α. Algorithm 5.2 instead selects candidate elements for $\alpha \in \mathcal{O}_K$ of prime norm p first. The p^2-Weil number is computed from that as $\pi = \alpha^2\beta$ with $\beta = p\alpha^{-1}\overline{\alpha}^{-1}$. In both algorithms, it can then be checked whether the group order $N_{K/\mathbb{Q}}(1-\pi)$ is prime. Finally the curve C is constructed by the CM method (see Subsection 5.2.2).

Input: A non-Galois CM field K of degree 4 and a positive integer n.
Output: A prime p of n bits, a prime r, and a curve C of genus 2 over $\mathbb{F}_{p^2}$ with p-rank 1 such that $r = \#J_C(\mathbb{F}_{p^2})$.
1: Take a random prime p of n bits.
2: If $p\mathcal{O}_K$ factors as $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, where $\mathfrak{p}_3$ has degree 2, continue. Otherwise, go to Step 1.
3: If $\mathfrak{p}_1$ is principal and generated by α, let $\pi = \alpha\overline{\alpha}^{-1}p$. Otherwise, go to Step 1.
4: If $N(1-u\pi)$ is prime for some root of unity $u \in K$, then replace π by $u\pi$ and set $r = N(1-\pi)$. Otherwise, go to Step 1.
5: Compute a curve C corresponding to K, p, and π using the CM method.
6: **return** p, r, C.

Algorithm 5.1: Generate p-rank-1 curves of genus 2 over $\mathbb{F}_{p^2}$ (I)

Input: A non-Galois CM field K of degree 4 with real quadratic subfield K_0 and a positive integer n.
Output: A prime p of n bits, a prime r, and a curve C of genus 2 over $\mathbb{F}_{p^2}$ with p-rank 1 such that $r = \#J_C(\mathbb{F}_{p^2})$.
1: Take a random element α of $\mathcal{O}_K \setminus \mathcal{O}_{K_0}$ the norm of which has n bits.
2: If $p = N(\alpha)$ is prime in $\mathbb{Z}$, continue. Otherwise, go to Step 1.
3: If $\beta = p\alpha^{-1}\overline{\alpha}^{-1}$ is prime in $\mathcal{O}_{K_0}$ and remains prime in $\mathcal{O}_K$, then let $\pi = \alpha^2\beta$. Otherwise, go to Step 1.
4: If $N(1-u\pi)$ is prime for some root of unity $u \in K$, then replace π by $u\pi$ and set $r = N(1-\pi)$. Otherwise, go to Step 1.
5: Compute a curve C corresponding to K, p, and π using the CM method.
6: **return** p, r, C.

Algorithm 5.2: Generate p-rank-1 curves of genus 2 over $\mathbb{F}_{p^2}$ (II)

Proposition 5.18. *For both Algorithms 5.1 and 5.2, the following holds: If the algorithm terminates, the output is correct, i. e. the constructed curve C of genus 2 has p-rank 1, is defined over $\mathbb{F}_{p^2}$, and has the stated prime number of $\mathbb{F}_{p^2}$-rational points.*

Proof. In both algorithms, we have $\pi\overline{\pi} = p^2$, so π is a p^2-Weil number. Let $\beta = p\alpha^{-1}\overline{\alpha}^{-1}$. Then p factors in K as a product of three primes $\alpha\overline{\alpha}\beta$, so the output has p-rank 1 by Lemma 5.16. By Section 5.1, the curve is defined over $\mathbb{F}_{p^2}$, and has a prime number $N(1-\pi)$ of $\mathbb{F}_{p^2}$-rational points on its Jacobian. □

Examples of curves such that their Jacobian group orders over $\mathbb{F}_{p^2}$ have cryptographic relevant bitsizes are given in the next subsection. The curves were constructed using Algorithm 5.1.

5.2.4 Examples

The following examples each describe a p-rank-1 curve C defined over a quadratic field $\mathbb{F}_{p^2}$ such that the Jacobian variety $J_C(\mathbb{F}_{p^2})$ has prime order. The CM field is $K = \mathbb{Q}(\omega)$ in each case, where ω is a root of $X^4 + 34X^2 + 217 \in \mathbb{Q}[X]$. We give the prime p, the coefficients a_1 and a_2 of the characteristic polynomial of the Frobenius endomorphism and the coefficients $c_i \in \mathbb{F}_{p^2}$ of the curve equation

$$C : y^2 = c_6x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0.$$

The group order of the Jacobian can be computed as $\#J_C(\mathbb{F}_{p^2}) = p^4 + 1 + a_1(p^2 + 1) + a_2$. The field $\mathbb{F}_q = \mathbb{F}_{p^2}$ is given as $\mathbb{F}_p(\sigma)$, where σ has the minimal polynomial $f_\sigma = X^2 + 3 \in \mathbb{F}_p[X]$ in each case, i. e. $\sigma = \sqrt{-3}$. Section headings describe the size of the group $J_C(\mathbb{F}_{p^2})$ in bits. The three example bit sizes are suitable for the 80-, 96- and 128-bit security levels.

160-bit groupsize

$$\begin{aligned}
p &= 924575392409 \\
a_1 &= -3396725192754 \\
a_2 &= 4585861472127472591045899 \\
c_6 &= 377266258806 \cdot \sigma + 915729517707 \\
c_5 &= 494539789092 \cdot \sigma + 415576796385 \\
c_4 &= 904019288751 \cdot \sigma + 345679289510 \\
c_3 &= 309144556572 \cdot \sigma + 430866212243 \\
c_2 &= 58888332305 \cdot \sigma + 588111907455 \\
c_1 &= 115624782924 \cdot \sigma + 580418244294 \\
c_0 &= 156203470202 \cdot \sigma + 110258906818
\end{aligned}$$

192-bit groupsize

$$\begin{aligned}
p &= 236691298903769 \\
a_1 &= 9692493559086 \\
a_2 &= 530533696777087086503612380 59 \\
c_6 &= 52558588104658 \cdot \sigma + 99902692259559 \\
c_5 &= 52389593530844 \cdot \sigma + 158973424741312 \\
c_4 &= 218737207208837 \cdot \sigma + 181252769658898 \\
c_3 &= 172428310717706 \cdot \sigma + 8801118005418 \\
c_2 &= 123239683911263 \cdot \sigma + 7283283410239 \\
c_1 &= 153772853838243 \cdot \sigma + 205198867568386 \\
c_0 &= 215981952231090 \cdot \sigma + 34417850754628
\end{aligned}$$

256-bit groupsize

$$
\begin{aligned}
p &= 15511800964685067143 \\
a_1 &= -2183138494024250742 \\
a_2 &= -39017145289396584451285841707586429955 9 \\
c_6 &= 4150612463019545210 \cdot \sigma + 12947607883594839049 \\
c_5 &= 1151467134418557330 \cdot \sigma + 14300579473277935991 \\
c_4 &= 1530498141898130345 \cdot \sigma + 14555772239394475007 \\
c_3 &= 1718208704069543708 \cdot \sigma + 3224111154139828576 \\
c_2 &= 13826236770513916637 \cdot \sigma + 8502326661843998285 \\
c_1 &= 1128433341144760472 \cdot \sigma + 6897664900087390978 \\
c_0 &= 456182377334184445 \cdot \sigma + 12945866133209209503
\end{aligned}
$$

5.3 Prescribed embedding degree in genus 2

In genus 2 similar to genus 1 we may take supersingular Jacobians for pairing-based cryptosystems, because as in genus 1 there also exists an upper bound on the embedding degree. Galbraith [Gal02] shows that this upper bound is 12 in genus 2. For achieving better security levels, one needs to find Jacobians for which it is larger. Again, we need to look for non-supersingular curves.

Example 5.19. Freeman, Stevenhagen, and Streng [FSS08] propose an algorithm to construct ordinary simple abelian varieties which have a prescribed embedding degree. By applying the CM method, the algorithm can be used to construct hyperelliptic curves of genus 2 or 3 with small embedding degree.
Let K be a quartic CM field, $k \in \mathbb{N}$ the desired embedding degree, and r a prime, the supposed prime divisor of the group order. A q-Weil number π fulfilling the conditions

$$
\begin{aligned}
\mathrm{N}_{K/\mathbb{Q}}(1-\pi) &\equiv 0 \pmod{r}, \\
\Phi_k(\pi\overline{\pi}) &\equiv 0 \pmod{r}.
\end{aligned}
$$

can be found as the type norm of an element in the ring $\mathcal{O}_{\widehat{K}}$ of integers of the reflex field $\widehat{K}$ of K. This element is constructed using the prime decomposition of r in $\mathcal{O}_{\widehat{K}}$. From Lemma 1.108 and Remark 5.7, it follows that r divides the group order and k is the embedding degree of the constructed curve.

Example 5.20. Freeman [Fre08] shows that it is possible to do the algorithm of Freeman, Stevenhagen, and Streng [FSS08] with the prime r parametrized by a polynomial $r(x) \in \mathbb{Z}[x]$. This results in parametrizations $\pi(x) \in K[x]$ such that $q(x) = \pi(x)\bar{\pi}(x)$ represents primes. Once such a parametrization is found, one looks

for an integer x_0 which leads to $\pi = \pi(x_0)$ and $q = q(x_0)$ fulfilling the conditions from the previous example. The CM method can be used to actually find examples. It turns out that, as in the elliptic curve case, ρ-values tend to be smaller than those obtained by the unparametrized method. Freeman gives examples with ρ-value around 6.

Example 5.21. Kawazoe and Takahashi [KT08] restrict to hyperelliptic curves of genus 2 with an equation $y^2 = x^5 + ax$. The advantage of using such a curve is that for certain primes p the group order of the Jacobian over $\mathbb{F}_p$ can directly be determined by a formula which depends on p and a. This means that one can directly choose parameters such that the conditions for a small embedding degree are satisfied.
As an example for primes $p \equiv 1, 3 \pmod 8$ of the form $p = c^2 + 2d^2$ where $c, d \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$, Kawazoe and Takahashi take explicit formulas for the characteristic polynomial $f_{J_C}(T)$ determined by Furukawa, Kawazoe, and Takahashi [FKT04] corresponding to a curve of the given form. The formulas can be found by computing Jacobsthal sums over characters of $\mathbb{F}_p$ which is possible for the curves of this form. Since these formulas depend on c, d, and a only, one may solve the system

$$\begin{aligned} f_{J_C}(1) &\equiv 0 \pmod r, \\ \Phi_k(p) &\equiv 0 \pmod r, \\ p &= c^2 + 2d^2, \text{ with } c \equiv 1 \pmod 4 \end{aligned}$$

for a prime r chosen in advance. This gives curve parameters directly without going through the effort of the CM method. Solutions to the above system are first computed modulo r and then lifted to the integers until a suitable prime p is found. Therefore, c and d are roughly of the size of r which leads to p being roughly of the size of r^2. This shows that such Jacobians have a ρ-value of about 4.

5.4 Prescribed embedding degree for p-rank 1

Algorithm 5.3 can be used to construct hyperelliptic curves of genus 2 with p-rank 1 and a prescribed embedding degree. It is modeled after the method by Freeman, Stevenhagen, and Streng [FSS08].

Proposition 5.22. *If Algorithm 5.3 terminates, then the constructed curve has p-rank 1 and embedding degree k with respect to the prime r.*

Proof. The number π is defined in Step 5 by $\pi = \alpha^2\beta$, where p factors into primes of $\mathcal{O}_K$ as $\alpha\overline{\alpha}\beta$, just as in Algorithm 5.2. In particular, the facts that the output has p-rank 1 and a Jacobian of order $N(1-\pi)$ are proved as in the proof of Proposition 5.18. We follow [FSS08] to proof that the embedding degree of the constructed curve is k. Recall that r splits completely in K, i. e. in $\mathcal{O}_K$ it decomposes as $(r) = \mathfrak{r}\overline{\mathfrak{r}}\mathfrak{q}\overline{\mathfrak{q}}$. We use the notation of the algorithm, where $\mathfrak{q}\overline{\mathfrak{q}} = \mathfrak{s}$. Furthermore, p decomposes in $\mathcal{O}_K$

Input: A non-Galois CM field K of degree 4 with real quadratic subfield K_0, a positive integer k, and a prime $r \equiv 1 \pmod{2k}$ which splits completely in K.
Output: A prime p and a curve C of genus 2 over $\mathbb{F}_{p^2}$ that has p-rank 1 and embedding degree k with respect to r.
1: Let $\mathfrak{r}$ be a prime of K dividing r and let $\mathfrak{s} = r\mathfrak{r}^{-1}\overline{\mathfrak{r}}^{-1}$.
2: Choose a random element x of $\mathbb{F}_r^*$ and a primitive $2k$th root of unity ζ.
3: Compute $\alpha \in \mathcal{O}_K \setminus \mathcal{O}_{K_0}$ such that

$$\alpha \bmod \mathfrak{r} = x, \ \alpha \bmod \overline{\mathfrak{r}} = x\zeta, \ \alpha \bmod \mathfrak{s} = x^{-1}$$

using the Chinese Remainder Theorem.
4: If $p = N(\alpha)$ is prime in $\mathbb{Z}$ and different from r, continue.
Otherwise, go to Step 2.
5: If $\beta = p\alpha^{-1}\overline{\alpha}^{-1}$ is prime in $\mathcal{O}_{K_0}$ and remains prime in $\mathcal{O}_K$, let $\pi = \alpha^2\beta$.
Otherwise, go to Step 2.
6: Compute a curve C corresponding to K, p, and π using the CM method.
7: **return** p, C.

Algorithm 5.3: Generate p-rank-1 curves of genus 2 over $\mathbb{F}_{p^2}$ with prescribed embedding degree

as $(p) = \alpha\overline{\alpha}\beta$, where β is a prime in $\mathcal{O}_K$ and in $\mathcal{O}_{K_0}$ and $\alpha\overline{\alpha}$ is a prime in $\mathcal{O}_{K_0}$. The field K_0 is normal of degree 2 over $\mathbb{Q}$, and thus it has a non-trivial automorphism ϕ. Since $\alpha\overline{\alpha}$ and β are not in $\mathbb{Q}$, it follows $\phi(\alpha\overline{\alpha}) = \beta$.
We find $\pi \bmod \mathfrak{r} = (\alpha \bmod \mathfrak{r})^2(\phi(\alpha\overline{\alpha}) \bmod \mathfrak{r})$. In $\mathbb{F}_r$, the right hand side is equal to $(\alpha \bmod \mathfrak{r})^2(\alpha \bmod \mathfrak{s})^2 = 1$, so $r \mid N(1-\pi)$. On the other hand,

$$\begin{aligned} p^2 \bmod \mathfrak{r} &= (\alpha \bmod \mathfrak{r})^2(\overline{\alpha} \bmod \mathfrak{r})^2(\phi(\alpha\overline{\alpha}) \bmod \mathfrak{r})^2 \\ &= (\alpha \bmod \mathfrak{r})^2(\alpha \bmod \overline{\mathfrak{r}})^2(\alpha\overline{\alpha} \bmod \mathfrak{s})^2. \end{aligned}$$

As $\mathfrak{s} = \overline{\mathfrak{s}}$, we have $(\overline{\alpha} \bmod \mathfrak{s}) = (\alpha \bmod \overline{\mathfrak{s}}) = (\alpha \bmod \mathfrak{s})$, so $p^2 \bmod r = (\alpha \bmod \mathfrak{r})^2(\alpha \bmod \overline{\mathfrak{r}})^2(\alpha \bmod \mathfrak{s})^4 = \zeta^2$ is a primitive kth root of unity. By Lemma 1.108 and Remark 5.7, the facts that p^2 is a primitive kth root of unity modulo r and that $r \mid N(1-\pi)$ imply that J_C has embedding degree k with respect to r. □

Freeman, Stevenhagen, and Streng [FSS08] give a heuristic analysis of their method. They show in [FSS08, Theorem 3.4] that one expects the prime q to yield a ρ-value of about 8 for genus 2, which means that $\log(q) = 4\log(r)$. The same reasoning holds for our algorithm. The prime p computed as the norm of the element α in Step 4 is therefore expected to give $\log(p) = 4\log(r)$. Since the constructed p-rank-1 curve is defined over $\mathbb{F}_{p^2}$, its ρ-value is $\rho = 2\log(p^2)/\log(r) \approx 16$.
Since the curves are defined over $\mathbb{F}_{p^2}$, and since pairing values are rth roots of unity, the embedding field could be smaller than indicated by the embedding degree k when working with odd k (as pointed out by Hitt [Hit07]). This influences the security of pairing-based protocols. But loss of security can easily be avoided by choosing

curves with an even embedding degree k or by explicitly checking if the rth roots of unity are already defined over a smaller extension of $\mathbb{F}_p$.
For cryptographic applications, one requires that the prime r has at least 160 bits, since r is the order of the subgroup used in protocols. Then p already has 640 bits. This makes field and curve arithmetic very slow, compared to elliptic curve implementations of the same security level, where it is possible to have r of the same size as p.
Thus the curves produced by algorithm 5.3 currently have no relevance for practical applications in cryptography. Still, we may conclude that in principle pairing-based cryptography seems possible for p-rank 1.

Appendix A

Compressed torus arithmetic

A.1 Verification of formulas

We verify the formulas given in Lemma 3.18: Let $\alpha, \beta \in T_6(\mathbb{F}_q) \setminus \{1\}$ with $\theta_6(\alpha) = (a_0, a_1)$, $\theta_6(\beta) = (b_0, b_1)$, and $(a_0, a_1) \neq (-b_0, -b_1)$. We first give the Magma [BCP97] code of the formulas in the lemma:

```
R<a0,b0,a1,b1,xi> := PolynomialRing(Rationals(),5);

r0 := a0^2 + 1/3*xi;
r1 := b0^2 + 1/3*xi;
s0 := xi*(a1*b1*(a0*b0 + xi) + a1^2*r1 + b1^2*r0);
s1 := a1*b1*xi*(a0*b1 + a1*b0) + r0*r1;
s2 := a1^2*b1^2*xi + a0*a1*r1 + b0*b1*r0;
t0 := a1*b1*xi*(a0 + b0);
t1 := a1*b1*xi*(a1 + b1);
t2 := b1*r0 + a1*r1;
u := t0^3 + t1^3*xi + t2^3*xi^2 - 3*xi*t0*t1*t2;
u0 := t0^2 - t1*t2*xi;
u1 := t2^2*xi - t0*t1;
u2 := t1^2 - t0*t2;
v0 := s0*u0 + s1*u2*xi + s2*u1*xi;
v1 := s0*u1 + s1*u0 + s2*u2*xi;
```

The compressed representative is then given as $(v_0/u, v_1/u)$. The formulas can be deduced as follows: Recall that

$$\begin{aligned} X_\alpha &= a_0 + a_1\tau + a_2\tau^2 \text{ with } a_2 = (3a_0^2 + \xi)/(3a_1\xi), \\ X_\beta &= b_0 + b_1\tau + b_2\tau^2 \text{ with } b_2 = (3b_0^2 + \xi)/(3b_1\xi). \end{aligned}$$

Then $\alpha\beta$ is represented by $\theta_6(\alpha\beta) = (c_0, c_1)$. It holds $X_{\alpha\beta} = c_0 + c_1\tau + c_2\tau^2$ and

$\alpha\beta = (X_{\alpha\beta} - \sigma)/(X_{\alpha\beta} + \sigma)$. By Lemma 3.8 it is

$$X_{\alpha\beta} = \frac{X_\alpha X_\beta + \xi}{X_\alpha + X_\beta}.$$

We multiply in numerator and denominator with $a_1 b_1 \xi$. The fraction $X_{\alpha\beta}$ can then be computed as $(d_0+d_1\tau+d_2\tau^2)/(e_0+e_1\tau+e_2\tau^2)$. The following code can be used to determine the coefficients of $d_0+d_1\tau+d_2\tau^2 := a_1 b_1 \xi(X_\alpha X_\beta+\xi)$ and $e_0+e_1\tau+e_2\tau^2 := a_1 b_1 \xi(X_\alpha + X_\beta)$:

```
d0 :=  a0*b0*a1*b1*xi + b0^2*a1^2*xi + 1/3*a1^2*xi^2
       + a0^2*b1^2*xi + 1/3*b1^2*xi^2 + a1*b1*xi^2;
d1 :=  a0*a1*b1^2*xi + a1^2*b0*b1*xi + a0^2*b0^2
       + 1/3*a0^2*xi + 1/3*b0^2*xi + (1/3*xi)^2;
d2 :=  a1^2*b1^2*xi + a0*a1*b0^2 + 1/3*a0*a1*xi
       + a0^2*b0*b1 + 1/3*b0*b1*xi;

e0 :=  (a0 + b0)*a1*b1*xi;
e1 :=  (a1 + b1)*a1*b1*xi;
e2 :=  b1*(a0^2 + 1/3*xi) + a1*(b0^2 + 1/3*xi);
```

We compute $1/(e_0 + e_1\tau + e_2\tau^2)$ as

$$\frac{(e_0 + e_1\zeta\tau + e_2\zeta^2\tau^2)(e_0 + e_1\zeta^2\tau + e_2\zeta\tau^2)}{N_{\mathbb{F}_{q^3}/\mathbb{F}_q}(e_0 + e_1\tau + e_2\tau^2)}.$$

where $\zeta \in \mathbb{F}_q$ is the primitive 3rd root of unity with $\tau^q = \zeta\tau$. The numerator $f_0 + f_1\tau + f_2\tau^2 := (e_0 + e_1\zeta\tau + e_2\zeta^2\tau^2)(e_0 + e_1\zeta^2\tau + e_2\zeta\tau^2)$ and the denominator $g := N_{\mathbb{F}_{q^3}/\mathbb{F}_q}(e_0 + e_1\tau + e_2\tau^2)$ can be computed as follows:

```
f0 :=  e0^2 - e1*e2*xi;
f1 :=  e2^2*xi - e0*e1;
f2 :=  e1^2 - e0*e2;

 g :=  (e0^3 + e1^3*xi + e2^3*xi^2 - 3*xi*e0*e1*e2);
```

Finally we calculate the product $(h_0+h_1\tau+h_2\tau^2) := (f_0+f_1\tau+f_2\tau^2)(d_0+d_1\tau+d_2\tau^2)$:

```
h0 :=  d0*f0 + d1*f2*xi + d2*f1*xi;
h1 :=  d0*f1 + d1*f0 + d2*f2*xi;
h2 :=  d0*f2 + d1*f1 + d2*f0;
```

The result is then given as $X_{\alpha\beta} = (h_0 + h_1\tau + h_2\tau^2)/g$, represented by $(h_0/g, h_1/g)$, and it can be checked that $h_0 = v_0$, $h_1 = v_1$, and $g = u$, and thus the formulas for multiplication given in Lemma 3.18 are correct.

The formulas for squaring can be checked similarly: We first give the Magma code of the squaring formulas.

```
R<a0,a1,xi> := PolynomialRing(Rationals(),3);

r0 := a0^5 + xi*(a0^3 - 2*a0^2*a1^3) + xi^2*(1/3*a0 - a1^3);
r1 := a0^5 + xi*(2*a0^3 - 2*a0^2*a1^3) + xi^2*(a0 - 2*a1^3);
s0 := a0*(a0*r0 + a1^6*xi^2 + 1/27*xi^3) - 1/3*a1^3*xi^3;
s1 := a1*(a0*r1 + a1^6*xi^2 + 4/27*xi^3);
s := 2*(a0*r0 + a1^6*xi^2 + 1/27*xi^3);
```

Then the square is represented as $(s_0/s, s_1/s)$. To obtain these formulas we conduct the following steps: Compute

$$X_{\alpha^2} = \frac{X_\alpha^2 + \xi}{2X_\alpha}$$

by $(d_0 + d_1\tau + d_2\tau^2)/(e_0 + e_1\tau + e_2\tau^2)$, where $d_0 + d_1\tau + d_2\tau^2 := a_1^2\xi(X_\alpha^2 + \xi)$ and $e_0 + e_1\tau + e_2\tau^2 := 2a_1^2\xi X_\alpha$.

```
d0 :=  3*a0^2*a1^2*xi + 5/3*a1^2*xi^2;
d1 :=  2*a0*a1^3*xi + a0^4 + 2/3*a0^2*xi + (1/3*xi)^2;
d2 :=  a1^4*xi + 2*a0^3*a1 + 2/3*a0*a1*xi;

e0 :=  2*a0*a1^2*xi;
e1 :=  2*a1^3*xi;
e2 :=  2*a0^2*a1 + 2/3*a1*xi;
```

We invert $e_0 + e_1\tau + e_2\tau^2$ and multiply the inverse with $d_0 + d_1\tau + d_2\tau^2$ exactly as for multiplication.

```
f0 :=  e0^2 - e1*e2*xi;
f1 :=  e2^2*xi - e0*e1;
f2 :=  e1^2 - e0*e2;

 g :=  (e0^3 + e1^3*xi + e2^3*xi^2 - 3*xi*e0*e1*e2);

h0 :=  d0*f0 + d1*f2*xi + d2*f1*xi;
h1 :=  d0*f1 + d1*f0 + d2*f2*xi;
h2 :=  d0*f2 + d1*f1 + d2*f0;
```

It can be checked that $g = 4s\xi^2 a_1^3$, $h_0 = 4s_0\xi^2 a_1^3$, and $h_1 = 4s_1\xi^2 a_1^3$. Therefore, $h_0/g = s_0/s$ and $h_1/g = s_1/s$, which shows that the formulas for squaring are also correct.

A.2 Pseudo code

The two algorithms given here show three-operand pseudo code for multiplication and squaring of elements of $T_6(\mathbb{F}_{p^2})$ in compressed representation. They realize the formulas in Example 3.25.

Input: $(A_0 : A_1 : A) \in \mathbb{P}^2(\mathbb{F}_{p^2}),\ A \in \mathbb{F}_p$
Output: $(C_0 : C_1 : C)$ representing the square of $(A_0 : A_1 : A)$

1: $r_1 \leftarrow A_0^2$,
2: $r_2 \leftarrow A_0 r_1$,
3: $S_0 \leftarrow r_1 r_2$,
4: $t_0 \leftarrow A^2$,
5: $r_4 \leftarrow r_2 t_0$,
6: $r_5 \leftarrow A_1^2$,
7: $r_5 \leftarrow A_1 r_5$,
8: $r_3 \leftarrow r_1 r_5$,
9: $r_4 \leftarrow r_4 - r_3$,
10: $r_0 \leftarrow r_4 \xi$,
11: $r_0 \leftarrow 2r_0$,
12: $S_1 \leftarrow S_0 + r_0$,
13: $r_4 \leftarrow r_4 - r_3$,
14: $r_4 \leftarrow r_4 \xi$,
15: $S_0 \leftarrow S_0 + r_4$,
16: $t_1 \leftarrow t_0^2$,
17: $r_4 \leftarrow t_1 A_0$,
18: $r_0 \leftarrow \frac{1}{3} r_4$,
19: $r_1 \leftarrow r_5 t_0$,
20: $r_0 \leftarrow r_0 - r_1$,
21: $r_1 \leftarrow 2r_1$,
22: $r_4 \leftarrow r_4 - r_1$,
23: $r_0 \leftarrow \xi^2 r_0$,
24: $r_4 \leftarrow \xi^2 r_4$,
25: $S_0 \leftarrow S_0 + r_0$,
26: $S_0 \leftarrow S_0 A_0$,
27: $S_1 \leftarrow S_1 + r_4$,
28: $S_1 \leftarrow S_1 A_0$,
29: $r_2 \leftarrow r_5^2$,
30: $r_2 \leftarrow r_2 \xi^2$,
31: $r_4 \leftarrow t_1 t_0$,
32: $r_4 \leftarrow \frac{1}{27} \xi^3 r_4$,
33: $r_1 \leftarrow r_2 + r_4$,
34: $S_0 \leftarrow S_0 + r_1$,
35: $S \leftarrow S_0 A$,
36: $S_0 \leftarrow S_0 A_0$,
37: $S \leftarrow 2S$,
38: $r_4 \leftarrow 4r_4$,
39: $r_1 \leftarrow r_2 + r_4$,
40: $S_1 \leftarrow S_1 + r_1$,
41: $S_1 \leftarrow S_1 A_1$,
42: $r_1 \leftarrow r_5 t_1$,
43: $r_1 \leftarrow \frac{1}{3} \xi^3 r_1$,
44: $S_0 \leftarrow S_0 - r_1$,
45: Write $S = s_0 + i s_1$,
46: $r_1 \leftarrow (s_0 - i s_1)$,
47: $C_0 \leftarrow S_0 r_1$,
48: $C_1 \leftarrow S_1 r_1$,
49: $C \leftarrow S r_1 = s_0^2 + c s_1^2$,
50: **return** $(C_0 : C_1 : C)$

Algorithm A.1: Compressed squaring in $T_6(\mathbb{F}_{p^2})$ for $k = 12$.

Input: $(A_0 : A_1 : A), (B_0 : B_1 : B) \in \mathbb{F}_{p^2} \times \mathbb{F}_{p^2} \setminus \{0\} \times \mathbb{F}_p$
Output: $(C_0 : C_1 : C) = (A_0 : A_1 : A) \cdot (B_0 : B_1 : B)$

1: $R_0 \leftarrow A_0^2$,
2: $t_1 \leftarrow A^2$,
3: $r_3 \leftarrow \frac{1}{3}\xi t_1$,
4: $R_0 \leftarrow R_0 + r_3$,
5: $R_1 \leftarrow B_0^2$,
6: $t_1 \leftarrow B^2$,
7: $r_3 \leftarrow \frac{1}{3}\xi t_1$,
8: $R_1 \leftarrow R_1 + r_3$
9: $r_3 \leftarrow A_1 B_1$,
10: $r_4 \leftarrow A_0 B_0$,
11: $t_1 \leftarrow AB$,
12: $r_5 \leftarrow t_1\xi$,
13: $r_4 \leftarrow r_4 + r_5$,
14: $S_0 \leftarrow r_3 r_4$,
15: $S_2 \leftarrow r_3^2$
16: $S_2 \leftarrow S_2\xi$,
17: $r_4 \leftarrow A_0 B_1$,
18: $r_5 \leftarrow A_1 B_0$,
19: $r_4 \leftarrow r_4 + r_5$,
20: $r_6 \leftarrow r_3\xi$,
21: $S_1 \leftarrow r_6 r_4$,
22: $r_4 \leftarrow R_0 R_1$
23: $S_1 \leftarrow S_1 + r_4$,
24: $r_4 \leftarrow A_1 R_1$,
25: $r_5 \leftarrow r_4 A_0$,
26: $S_2 \leftarrow S_2 + r_5$,
27: $T_2 \leftarrow r_4 A$,
28: $r_4 \leftarrow r_4 A_1$,
29: $S_0 \leftarrow S_0 + r_4$,
30: $r_4 \leftarrow B_1 R_0$,
31: $r_5 \leftarrow r_4 B$,
32: $T_2 \leftarrow T_2 + r_5$,
33: $r_5 \leftarrow r_4 B_0$,
34: $S_2 \leftarrow S_2 + r_5$,
35: $r_4 \leftarrow r_4 B_1$,
36: $S_0 \leftarrow S_0 + r_4$,
37: $S_0 \leftarrow S_0\xi$,
38: $T_0 \leftarrow A_0 B$,
39: $r_4 \leftarrow B_0 A$,
40: $T_0 \leftarrow T_0 + r_4$,
41: $T_0 \leftarrow r_6 T_0$,
42: $T_1 \leftarrow A_1 B$,
43: $r_4 \leftarrow B_1 A$,
44: $T_1 \leftarrow T_1 + r_4$,
45: $T_1 \leftarrow T_1 r_6$
46: $r_0 \leftarrow T_0^2$,
47: $r_1 \leftarrow T_1^2$,
48: $r_2 \leftarrow T_2^2$,
49: $T \leftarrow r_0 T_0$,
50: $r_3 \leftarrow r_1 T_1$,
51: $r_3 \leftarrow r_3\xi$,
52: $T \leftarrow T + r_3$
53: $r_3 \leftarrow r_2 T_2$,
54: $r_3 \leftarrow r_3\xi^2$,
55: $T \leftarrow T + r_3$,
56: $r_3 \leftarrow T_1 T_2$,
57: $r_3 \leftarrow r_3\xi$,
58: $U_0 \leftarrow r_0 - r_3$,
59: $r_3 \leftarrow r_3 T_0$
60: $r_3 \leftarrow 3r_3$,
61: $T \leftarrow T - r_3$,
62: $r_3 \leftarrow T_0 T_1$,
63: $U_1 \leftarrow r_2\xi$,
64: $U_1 \leftarrow U_1 - r_3$,
65: $r_3 \leftarrow T_0 T_2$,
66: $U_2 \leftarrow r_1 - r_3$,
67: $V_0 \leftarrow S_0 U_0$,
68: $r_0 \leftarrow S_1 U_2$,
69: $r_1 \leftarrow S_2 U_1$,
70: $r_0 \leftarrow r_0 + r_1$,
71: $r_0 \leftarrow r_0\xi$,
72: $V_0 \leftarrow V_0 + r_0$,
73: $V_1 \leftarrow S_0 U_1$,
74: $r_0 \leftarrow S_1 U_0$,
75: $V_1 \leftarrow V_1 + r_0$,
76: $r_0 \leftarrow S_2 U_2$,
77: $r_0 \leftarrow r_0\xi$,
78: $V_1 \leftarrow V_1 r_0$,
79: Write $T = t_0 + it_1$,
80: $r_1 \leftarrow (t_0 - it_1)$,
81: $C_0 \leftarrow V_0 r_1$,
82: $C_1 \leftarrow V_1 r_1$,
83: $C \leftarrow Sr_1 = t_0^2 + ct_1^2$,
84: **return** $(C_0 : C_1 : C)$

Algorithm A.2: Compressed multiplication in $T_6(\mathbb{F}_{p^2})$ for $k = 12$.

Bibliography

[AM93] A. O. L. Atkin and Francois Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61:29–68, 1993. 43, 44

[Arè08] Christophe Arène. Etude d'un nouveau modèle pour les courbes elliptiques. Master Thesis at Institut de Mathématiques de Luminy, Marseille, 2008. 90

[BBJ+08] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. In *Progress in Cryptology – AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 389–405. Springer-Verlag, 2008. 26, 27, 100

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computing*, 24(3-4):235–265, 1997. 119

[BF01] Dan Boneh and Matthew Franklin. Identity-based encryption from the Weil pairing. In *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer-Verlag, 2001. 2, 32

[BF03] Dan Boneh and Matthew Franklin. Identity-based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003. 2, 32, 35

[BGOS07] Paulo S. L. M. Barreto, Steven D. Galbraith, Colm Ó hÉigeartaigh, and Michael Scott. Efficient pairing computation on supersingular abelian varieties. *Designs, Codes and Cryptography*, 42(3):239–271, 2007. 40

[BH62] Paul T. Bateman and Roger A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Mathematics of Computation*, 16(79):363–367, 1962. 49

[BK98] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes—Okamoto—Vanstone algorithm. *Journal of Cryptology*, 11(2):141–145, 1998. 3, 25, 42

[BL07] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *Advances in Cryptology – ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer-Verlag, 2007. 26, 27

[BLS04a] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Efficient implementation of pairing-based cryptosystems. *Journal of Cryptology*, 17(4):321–334, 2004. 38, 40

[BLS04b] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. *Journal of Cryptology*, 17(4):297–319, 2004. 32

[BN06] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptography – SAC 2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer-Verlag, 2006. 4, 47, 101

[BSS05] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, editors. *Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2005. 129, 132

[Can87] David G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Mathematics of Computation*, 48:95–101, 1987. 29

[CFD05] Henri Cohen, Gerhard Frey, and Christophe Doche, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall/CRC, 2005. 127, 128

[CMO98] Henri Cohen, Atsuko Miyaji, and Takatoshi Ono. Efficient elliptic curve exponentiation using mixed coordinates. In *Advances in Cryptology - ASIACRYPT '98*, volume 1514 of *Lecture Notes in Computer Science*, pages 51–65. Springer-Verlag, 1998. 101

[CN05] Zhaohui Cheng and Manos Nistazakis. Implementing pairing-based cryptosystems. In *3rd International Workshop on Wireless Security Technologies IWWST-2005*, 2005. 101, 102

[Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate texts in mathematics*. Springer-Verlag, 1993. 44

[CSB05] Sanjit Chatterjee, Palash Sarkar, and Rana Barua. Efficient computation of Tate pairing in projective coordinate over general characteristic fields. In *Information Security and Cryptology - ICISC 2004*, volume 3506 of *Lecture Notes in Computer Science*, pages 168–181. Springer-Verlag, 2005. 101, 102

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941. 24, 111

[DF05a] Sylvain Duquesne and Gerhard Frey. *Background on Pairings*, chapter 6 in [CFD05], pages 115–124. CRC press, 2005. 32, 33, 42

[DF05b] Sylvain Duquesne and Gerhard Frey. *Implementation of Pairings*, chapter 16 in [CFD05], pages 389–404. CRC press, 2005. 34

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976. 1

[DL05a] Christophe Doche and Tanja Lange. *Arithmetic of Elliptic Curves*, chapter 13 in [CFD05], pages 267–302. CRC press, 2005. 27, 59, 84

[DL05b] Sylvain Duquesne and Tanja Lange. *Arithmetic of Hyperelliptic Curves*, chapter 14 in [CFD05], pages 303–354. CRC press, 2005. 29, 30, 31

[Doc05a] Christophe Doche. *Exponentiation*, chapter 9 in [CFD05], pages 145–168. CRC press, 2005. 38

[Doc05b] Christophe Doche. *Finite Field Arithmetic*, chapter 11 in [CFD05], pages 201–237. CRC press, 2005. 38, 81

[DOSD06] Augusto J. Devegili, Colm Ó hÉigeartaigh, Michael Scott, and Ricardo Dahab. Multiplication and squaring on pairing-friendly fields. Cryptology ePrint Archive, Report 2006/471, 2006. http://eprint.iacr.org/. 83, 84

[DS08] M. Prem Laxman Das and Palash Sarkar. Pairing computation on twisted Edwards form elliptic curves. In *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 192–210. Springer-Verlag, 2008. 101

[DSD07] Augusto J. Devegili, Michael P. Scott, and Ricardo Dahab. Implementing cryptographic pairings over Barreto-Naehrig curves. In *Pairing-Based Cryptography – Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 197–207. Springer-Verlag, 2007. 63, 64, 65, 83, 84

[Edw07] Harold M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, 2007. 26

[EL04] Kirsten Eisentraeger and Kristin Lauter. A CRT algorithm for constructing genus 2 curves over finite fields, 2004. In Arithmetic, Geometry and Coding Theory - AGCT-10 (Marseille), 2005. 110

[FKT04] Eisaku Furukawa, Mitsuru Kawazoe, and Tetsuya Takahashi. Counting points for hyperelliptic curves of type $y^2 = x^5 + ax$ over finite prime fields. In *Selected Areas in Cryptography – SAC'2003*, volume 3006 of *Lecture Notes in Computer Science*, pages 26–41. Springer-Verlag, 2004. 116

[FL05a] Gerhard Frey and Tanja Lange. *Background on Curves and Jacobians*, chapter 4 in [CFD05], pages 45–85. CRC press, 2005. 5, 9, 15, 16, 17, 18, 20, 28, 29, 30, 103, 104, 105

[FL05b] Gerhard Frey and Tanja Lange. *Complex Multiplication*, chapter 18 in [CFD05], pages 455–473. CRC press, 2005. 44, 45, 109, 111

[FL05c] Gerhard Frey and Tanja Lange. *Varieties over Special Fields*, chapter 5 in [CFD05], pages 87–113. CRC press, 2005. 43, 109, 110, 111

[FR94] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206):865–874, 1994. 2, 32, 33

[Fre06] David S. Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. In *ANTS-VII: 7th International Symposium on Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Computer Science*, pages 452–465. Springer-Verlag, 2006. 46

[Fre08] David S. Freeman. A generalized Brezing-Weng method for constructing pairing-friendly ordinary abelian varieties. In *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 146–163. Springer-Verlag, 2008. 115

[FSS08] David S. Freeman, Peter Stevenhagen, and Marco Streng. Abelian varieties with prescribed embedding degree. In *ANTS-VIII: 8th International Symposium on Algorithmic Number Theory*, volume 5011 of *Lecture Notes in Computer Science*, pages 60–73. Springer-Verlag, 2008. 115, 116, 117

[FST06] David S. Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2006/372, 2006. Available from `http://eprint.iacr.org/2006/372`. 46

[Ful69] William Fulton. *Algebraic Curves*. W. A. Benjamin, Inc., 1969. 5, 9, 10, 12, 13, 87, 104

[Gal02] Steven D. Galbraith. Supersingular curves in cryptography. In *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 495–513. Springer-Verlag, 2002. 115

[Gal05] Steven D. Galbraith. *Pairings*, chapter IX in [BSS05], pages 183–214. Cambridge University Press, 2005. 37

[GH99] Guang Gong and Lein Harn. Public-key cryptosystems based on cubic finite field extensions. *IEEE Transactions on Information Theory*, 45(7):2601–2605, 1999. 71

[GHK+05] Pierrick Gaudry, Thomas Houtmann, David Kohel, Christophe Ritzenthaler, and Annegret Weng. The p-adic CM-method for genus 2, 2005. Available at http://arxiv.org/abs/math.NT/0503148. 111, 112

[GHK+06] Pierrick Gaudry, Thomas Houtmann, David Kohel, Christophe Ritzenthaler, and Annegret Weng. The 2-adic CM-method for genus-2 curves with application to cryptography. In *Advances in Cryptology - ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 114–129, Berlin, 2006. Springer-Verlag. 111

[GHW01] Guang Gong, Lein Harn, and Huapeng Wu. The GH public-key cryptosystem. In *Selected Areas in Cryptography – SAC 2001*, volume 2259 of *Lecture Notes in Computer Science*, pages 284–300. Springer-Verlag, 2001. 71

[GLV01] Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 190–200. Springer-Verlag, 2001. 56

[GMV07] Steven D. Galbraith, James F. McKee, and Paula C. Valença. Ordinary abelian varieties having small embedding degree. *Finite Fields and their Applications*, 13:800–814, 2007. 42, 46, 47, 48

[Gon98] Josep González. On the p-rank of an abelian variety and its endomorphism algebra. *Publicacions Matematiques*, 42(1):119–130, 1998. 108

[Gor97] Eyal Z. Goren. On certain reduction problems concerning abelian surfaces. *Manuscripta Mathematica*, 94(1):33–43, 1997. 111

[GPS06] Robert Granger, Dan Page, and Martijn Stam. On small characteristic algebraic tori in pairing based cryptography. *LMS Journal of Computation and Mathematics*, 9:64–85, March 2006. 71, 75, 78

[GS08] Steven D. Galbraith and Michael P. Scott. Exponentiation in pairing-friendly groups using homomorphisms. In *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 211–224. Springer-Verlag, 2008. 38, 56, 59

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate texts in mathematics*. Springer-Verlag, 1977. 5, 7, 9, 13, 17, 104, 107

[Heß08] Florian Heß. Pairing lattices. In *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 18–38. Springer-Verlag, 2008. 2, 41

[Hit07] Laura Hitt. On the minimal embedding field. In *Pairing-Based Cryptography – Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 294–301. Springer-Verlag, 2007. 33, 35, 117

[HMNS08] Laura Hitt O'Connor, Gary McGuire, Michael Naehrig, and Marco Streng. CM-construction of genus-2 curves of p-rank 1. Cryptology ePrint Archive, Report 2008/491, 2008. Available from http://eprint.iacr.org/2008/491. 4, 103

[HMS09] Darrel Hankerson, Alfred J. Menezes, and Michael Scott. *Software Implementation of Pairings*, chapter in [JN09], pages 188–206. IOS Press, 2009. 101

[Hon68] Taira Honda. Isogeny classes of abelian varieties over finite fields. *Journal of the Mathematical Society of Japan*, 20:83–95, 1968. 105

[HSV06] Florian Heß, Nigel P. Smart, and Frederik Vercauteren. The eta pairing revisited. *IEEE Transactions on Information Theory*, 52:4595–4602, 2006. 2, 24, 25, 39, 40, 55

[HWCD08] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Twisted Edwards curves revisited. In *Advances in Cryptology – ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Computer Science*, pages 326–343. Springer-Verlag, 2008. 99, 101

[Igu60] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *The Annals of Mathematics*, 72(3):612–649, 1960. 110

[IJ08] Sorina Ionica and Antoine Joux. Another approach to pairing computation in Edwards coordinates. In *Progress in Cryptology – INDOCRYPT 2008*, volume 5365 of *Lecture Notes in Computer Science*, pages 400–413. Springer-Verlag, 2008. 101, 102

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate texts in mathematics*. Springer-Verlag, 1990. 43, 53

[JN09] Marc Joye and Gregory Neven, editors. *Identity-Based Cryptography*, volume 2 of *Cryptology and Information Security Series*. IOS Press, 2009. 130

[Jou00] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. In *ANTS-IV: 4th International Symposium on Algorithmic Number Theory*, volume 1883 of *Lecture Notes in Computer Science*, pages 385–394. Springer-Verlag, 2000. 2, 32

[Kob87] Neil Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987. 1

[Kob89] Neil Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1(3):139–150, 1989. 1

[KT08] Mitsuru Kawazoe and Tetsuya Takahashi. Pairing-friendly hyperelliptic curves with ordinary Jacobians of type $y^2 = x^5 + ax$. In *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 164–177. Springer-Verlag, 2008. 116

[Lan83] Serge Lang. *Abelian Varieties*. Springer-Verlag, 1983. 103

[Lan87] Serge Lang. *Elliptic Functions*, volume 112 of *Graduate texts in mathematics*. Springer-Verlag, 1987. 44

[LLP08] Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park. Efficient and generalized pairing computation on abelian varieties. Cryptology ePrint Archive, Report 2008/040, 2008. http://eprint.iacr.org/2008/040. 2, 41

[LMS04] Florian Luca, David J. Mireles, and Igor E. Shparlinski. MOV attack in various subgroups on elliptic curves. *Illinois Journal of Mathematics*, 48(3):1041–1052, 2004. 3, 42

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1997. 41, 72

[Lor96] Dino Lorenzini. *An Invitation to Arithmetic Geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, 1996. 5, 10, 11, 14, 43

[LV00] Arjen K. Lenstra and Eric R. Verheul. The XTR public key system. In *Advances in Cryptology – CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 1–19. Springer-Verlag, 2000. 65, 71

[Mes91] Jean-Francois Mestre. Construction des courbes de genre 2 à partir de leurs modules. *Progress in Mathematics*, 94:313–334, 1991. 110

[Mil86a] Victor S. Miller. Short programs for functions on curves, 1986. Unpublished manuscript. http://crypto.stanford.edu/miller/. 3, 35

[Mil86b] Victor S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology – CRYPTO 1985*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer-Verlag, 1986. 1

[Mil04] Victor S. Miller. The Weil pairing and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, 2004. 35, 36, 37

[MKHO07] Seiichi Matsuda, Naoki Kanayama, Florian Heß, and Eiji Okamoto. Optimised versions of the ate and twisted ate pairings. In *Cryptography and Coding*, volume 4887 of *Lecture Notes in Computer Science*, pages 302–312. Springer-Verlag, 2007. 2, 41

[MN02] Daniel Maisner and Enric Nart. Abelian surfaces over finite fields as Jacobians. *Experimental Mathematics*, 11(3):321–337, 2002. With an appendix by Everett W. Howe. 107, 108, 109

[MNT01] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals*, E84-A(5):1234–1243, 2001. 45

[MOV93] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993. 2, 32, 35, 45

[Mum74] David Mumford. *Abelian Varieties*. Oxford University Press, 1974. 103, 104, 105, 106

[NBS08] Michael Naehrig, Paulo S. L. M. Barreto, and Peter Schwabe. On compressible pairings and their computation. In *Progress in Cryptology – AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 371–388. Springer-Verlag, 2008. 4, 71

[Pat05] Kenneth G. Paterson. *Cryptography from Pairings*, chapter X in [BSS05], pages 215–251. Cambridge University Press, 2005. 2

[RS03] Karl Rubin and Alice Silverberg. Torus-based cryptography. In *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 349–365. Springer-Verlag, 2003. 71, 72, 73

[RS08] Karl Rubin and Alice Silverberg. Using abelian varieties to improve pairing-based cryptography. *Journal of Cryptology*, 2008. to appear, DOI 10.1007/s00145-008-9022-1. 35

[Rüc90] Hans-Georg Rück. Abelian surfaces and Jacobian varieties over finite fields. *Compositio Mathematica*, 76(3):351–366, 1990. 31, 107, 108

[SB04] Michael P. Scott and Paulo S. L. M. Barreto. Compressed pairings. In *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 140–156. Springer-Verlag, 2004. 65, 71

[SBC+08] Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa. On the final exponentiation for calculating pairings on ordinary elliptic curves. Cryptology ePrint Archive, Report 2008/490, 2008. http://eprint.iacr.org/2008/490. 38, 63

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44:483–494, 1985. 23

[Sch87] René Schoof. Nonsingular plane cubic curves over finite fields. *Journal of Combinatorial Theory, series A*, 46:183–211, 1987. 24

[Shi97] Goro Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1997. 103, 107, 111

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate texts in mathematics*. Springer-Verlag, 1986. 5, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 36, 43, 53, 106

[SL93] Peter J. Smith and Michael J. J. Lennon. LUC: A new public key system. In E. Graham Dougall, editor, *Computer Security, Proceedings of the IFIP TC11, Ninth International Conference on Information Security, IFIP/Sec '93, Toronto, Canada, 12-14 May 1993*, volume A-37 of *IFIP Transactions*, pages 103–117. North-Holland, 1993. 71

[SOK00] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems based on pairing. In *2000 Symposium on Cryptography and Information Security – SCIS 2000*, 2000. 2, 32

[Spa94] Anne-Monika Spallek. *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994. 110

[Sti93] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, 1993. 5, 11, 13, 14, 17

[Str08] Marco Streng. Computing Igusa class polynomials. preprint on http://www.math.leidenuniv.nl/∼streng/icp.pdf, 2008. 110

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2:134–144, 1966. 105, 106

[Tat71] John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda). *Séminaire N. Bourbaki 1968/69, No.352*, pages 95–110, 1971. 105, 106

[Ver08] Frederik Vercauteren. Optimal pairings. Cryptology ePrint Archive, Report 2008/096, 2008. http://eprint.iacr.org/2008/096. 2, 41, 65

[vW99] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Mathematics of Computation*, 68(225):307–320, 1999. 110

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieur, 4e série*, 2(4):521–560, 1969. 24, 48

[Wen01] Annegret Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 2001. 110

[ZZH08] Chang-An Zhao, Fangguo Zhang, and Jiwu Huang. A note on the ate pairing. *International Journal of Information Security*, 7(6):379–382, 2008. 2, 40, 63

Index

$\mathbb{F}$-rational divisor, 16
ρ-value, 41
j-invariant, 18
m-torsion points, 30
p-rank, 30, 104
    of abelian variety, 104
q-Weil number, 105
q-Weil polynomial, 105

abelian variety, 17, 103
    simple, 104
absolutely irreducible, 9
addition, 20
affine space, 5
algebraic group, 17
algebraic set, 9
algebraic torus, 71
ate pairing, 40, 64
    twisted, 40, 63
automorphism, 21

Bézout's Theorem, 13
birational equivalence, 26
birational map, 15
birationally equivalent, 15
BN curve, 47
    automorphisms, 53
    construction of, 48, 51
    endomorphism ring, 52
    Frobenius endomorphism, 53
    pairings, 61
    parametrization, 48
    twist of, 54
BN prime pair, 49

Cantor's algorithm, 29
characteristic polynomial, 104
class number, 43
CM, 22, 42, 106
CM field, 106
CM method, 43–45, 109
CM norm equation, 45
CM type, 106
    primitive, 106
complex multiplication, 22, 42, 43, 103
complex torus, 109
compressed pairing, 76, 80
compressed pairing computation, 71
compression, 65, 66
conic, 6, 8, 86
    affine (plane), 6
    projective (plane), 8
coordinate ring, 13
    homogeneous, 14
cryptographic pairing, 32
cubic, 6, 8
    affine (plane), 6
    projective (plane), 8
cubic twist, 16
curve
    absolutely irreducible, 9
    affine, 6
    affine plane, 6
    elliptic, 17
    nonsingular, 10
    projective, 7
    projective plane, 8
    singular, 10
cyclotomic polynomial, 72

degree, 15, 16
    of a divisor, 16
    of a morphism, 15

of a twist, 16
degree of twist, 23
dehomogenization, 8
discriminant, 18
divisor, 16
defined over $\mathbb{F}$, 16
effective, 17
positive, 17
principal, 16
divisor class group, 16
doubling, 20
dual lattice, 109

Edwards curve, 26, 85, 90
conic, 87
functions, 93
geometric interpretation of group law, 93
group law, 26, 90
Miller's formula, 93
twisted, 85
effective divisor, 17
efficient endomorphism, 56
eigenspace, 25
eigenvalue, 25
elliptic curve, 17
j-invariant, 18
automorphism, 21
discriminant, 18
endomorphism ring, 21
group law, 19
ordinary, 24
supersingular, 24, 45
torsion subgroup, 21
twist, 22, 24
embedding degree, 25, 33, 41
endomorphism, 29, 104
endomorphism algebra, 104
endomorphism ring, 21, 104
of abelian variety, 104
Eta pairing, 40

final exponentiation, 34, 73, 75, 78
form, 14

Freeman curves, 46
Frobenius endomorphism, 23, 53, 105
characteristic polynomial, 53
eigenspace, 25, 39, 62
eigenvalue, 25
function field, 13, 14
rational, 11

Galois group, 14
genus, 17
geometric interpretation of group law, 20

Hasse's Theorem, 23
Hilbert class polynomial, 44
homogeneous polynomial, 7
homogenization, 8
homomorphism, 104
hyperelliptic curve, 28
hyperelliptic involution, 28

ideal class group, 43
Igusa class polynomial, 110
Igusa invariants, 110
imaginary quadratic field, 21
intersection multiplicity, 87
intersection number, 12
irreducibility, 9
irreducible
absolutely, 9
irreducible components, 9
irreducible space, 9
isogenous, 21, 104
isogeny, 21, 104
isomorphism, 15
of affine curves, 15
of projective curves, 15
isomorphism class, 19

Jacobian
endomorphism of, 29
Jacobian variety, 16

lattice, 43, 109
dual, 109
line, 6, 8, 86

affine, 5
affine (plane), 6
projective, 7
projective (plane), 8
line function, 76, 77
localization, 11
localization of the coordinate ring, 14

Miller function, 36, 76, 97
Miller's algorithm, 35, 38, 76
Miller's formula, 93
MNT curves, 45
Montgomery curve, 27
morphism, 15
of affine curves, 15
of projective curves, 15
multiplication-by-m map, 21, 29
Mumford representation, 29

norm, 72

optimal pairings, 41, 65
order, 14, 43
ordinary, 24
ordinary abelian variety, 105

pairing compression, 65, 71
pairings, 61
BN curves, 61
optimal, 41
Picard group, 16
plane
affine, 5
projective, 7
point
at infinity, 8
nonsingular, 10
projective, 7
rational, 6, 8
simple, 10
singular, 9, 10
point compression, 66
points at infinity, 8
polynomial
absolutely irreducible, 9
cyclotomic, 72
homogeneous, 7
positive divisor, 17
principal divisor, 16
principally polarized, 109
projective space, 6

quadratic twist, 16
quartic, 6, 8
affine (plane), 6
projective (plane), 8
quaternion algebra, 21

rational function, 11, 13
rational map, 15
defined over $\mathbb{F}$, 15
rational points, 6, 8
reduced Tate pairing, 34, 36
reflex field, 106
regular, 15
rho-value, 41
Riemann-Roch theorem, 17, 28

simple, 104
singular point, 9, 10
space
affine, 5
irreducible, 9
projective, 6
topological, 9
supersingular, 24, 45
supersingular abelian variety, 105
support of divisor, 16

tangent line, 10
Tate pairing, 33, 63
twisted, 39
topological space, 9
torsion point, 21, 104
torsion subgroup, 21
torus, 71, 72
trace, 65, 66
trace of Frobenius, 23

twist, 15, 22
    cubic, 16
    degree, 16, 23
    quadratic, 16
twisted ate pairing, 40, 63
twisted Edwards curve, 26
    group law, 27
twisted Tate pairing, 39, 77

uniformizing parameter, 14

valuation, 14

Weierstraß equation, 18
    short, 18
Weierstraß point, 28
Weil pairing, 35, 36

Zariski topology, 9

Summary

Constructive and Computational Aspects of Cryptographic Pairings

The security of many public-key cryptosystems relies on the existence of groups in which the discrete logarithm problem (DLP) is infeasible. Subgroups of the Jacobian varieties of elliptic and hyperelliptic curves over finite fields are widely used to realize such cryptosystems. On these groups, it is possible to define pairings. A cryptographic pairing is a bilinear, non-degenerate map that can be computed efficiently. It maps a pair of points in the Jacobian variety into the multiplicative group of a finite field.

Pairings were first used in cryptography to attack the DLP on a supersingular elliptic curve by reducing it to the DLP in a finite field that is easier to solve. Later on, they led to a variety of constructive applications. When aiming at practical implementation of pairings, there are two main problems arising: The first is to find pairing-friendly curves which allow an efficient pairing computation. The second is to make computations more efficient and suitable for different applications. This dissertation addresses aspects of both problems and advances the state of the art in the associated research areas.

An important condition for a pairing-friendly curve is to have an embedding degree that is small enough. Curves with this property are rare and need to be constructed. We give a method to construct pairing-friendly elliptic curves with embedding degree 12. The proposed curves have many nice properties favoring very efficient implementation, such as a prime order group of rational points over the ground field and a twist of degree 6.

The Jacobian group order of a pairing-friendly curve must have a large prime divisor which satisfies the embedding degree condition. It is therefore necessary to first fix the group order and then construct the curve. As an essential tool for the construction, one uses the complex multiplication (CM) method. We show how to use the CM method to construct curves of genus 2 with p-rank 1.

If pairings need to be implemented on devices with restricted memory, it may be interesting to compute pairings in compressed form. Using the fact that pairing values are elements of algebraic tori, they can be represented in a more efficient way, requiring less storage space than general field elements. We show how to do pairing

computation in a compressed form. On curves with a twist of degree 6 the proposed variant of Miller's algorithm can be done without any field inversions.
Recently, it has been shown, that in many cases the elliptic curve group law can be implemented most efficiently using Edwards curves. It was an open problem to find advantageous formulas for pairing computation on Edwards curves. We state a geometric interpretation of the group law on twisted Edwards curves, give the corresponding functions, and show how to use them to compute pairings on Edwards curves. We present explicit formulas for the doubling and addition steps in Miller's algorithm that are more efficient than all previously proposed formulas for pairings on Edwards curves and are competitive with formulas for pairing computation on Weierstraß curves.

Curriculum vitae

Michael Naehrig was born on February 17, 1977 in Stolberg (Rhld.), Germany.
In 1996, he graduated from the secondary school Goethe-Gymnasium in Stolberg. After his civilian service, he started his studies in mathematics and physics at RWTH Aachen University in 1997. He graduated with distinction in mathematics in 2002. Michael specialized in the representation theory of finite groups. His master's thesis is entitled *The Brauer Trees of the Monster M in Characteristic 29* and was supervised by Prof. Dr. Gerhard Hiß. During his studies, he worked as a student assistant. He led student problem sessions for various lectures, mainly in algebra and discrete mathematics.
From 2002 until the end of 2003, he worked as research and teaching assistant at the Institute of Transport Science at RWTH Aachen University, where he investigated the optimization of railway networks. Michael started his PhD studies in cryptography in 2004, when he worked as research and teaching assistant at the Institute for Theoretical Information Technology at RWTH Aachen University. He began research cooperation with Prof. Dr. Paulo S. L. M. Barreto and Prof. Dr. Tanja Lange. He supervised several master students in mathematics, computer science, and electrical engineering.
From April 2008 to May 2009, Michael was a PhD student in the coding theory and cryptology group at Technische Universiteit Eindhoven, the Netherlands, under the supervision of Prof. Dr. Tanja Lange. The present dissertation contains the results of his work between 2004 and 2009.
His research interests are in the areas of curve-based cryptography, pairing-based cryptography, and arithmetic geometry.