Sebastian Ramacher, MSc BSc BSc

Bilinear Pairings on Elliptic Curves

Master Thesis

to achieve the university degree of

Diplom-Ingenieur

Master degree programme: Computer Science

submitted to

Graz University of Technology

Supervisor: Dipl.-Ing. Christian Hanser
Assessor: Univ.-Prof. Dipl.-Ing. Dr.techn. Stefan Mangard

Institute for Applied Information
Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a
8010 Graz, Austria

October, 2015

Affidavit

I declare that I have authored this thesis independently, that I have not used other than the dclard sources/resources, and that I have explicitely indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master thesis.

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbständig verfasst, anders als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Masterarbeit identisch.

Sebastian Ramacher

Acknowledgements

I would like to express my sincere gratitude to my advisor Christian Hanser for the continuous support while writing this thesis and implementing bilinear pairings. Christian provided my with the possibility to work on IAIK ECCelerate™. I am also very thankful for effort he spent on discussions about bilinear pairings and the corrections and pointers he offered on this thesis.

I would like to thank my parents, Johanna and Jürgen Ramacher, for the all their support and encouragement throughout my studies. I am also very grateful to Theresa Bernardi for being there for me whenever needed.

I would also like to thank Andreas Stührk and Lukas Prokop for the countless discussions about Java while working on the implementation.

Abstract

Elliptic curves emerged from the theory of elliptic integrals and elliptic functions, which were studied in the 18th and 19th century, and were introduced into cryptography in the 1980s. First constructions of bilinear pairings were known since the 1940s. In a cryptographic context bilinear pairings on elliptic curves were first used to attack the Elliptic Curve Discrete Logarithm Problem in the 1990s. However, it turned out that the properties of bilinear pairings are also immensely useful for developing new cryptographic protocols and for providing solutions to challenging open problems, such as the construction of an efficient identity-based encryption scheme. Other protocols that have been built using bilinear pairings include a signature scheme which produces shorter signatures than the Elliptic Curve Digital Signature Algorithm, group signature schemes, blind signature schemes and structure-preserving signatures. All in all, the successful application of bilinear pairings in the design of new protocols led to a tremendous growth of cryptography and an explosion of protocols exploring the new possibilities.

This master thesis gives an overview of necessary results to construct bilinear pairings over elliptic curves and demonstrates different kinds of constructions ranging from the Weil pairing to the Optimale Ate pairing. We also discuss Miller's algorithm, which makes the computation of bilinear pairings feasible, and other state-of-the-art techniques to further improve the performance of bilinear pairing evaluations. We present algorithms to find suitable finite fields and elliptic curve parameters to obtain pairing-friendly elliptic curves from the family of Barreto-Naehrig curves. Finally, we present the implementation of bilinear pairings using state-of-the-art techniques in the IAIK ECCelerate™ library and give performance comparisons to other Java™-based pairing implementations.

Keywords: elliptic curves, Barreto-Naehrig curves, bilinear pairings, Weil pairing, Tate pairing, Ate pairing, Optimal Ate pairing, Miller's algorithm, denominator elimination, final exponentiation, cyclotomic subgroups, IAIK ECCelerate™

Kurzfassung

Elliptische Kurven entstanden aus der Theorie elliptischer Integrale und elliptischer Funktionen, die im 18. und 19. Jahrhundert untersucht wurden. In den 1980er Jahren wurden elliptische Kurven erstmals in der Kryptographie verwendet. Konstruktionen von bilinearen Pairings sind seit den 1940er Jahren bekannt. In einem kryptographischen Kontext wurden bilineare Pairings in den 1990er Jahren zuerst verwendet um das Diskrete Logarithmus Problem auf elliptischen Kurven anzugreifen. Es stellte sich allerdings heraus, dass sich die Eigenschaften von bilinearen Pairings zur Entwicklung neuer kryptographischer Protokolle eignen und ermöglichten es Lösungen für schwierige Probleme, wie etwa die Konstruktion eines auf Identitäten basierendes Verschlüsselungsschema, zu finden. Weitere Protokolle, die basierend auf bilinearen Pairings konstruiert wurden, umfassen etwa ein Signaturschema, das kürze Signaturen als der Elliptic Curve Digital Signature Algorithm produziert, Gruppensignaturen, blinde Signaturen und strukturerhaltende Signaturen. Der erfolgreichen Einsatz von bilinearen Pairings im Design neuer Protokolle führte zu einem immensen Wachstum der Kryptographie.

Wir geben einen Überblick über die nötigen Resultate, die es ermöglichen bilineare Pairings über elliptischen Kurven zu konstruieren, und demonstrieren verschiedene Möglichkeiten Pairings zu konstruieren. Wir diskutieren auch den Algorithmus von Miller und andere moderne Techniken, die es ermöglichen, Pairings effizient zu berechnen. Außerdem präsentieren wir Algorithmen, die das Auffinden von passenden endlichen Körpern und Parametern für Pairing-freundlichen Barreto-Naehrig Kurven ermöglichen. Schlussendlich wird die Implementierung von bilinearen Pairings in der IAIK ECCelerate$^{\text{TM}}$ Bibliothek präsentiert und mit anderen Java$^{\text{TM}}$-basierten Pairing-Implementation verglichen.

Stichwörter: Elliptische Kurven, Barreto-Naehrig Kurven, bilineare Pairings, Weil Pairing, Tate Pairing, Ate Pairing, Optimales Ate Pairing, Algorithmus von Miller, Nennereliminerung, finale Potenzierung, zyklotomische Untergruppe, IAIK ECCelerate$^{\text{TM}}$

Contents

List of Figures

List of Tables

List of Algorithms

1. Introduction

Elliptic curves emerged from the theory of elliptic integrals and elliptic functions, which were studied in the 18th and 19th century. Initially, elliptic curves were primarily used as theoretical tool in function theory and number theory. They were introduced into cryptography in the 1980s when Koblitz and Miller [Mil86b, Kob87] proposed protocols which were based on the hardness of the Elliptic Curve Discrete Logarithm Problem.

The first construction of a bilinear pairing dates back to 1940 when Weil introduced a pairing on Abelian varieties [Wei40]. Almost two decades later, Tate [Tat58, Tat63] presented another pairing which was later refined by Lichtenbaum [Lic69]. At this time, these pairings were mostly used as a theoretical tool and have found applications in number theory and algebraic geometry. Until the 1980s no efficient algorithm was known to actually compute pairings. A first step towards efficiently computable pairings was a polynomial time algorithm to compute functions on algebraic curves with given roots and poles by Miller [Mil86a]. This new algorithm made it possible to compute the pairings by Weil and Tate.

With the invention of Miller's algorithm, pairings found their first application in cryptography in the 1990s. The Weil pairing was first used to attack the Elliptic Curve Discrete Logarithm problem for elliptic curves with small embedding degree in subexponential time. Using the pairing, Menezes, Okamoto and Vanstone [MVO91] transported the discrete logarithm problem from the elliptic curve to the multiplicative group of a finite field. Provided that the embedding degree is sufficiently small, the index calculus method can then be applied in the latter group. Frey and Rück introduced the Tate pairing into cryptography with a similar attack [FR94].

Starting with a one-round Diffie-Hellman key exchange protocol proposed by Joux in 2000 [Jou00] and identity-based non-interactive authenticated key agreement protocol by Sakai, Ohgishi and Kasahara [SOK00], bilinear pairings were used more and more to build new cryptographic protocols and to provide solutions for challenging open problems. For example, Boneh and Franklin [BF01] provided a solution to an old question of Shamir [Sha84], who asked whether an efficient identity-based encryption could be devised. Other early applications of pairings include a signature scheme by Boneh, Lynn and Shacham [BLS01] producing shorter signatures than the Elliptic Curve Digital Signature Algorithm. Pairings have also been used to build protocols like blind signature schemes [Bol03, FHS15], group signature schemes [BBS04] and structure-preserving signatures [AFG$^+$10]. All in all, the introduction of pairings into cryptography led to an explosion of protocols exploring new possibilities.

However, the use of pairings comes at a price. The evaluation of a bilinear pairing is by far more expensive than the comparatively simple arithmetic in a finite field or on elliptic curves. To make pairings practical, elliptic curves and algorithms to compute the pairings have to be chosen carefully. Suitable curves can be found using the complex multiplication method which was first used by Miyaji, Nakabayashi and Takano [MNT01] to find a family of pairing-friendly curves. Over the years many other families were constructed using this method by Barreto, Naehrig, Freeman, Scott and others [SB04, BN06, Fre06].

To improve the performance of pairing-based protocols, new pairings have been proposed that reduce the number of iterations required in Miller's algorithm. These pairings came with a shortened loop and include pairings like the Ate pairing introduced by Hess, Smart and Vercauteren [HSV06] and the η pairing by Barreto, Galbraith, Ó hÉigeartaigh and Scott [BGÓS04]. Loop shortening culminated in the construction of optimal pairings [Ver08], which require the minimal number of iterations in Miller's algorithm.

Besides optimizing Miller's algorithm, the performance of pairing evaluation benefits from fast finite field arithmetic. In particular, the final exponentiation that is required for the Tate and any related pairing turned out to be major bottleneck. Improvements to the final exponentiation can be achieved by using the special structure of the involved exponent as shown by Scott, Benger, Charlemagne, Dominguez Perez and Kachisa [SBC$^+$08]. But also the cyclotomic subgroup provides further improvements as it allows faster exponentiation and inversions [Kar10].

In this thesis we will give a comprehensive overview of the construction and implementation of bilinear pairings on elliptic curves. We will provide the necessary background in algebra and algebraic geometry to introduce elliptic curves and their divisor groups. Using these divisors, we present the Weil and Tate pairing as well as the pairings derived from the Tate pairing. We will also discuss optimal pairings and the associated optimality conjecture. We will continue by investigating pairing-friendly Barreto-Naehrig curves, a family of elliptic curves. After that we will turn to state-of-the-art implementation techniques to improve the performance of pairing evaluations. Finally, the implementation of the Optimal Ate pairing on Barreto-Naehrig curves using these techniques in the IAIK ECCelerate™ will be presented.

1.1. Outline

The first part of this thesis gives an introduction to the necessary theory on elliptic curves. Chapter 2 recalls definitions and facts from algebra and algebraic geometry that are required for the later parts of the thesis. An overview of elliptic curves and their properties are outlined in Chapter 3.

The second part is dedicated to the description of bilinear pairings. Chapter 4 discusses divisors on elliptic curves and some results that are necessary to construct bilinear pairings. In Chapter 5 bilinear pairings are defined and various constructions of pairings are presented. The last chapter of this part, Chapter 6, discusses pairing-friendly elliptic curves and covers the family of Barreto-Naehrig curves.

The third part of the thesis focuses on the implementation of bilinear pairings.

Chapter 7 describes several state-of-the-art techniques that are useful for the implementation of bilinear pairings in general and make the use of pairings practical. The implementation of bilinear pairings in the Java™ based IAIK ECCelerate™ library is presented in Chapter 8.

Part I.

Introduction to Elliptic Curves

2. Preliminaries

We will need some definitions and facts from algebra and algebraic geometry. This chapter serves as short overview of groups, rings, fields and smooth algebraic curves. For a detailed and in-depth coverage of these topics we refer to [Hun03, Lan02, Sti09, Was08].

2.1. Group Theory

Groups are one of the basic structures of modern algebra. A group consists of a set together with an operation that combines two elements to a third element where the operation satisfies certain natural properties like associativity.

Law of composition Let S be a set. A map $\cdot : S \times S \to S$ is called a *law of composition.* For $x, y \in S$ the image of the pair (x, y) under this law of composition will be denoted by $x \cdot y$. If a multiplicative notation is used, we also write xy.

Let S be a set and $\cdot$ a law of composition. The law of composition is called *associative* if $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ holds for all $g, h, k \in S$. It is called *commutative* if $g \cdot h = h \cdot g$ holds for all $g, h \in S$.

Groups

Definition 2.1. Let G be a set and $\cdot : G \times G \to G$ be a law of composition, then $(G, \cdot)$ is called a *group* if all of the following conditions are satisfied:

1. The law of composition $\cdot$ is associative.
2. There exists an element $e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$. This element is called *identity element.*
3. For each element $g \in G$ there exists an *inverse element* $g^{-1} \in G$ such that $g^{-1} \cdot g = g \cdot g^{-1} = e$.

If $\cdot$ is also commutative, then $(G, \cdot)$ is called *Abelian.*

A group $(H, *)$ is called a *subgroup* of $(G, \cdot)$ if H is a subset of G and $\cdot$ restricted to H coincides with $*$.

Whenever we have a set H together with an associative law of composition $\cdot$, we refer to the set of invertible elements of H with respect to $\cdot$ as $(H, \cdot)^\times$ or simply $H^\times$. Note that $H^\times$ is always a group.

Example 2.2.

1. $(\mathbb{Z}, +)$ is a group with identity element 0.
2. $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a group. Only 1 and -1 are invertible.

Homomorphisms Homomorphisms are structure-preserving maps between two algebraic structures. They allow to study the relationship between certain structures. For groups, a homomorphism is defined in the following way:

Definition 2.3. Let $(G, \cdot)$ and $(G', *)$ be groups. A map $f : G \to G'$ is called a *(group) homomorphism* if $f(g \cdot h) = f(g) * f(h)$ holds for all $g, h \in G$.

Group homomorphisms preserve the neutral element, that is $f(1_G) = 1_{G'}$. An injective group homomorphism is called *monomorphism*. If a group homomorphism is surjective it is called *epimorphism*. An *isomorphism* is a bijective group homomorphism. An *endomorphism* is a group homomorphism mapping a group to itself. An isomorphism that is also an endomorphism is called *automorphism*.

If an isomorphism exists between two groups, they are called *isomorphic* and we write $G \simeq G'$.

Cyclic groups and generators Cyclic groups have a very simple description in terms of one group element.

Let $(G, \cdot)$ be a group. For an element $g \in G$, the set of elements generated by g is denoted by $\langle g \rangle$ and consists of all elements of the form g^k for all $k \in \mathbb{Z}$. This set is a subgroup of G.

If for a group $(G, \cdot)$ there exists an element $g \in G$ such that $G = \langle g \rangle$, then the G is called *cyclic* and g is called a *generator* of the group.

Example 2.4.
1. The group $(\mathbb{Z}, +)$ is cyclic and generated by 1.
2. The group $(\mathbb{Q}, +)$ is not cyclic and is generated by the infinitely large set $\{\frac{1}{n!} \mid n \in \mathbb{N}\}$.

Order The order of an element $h \in G$, denoted by $\mathrm{ord}_G(h)$, is defined as the smallest positive integer k such that $h^k = 1$. If no such k exists, then $\mathrm{ord}_G(h)$ is set to ∞. Group elements with finite order are called *torsion elements*. The order of the group, $\mathrm{ord}(G)$, is defined to be its cardinality. If a group has prime order, the group is cyclic.

Example 2.5.
- In $(\mathbb{Z}, +)$ the order of 0 is 1 and the order of every non-zero element is ∞.
- For $G = (\mathbb{Z}/6\mathbb{Z}, +)$ and $H = (\mathbb{Z}/6\mathbb{Z}, \cdot)^\times$ the orders are as follows:

g	$\mathrm{ord}_G(g)$	$\mathrm{ord}_H(g)$
0	1	-
1	6	1
2	3	-
3	2	-
4	3	-
5	6	2

Free Abelian Groups A *free Abelian group* is an Abelian group G that admits a basis $B \subset G$.

Definition 2.6. An Abelian group $(G, +)$ is called *free* if there exists a subset $B \subset G$ such that any element $g \in G$ can be written uniquely as

$$g = \sum_{b \in B} a_b b$$

with $a_b \in \mathbb{Z}$ and only finitely many a_b are non-zero.

If the basis B is finite, G is called *finitely generated.*

Example 2.7. The group $(\mathbb{Z}, +)$ is a free Abelian group with basis $\{1\}$. In fact, any free Abelian group is isomorphic to a direct sum of copies of $(\mathbb{Z}, +)$.

Lattices A lattice is a special subgroup of real vector space.

Definition 2.8. Let $n \in \mathbb{N}$ and $v_1, \ldots, v_n \in \mathbb{R}^n$ be a vector space basis for $\mathbb{R}^n$. Then the set

$$\Lambda = \left\{ \sum_{i=1}^{n} a_i v_i \mid a_i \in \mathbb{Z} \right\}$$

is called a *lattice in* $\mathbb{R}^n$.

In other words, a lattice is a finitely generated free Abelian group generated by a basis $\{v_1, \ldots, v_n\}$. While the same lattice may be generated by a different basis, the absolute values of the determinant of the vectors v_i is uniquely determined by the lattice.

2.2. Ring Theory

A ring is an algebraic structure with two distinct but compatible laws of composition that generalize the arithmetic operations of addition and multiplication. One can think of $\mathbb{Z}$ as the prime example of a ring and many of concepts found here a direct generalization of properties of $\mathbb{Z}$.

Definition 2.9. A set R together with two laws of composition $+$ and $\cdot$ is called a *ring* (with unity) if all of the following conditions are satisfied

1. $(R, +)$ is an Abelian group with identity element 0.
2. $\cdot$ is associative with neutral element 1.
3. $\cdot$ is distributive with respect to $+$, that is

   $$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and } (a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

   for all $a, b, c \in R$.

If $(R, \cdot)$ is also commutative, $(R, +, \cdot)$ is called a *commutative ring.* If for a commutative ring the product of every two non-zero elements is again non-zero, the ring is called an *integral domain.*

Since it is often useful to refer to the all non-zero elements of a ring, the set of all non-zero elements is denoted by $R^\bullet$.

Ideals and quotient rings Ideals are special subsets of rings. They generalize the properties of certain subsets of the integers like the even numbers.

Definition 2.10. Let $(R, +, \cdot)$ be a commutative ring. A subset $I \subset R$ is called an *ideal of R* if

- $(I, +)$ is a subgroup of $(R, +)$, and
- For all $x \in I$ and $r \in R$ both $x \cdot r \in I$ and $r \cdot x \in I$.

The first condition can be replaced by requiring I to be non-empty and that for all $x, y \in I$ also $x - y \in I$.

Example 2.11. 1. Let R be any ring $r \in R$. The set $rR = \{rx \,|\, x \in R\}$ consisting of all multiples of r forms an ideal. An element $x \in R$ is contained in rR if and only if x is divisible by r.

If an ideal I can be written as rR for some $r \in R$, then the ideal is called *principal.*

2. In $\mathbb{Z}$ the situation is very simple, since all ideals of $\mathbb{Z}$ are principal.

Ideals can now be used to construct new rings from existing rings. Let I be an ideal of a ring R. Then we can define an equivalence relation $\sim_I$ in the following way: $a \sim_I b$ for $a, b \in R$ if and only if $a - b \in I$. We then set $R/I = R/\sim_q$, the *quotient ring of R modulo I.*

Example 2.12. Consider $\mathbb{Z}$ and a prime p. We can then form the quotient ring modulo $p\mathbb{Z}$. However, instead of working with the equivalence classes in $\mathbb{Z}/p\mathbb{Z}$, we can simply represent it by the set $\{0, \ldots, p-1\}$ where all operations are performed modulo p.

Euler's totient function We consider $n \in \mathbb{N}$ and the order of the multiplicative group of $\mathbb{Z}/n\mathbb{Z}$.

Definition 2.13. The map

$$\phi : \begin{cases} \mathbb{N} & \to \mathbb{N} \\ n & \mapsto \left|\mathbb{Z}/n\mathbb{Z}^\times\right| \end{cases}$$

is called *Euler's totient function.*

In other words, Euler's totient function counts the number of positive integers less or equal n that are coprime to n. It satisfies

$$\phi(p^k) = p^{k-1}(p-1), \text{ and } \phi(nm) = \phi(n)\phi(m)$$

for $p \in \mathbb{P}$ and $k \in \mathbb{N}$ and coprime $m, n \in \mathbb{N}$.

Polynomial rings From any commutative ring it is possible to create a canonical ring extension, the polynomial ring.

Definition 2.14. Let R be a commutative ring. The *ring of polynomials* in variables $X_1, \dots, X_n$ over R is given by

$$R[X_1, \dots, X_n] = \left\{ \sum_{\nu_1,\dots,\nu_n \in \mathbb{N}_0} a_{\nu_1,\dots,\nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n} \mid a_{\nu_1,\dots,\nu_n} \in R \text{ for all } \nu_1, \dots, \nu_n \in \mathbb{N}_0 \right\}$$

The addition is defined component-wise and the multiplication is defined by the typical polynomial multiplication. The coefficient ring R is a subring of the polynomial ring $R[X_1, \dots, X_n]$.

The *degree of a polynomial* $f \in R[X_1, \dots, X_n]$ is defined as

$$\deg(f) = \max \left\{ \sum_{j=1}^{n} \nu_j \mid a_{\nu_1,\dots,\nu_n} \neq 0 \right\}.$$

If $f = 0$, we set $\deg(f) = -\infty$.

Irreducible and monic polynomials A polynomial $f \in R[X] \setminus R$ is called *irreducible* if it cannot be factored into non-constant polynomials, that is if $f = gh$ for $g, h \in R[X]$ then either $g \in R$ or $h \in R$. The notion of irreducibility is similar to the notion of prime numbers in $\mathbb{Z}$. If the polynomial has the form $f = X^d + \sum_{i=0}^{d-1} a_i X^i$, then it is called *monic*.

Cyclotomic polynomial Cyclotomic polynomials are irreducible polynomials with integer coefficients which divide $X^n - 1 \in \mathbb{Z}[X]$ for some $n \in \mathbb{N}$.

Definition 2.15. Let $n \in \mathbb{N}$. An irreducible polynomial $f \in \mathbb{Z}[X]$ is called *n-th cyclotomic polynomial* if

1. $f \mid X^n - 1$, and
2. $f \nmid X^k - 1$ for any $k < n$.

The n-th cyclotomic polynomial is unique and is denoted by Φ_n.

Example 2.16.

1. For $n = 1$ we have $\Phi_1 = X - 1$.
2. If $n \in \mathbb{P}$, then $\Phi_n = \sum_{i=0}^{n-1} X^i$.
3. For $n = 2^a 3^b$ where $a, b \in \mathbb{N}$, we have

$$\Phi_{2^a 3^b} = X^{2^a 3^{b-1}} - X^{2^{a-1} 3^{b-1}} + 1.$$

2.3. Field Theory

Fields are an algebraic structure that posses a notion of addition, subtraction, multiplication and division. They are rings where every non-zero element has a multiplicative inverse and thus division by non-zero elements is possible. Especially finite fields are used extensively in cryptography. Also, fields are required to describe the notions of algebraic geometry we are interested in.

Definition 2.17. A commutative ring $(K, +, \cdot)$ is called a *field* if $(K^{\bullet}, \cdot)$ is an Abelian group.

Example 2.18.

- $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ with respect to the usual addition and multiplication are fields.
- For a prime $p \in \mathbb{P}$ the ring $\mathbb{Z}/p\mathbb{Z}$ is in fact a field. We denote this field by $\mathbb{F}_p$, the finite field of p elements.

Quotient field Let R be an integral domain. The smallest field Q such that R is embedded in Q is called *quotient field* (or *field of fractions*). This field can be constructed the same way as $\mathbb{Q}$ can be constructed from $\mathbb{Z}$: for $n \in R, m \in R^{\bullet}$ look at the formal quotient $\frac{n}{m}$. Two quotients $\frac{n}{m}$ and $\frac{n'}{m'}$ are considered equal if $m'n = n'm$. The addition is defined as $\frac{n}{m} + \frac{n'}{m'} = \frac{nm'+n'm}{mm'}$ and the multiplication is defined as $\frac{n}{m} \cdot \frac{n'}{m'} = \frac{nn'}{mm'}$.

Example 2.19.

- The quotient field of $\mathbb{Z}$ is the field of rational numbers $\mathbb{Q}$.
- For a field K, the field of fractions of the polynomial ring $K[X]$ is denoted by $K(X)$ and called *field of rational functions*.

Field characteristic For any field K, there is a ring homomorphism $\psi : \mathbb{Z} \to K$ with $\psi(1) = 1_K$. If ψ is injective, K is said to have *characteristic* 0. If instead ψ is not injective, there is a prime $p \in \mathbb{P}$ such that $\psi(p) = 0$ and it is the smallest positive integer that satisfies this property. In this case, K is said to have *characteristic* p. The characteristic of a field K is denoted by $\operatorname{char}(K)$. Furthermore, if K has characteristic p, then an isomorphic copy of $\mathbb{F}_p$ is contained in K.

Algebraic extension fields Take two fields K and L with $K \subset L$. An element $\alpha \in L$ is called *algebraic* over K if there exists a non-constant polynomial $f \in K[X] \setminus K$ such that $f(\alpha) = 0$. If every element of L is algebraic over K, then L is called *algebraic extension* of K. Otherwise L is called *transcendental extension* of K.

An extension field L over K can always be viewed as K-vector space. The K-vector space dimension of L is called *extension degree* and written as $[L : K]$. If the field extension is algebraic, the extension degree is finite.

A field $\overline{K}$ containing K is called *algebraic closure* of K if $\overline{K}$ is algebraic over K and $\overline{K}$ is *algebraically closed*, i.e. for every $f \in \overline{K}[X] \setminus \overline{K}$ all roots are in $\overline{K}$. Every field K has an algebraic closure. Furthermore, two algebraic closures of K

are isomorphic. So from now on, we assume that one algebraic closure of a field K has been chosen, and we call it the algebraic closure of K.

Field extensions from polynomial rings For any field K algebraic extension fields of K can be constructed by taking a monic, irreducible polynomial $f \in K[X]$ and looking at the quotient ring $L = K[X]/fK[X]$. Since the polynomial f is irreducible, L is in fact a field and the extension degree of L over K is $\deg(f)$.

Similarly, if we take a root $\alpha \in \overline{K}$ of f instead and construct the extension field L' by adjoining α, that is

$$L' = K(\alpha) = \left\{ \sum_{i=0}^{\deg(f)-1} a_i \alpha^i \mid a_i \in K \right\},$$

then we obtain a field that is isomorphic to L'. Note that the choice of the root of f does not matter.

Example 2.20. We consider the construction of $\mathbb{C}$. We start from $\mathbb{R}$ and take $f = X^2 + 1 \in \mathbb{R}[X]$ which is irreducible. Hence $\mathbb{R}[X]/f\mathbb{R}[X]$ is a field. This field is isomorphic to $\mathbb{C} = \mathbb{R}(i)$ with $i^2 = -1$.

Roots of unity Roots of unity are field elements that give 1 when raised to some power $r \in \mathbb{N}$. They form a special subgroup of the multiplicative group of a field.

Definition 2.21. Let K be a field and $r \in \mathbb{N}$. Elements of the set

$$\mu_r(K) = \{x \in K \mid x^r = 1_K\}$$

are called *r-th root of unity.*

The product of two r-th roots of unity is again an r-th root of unity. So the roots of unity form a subgroup of the multiplicative group of K. Also, $\mu_r(K)$ is a cyclic group and generators of the group are called *primitive r-th roots of unity.* If K is algebraically closed and the characteristic of K does not divide r, $\mu_r(K)$ has order r.

Example 2.22.

- In $\mathbb{C}$, the r-th roots of unity are given by

  $$e^{2\pi i \frac{k}{r}}$$

  for $0 \leq k < r$. They can also be obtained by inscribing a regular r-sided polygon in the unit circle such that one vertex is located at 1.

- The primitive r-th roots of unity in $\mathbb{C}$ are exactly the roots of the r-th cyclotomic polynomial.

- In $\mathbb{Q}$ and $\mathbb{R}$ the only roots of unity are 1 if r is odd and 1 and -1 if r is even.

Finite fields Now let $p \in \mathbb{P}$. We have already seen that the integers modulo p form a field $\mathbb{F}_p$. Note that any other field L with p elements has characteristic p and thus $\mathbb{F}_p$ is isomorphic to L. So if we talk about a field with p elements, we can always assume it to be $\mathbb{F}_p$.

Let $q \in \mathbb{N} \setminus \mathbb{P}$. It can be shown that there exists a field with q elements if and only if q is a prime power. So let $q = p^n$ for some prime p. A field with q elements can be constructed in a natural way: let $f \in \mathbb{F}_p[X] \setminus \mathbb{F}_p$ be a monic, irreducible polynomial of degree n. Then $\mathbb{F}_p[X]/f\mathbb{F}_p[X]$ is a field with q elements. Furthermore, it is possible to show that there is a unique (up to isomorphism) field with q elements. So we refer to the field with q elements as $\mathbb{F}_q$ and we can always use polynomials over $\mathbb{F}_p$ modulo a suitable polynomial to represent this field.

The algebraic closure of $\mathbb{F}_p$ is $\overline{\mathbb{F}_p} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$. Furthermore, $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ if and only if $m \mid n$.

***n*-th non-residues** Let $K = \mathbb{F}_p, p \in \mathbb{P}$ and $n \in \mathbb{N}$. An element $x \in K^\times$ is called a *n-th non-residue modulo p* if $X^n - x \in K[X]$ has no roots in K and a *n-th residue modulo p* otherwise. For $n = 2$, we will also denote non-residues as non-squares and residues as squares. Similarly, for $n = 3$ we also call them non-cubes and cubes.

For quadratic residues, we can define the *Legendre symbol* for $a \in \mathbb{Z}$ and $p \in \mathbb{P}$ as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue} \mod p \\ 0, & \text{if } p \mid a \\ -1, & \text{if } a \text{ is a quadratic non-residue in} \mod p \end{cases}$$

or equivalently as

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p.$$

For odd primes p and $a = -1$ the following statement is from importance to us:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \mod 4 \\ -1, & \text{if } p \equiv 3 \mod 4 \end{cases}.$$

When fixing a $p \in \mathbb{P}$ we will also write $\chi_p(a)$ instead of the Legendre symbol, and refer to χ as *quadratic character modulo p.*

Example 2.23. Let $p \equiv 3 \mod 4$. In a similar way to $\mathbb{C}$, $\mathbb{F}_{p^2}$ can be constructed by adjoining a square root of -1 to $\mathbb{F}_p$: We take $i \in \overline{\mathbb{F}_p}$ to be a square root of -1. Since $p \equiv 3 \mod 4$, -1 is a quadratic non-residue and so $i \notin \mathbb{F}_p$. Now define the quadratic extension field as

$$\mathbb{F}_{p^2} = \mathbb{F}_p(i) = \{a + bi \mid a, b \in \mathbb{F}_p\}$$

using component-wise addition and use

$$(a + bi)(a' + b'i) = (aa' - bb') + (ab' + a'b)i$$

as multiplication.

The polynomial $f = X^2 + 1 \in \mathbb{F}_p[X]$ is monic and irreducible over $\mathbb{F}_p$ since -1 is a quadratic non-residue modulo p. So $\mathbb{F}_p[X]/f\mathbb{F}_p[X]$ is an extension field of $\mathbb{F}_p$ of degree 2. Since i is a root of f, both constructions are isomorphic.

Frobenius map Consider the finite field $\mathbb{F}_q$ and its algebraic closure $\overline{\mathbb{F}_q}$. The map

$$\pi_q : \begin{cases} \overline{\mathbb{F}_q} & \to \overline{\mathbb{F}_q} \\ x & \mapsto x^q \end{cases}$$

is called *Frobenius map* of $\mathbb{F}_q$. This map is in fact a field automorphism due to the following lemma:

Lemma 2.24 (Freshman's dream)**.** *Let K be a field of characteristic $p \in \mathbb{P}$. Then*

$$(x + y)^p = x^p + y^p$$

holds for every $x, y \in K$.

Note that for $x \in \overline{\mathbb{F}_q}$ we have $x^q = x$ if and only if $x \in \mathbb{F}_q$ and thus π_q fixes $\mathbb{F}_q$.

Example 2.25. Let $p \equiv 3 \mod 4$ and consider $K = \mathbb{F}_p$ and $L = \mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i^2 = -1$. For an element $x + iy \in L$, the image of the Frobenius map of K is $\pi_p(x + iy) = x - iy$.

For quadratic extensions, we also write $\overline{x + iy} = \pi_p(x + iy)$ and call it *conjugate of* $x + iy$.

Norm of finite fields The Frobenius map can now be used to define the field norm: let $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^n}$. The map

$$\mathcal{N}_{L/K} : \begin{cases} L & \to K \\ \alpha & \mapsto \prod_{i=0}^{n-1} \pi_q^i(\alpha) \end{cases}$$

is called the *norm* from L to K. Note that $\mathcal{N}_{L/K}$ restricted to the multiplicative group of L is a group homomorphism $L^\times \to K^\times$. If additionally $M = \mathbb{F}_{q^{nm}}$, then we can view the norm from M to K as composition of the norm from M to L and the norm from L to K, i.e. $\mathcal{N}_{M/K} = \mathcal{N}_{L/K} \circ \mathcal{N}_{M/L}$.

Example 2.26. Let again $p \equiv 3 \mod 4$ and consider $K = \mathbb{F}_p$ and $L = \mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i^2 = -1$. For an element $x + iy \in L$, its norm over K is $\mathcal{N}_{L/K}(x + iy) = (x + iy)(x - iy) = x^2 + y^2$.

2.4. Affine and Projective Space

There are two coordinate systems that are important when studying algebraic functions: affine and projective coordinates.

Definition 2.27. Let K be a field. The affine space of dimension n over K is given by $\mathbb{A}^n(K) = \{(a_1, \ldots, a_n) \,|\, a_1, \ldots, a_n \in K\}$, the set of n-tuples consisting of elements of K.

To define the projective space of dimension n, we first need to introduce an equivalence relation on $\mathbb{A}^{n+1}(K) \setminus \{(0, \ldots, 0)\}$: for $a = (a_1, \ldots, a_{n+1}), b = (b_1, \ldots, b_{n+1}) \in \mathbb{A}^{n+1}(K)$ define $a \sim b$ if and only if there exists a $\lambda \in K^\times$ such that $a = \lambda b$. These equivalence classes capture all points on a line through $(0, \ldots, 0)$.

Definition 2.28. The set

$$\mathbb{P}^n(K) = \mathbb{A}^{n+1}(K) \setminus \{(0, \ldots, 0)\}/\sim .$$

is called the n-dimensional *projective space* over K.

Points in the projective space are usually written as $(a_1 : \ldots : a_{n_1})$. Points of the projective space where the last component is 0 are called *points at infinity.* All points at infinity form the *line at infinity.*

Canonical maps between affine and projective space There is a canonical relation between affine and projective coordinates of the same dimension. The n-dimensional affine space can be injected into the projective space of the same dimension. The injection is given by the map

$$\begin{cases} \mathbb{A}^n(K) & \hookrightarrow \mathbb{P}^n(K) \\ (a_1, \ldots, a_n) & \mapsto (a_1 : \ldots : a_n : 1) \end{cases}.$$

Any projective point with a non-zero last component can also be projected back to affine space. The projection is given by the map

$$\begin{cases} \{(a_1 : \ldots : a_{n+1}) \in \mathbb{P}^n(K) \mid a_{n+1} \neq 0\} & \to \mathbb{A}^n(K) \\ (a_1 : \ldots : a_{n+1}) & \mapsto \left(\frac{a_1}{a_{n+1}}, \ldots, \frac{a_n}{a_{n+1}}\right) \end{cases}.$$

Homogeneous polynomials A polynomial $f \in K[X_1, \ldots X_n]$ is called *homogeneous* if all its non-zero terms have the same degree, that is it has the form

$$f = \sum_{\nu_1, \ldots, \nu_n \in \mathbb{N}_0, \sum_{j=1}^n \nu_i = d}^{k} a_{\nu_1, \ldots, \nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n}$$

with $a_{\nu_1, \ldots, \nu_n} \neq 0$.

One of the nice properties of homogeneous polynomials is that roots can be considered elements of $\mathbb{P}^{n-1}(K)$. Indeed, let $(x_1, \ldots, x_n)$ be a root of f, then for any $\lambda \in K^\times$ the multiple $\lambda(x_1, \ldots, x_n)$ is also a root of f. Hence every representative of $(x_1 : \ldots : x_n) \in \mathbb{P}^{n-1}(K)$ is a root of f and thus we write $f((x_1 : \ldots : x_n)) = 0$.

Projective closure of polynomials Every polynomial can be split into a sum of homogeneous polynomials: let $f \in F[X_1, \dots X_n]$ be of degree d. Then $f = \sum_{i=0}^{d} f_i$ such that every f_i is a homogeneous polynomial of degree i.

Any polynomial in n variables can be mapped to a homogeneous polynomial in $n+1$ variables. The map

$$\bar{\cdot} : \begin{cases} F[X_1, \dots X_n] & \to F[X_1, \dots X_{n+1}] \\ f & \mapsto \overline{f} = \sum_{i=0}^{\deg(f)} f_i X_{n+1}^{\deg(f)-i} \end{cases}$$

defines the homogenization of a polynomial. For a polynomial f the image $\overline{f}$ is called the *projective closure* of f. Clearly we have $\overline{f}(X_1, \dots, X_n, 1) = f$.

Note that if $(x_1, \dots, x_n)$ is a root of f, then $(x_1, \dots, x_n, 1)$ is a root of $\overline{f}$. Also, every root of $\overline{f}$ that is not a point at infinity, can be mapped back to a root of f by mapping the root back to an affine point.

2.5. Algebraic Geometry

Algebraic geometry studies roots of multivariate polynomial equations using techniques from commutative algebra. It translates geometric problems into the language of algebra.

Affine algebraic curves Let K be a field and $\overline{K}$ its algebraic closure. Consider a polynomial $f \in K[X_1, \dots, X_n]$. For a field $L \supset K$ the set $C_f(L)$ consists of all roots of f over L:

$$C_f(L) = \{(x_1, \dots, x_n) \in \mathbb{A}^n(L) \mid f(x_1, \dots, x_n) = 0\}$$

For $\overline{K}$ we usually write C_f instead of $C_f(\overline{K})$. We say that C_f is defined over K.

Definition 2.29. Let K be a field and $f \in K[X_1, \dots, X_n]$. If f is irreducible, then C_f is called *affine algebraic curve.*

For any field $L \supset K$ the set $C_f(L)$ is called the set of all *L-rational points* of C_f.

For any point $P = (x_1, \dots, x_n) \in C_f$ we can look at the Taylor series expansion of f at P:

$$\sum_{\nu_1, \dots, \nu_n \in \mathbb{N}_0} \tilde{c}_{\nu_1, \dots, \nu_n} (X_1 - x_1)^{\nu_1} \cdots (X_n - x_n)^{\nu_n}.$$

The *order* of a curve C_f at point P is defined by $\operatorname{ord}_P(C_f) = \min\{\sum_{i=1}^{n} \nu_i \,|\, \tilde{c}_{\nu_1, \dots, \nu_n} \neq 0\}$. If $\operatorname{ord}_P(C_f) = 1$, then P is called *regular* and if $\operatorname{ord}_P(C_f) > 1$, it is called *singular.* Equivalently, a point is singular if all partial derivatives of f at P vanish. The curve C_f is called *regular* (or *smooth*) if all points $P \in C_f$ are regular.

Definition 2.30. Let C_f be a regular algebraic affine curve defined over K. The ring $K[C_f] = K[X_1, \dots, X_n]/fK[X_1, \dots, X_n]$ is called *the ring of regular functions defined over K of the affine curve C_f.* The quotient field of $K[C_f]$, denoted by $K(C_f)$, is called the *field of rational functions defined over K of C_f.*

The field $K(C_f)$ is also called the *function field of C_f.*

Projective curves and projective closure If the polynomial is homogeneous we can consider curves in the projective space instead of the affine space. So if f is homogeneous, $C_f(L)$ can be considered as

$$C_f(L) = \{(x_1 : \ldots : x_n) \in \mathbb{P}^n(L) \mid f((x_1 : \ldots : x_n)) = 0\}$$

For non-homogeneous polynomials f we can consider the homogenization $\overline{f}$.

Definition 2.31. Let f be a polynomial and $\overline{f}$ its homogenization. The curve $C_{\overline{f}}$ is called the *projective closure* of C_f.

As we have seen before, roots of f can mapped to roots of $\overline{f}$, so $C_{\overline{f}}$ contains all points of C_f. Additionally, $C_{\overline{f}}$ may contain further roots on the line at infinity.

Example 2.32. Let $K = \mathbb{F}_7$ and $f = Y^2 - X^3 - X \in K[X, Y]$. First we take a look at C_f: it consists of the points

$$(1, 3), (1, 4), (3, 3), (3, 4), (5, 2), (5, 5).$$

The homogenization of f is $\overline{f} = Y^2Z - X^3 - XZ^2 \in K[X, Y, Z]$. Now $C_{\overline{f}}$ consists of the points of C_f in their projective representation

$$(1 : 3 : 1), (1 : 4 : 1), (3 : 3 : 1), (3 : 4 : 1), (5 : 2 : 1), (5 : 5 : 1)$$

and additionally one point at infinity, namely $(0 : 1 : 0)$.

3. Elliptic Curves

In this chapter we will recall the definition of elliptic curves and discuss some theorems and notations that are needed to develop bilinear pairings on elliptic curves. This chapter follows the discussion of elliptic curves in [Sil09, Chapter III, Chapter IV, Chapter V], [Was08, Chapter 2, Chapter 3, Chapter 4] and [HPS08, Chapter 6].

We fix a field K and let $\overline{K}$ be the algebraic closure of K. An elliptic curve E is the set of solutions to an equation of the form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{3.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in \overline{K}$ or its projective counterpart

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{3.2}$$

Equation (3.1) is called the *general Weierstrass equation* for elliptic curves.

Definition 3.1 (Elliptic curve)**.** Let K be a field. An elliptic curve E over the field K is a smooth algebraic curve defined by equation (3.1) respectively its projective equivalent (3.2).

The projective closure of the elliptic curve contains only one point at infinity: $(0 : 1 : 0)$. This point is denoted by $\mathcal{O}$. This allows us to consider points on elliptic curves as the affine points on the curve together with $\mathcal{O}$:

$$E(\overline{K}) = C_f \cup \{\mathcal{O}\}$$

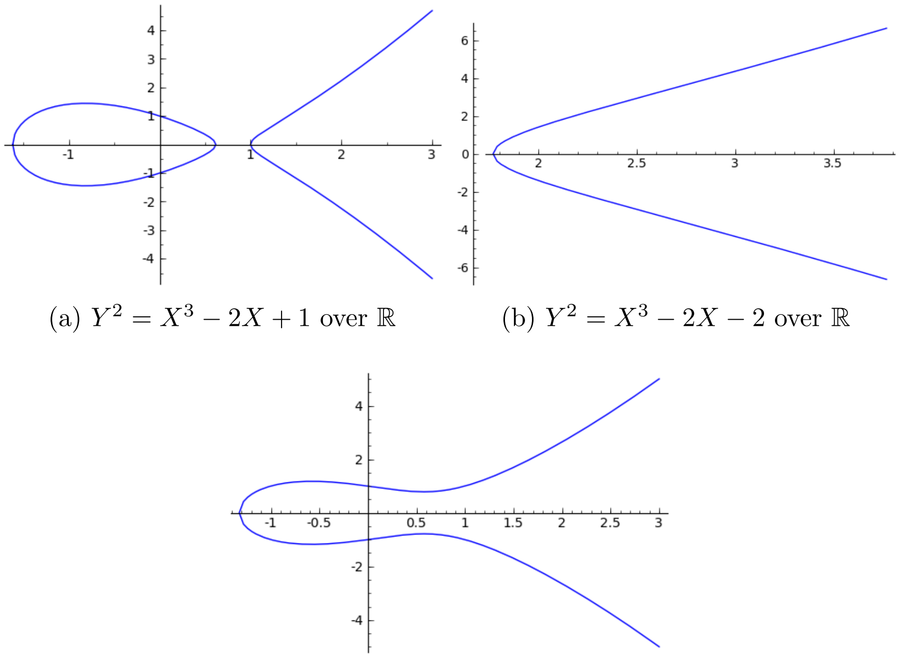
where $f = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6$. For a field $L \supset K$ we denote the L-rational points by $E(L) = C_f(L) \cup \{\mathcal{O}\}$.

3.1. Group Law

We now turn our focus to the group law. First we describe the *chord-and-tangent rule* to give the geometric idea of the group law. After that, we give explicit formulas to compute the group operation.

The chord-and-tangent rule is based on the fact that over any field a line, i.e. a degree one equation in X and Y, and a cubic curve, i.e. a degree three equation in X and Y, always intersect at exactly three points. This fact is a special case of the following more general theorem:

Theorem 3.2 (Bézout's theorem)**.** *Let X and Y be two plane projective curves defined over a field K whose defining polynomials f_X and f_Y are coprime. Then X and Y intersect in exactly $\deg f_X \deg f_Y$ points (including multiplicities) with coordinates in the algebraic closure $\overline{K}$.*



(a) $Y^2 = X^3 - 2X + 1$ over $\mathbb{R}$

(b) $Y^2 = X^3 - 2X - 2$ over $\mathbb{R}$

(c) $Y^2 = X^3 - 1X + 1$ over $\mathbb{R}$

Figure 3.1.: Examples of elliptic curves over $\mathbb{R}$

So whenever P and Q are points on an elliptic curve and ℓ is a line running through P and Q, ℓ intersects E in P, Q and one additional point. Furthermore we require the reflection of a point $P = (x, y) \in E(\overline{K}) \setminus \{\mathcal{O}\}$ which is given by $(x, -y - a_1x - a_3)$. The reflection of $\mathcal{O}$ is again $\mathcal{O}$.

The chord-and-tangent rule now distinguishes two cases to compute the sum $R = P \oplus Q$:

- P and Q are two distinct points: set ℓ to be the line running through P and Q. The third intersection point when intersecting E and ℓ is denoted by R'. The result R is the reflection of R'.
- P and Q are the same point: set ℓ to be the tangent on E at P. The curve E and ℓ again intersect in a third point R'. The result R is again obtained by reflecting R'.

Figure 3.2 illustrates the chord-and-tangent rule on an elliptic curve defined over $\mathbb{R}$. The chord-and-tangent rule now turns E into a group:

Theorem 3.3. *Let E be an elliptic curve defined over a field K. $E(\overline{K})$ together with the law of composition $\oplus$ given by the chord-and-tangent rule forms an Abelian group where the inverse of a point is given by its reflection and $\mathcal{O}$ is the neutral element.*

Similarly, if one considers only L-rational points, $E(L)$ is also a group with the same law of composition. We always use additive notation for $E(\overline{K})$ and just write $+$ instead of $\oplus$.

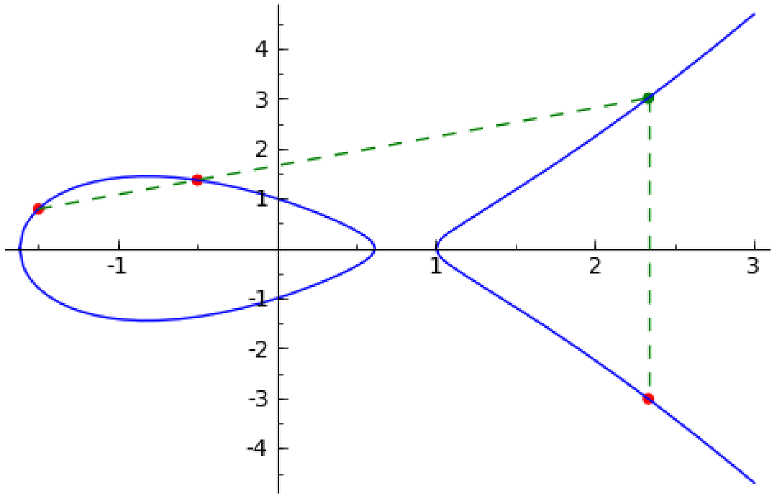


Figure 3.2.: Visualization of the chord-and-tangent rule on $Y^2 = X^3 - 2X + 1$ over $\mathbb{R}$.

Explicit formulas for the law of composition can be derived by first computing the line $\ell : Y = \lambda X + \nu$ running through P and Q and then intersecting the line with the curve and computing the third intersection point. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ and assume that $P \neq -Q$. We consider the first case where $P \neq Q$. Then λ and ν are given by

$$\lambda = \frac{y_2 - y_2}{x_2 - x_1} \text{ and } \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

If $P = Q$, then λ and ν are given by

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} \text{ and } \nu = \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}.$$

The third intersection point $R' = (x_3', y_3')$ is then given by

$$x_3' = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \text{ and } y_3' = \lambda x_3 + \nu.$$

After the reflection we obtain $R = -R' = (x_3, y_3)$ as

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \text{ and } y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

See Algorithm 1 for an algorithmic description of the group law.

3.2. Curve Invariants and Isomorphisms

Now we look at two important invariants of an elliptic curve: the j-invariant and the discriminant. To define those two values, we first need to introduce some helper

Algorithm 1 Addition of two points on an elliptic curve E defined over K in Weierstrass form

```
Input: $P, Q \in E(\overline{K})$.
Output: $R = P + Q$.
  if $P = -Q$ then
      return $\mathcal{O}$
  end if
  if $P \neq Q$ then
      $\lambda \leftarrow \frac{y_2 - y_1}{x_2 - x_1}$
      $\nu \leftarrow \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$
  else
      $\lambda \leftarrow \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}$
      $\nu \leftarrow \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}$
  end if
  $x_3 \leftarrow \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$
  $y_3 = -(\lambda + a_1)x_3 - \nu - a_3$.
  return $R = (x_3, y_3)$
```

values. For an elliptic curve $E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ we set

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \text{ and} \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

Definition 3.4 (j-invariant and discriminant)**.** Let E be an elliptic curve defined over K. The *discriminant of* E is defined as

$$\Delta(E) = -b_2^2b_8 + 9b_2b_4b_6 - 8b_4^3 - 27b_6^2$$

and the *j-invariant of* E is defined as

$$j(E) = \begin{cases} c_4^3\Delta(E)^{-1}, & \text{char}(K) \in \{2,3\} \\ 1728\frac{c_4^3}{c_4^3 - c_6^2}, & \text{otherwise} \end{cases}.$$

The discriminant indicates whether the curve is non-singular. In fact, the curve E is non-singular if and only if $\Delta(E) \neq 0$. The j-invariant is closely related to the notion of elliptic curve isomorphisms.

Definition 3.5 (Isomorphic Curves)**.** Let $E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ and $E' : Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6'$ be two elliptic curves defined over the same base field K. The two curves are said to be *isomorphic* over

K, $E(K) \simeq E'(K)$, if there exists $u \in K^\times$ and $r, s, t \in K$ such that the change of variables

$$X = u^2X' + r, Y = u^3Y' + suX' + t$$

transforms E into E'.

Over the algebraic closure $\overline{K}$, the j-invariant characterizes the isomorphism classes of elliptic curves, as the following theorem shows.

Theorem 3.6. *Let E and E' be two elliptic curves defined over the field K. If E and E' are isomorphic over K, then $j(E) = j(E')$. Conversely, if $j(E) = j(E')$, E and E' are isomorphic over some algebraic extension L over K.*

Proof. For a proof see [Sil09, Proposition III.1.4] □

So whenerver $j(E) = j(E')$, then E and E' are at least isomorphic over the algebraic closure $\overline{K}$.

3.3. Elliptic Curves in Short Weierstrass Form

For an elliptic curve E defined over a field K whose characteristic is not 2 nor 3, we can simplify the Weierstrass equation in the following way: first we substitute $(x, y) \mapsto (x, \frac{y-a_1x-a_3}{2})$ to obtain $Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6$ and then $(x, y) \mapsto (\frac{x-3b_2}{36}, \frac{y}{108})$ yields the simplified equation

$$Y^2 = X^3 + aX + b. \tag{3.3}$$

The projective version (3.2) simplifies to

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{3.4}$$

Equation (3.3) is called *short Weierstrass equation* for elliptic curves. The curve E' obtained by this change of variables is isomorphic to E.

The group law as well as the j-invariant and discriminant can also be simplified. The j-invariant and the discriminant become

$$j(E') = 6912a^3(4a^3 + 27b^2), \text{ and } \Delta(E') = -16(4a^3 + 27b^2).$$

The algorithm to compute the group law is listed in Algorithm 2.

A similar transformation is also possible if the characteristic is 2. But since we will always work with fields that do not have characteristic 2 or 3, we use the short Weierstrass form from now on.

Algorithm 2 Addition of two points on an elliptic curve E defined over K in short Weierstrass form

```
Input: $P, Q \in E(\overline{K})$.
Output: $R = P + Q$.
  if $P = -Q$ then
      return $\mathcal{O}$
  end if
  if $P \neq Q$ then
      $\lambda \leftarrow \frac{y_2 - y_1}{x_2 - x_1}$
  else
      $\lambda \leftarrow \frac{3x_1^2 + a}{2y_1}$
  end if
  $x_3 \leftarrow \lambda^2 - x_1 - x_2$
  $y_3 = \lambda(x_1 - x_3) - y_1$.
  return $R = (x_3, y_3)$
```

3.4. Torsion Subgroups

We will now look at the torsion subgroups of elliptic curves. Let E be an elliptic curve defined over K. For an extension field L of K and an $r \in \mathbb{N}$ we are interested in the groups

$$E(L)[r] = \{P \in E(L) \mid rP = \mathcal{O}\}.$$

If $L = \overline{K}$, we simply write $E[r]$ instead. These groups have a fairly simple structure if we allow the coordinates to be in a sufficiently large field. The subsequent proposition describes the structure of the torsion subgroups of an elliptic curve.

Proposition 3.7. *Let $r \in \mathbb{N}$.*

1. *If E is an elliptic curve defined over $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, then*

$$E(\mathbb{C})[r] \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}.$$

2. *If E is an elliptic curve defined over $\mathbb{F}_p$ and r and p are coprime, then there exists a $k \in \mathbb{N}$ such that*

$$E(\mathbb{F}_{p^{jk}})[r] \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$$

for all $j \in \mathbb{N}$ as well as

$$E[r] \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}.$$

Proof. For a proof we refer to [Sil09, Corollary III.6.4]. □

So for large enough fields the torsion subgroup of order r is a product of two cyclic groups of order r. The number k in this theorem has a special meaning:

Definition 3.8. Let E be an elliptic curve defined over a finite field $\mathbb{F}_p$. The smallest positive integer k such that $E[r] \subset E(\mathbb{F}_{p^k})$ is called *embedding degree* of E with respect to r.

Note that the embedding degree depends on both p and r. The next result captures important equivalent characterizations of the embedding degree.

Proposition 3.9. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_p$ where r and the characteristic are coprime. Then the following statements are equivalent:*

- *The embedding degree with respect to r is k.*
- *k is the smallest positive integer such that $r \,|(p^k - 1)$.*
- *k is the smallest positive integer such that $\mathbb{F}_{p^k}$ contains all r-th roots of unity in $\overline{\mathbb{F}_p}$.*

Example 3.10 and Example 3.11 show curves with different embedding degrees and the consequences on the structure of the torsion subgroups.

Example 3.10. Let $p = 11$ and consider the elliptic curve $E : Y^2 = X^3 + 4$ defined over $\mathbb{F}_p$. The curve consists of the following 12 $\mathbb{F}_p$-rational points:

$$\mathcal{O}, (0, 2), (0, 9), (1, 4), (1, 7), (2, 1), (2, 10), (3, 3), (3, 8), (6, 0), (10, 5), (10, 6)$$

We consider $r = 3 \,|\, E(\mathbb{F}_p)$. From Proposition 3.7 we know that there are 9 points in $E[3]$. By checking all the points in $E(\mathbb{F}_p)$ one can observe that only the 3 points $\mathcal{O}$, $(0, 2)$ and $(0, 9)$ are contained in the 3-torsion. This observation agrees with the fact that the embedding degree $k \neq 1$ since $(p^1 - 1) \not\equiv 0 \mod r$. But, $(p^2 - 1) \equiv 0 \mod r$, so the embedding degree $k = 2$. Since $p \equiv 3 \mod 4$ we can construct $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i^2 + 1 = 0$. Hence the whole 3-torsion is contained in $E(\mathbb{F}_{p^2})$, which is structured as four cyclic subgroups of order 3:

$$\begin{aligned}
G_1 &= \{\mathcal{O}, (0, 2), (0, 9)\}, \\
G_2 &= \{\mathcal{O}, (8, i), (8, 10i)\}, \\
G_3 &= \{\mathcal{O}, (2i + 7, 10i), (2i + 7, i)\}, \text{ and} \\
G_4 &= \{\mathcal{O}, (9i + 7, i), (9i + 7, 10i)\}.
\end{aligned}$$

Example 3.11. Now consider $p = 31$ and the elliptic curve $E : Y^2 = X^3 + 13$ defined over $\mathbb{F}_p$. In this case the curve has 25 $\mathbb{F}_p$ rational points, so take $r = 5$. Since $p^1 - 1 \equiv 0 \mod r$, the embedding degree with respect to r is $k = 1$. Hence $E[r]$ is fully contained in $E(\mathbb{F}_p)$. Since $E[r] \simeq \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$, the r-torsion consists of 6 cyclic subgroups of order 5.

3.5. Frobenius Endomorphism

In this section we switch our focus to elliptic curves defined over finite fields. The next theorem gives a bound on the number of $\mathbb{F}_q$-rational points an elliptic curve can contain.

Theorem 3.12 (Hasse bound)**.** *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then*

$$|E(\mathbb{F}_q)| = q + 1 - t$$

with some $t \in \mathbb{Z}$ with $|t| \leq 2\sqrt{q}$.

Proof. For a proof see [Was08, Theorem 4.2] □

The value $t = q + 1 - |E(\mathbb{F}_q)|$ is called *trace of Frobenius for E over $\mathbb{F}_q$*. It allows to classify elliptic curves into two groups:

Definition 3.13. Let E be an elliptic curve defined over $\mathbb{F}_q$ with $q = p^n$ for some prime $p \in \mathbb{P}$. Let t be the trace of Frobenius.

1. If p divides t, then E is called *supersingular.*

2. If p does not divide t, then E is called *ordinary.*

The trace of Frobenius is closely related to the Frobenius endomorphism on E, which is defined in the following way:

Definition 3.14 (Frobenius endomorphism)**.** Let E be an elliptic curve defined over $\mathbb{F}_q$. The map

$$\pi_q : \begin{cases} E(\overline{\mathbb{F}_q}) & \to E(\overline{\mathbb{F}_q}) \\ (x, y) & \mapsto (x^q, y^q) \end{cases}$$

is called *Frobenius endomorphism on E.*

The Frobenius endomorphism on E is the continuation of the Frobenius endomorphism of the underlying field to E. The endomorphism is connected to the Hasse bound via the subsequent theorem:

Theorem 3.15. *Let E be an elliptic curve defined over $\mathbb{F}_p$ and $t = p + 1 - |E(\mathbb{F}_p)|$.*

1. *Let $\alpha, \beta \in \mathbb{C}$ be the complex roots of the polynomial $Z^2 - tZ + p$. Then $|\alpha| = |\beta| = \sqrt{p}$ and*

$$\left|E(\mathbb{F}_{p^k})\right| = p^k + 1 - \alpha^k - \beta^k.$$

2. *Let π_p be the Frobenius map on E. Then for every point $P \in E(\overline{\mathbb{F}_q})$ we have*

$$\pi_p^2(P) - t\pi_p(P) + pP = \mathcal{O}.$$

Proof. For a proof see [Sil09, Theorem V.2.3.1]. □

Besides counting the number of points on a curve, the Frobenius endomorphism gives rise to the trace map. This map plays an intricate role within the torsion subgroups.

Definition 3.16 (Trace map)**.** Let E be an elliptic curve defined over $\mathbb{F}_q$ and $k \in \mathbb{N}$.

1. The map
$$\mathrm{Tr} : \begin{cases} E(\mathbb{F}_{q^k}) & \to E(\mathbb{F}_q) \\ P & \mapsto \sum_{i=0}^{k-1} \pi_q^i(P) \end{cases}$$
is called the *trace map.*

2. The map
$$\mathrm{aTr} : \begin{cases} E(\mathbb{F}_{q^k}) & \to E(\mathbb{F}_{q^k}) \\ P & \mapsto kP - \mathrm{Tr}(P) \end{cases}$$
is called the *anti trace map.*

The trace map is in fact a group homomorphism. Since the Frobenius endomorphism is trivial for $\mathbb{F}_p$-rational points, the trace map acts as multiplication by k, that is $\mathrm{Tr}(P) = kP$ for all $P \in E(\mathbb{F}_p)$. One interesting property of the trace map is that for $r \| \, |E(\mathbb{F}_q)|$ it maps all r-torsion points into one particular subgroup of the r-torsion.

Example 3.17. Let $p = 11$ and consider the elliptic curve $E : Y^2 = X^3 + 7x + 2$ defined over $\mathbb{F}_p$. The curve consists of 7 $\mathbb{F}_p$-rational points, so we take $r = 7$. Since the smallest k such that $r \mid q^k - 1$ is $k = 3$, the embedding degree with respect to r is 3. Hence $E[7] \subset E(\mathbb{F}_{p^3})$. We already know that Tr maps as multiplication with k on $E(\mathbb{F}_p)$. Every other point of the r-torsion will be sent to $E(\mathbb{F}_p)[r]$. We will check that for one point.

Write $\mathbb{F}_{p^3}$ as $\mathbb{F}_p(u)$ with $u^3 + u + 4 = 0$. The point $Q = (u^{481}, u^{1049}) \in E[r]$ is mapped to $(8, 8)$ as it can be verified easily:

$$\begin{aligned} \mathrm{Tr}(Q) = {} & (u^{481}, u^{1049}) + (u^{4291}, u^{11539}) + (u^{58201}, u^{126929}) \\ = {} & (u^{481}, u^{1049}) + (u^{1301}, u^{899}) + (u^{1011}, u^{579}) \\ = {} & (4u^2 + 7u + 4, 10u^2 + 2u + 6) + (6u^2 + 7u + 9, 8u + 3) + \\ & (u^2 + 8u + 2, u^2 + u) \\ = {} & (8, 8) \end{aligned}$$

Now let E be an elliptic curve defined over $\mathbb{F}_q$ and let $r \| E(\mathbb{F}_q)$ be prime. We assume that the embedding degree k with respect to r is greater than 1. There are two subgroups of $E[r]$ arising from the eigenspaces of the Frobenius endomorphism π. To describe this two subgroups, we define the following two group homomorphisms first:

$$\pi - 1 : \begin{cases} E(\overline{\mathbb{F}_q}) & \to E(\overline{\mathbb{F}_q}) \\ P & \mapsto \pi(P) - P \end{cases} \text{ and } \pi - q : \begin{cases} E(\overline{\mathbb{F}_q}) & \to E(\overline{\mathbb{F}_q}) \\ P & \mapsto \pi(P) - qP \end{cases}.$$

The subgroups from the eigenspaces of π are now given by

$$\mathcal{G}_1 = E[r] \cap \ker(\pi - 1), \text{ and } \mathcal{G}_2 = E[r] \cap \ker(\pi - q).$$

Since π acts trivially on $E(\mathbb{F}_q)[r]$ but nowhere else in $E[r]$, $\mathcal{G}_1$ only consists of $\mathbb{F}_q$ rational points. It is thus also called *base-field subgroup* and it is the unique subgroup of order r which is defined over $\mathbb{F}_q$. For all points $P \in \mathcal{G}_2$ we have that $\mathrm{Tr}(P) = \mathcal{O}$ and it is called *trace zero subgroup.*

The trace map and anti-trace map are closely related to the base-field subgroup and trace zero subgroup. The following proposition illustrates the relationship.

Proposition 3.18. *1. The image of $E[r]$ under Tr is $\mathcal{G}_1$.*

2. The image of $E[r]$ under aTr is $\mathcal{G}_2$.

3. The image of $\mathcal{G}_2$ under Tr is $\{\mathcal{O}\}$.

Proof. For a proof we refer to [Gal05, Section IX.7.4, Lemma IX.16]. □

3.6. Twists

We have seen earlier, that two elliptic curves defined over K with the same j-invariant are isomorphic over the algebraic closure $\overline{K}$, but they do not necessarily need to be isomorphic over K. In this case they are *twists* of each other.

Definition 3.19 (Twists)**.** Let E and E' be elliptic curves defined over K. If $j(E) = j('E)$ and $E(K) \not\cong E'(K)$, then E and E' are called *twists* of each other.

If E and E' are twists of each other, they are isomorphic over the algebraic closure. Furthermore, there is a smallest extension field K' over K such that E and E' are isomorphic over K' but are not isomorphic over any of the proper subfields of K'.

For elliptic curves defined over finite fields, we can further characterize the nature of the possible twists. First we define a degree of a twist:

Definition 3.20. Let E be an elliptic curve defined over $\mathbb{F}_q$, where $E(\mathbb{F}_q)$ has prime order and let k be its embedding degree. Let $d \,|\, k$. An elliptic curve E' defined over $\mathbb{F}_{q^{k/d}}$ is called a *twist of degree d of E* if there is an isomorphism $\psi : E'(\overline{\mathbb{F}_{q^{k/d}}}) \to E(\overline{\mathbb{F}_q})$ defined over $\mathbb{F}_{q^k}$, and this is the smallest extension of $\mathbb{F}_{q^{k/d}}$ over which ψ is defined.

Let $E : Y^2 = X^3 + aX + b$ be a curve defined over $\mathbb{F}_q$. Then a twist E' of E is given by

$$E' : Y^2 = X^3 + a\omega^4 X + b\omega^6, \text{ where } \omega \in \mathbb{F}_{q^k}.$$

The isomorphism between E' and E is given by

$$\psi : \begin{cases} E'(\overline{\mathbb{F}_{q^{k/d}}}) & \to E(\overline{\mathbb{F}_q}) \\ (x, y) & \mapsto \left(\frac{x}{\omega^2}, \frac{y}{\omega^3}\right) \end{cases}$$

	$j(E)$	fields of definition	$Q' = (x_{Q'}, y_{Q'})$	$Q = \psi(Q')$
d	a, b	for powers of ω	$P = (x_P, y_P)$	$P' = \psi^{-1}(P)$
	$\notin \{0, 1728\}$	$\omega^2, \omega^3, \omega^4 \in \mathbb{F}_{q^{k/2}}$	$(\mathbb{F}_{q^{k/2}}, \mathbb{F}_{q^{k/2}})$	$(\mathbb{F}_{q^{k/2}}, \mathbb{F}_{q^k})$
2	$a \neq 0, b \neq 0$	$\omega^3 \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^{k/2}}$	$(\mathbb{F}_q, \mathbb{F}_q)$	$(\mathbb{F}_{q^{k/2}}, \mathbb{F}_{q^k})$
	0	$\omega^3, \omega^6 \in \mathbb{F}_{q^{k/3}}$	$(\mathbb{F}_{q^{k/3}}, \mathbb{F}_{q^{k/3}})$	$(\mathbb{F}_{q^k}, \mathbb{F}_{q^{k/3}})$
3	$a = 0, b \neq 0$	$\omega^3 \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^{k/3}}$	$(\mathbb{F}_q, \mathbb{F}_q)$	$(\mathbb{F}_{q^k}, \mathbb{F}_{q^{k/3}})$
	1728	$\omega^4 \in \mathbb{F}_{q^{k/4}}, \omega^2 \in \mathbb{F}_{q^{k/2}}$	$(\mathbb{F}_{q^{k/4}}, \mathbb{F}_{q^{k/4}})$	$(\mathbb{F}_{q^{k/2}}, \mathbb{F}_{q^k})$
4	$a \neq 0, b = 0$	$\omega^3 \in \mathbb{F}_{q^k} \setminus \mathbb{F}_{q^{k/2}}$	$(\mathbb{F}_q, \mathbb{F}_q)$	$(\mathbb{F}_{q^{k/2}}, \mathbb{F}_{q^k})$
	0	$\omega^6 \in \mathbb{F}_{q^{k/6}}, \omega^3 \in \mathbb{F}_{q^{k/3}}$	$(\mathbb{F}_{q^{k/6}}, \mathbb{F}_{q^{k/6}})$	$(\mathbb{F}_{q^{k/2}}, \mathbb{F}_{q^{k/3}})$
6	$a = 0, b \neq 0$	$\omega^2 \in \mathbb{F}_{q^{k/2}}$	$(\mathbb{F}_q, \mathbb{F}_q)$	$(\mathbb{F}_{q^{k/2}}, \mathbb{F}_{q^{k/3}})$

Table 3.1.: Nature of degree 2, 3, 4 and 6 twists [CLN10, Table 1].

and its inverse is

$$\psi^{-1} : \begin{cases} E(\overline{\mathbb{F}_q}) & \to E'(\overline{\mathbb{F}_{q^{k/d}}}) \\ (x, y) & \mapsto (x\omega^2, y\omega^3) \end{cases} .$$

In particular, this isomorphism induces a group isomorphism $\mathcal{G}_2 \to E'(\mathbb{F}_{q^{k/d}})[r]$.

The j-invariant of E and ω determine the possible twist degrees. Table 3.1 lists the possibilities for twists of degree 2, 3, 4 and 6. The last two columns of the table show the subfields of $\mathbb{F}_{q^k}$ in which the coordinates of the specific points are contained when ψ^{-1} and ψ are applied to $P \in E(\mathbb{F}_q)$ and $Q \in E'(\mathbb{F}_{q^{k/d}})$.

3.7. Elliptic Curve Cryptography

Recall that in a cyclic group G every element $h \in G$ can be represented as $h = g^k$ for some generator g of K and $k \in \mathbb{N}_0$. The exponent k is also called the *discrete logarithm of* h *to the base* g, written as $\log_g(h)$. If only h is known, finding $\log_g(h)$ is presumably a hard problem in some groups. This motivates the definition of the Discrete Logarithm Problem:

Definition 3.21 (Discrete Logarithm Problem (DLP))**.** Let G be a cyclic group. Given a generator g of G and an element h, the problem of finding $\log_g(h)$ is called *Discrete Logarithm Problem.*

The hardness of the problem depends on the structure of the group G. Although the problem is assumed to be hard for large prime order subgroups of $(\mathbb{Z}/p\mathbb{Z}, \cdot)^\times$, it is easy to solve for $(\mathbb{Z}/p\mathbb{Z}, +)$ due to the existence of the extended Euclidean algorithm.

The use of elliptic curves in cryptographic applications usually relies on the hardness of the DLP for elliptic curves:

Definition 3.22 (Elliptic Curve Discrete Logarithm Problem (ECDLP))**.** Let E be an elliptic curve and G be a point on the curve. Given a second point $P \in \langle G \rangle$, the problem of finding a $k \in \mathbb{N}$ such that $P = kG$ is called the *Elliptic Curve Discrete Logarithm Problem.*

Solving the ECDLP is generally assumed to be hard. So far no subexponential algorithms are known to solve this problem. However, there are certain elliptic curve groups where the ECDLP is comparatively easy to solve. We will see one type of such elliptic curves later.

Another interesting problem is the Diffie-Hellman problem. For general groups it can be defined in the following way:

Definition 3.23 (Diffie-Hellman Problem (DHP))**.** Let G be a cyclic group. Given a generator g of G and two elements g^a and g^b for $a, b \in \mathbb{Z}$, the problem of finding g^{ab} is called *the Diffie-Hellman problem.*

Similarly to the ECDLP, the variant of DHP for elliptic curves is defined as follows:

Definition 3.24 (ECDHP)**.** Let E be an elliptic curve and G be a point on the curve. Given two points aG and bG for some $a, b \in \mathbb{Z}$, finding the point abG is called the *Elliptic Curve Diffie-Hellman problem.*

The ECDHP is assumed to be hard problem. However, if one can solve the ECDLP, one can also solve the ECDHP. But it is not known if the other implication holds as well.

Part II.

Bilinear Pairings

4. Divisors

In this section we introduce some basic definitions and facts from the theory of algebraic function fields that are fundamental to the understanding of cryptographic pairing computations. We will introduce the group of divisors and discuss some of the properties. However, we specialize the discussion to the case of elliptic curves. It should be noted though, that divisors can also be introduced for any algebraic curve and its function field, but this would require the more general notion of places of a function field, which we have not introduced.

The discussion of divisors is based on [Was08, HPS08, Sti09, Gal05, Sil09, Cos12].

Unless noted otherwise, we assume that the field K is algebraically closed throughout this section.

Definition 4.1. Let E be an elliptic curve defined over K. The *group of divisors* of E is given by the set of formal sums

$$\mathrm{Div}(E) = \left\{ \sum_{P \in E(\overline{K})} n_P(P) \mid n_P \in \mathbb{Z}, n_P = 0 \text{ for all but finitely many} \right\}.$$

For each point $P \in E(\overline{K})$ we introduce a formal symbol (P) and form formal sums using these symbols. So the sum in the definition of the divisors is not to be confused with a sum of some points on an elliptic curve. In other words, $\mathrm{Div}(E)$ is the free Abelian group generated by E.

Example 4.2. Let E be an elliptic curve defined over K and let $\mathcal{O} \neq P \in E(\overline{K})$. The divisors $2(3P)$ and $3(2P)$ are distinct, whereas the points $2 \cdot 3P$ and $3 \cdot 2P$ are the same.

Divisors form a group in a very natural way and we always write it additively. The identity element is the zero divisor, the divisor with $n_P = 0$ for all P. The law of composition is given by the component-wise addition:

$$+ : \begin{cases} \mathrm{Div}(E) \times \mathrm{Div}(E) & \to \mathrm{Div}(E) \\ (\sum_{P \in E(\overline{K})} n_P(P), \sum_{P \in E(\overline{K})} m_P(P)) & \mapsto \sum_{P \in E(\overline{K})} (n_P + m_P)(P) \end{cases}$$

Each divisor has a degree and support which are defined as follows:

Definition 4.3. The *degree* of a divisor D is denoted by

$$\mathrm{Deg}(D) = \sum_{P \in E(\overline{K})} n_P,$$

and the *support* of D is defined as

$$\mathrm{supp}(D) = \{P \in E(\overline{K}) \mid n_P \neq 0\}.$$

Example 4.4 gives examples of divisors together with their support and degree.

Example 4.4. Let $P, Q, R, S \in E(\overline{K})$. Set

$$D_1 = 2(P) - 3(Q), \text{ and } D_2 = 3(Q) + (R) - (S).$$

The degrees of two divisors are

$$\operatorname{Deg}(D_1) = 2 - 3 = -1, \text{ and } \operatorname{Deg}(D_2) = 3 + 1 - 1 = 3.$$

The sum of the two divisors is

$$D_1 + D_2 = 2(P) + (R) - (S)$$

and its degree is

$$\operatorname{Deg}(D_1 + D_2) = 2 + 1 - 1 = 2.$$

The supports of D_1, D_2 and $D_1 + D_2$ are

$$\operatorname{supp}(D_1) = \{P, Q\}, \operatorname{supp}(D_2) = \{Q, R, S\}, \text{ and } \operatorname{supp}(D_1 + D_2) = \{P, R, S\}.$$

Associating divisors with a function $f \in K(E)$ is a convenient way to write down the intersection points and their multiplicities of f and E. We are especially interested in zeros and poles of f. Let $P \in E(\overline{K})$. Then there exists a non-zero function u_p, called the *uniformizer at* P, with $u(P) = 0$ and such that every function $f \in K(E)$ can be written in the form

$$f = u_P^r g$$

with $r \in \mathbb{Z}$ and $g \in K(E)$ such that $g(P) \neq 0$ and g is defined at P. We are now able to define the *order* of f at P and the divisor of f:

Definition 4.5. Let $f \in K(E)^\times$.

1. Let $P \in E(\overline{K})$ and u_P be a uniformizer at P. Let $g \in K(E)$ be such that $f = u_P^r g$ for some $r \in \mathbb{Z}$. We define the *order of* f *at* P as
$$\operatorname{ord}_P(f) = r.$$
2. The *divisor of* f is defined as
$$(f) = \sum_{P \in E} \operatorname{ord}_P(f)(P).$$

Note that the order of the function at a point is independent of the choice of the uniformizer.

The arithmetic of functions directly translates to their divisors. Let $f, g \in K(E)^\times$, then $(fg) = (f) + (g)$ and $(f/g) = (f) - (g)$ if g is not zero. So the map given by

$$(\cdot) : \begin{cases} K(E)^\times & \to \operatorname{Div}(E) \\ f & \mapsto (f) \end{cases}$$

is a group homomorphism. The existence of this relation is not surprising since divisors of functions capture zeros and poles. So the divisor of the product of two functions needs to include all zeros and poles from each function except for those zeros and poles which cancel out.

Example 4.6, Example 4.7 and Example 4.8 demonstrate the computation of the order of a function at a point and the computation of the divisor of a function.

Example 4.6. We look at uniformizers of affine points. Let $P = (P_x, P_y) \in E(\overline{K}) \setminus \{\mathcal{O}\}$. In this case the uniformizer can be taken from the equation of any line that passes through P, but is not tangent to E. If $P_y \neq 0$, one can take $u_P(x, y) = x - P_x$ and if $P_y = 0$, then one can take $u_P(x, y) = y$.

Let $E : Y^2 = X^3 + 72$, $P = (-2, 8)$ and consider the function

$$f(x, y) = x + y - 6.$$

Clearly, f vanishes at P. We take $u_P(x, y) = x + 2$ as uniformizer at P. Note that the curve equation can be rewritten as

$$(Y + 8)(Y - 8) = (X + 2)^3 - 6(X + 2)^2 + 12(X + 2)$$

and therefore

$$f(x, y) = (x + 2) + (y - 8) = (x + 2) \underbrace{\left(1 + \frac{(x + 2)^2 - 6(x + 2) + 12}{y + 8}\right)}_{g(x,y)}.$$

The function g is finite at P and does not vanish, so from $f = u_p^1 g$ we obtain that $\mathrm{ord}_P(f) = 1$.

Now consider the function

$$t(x, y) = \frac{3(x + 2)}{4} - y + 8$$

coming from the tangent line to E at P. Using the same approach as for f, t can be rewritten as

$$t(x, y) = (x + 2)^2 \underbrace{\left(\frac{-(x + 2) + 6}{y + 8} + 3\frac{(x + 2)^2 - 6(x + 2) + 12}{4(y + 8)^2}\right)}_{g(x,y)}.$$

Again, g is finite at P and does not vanish at P, so from $t = u_P^2 g$ we obtain $\mathrm{ord}_P(f) = 2$.

Example 4.7. The uniformizer at $\mathcal{O}$ is not as straight forward as the case for affine points. Consider an elliptic curve $E : Y^2 = X^3 + aX + b$. A uniformizer at $\mathcal{O}$ is given by $u_{\mathcal{O}}(x, y) = \frac{x}{y}$. Clearly, $u_{\mathcal{O}}(\mathcal{O}) = 0$, as it can easily seen from the projective version of $u_{\mathcal{O}}$.

The defining equation of E can be easily rewritten in terms of $u_{\mathcal{O}}$:

$$\left(\frac{X}{Y}\right)^2 = \frac{X^2}{X^3 + aX + b} = \frac{1}{X\left(1 + \frac{a}{X^2} + \frac{b}{X^3}\right)}.$$

From this equation we can observe that the function $f(x,y) = x$ has order $\mathrm{ord}_{\mathcal{O}}(f) = -2$ and the order of $g(x,y) = y$ can now be derived from the equation $y = x\frac{y}{x}$, hence $\mathrm{ord}_{\mathcal{O}}(g) = -3$.

Example 4.8. We consider the lines that are used in the chord-and-tangent rule. Let $E : Y^2 = X^3 + aX + b$ be an elliptic curve defined over some field K. Let $\ell : Y = \lambda X + \nu$ be the line that represents the chord while adding the points P and Q. We are interested in the points where ℓ intersects E, as this is exactly the information the divisor of (ℓ) tells us. Clearly, the line ℓ intersects E in P, Q and $-(P+Q)$ all with multiplicity 1 and these are all affine intersection points (assuming $P \neq -Q$). To investigate ℓ on E at $\mathcal{O}$ we use a different approach than the previous example and do not express the function in terms of a uniformizer at $\mathcal{O}$. Instead we look at the projective version of ℓ by sending $X \mapsto \frac{X}{Z}$ and $Y \mapsto \frac{Y}{Z}$ which gives:

$$\ell' : \frac{Y}{Z} = \left(\frac{\lambda X + \nu Z}{Z}\right)^2$$

and thus

$$\left(\frac{X}{Z}\right)^3 + a\frac{X}{Z} + b = \left(\frac{\lambda X + \nu Z}{Z}\right)^2.$$

From this equation we are able to infer that there is pole of order 3 when $Z = 0$. So ℓ has the divisor

$$(\ell) = (P) + (Q) + (-(P+Q)) - 3(\mathcal{O}).$$

If $P = Q$, then the divisor simplifies to

$$(\ell) = 2(P) + (-2P) - 3(\mathcal{O}).$$

In any case, the degree of (ℓ) is 0.

The balance between zeros and poles that occurred in Example 4.8 is not a coincidence. In fact, this is true for any function on E. The following result captures some of the properties of divisors of functions and ensures that they are well-defined:

Proposition 4.9. *Let E be an elliptic curve and let $f \in K(E)$ be non-zero.*

1. *f has only finitely many zeros and poles.*

2. $\mathrm{Deg}((f)) = 0$.

3. *If f has no zeros or poles, then f is constant.*

Proof. For a proof we refer to [Sil09, Proposition II.3.1] and [Sti09, Corollary 1.1.20]. □

The last statement of Proposition 4.9 is important. It implies that for any two f and g on E that have the same divisors, there exists a $c \in K^\times$ such that $f = cg$. So the divisor (f) determines f up to a non-zero scalar factor.

As we will see in the coming chapters, the language of divisors is essential in the description of pairings. We will compute functions with very large degree on E with prescribed divisors and then evaluate these functions at other divisors. The evaluation of a function $f \in K(E)$ at a divisor D has a natural definition provided that (f) and D have disjoint supports:

Definition 4.10. Let $f \in K(E)^\times$ and $D = \sum_{P \in E} n_P(P) \in \mathrm{Div}(E)$ such that $\mathrm{supp}((f)) \cap \mathrm{supp}(D) = \emptyset$. Then define the evaluation of f at D, written as $f(D)$, by

$$f(D) = \prod_{P \in E(\overline{K})} f(P)^{n_P}.$$

Example 4.11 demonstrates the evaluation of a function at a divisor. It also gives an example of the more general fact, that if for two functions f and g there is some constant $c \in K$ such that $g = cf$, then $f(D) = g(D)$ for any divisor D with disjoint support.

Example 4.11. Consider $E : Y^2 = X^3 - X - 2$ defined over $\mathbb{F}_{163}$ and let

$$P = (43, 154), Q = (46, 38), R = (12, 35), \text{ and } S = (5, 66).$$

Let $\ell_{P,Q}$ be the line through P and Q, $\ell_{P,P}$ the tangent to P on E and $\ell_{Q,Q}$ the tangent to Q and E. Explicitly written down, these functions are defined as

$$\begin{aligned}\ell_{P,Q}(x, y) &= y + 93x + 85,\\ \ell_{P,P}(x, y) &= y + 127x + 90, \text{ and}\\ \ell_{Q,Q}(x, y) &= y + 13x + 16.\end{aligned}$$

Now let $D_1 = 2(R) + (S)$, $D_2 = 3(R) - 3(S)$, and $D_3 = (R) + (S) - 2(\mathcal{O})$. Note that we cannot evaluate any of these functions at D_3 since the supports of $(\ell_{P,Q})$, $(\ell_{P,P})$ and $(\ell_{Q,Q})$ all contain $\mathcal{O}$. We evaluate $\ell_{P,Q}$ at D_1 and $\ell_{P,P}$ at D_2:

$$\begin{aligned}\ell_{P,Q}(D_1) &= \ell_{P,Q}(R)^2 \ell_{P,Q}(S) = (y_R + 93x_R + 85)^2(y_S + 93x_S + 85) = 122\\ \ell_{P,P}(D_2) &= \frac{\ell_{P,P}(R)^3}{\ell_{P,P}(S)^3} = \frac{(y_R + 127x_R + 90)^3}{(y_S + 127x_S + 90)^3} = 53\end{aligned}$$

Now we look at a scalar multiple of $\ell_{P,P}$: $\ell'_{P,P} = 17\ell_{P,P}$. We evaluate at D_2 again:

$$\ell'_{P,P}(D_2) = \frac{\ell_{P,P}(R)^3}{\ell_{P,P}(S)^3} = \frac{(17y_R + 40x_R + 63)^3}{(17y_S + 40x_S + 63)^3} = 53$$

4.1. The Divisor Class Group

The divisor group contains important subgroups, namely the degree-zero divisors and the group of principal divisors. These two groups are used to construct the divisor class group.

Definition 4.12. Let E be an elliptic curve.

1. The set
$$\operatorname{Div}^0(E) = \{D \in \operatorname{Div}(E) \mid \operatorname{Deg}(D) = 0\}$$
is the set of degree-zero divisors.
2. A divisor $D \in \operatorname{Div}(E)$ is called a *principal* divisor if there exists a function $f \in K(E)$ such that $D = (f)$. The set of all principal divisors is denoted by $\operatorname{Prin}(E)$.

The set of degree-zero divisors $\operatorname{Div}^0(E)$ forms a proper subgroup of $\operatorname{Div}(E)$. Similarly, $\operatorname{Prin}(E)$ naturally forms a subgroup of $\operatorname{Div}(E)$. We have seen earlier that principal divisors have degree zero, so $\operatorname{Prin}(E) \subset \operatorname{Div}^0(E)$. But in general not all degree zero divisors are principal. There is an extra condition on degree zero divisors to be principal:

Theorem 4.13. *A divisor $D = \sum_{P \in E} n_P(P) \in \operatorname{Div}^0(E)$ is principal if and only if*
$$\sum_{P \in E} n_P P = \mathcal{O}.$$

Proof. For a proof see [Was08, Theorem 11.2]. □

Example 4.14 shows an application of Theorem 4.13.

Example 4.14. Consider the elliptic curve $E : Y^2 = X^3 + 20X + 20$ defined over $\mathbb{F}_{103}$ and the points
$$P = (26, 20), Q = (63, 78), R = (59, 95),$$
$$S = (24, 25), T = (77, 84), U = (30, 99).$$

The divisor $(S) + (T) - (P) \in \operatorname{Div}(E)$ has degree 1, so it is clearly not in the subgroup $\operatorname{Div}^0(E)$. The divisor $(P) + (Q) - (R) - (S)$ has degree 0, so it is in $\operatorname{Div}^0(E)$. However, it is not principal, since
$$P + Q - R - S = (18, 49) \neq \mathcal{O}.$$

Hence there does not exist a function f on E with divisor $(f) = (P)+(Q)-(R)-(S)$. The divisor $(P) + (Q) - (R) - (T)$ has degree 0 and also
$$P + Q - R - T = \mathcal{O},$$

so it is principal. A function with divisor $(P)+(Q)-(R)-(T)$ is given by

$$f(x,y)=\frac{6y+71x^2+91x+91}{x^2+70x+11}.$$

Note that $P+Q=U$, so the $P+Q-U=\mathcal{O}$, but the divisor $(P)+(Q)-(U)$ does not have degree 0, so it is not principal. If we instead take the divisor $(P)+(Q)-(U)-(\mathcal{O})$, we again have principal divisor. The function

$$g(x,y)=\frac{y+4x+82}{x+73}$$

has the divisor $(P)+(Q)-(U)-(\mathcal{O})$.

We now compare f and g in the projective space. The projective representations of f and g are

$$\begin{aligned} f(x,y,z)&=\frac{6xz+71x^2+91xz+91z^2}{x^2+70xz+11z^2}, \text{ and}\\ g(x,y,z)&=\frac{y+4x+82z}{x+73z}. \end{aligned}$$

For f, both the nominator and denominator evaluate to 0 at $\mathcal{O}$, which gives a pole and a zero at $\mathcal{O}$ which cancel out in (f). However, for g only the denominator evaluates to 0 at $\mathcal{O}$, so we have a pole at $\mathcal{O}$ and $\mathcal{O}\in\operatorname{supp}((g))$, but $\mathcal{O}\notin\operatorname{supp}((f))$.

Before we define the divisor class group of E, we need to define an equivalence relation on $\operatorname{Div}(E)$. Two divisors D_1 and D_2 are said to be *linearly equivalent*, $D_1\sim D_2$, if there exists a function f such that $D_1=D_2+(f)$. From the definition it is clear that $D_1\sim D_2$ is equivalent to $D_1-D_2\in\operatorname{Prin}(E)$.

Example 4.15. Let $E: Y^2=X^3+8X+1$ be an elliptic curve defined over $\mathbb{F}_{61}$. We look at the points

$$P=(57,24), Q=(25,37), R=(17,32), \text{ and } S=(42,35).$$

We now consider the divisors $D_1=(P)+(Q)+(R)$ and $D_2=-(S)+4(\mathcal{O})$. Note that

$$D_1-D_2=(P)+(Q)+(R)+(S)-4(\mathcal{O})$$

which has degree zero 0 and $P+Q+R+S-4\mathcal{O}=\mathcal{O}$. So there exists a function f on E such that $D_1-D_2=(f)$ and $D_1-D_2\in\operatorname{Prin}(E)$ or alternatively, $D_1\sim D_2$.

Definition 4.16. The *divisor class group* (*Picard group*) of E is defined as the quotient group

$$\operatorname{Pic}^0(E)=\operatorname{Div}^0(E)/\sim\,=\operatorname{Div}^0(E)/\operatorname{Prin}(E).$$

The divisor class group gives an alternative description of the law of composition, which is based on divisors. The following example describes the connection between $\operatorname{Pic}^0(E)$ and E.

Example 4.17. Let P and Q be two distinct points on an elliptic curve E. Recall from Example 4.8 that line ℓ through P and Q has the divisor $(\ell) = (P) + (Q) + (-R) - 3(\mathcal{O})$. The vertical line ν running through R has the divisor $(\nu) = (-R)+(R)-2(\mathcal{O})$. Hence the quotient $\frac{\ell}{\nu}$ has the divisor

$$\left(\frac{\ell}{\nu}\right) = (P) + (Q) - (R) - (\mathcal{O}).$$

Note that both $(R) - (\mathcal{O})$ and $(P) + (Q) - 2(\mathcal{O})$ are clearly in $\mathrm{Div}^0(E)$. Since they are connected via the equation

$$(R) - (\mathcal{O}) = (P) + (Q) - 2(\mathcal{O}) - \left(\frac{\ell}{\nu}\right), \tag{4.1}$$

they represent the same class in $\mathrm{Pic}^0(E)$. Hence we have a connection between the equation $R = P + Q$ in E and Equation 4.1 via the group homomorphism induced by the map

$$\begin{cases} E & \to \mathrm{Div}^0(E) \\ P & \mapsto (P) - (\mathcal{O}). \end{cases}$$

4.2. A Corollary to the Riemann-Roch Theorem

We will now present a corollary to the Riemann-Roch Theorem. We do not state the Riemann-Roch theorem in full detail, since we are only interested in the corollary. We refer the interested reader to [Sti09, Chapter 1.5] and [Sil09, Chapter II.5] for an in-depth discussion.

To state the corollary, we first consider some further properties of divisors.

Definition 4.18. Let $D = \sum_{P \in E(\overline{K})} n_P(P) \in \mathrm{Div}(E)$.

1. If $n_P \geq 0$ for all $P \in E$, then D is called *effective*.
2. The *effective part of* D is given by

$$\epsilon(D) = \sum_{P \in E(\overline{K}), n_P \geq 0} n_P(P)$$

3. The *size* of a divisor is the degree of its effective part.

The only effective divisor in $\mathrm{Div}^0(E)$ is the zero divisor. The following example shows these notions in use.

Example 4.19. Let E be an elliptic curve and $P, Q \in E(\overline{K})$ be two distinct points. The divisor $D = (P) + (Q) - 2(\mathcal{O})$ is not effective. Its effective part is $\epsilon(D) = (P) + (Q)$ and the size of D is 2, although the degree of D is 0.

The corollary that we are interested in can be stated as follows:

Corollary 4.20. *Let E be an elliptic curve. Then there exists a $g \in \mathbb{Z}$ such that every divisor $D \in \mathrm{Pic}^0(E)$ is equivalent to a divisor D' with $\mathrm{Deg}(\epsilon(D')) \leq g$.*

This integer is called *genus* of the curve. The corollary is also true for general algebraic curves where one can also introduce the divisor class group. For elliptic curves however, the situation is very simple: for any elliptic curve the genus is 1 and hence every $D \in \mathrm{Pic}^0(E)$ is equivalent to a divisor of the form $(P) - (Q)$ for some $P, Q \in E(\overline{K})$. So the group homomorphism induced by $P \mapsto (P) - (\mathcal{O})$ that we have seen in Example 4.17 is actually a group isomorphism. This makes it possible to use the very simple description of the group law without the introduction of divisors and the divisor class group and can simply talk about the group elements being points on the curve. For other algebraic curves of larger genus, this is not possible. We would have to relay on the divisor class group to obtain some arithmetic on a curve of higher genus.

Example 4.21 shows how a given divisor of larger size can be reduced to a divisor of size 1.

Example 4.21. Let $E : Y^2 = X^3 + aX + b$ be an elliptic curve defined over K where K is not necessarily algebraically closed. Assume there is a divisor of the form $D = \sum_{i=1}^{11}(P_i) - 11(\mathcal{O})$ with size 11 in $\mathrm{Pic}^0(E)$ where the P_i are all K-rational. The P_i do not need to be distinct. We want to find a divisor of size 1 that is equivalent to D.

We start with constructing a function $\ell_{10} : Y = \sum_{i=0}^{10} a_i X^i$ to interpolate the distinct points in $\mathrm{supp}(D)$. By substituting ℓ_{10} into E, we obtain a polynomial of degree 20 in X. The roots of this polynomial reveal the 20 affine intersection points between ℓ_{10} and E. $P_1, \ldots P_{11}$ are 11 of these intersection points, so denote by $P'_1, \ldots, P'_9$ the other 9 intersection points, which might not be K-rational. Define the divisor D' as $D' = -\left(\sum_{i=1}^{9}(P'_i) - 9(\mathcal{O})\right)$. Since $(\ell_{10}) = \sum_{i=1}^{11}(P_i) + \sum_{i=1}^{9}(P'_i) - 20(\mathcal{O}) \in \mathrm{Prin}(E)$, D' is equivalent to D in $\mathrm{Pic}^0(E)$.

This process can repeated with a degree 8 polynomial interpolating the points in $\mathrm{supp}(D')$. This polynomial then has 16 affine intersection points with E. In each iteration the maximum number of divisors in the support decreases by two, so repeating the process often enough we will end up at divisor $\hat{D} = \sum_{i=1}^{3}(\hat{P}_i) - 3(\mathcal{O})$. The three affine points in the support of $\hat{D}$ can be interpolated by a quadratic polynomial $\hat{\ell}$, which gives one more affine intersection point with E. Call this point Q. We have $(\hat{\ell}) = \sum_{i=1}^{3}(\hat{P}_i) + (Q) - 4(\mathcal{O})$ and since $(\hat{\ell}) \in \mathrm{Prin}(E)$, also $(\hat{D}) \sim (\mathcal{O}) - (Q)$.

Now look at the vertical line ν running through Q. It has the divisor $(\nu) = (Q) + (R) - 2(\mathcal{O})$ for some $R \in E$. From this we can deduce that $(\mathcal{O}) - (Q) \sim (R) - (\mathcal{O})$, which gives $D \sim \hat{D} \sim (R) - (\mathcal{O})$.

4.3. Weil Reciprocity

The next theorem a useful tool for evaluating functions on an elliptic curve. It allows to evaluate a function when only the divisor is known but not the function itself.

Theorem 4.22 (Weil reciprocity)**.** *Let E be an elliptic curve and let f and g be non-zero functions on E. If (f) and (g) have disjoint supports, then*

$$f((g)) = g((f)).$$

Proof. For a proof we refer to [Gal05, Theorem IX.3]. □

Theorem 4.22 can also be used to evaluate a function at a divisor where the divisors are not distinct. Example 4.23 demonstrates a construction that uses this theorem to evaluate a function in this case.

Example 4.23. Let $P, S, R \in E(\overline{K})$ and set $T = -(R + S)$. We consider the line ℓ through R, S and T and the tangent $\ell' : Y = \lambda' X + \nu'$ to E at P. The divisors of these two lines are

$$(\ell) = (R) + (S) + (T) - 3(\mathcal{O}), \text{ and } (\ell') = 2(P) + (-2P) - 3(\mathcal{O}).$$

Suppose we want to compute $\ell((\ell'))$ which is not directly possible since the supports of (ℓ) and (ℓ') are not disjoint.

This problem can be circumvented by finding a divisor equivalent to (ℓ) whose support is disjoint to $\text{supp}((\ell'))$. This can be easily achieved by picking a random $U \notin \text{supp}((\ell'))$. Then define $D = (R + U) + (S + U) + (T + U) - 3(U)$. Observe that $(R+U)-(U) = (R)-(\mathcal{O})$, so $D \sim (\ell)$. We would now need to find a function whose divisor is D to compute $\ell((\ell'))$. However, by Theorem 4.22 it is possible to compute $\ell'(D)$ instead:

$$\ell'(D) = \frac{(y_{R'} - (\lambda' x_{R'} + \nu'))(y_{S'} - (\lambda' x_{S'} + \nu'))(y_{T'} - (\lambda' x_{T'} + \nu'))}{y_U - (\lambda' x_U + \nu')}$$

where $R + U = (x_{R'}, y_{R'})$, $S + U = (x_{S'}, y_{S'})$, $T + U = (x_{T'}, y_{T'})$ and $U = (x_U, y_U)$.

5. Bilinear Pairings

After introducing divisors and discussing their properties, we are now able to define and construct bilinear pairings. First we will look at the definition of bilinear pairings and discuss the their construction over elliptic curves. We then present Miller's algorithm that enables us to compute pairings efficiently.

This chapter is based on [Was08, HPS08, Ver08, BLS01, Gal05, Cos12, CCS06].

5.1. Bilinear Maps and Pairings

We first define what it means for a map to be bilinear. For that, let $(M, +)$ and $(R, \cdot)$ be Abelian groups. A map $\langle \cdot, \cdot \rangle : M \times M \to R$ is called *bilinear* if for all $x, y, z \in M$ the following two conditions are satisfied:

- $\langle x + y, z \rangle = \langle x, z \rangle \cdot \langle y, z \rangle$
- $\langle x, y + z \rangle = \langle x, y \rangle \cdot \langle x, z \rangle$

In other words, a bilinear map is a map that is linear in both its arguments. For our purposes, we will slightly relax the condition that the two arguments come from the same group. Instead we will require that the inputs come from cyclic groups of the same order which are therefore isomorphic. We will often write

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

which is the commonly used notation for bilinear pairings. The groups $\mathbb{G}_1$ and $\mathbb{G}_2$ will be defined in $E(\mathbb{F}_{q^k})$ and the target group $\mathbb{G}_T$ will be a subgroup of the multiplicative group $\mathbb{F}_{q^k}^{\times}$. So we usually write $\mathbb{G}_1$ and $\mathbb{G}_2$ additive and $\mathbb{G}_T$ multiplicative.

Example 5.1. Bilinear maps appear in many different areas of mathematics. Let $V = \mathbb{R}^n$ be the canonical n-dimensional $\mathbb{R}$-vector space. The scalar product on V

$$\langle \cdot, \cdot \rangle : \begin{cases} V \times V & \to \mathbb{R} \\ (x, y) & \mapsto \sum_{i=1}^{n} x_i y_i \end{cases}$$

is clearly a bilinear map.

A bilinear pairing is a bilinear map with two additional conditions. We require the map to be non-degenerate and efficiently computable:

Definition 5.2 (Bilinear pairing)**.** Let $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ be groups and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. The map e is called a *pairing* if

- e is bilinear.
- e is non-degenerate, that is there exist non-trivial $G_1 \in \mathbb{G}_1$ and $G_2 \in \mathbb{G}_1$ such that $e(G_1, G_2) \neq 1$.
- e is efficiently computable, i.e there exists a polynomial time algorithm to compute e.

We require pairings to be efficiently computable since otherwise they are only of theoretical interest. Bilinear pairings can be classified into different types which is based on the choice of $\mathbb{G}_1$ and $\mathbb{G}_2$:

Definition 5.3. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a bilinear pairing.

1. The pairing e is said to be of *Type 1* if $\mathbb{G}_1 = \mathbb{G}_2$.
2. The pairing e is said to be of *Type 2* if $\mathbb{G}_1 \neq \mathbb{G}_2$ and there exists an efficiently computable group isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$.
3. The pairing e is said to be of *Type 3* if $\mathbb{G}_1 \neq \mathbb{G}_2$ and no efficiently computable group isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ is known to exist.

Type 1 pairings are also referred to as *symmetric pairings* and Type 2 and Type 3 pairings are called *asymmetric pairings*. We now consider the case where both $\mathbb{G}_1$ and $\mathbb{G}_2$ are subgroups of an elliptic curve: let E be an elliptic curve over $\mathbb{F}_p$ and let $r \in \mathbb{N}$ be coprime to p. Remember that we denote by $\mathcal{G}_1 = E[r] \cap \ker(\pi - 1)$ the base-field subgroup and by $\mathcal{G}_2 = E[r] \cap \ker(\pi - p)$ the trace zero subgroup. Now let $\mathcal{P}_1 \in \mathcal{G}_1$ be a generator of $\mathcal{G}_1$ and $\mathcal{P}_2 \in \mathcal{G}_2$ be a generator of $\mathcal{G}_2$. Let k be the embedding degree of E with respect to r. The three pairing types can now be described in the following way:

- Type 1: In this case E is a supersingular curve and $\mathbb{G}_1 = \mathbb{G}_2 = \mathcal{G}_1$. We take $P_1 = P_2 = \mathcal{P}_1$ and there is a trivial group isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ mapping P_2 to P_1.
- Type 2: E is an ordinary elliptic curve and $\mathbb{G}_1$ is set to $\mathcal{G}_1$. Any order r subgroup of $E[r]$ that is neither $\mathcal{G}_1$ nor $\mathcal{G}_2$ is taken as $\mathbb{G}_2$. We set $P_1 = \mathcal{P}_1$ and $P_2 = \frac{1}{k}\mathcal{P}_1 + \mathcal{P}_2$. The trace map restricted to $\mathbb{G}_2$ gives an efficiently computable group isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ which maps P_2 to P_1.
- Type 3: E is again an ordinary elliptic curve and $\mathbb{G}_1 = \mathcal{G}_1$. In this case $\mathbb{G}_2 = \mathcal{G}_2$ and we set the generators to be $P_1 = \mathcal{P}_1$ and $P_2 = \mathcal{P}_2$.

In all three cases $\mathbb{G}_T$ is set to be the subgroup of order r of the finite field $\mathbb{F}_{p^k}$, the r-th roots of unity. There is also another variant of the Type 2 pairing, where $\mathbb{G}_2$ is taken to be the whole r-torsion $E[r]$.

For all three types we have that P_1 is a generator of $\mathbb{G}_1$ and P_2 is a fixed element of $\mathbb{G}_2$ of prime order r. Except for Type 3 pairings, we have a computable group isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ that maps P_2 to P_1. We refer to the three groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$, the elements P_1 and P_2 as well as the pairing e as pairing parameters.

5.2. Pairing-based Cryptography

For bilinear pairings to be useful in cryptographic applications, it is necessary to find hard problems based on pairings. Each problem that is presented here, is defined for a given set of pairing parameters.

So let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a bilinear pairings and let $P_1 \in \mathbb{G}_1$ and $P_2 \in \mathbb{G}_2$ generators for the respective groups. We denote their order by n. The first problem is defined for the symmetric setting.

Definition 5.4. Let e be a symmetric pairing. Given P_1, P_1^a, P_1^b and P_1^c for some $a, b, c \in \mathbb{Z}/n\mathbb{Z}$, the problem of finding $e(P_1, P_1)^{abc}$ is called *Bilinear Diffie-Hellman Problem (BDHP).*

Clearly, the BDHP can not be harder than the ECDHP. If one can find P_1^{abc} it is easy to compute $e(P_1, P_1)^{abc}$. For the asymmetric setting, the previous definition is not adequate. Instead we define two other problems for groups G_1 and G_2 both of order n.

Definition 5.5. Given $g_2, g_2^a \in G_2$ for some $a \in \mathbb{Z}/n\mathbb{Z}$, the problem of finding g_1^a for $g_1 \in G_1$ is called *Computational co-Diffie-Hellman Problem (co-CDHP).*

Clearly, if the DLP in G_2 is easy to solve, the co-CDHP is also easy.

Definition 5.6. Given $g_1, g_1^a \in G_1$ and $g_2, g_2^b \in G_2$ for $a, b \in \mathbb{Z}/n\mathbb{Z}$, deciding whether $a = b$ is called the *Decision co-Diffie-Hellman Problem (co-DDHP).*

Note that when using a bilinear pairing, the co-DDHP can be efficiently solved. For any instance of the problem, $a = b$ can be checked via $e(P_1, P_2^b) = e(P_1^a, P_2)$. This observations leads to the definition of *gap co-Diffie-Hellman group pairs*, which is a pair of groups where the co-DDHP is easy to solve, but the co-CDHP remains a hard problem. Bilinear pairings on elliptic curves are assumed to give rise to such gap co-Diffie-Hellman group pairs.

5.3. Weil, Tate and Ate Pairing

In this section we give the definitions for various pairings. We fix an elliptic curve E which is defined over a finite field $K = \mathbb{F}_q$ We also consider a fixed prime r such that $r \| \, |E(\mathbb{F}_q)|$ which is coprime to q and denote the embedding degree with respect to r by k, i.e. $r \mid q^k - 1$.

Definition 5.7. Let $P \in E(\overline{K})$, $s \in \mathbb{Z}$ and let $f_{s,P}$ be a function over E. If the divisor of $f_{s,P}$ satisfies

$$(f_{s,P}) = s(P) - (sP) - (s-1)\mathcal{O},$$

then $f_{s,P}$ is called a *Miller function.*

Miller functions are an essential tool to compute pairings. For the remainder of this section we denote by $f_{s,P}$ a Miller function. All pairings discussed in this section make use of Miller functions.

We will now take a look at some basic properties of Miller functions. The first important property is that Miller functions exist for every $P \in E(\overline{K})$ and $s \in \mathbb{Z}$. To see that, define the divisor $D = s(P) - (sP) - (s-1)\mathcal{O}$. Since $\deg D = 0$ and $sP - sP - (s-1)\mathcal{O} = \mathcal{O}$ the divisor D is principal by Theorem 4.13.

For $s = 0$ Miller functions are very simple. One can take $f_{0,P} = 1$ with $(f_{0,P}) = 0(P) - (0P) - (0-1)(\mathcal{O}) = 0$. If $P \in E[r]$, then the divisor of $f_{r,P}$ simplifies to $(f_{r,P}) = r(P) - r(\mathcal{O})$.

Before discussing a way to find Miller functions and evaluate them, we first look at bilinear pairings that use them.

5.3.1. Weil Pairing

The Weil pairing is a Type 1 pairing and was introduced by Weil in 1940 [Wei40]. It is based on the Miller function $f_{r,P}$ for a point $P \in E[r]$.

Definition 5.8. Let $P, Q \in E[r]$ and let D_P and D_Q be degree zero divisors with disjoint supports such that $D_P \sim (P) - (\mathcal{O})$ and $D_Q \sim (Q) - (\mathcal{O})$. Let $f \in K(E)$ and $g \in K(E)$ be such that $(f) = rD_P$ and $(g) = rD_Q$. The map

$$w_r : \begin{cases} E[r] \times E[r] & \to \mu_r(\mathbb{F}_{q^k}) \\ (P, Q) & \mapsto \frac{f(D_Q)}{g(D_P)} \end{cases}$$

is called *Weil pairing of order r*.

Note that the Weil pairing can not simply be defined as

$$\frac{f_{r,P}(D_Q)}{f_{r,Q}(D_P)}$$

because the divisors of $f_{r,P}$ and $f_{r,Q}$ have the divisors

$$(f_{r,P}) = r(P) - r(\mathcal{O}) \text{ and } (f_{r,Q}) = r(Q) - r(\mathcal{O}).$$

These two divisors correspond to the divisors $(P) - (\mathcal{O})$ and $(Q) - (\mathcal{O})$ which do not satisfy the requirement that D_P and D_Q have disjoint supports.

However, the definition of the Weil pairing of $P, Q \in E[r]$ can easily be described in terms of a third point $S \in E$ satisfying $S \notin \{\mathcal{O}, P, -Q, P - Q\}$. To see that, let f_P and f_Q be the Miller functions $f_{r,P}$ respectively $f_{r,Q}$. They have divisors $(f_P) = r(P) - r(\mathcal{O})$ and $(f_Q) = r(Q) - r(\mathcal{O})$. From these two functions we now obtain functions f and g on E with divisors equivalent to $r(P) - r(\mathcal{O})$ respectively $r(Q) - r(\mathcal{O})$ easily. For a point R we set

$$f(R) = f_P(R + S), \text{ and } g(R) = f_Q(R - S).$$

The functions f and g satisfy the properties from the definition and so we can compute $w_r(P,Q)$ as

$$w_r(P,Q) = \frac{f((Q)-(\mathcal{O}))}{g((P)-(\mathcal{O}))} = \frac{\frac{f(Q)}{f(\mathcal{O})}}{\frac{g(P)}{g(\mathcal{O})}} = \frac{\frac{f_P(Q+S)}{f_P(S)}}{\frac{f_Q(P-S)}{f_Q(-S)}}.$$

Theorem 5.9. *The map w_r is a bilinear pairing. In addition, w_r is alternating, which means that*

$$w_r(P,P) = 1 \textit{ for all } P \in E[r].$$

Proof. For a proof see [Was08, Theorem 11.7]. □

Example 5.10. We consider the elliptic curve $E : Y^2 = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ defined over a field K with $\alpha_1+\alpha_2+\alpha_3 = 0$. The thread points

$$P_1 = (\alpha_1, 0), P_2 = (\alpha_2, 0), P_3 = (\alpha_3, 0)$$

have all order 2. We now compute $w_2(P_1, P_2)$ directly.

To compute the pairing, we pick an arbitrary point $S = (x,y) \in E$. From the addition formula we are able to compute the x-coordinate of $P_1 - S$ and can observe that is equal to

$$\begin{aligned}\left(\frac{-y}{x-\alpha_1}\right)^2 - x - \alpha_1 &= \frac{y^2 - (x-\alpha_1)^2(x+\alpha_1)}{(x-\alpha_1)^2} \\ &= \frac{(x-\alpha_1)(x-\alpha_2)(x-\alpha_3) - (x-\alpha_1)^2(x+\alpha_1)}{(x-\alpha_1)^2} \\ &= \frac{(x-\alpha_2)(x-\alpha_3) - (x-\alpha_1)(x+\alpha_1)}{x-\alpha_1} \\ &= \frac{(-\alpha_2-\alpha_3)x + \alpha_2\alpha_3 + \alpha_1^2}{x-\alpha_1} \\ &= \frac{\alpha_1 x + \alpha_2\alpha_3 + \alpha_1^2}{x-\alpha_1}\end{aligned}$$

by applying the equations $\alpha_1+\alpha_2+\alpha_3 = 0$ and $y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$. Similarly the x-coordinate of $P_2 - S$ can be written as

$$\frac{\alpha_2 x + \alpha_1\alpha_3 + \alpha_2^2}{x-\alpha_1}.$$

Note that the rational functions $f_{P_i} = X - \alpha_1$ have the divisors $(f_{P_i}) = 2(P_i) - 2(\mathcal{O})$, so we can compute the pairing using f_{P_1} and f_{P_2}. Now assuming that P_1 and P_2 are two distinct points, we can compute $w_2(P_1, P_2)$ directly from the definition:

$$\begin{aligned} w_2(P_1, P_2) &= \frac{\frac{f_{P_1}(P_2+S)}{f_{P_1}(S)}}{\frac{f_{P_2}(P_1-S)}{f_{P_2}(-S)}} = \frac{f_{P_1}(P_2+S)f_{P_2}(-S)}{f_{P_1}(S)f_{P_2}(P_1-S)} \\ &= \frac{\left(\frac{\alpha_1 x+\alpha_2\alpha_3+\alpha_1^2}{x-\alpha_1} - \alpha_1\right)(x-\alpha_2)}{\left(\frac{\alpha_2 x+\alpha_1\alpha_3+\alpha_2^2}{x-\alpha_1} - \alpha_2\right)(x-\alpha_1)} \\ &= \frac{(\alpha_2-\alpha_1)x+\alpha_1\alpha_3+\alpha_2^2+\alpha_1\alpha_2}{(\alpha_1-\alpha_2)x+\alpha_2\alpha_3+\alpha_1^2+\alpha_1\alpha_2} \\ &= \frac{(\alpha_2-\alpha_1)x+\alpha_2^2-\alpha_1^2\alpha_2}{(\alpha_1-\alpha_2)x+\alpha_1^2-\alpha_2^2\alpha_2} = -1. \end{aligned}$$

If one wants to evaluate the Weil pairing at two points $P_1 = aP$ and $P_2 = bP_2$, the alternating nature of the Weil pairing ensures that $w_r(P_1, P_2) = 1$. This renders the Weil pairing unusable for applications where points of this kind occur as inputs. However, if the elliptic curve is chosen in such a way that distortion map exist, this problem can be circumvented.

Definition 5.11 (Distortion map)**.** Let E be an elliptic curve defined over K, $r \in \mathbb{P}$ and $P \in E[r]$ be a point of order r. A map $\phi : E(\overline{K}) \to E(\overline{K})$ satisfying

1. $\phi(nP) = n\phi(P)$ for all $n \in \mathbb{N}$, and
2. $w_r(P, \phi(P))$ is primitive r-th root of unity

is called *r-distortion map for P*.

The modified Weil pairing uses a distortion map to ensure that the pairing is not alternating. It is defined in the following way:

Definition 5.12 (Modified Weil pairing)**.** Let E be an elliptic curve defined over K, $r \in \mathbb{P}$, $P \in E[r]$ be a point of order r and $\phi : E(\overline{K}) \to E(\overline{K})$ be a distortion map for P. The *modified Weil pairing of order* r, $\hat{w}_r$, is defined as

$$\hat{w}_r : \begin{cases} E[r] \times E[r] & \to \mu_r \\ (Q, Q') & \mapsto w_r(Q, \phi(Q')) \end{cases}.$$

This map is again a pairing. It additionally satisfies the property that $\hat{w}_r(Q, Q') = 1$ if and only if $Q = \mathcal{O}$ or $Q' = \mathcal{O}$ [HPS08, Proposition 5.50]. The next proposition shows that distortion maps exist and gives an explicit map for a class of elliptic curves.

Proposition 5.13. *Let K be field with an element $\alpha \in K$ such that $\alpha^2 = -1$. Let $E : Y^2 = X^3 + X$ be an elliptic curve defined over K. Then the map*

$$\phi : \begin{cases} E(\overline{K}) & \to E(\overline{K}) \\ (x, y) & \mapsto (-x, \alpha y) \\ \mathcal{O} & \mapsto \mathcal{O} \end{cases}$$

is a distortion map.

Proof. For a proof we refer to [HPS08, Proposition 5.51, Proposition 5.52]. □

5.3.2. Tate Pairing

The Tate pairing was first introduced by Tate [Tat58, Tat63] and later extended by Lichtenbaum [Lic69]. Frey and Rück later gave the first application of the Tate pairing over finite fields in cryptography [FR94]. We will start with a more general definition of the Tate pairing and then derive a bilinear pairing in the Type 3 setting.

The first definition of the Tate pairing only requires the first argument to be in the r-torsion. The second argument can be any point in $E(\mathbb{F}_{q^k})$. However, any part of the second argument that lies in the r-torsion does not affect value of the pairing, hence the second argument is taken from the quotient group

$$E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}).$$

If h is the cofactor, that is $h = \frac{E(\mathbb{F}_{q^k})}{r^2}$, then the coset $rE(\mathbb{F}_{q^k})$ consists of exactly h points. So the quotient group $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ contains exactly r^2 elements. The target group of the pairing is also a quotient group:

$$\mathbb{F}_{q^k}^{\times}/(\mathbb{F}_{q^k}^{\times})^r$$

where $(\mathbb{F}_{q^k}^{\times})^r$ is the subgroup of $\mathbb{F}_{q^k}^{\times}$ defined as:

$$(\mathbb{F}_{q^k}^{\times})^r = \{u^r \mid u \in \mathbb{F}_{q^k}\}.$$

Definition 5.14 (Tate pairing)**.** Let $P \in E(\mathbb{F}_{q^k}[r])$ and $Q' \in E(\mathbb{F}_{q^k})/E(\mathbb{F}_{q^k})$. Let $Q \in E(\mathbb{F}_{q^k})$ be a representative of Q' and $D_Q \in \mathrm{Div}^0(E)$ be a divisor equivalent to $(Q) - (\mathcal{O})$ with disjoint support to $(f_{r,P})$. The *Tate pairing* is defined as

$$T_r : \begin{cases} E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) & \to \mathbb{F}_{q^k}^{\times}/(\mathbb{F}_{q^k}^{\times})^r \\ (P, Q') & \mapsto f_{r,P}(D_Q) \end{cases}.$$

This map is well-defined and a bilinear pairing as Theorem 5.15 shows. Example 5.16 demonstrates the computation of the Tate pairing.

Theorem 5.15. *The map T_r is well-defined and a bilinear pairing.*

Proof. For a proof we refer to [Was08, Theorem 11.8]. □

Example 5.16. Let $q = 5$. We consider the elliptic curve $E : Y^2 = X^3 - 3$ defined over $\mathbb{F}_q$. This curve has 6 $\mathbb{F}_q$-rational points. We take $r = 3$ and find that the embedding degree with respect to r is $k = 2$. We can construct $\mathbb{F}_{q^2}$ as $\mathbb{F}_q(i)$ with $i^2 + 2 = 0$.

We consider $P = (3, 2)$ and $Q = (i + 1, 4i + 2)$ and want to compute the Tate pairing for P and Q (respectively the coset $Q' = Q + rE(\mathbb{F}_{q^2})$). The function $f : Y^2 + 2X + 2 = 0$ on E has the divisor $3(P) - 3(\mathcal{O})$, so is a Miller function of the correct type. We need a divisor $D_Q \sim (Q) - (\mathcal{O})$. For that we take $R = (2i, i + 2)$

and set $D_Q = (Q+R)-(R)$, where $Q+R = (3i+1, 2)$. We are now able to compute the Tate pairing as

$$T_r(P, Q') = f(D_Q) = \frac{f(Q+R)}{f(R)} = \frac{2+2(3i+1)+2}{(i+2)+4i+2} = 4i+4.$$

To illustrate the bilinearity and the fact that the value is only unique up to a coset, we also compute $T_r(P, 2Q)$ and $T_r(2P, Q)$. For the first one we take $D_{2Q} = (2Q+R)-(R)$ with $2Q+R = (i+2, i)$ and we obtain:

$$T_r(P, 2Q) = f(D_{2Q}) = \frac{i+2(i+2)+2}{(i+2)+4i+2} = 2i+4.$$

For the second value we need to find a new Miller function. We can take f' : $Y + 3X + 3 = 0$ which has the divisor $(f') = r(2P) - r(\mathcal{O})$. The Tate pairing can now be computes as

$$T_r(2P, Q) = f(D_Q) = \frac{2+3(3i+1)+3}{(i+2+6i+3} = 3i+2.$$

Now note that when considering the pairing values in $\mathbb{F}_{q^k}$, we have $T_r(P, 2Q) = 2i+4 = (4i+4)^2 = T_r(P, Q)^2$, but $T_r(2P, Q) \neq T_r(P, Q)^2$. However, if we look at them modulo the r-th powers, we have $T_r(P, 2) = T_r(2P, Q) = T_r(P, Q)^2$ since

$$\frac{T_r(P, 2Q)}{T_r(2P, Q)} \in (\mathbb{F}_{q^k}^{\times})^r.$$

That the value of the Tate pairing is only unique up to an r-th root is an undesirable property in cryptographic applications. Checking that two values of the Tate pairing are contained in the same equivalence class requires checking if their quotient is an r-th root which is much more work than simply comparing two elements of $\mathbb{F}_{q^k}$. With a small modification, this problem can be easily circumvented. Raising the values to the power of $\frac{|\mathbb{F}_{q^k}-1|}{r}$ kills r-th powers and sends them to an unique r-th root of unity of $\mathbb{F}_{q^k}$. This observation leads to the definition of the reduced Tate pairing:

Definition 5.17 (Reduced Tate pairing)**.** Let $P \in E(\mathbb{F}_{q^k})[r]$, $Q' \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ and $Q \in E(\mathbb{F}_{q^k})$ be a representative of Q'. Let $D_Q \in \mathrm{Div}^0(E)$ be a divisor equivalent to $(Q)-(\mathcal{O})$ with disjoint support to $(f_{r,P})$. The *reduced Tate pairing* is defined as

$$t_r : \begin{cases} E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) & \to \mu_r(\mathbb{F}_{q^k}) \\ (P, Q) & \mapsto f_{r,P}(D)^{\frac{q^k-1}{r}} \end{cases}.$$

We will now transform the reduced Tate pairing into a Type 3 pairing. Note that $r \| E(\mathbb{F}_{q^k})$ implies that $E(\mathbb{F}_{q^k})[r] \cap rE(\mathbb{F}_{q^k}) = \{\mathcal{O}\}$. This means that every element of r-torsion represents a unique coset in $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ and we can thus simply represent $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ by $E(\mathbb{F}_{q^k})[r]$. So we can view the reduced Tate pairing as a map

$$t_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r] \to \mu_r(\mathbb{F}_{q^k}).$$

We can go a step further and restrict the map to $\mathcal{G}_1 \times \mathcal{G}_2$:

$$t_r : \mathcal{G}_1 \times \mathcal{G}_2 \to \mu_r(\mathbb{F}_{q^k}).$$

This restriction does not reduce the image set and it is still possible to reach any r-th root of unity. Indeed, take a non-zero $P \in \mathcal{G}_1$ and $Q \in \mathcal{G}_2$. Then $t_r(P, Q')$ will reach every value in $\mu_r(\mathbb{F}_{q^k})$ when Q' runs through $\langle Q \rangle$, a group of order r.

Example 5.18 demonstrates the difference between the Tate pairing and the reduced Tate pairing.

Example 5.18. We take $q = 19$ and let $E : Y^2 = X^3 + 14X + 3$ be defined over $\mathbb{F}_q$. We have $|E(\mathbb{F}_q)| = 20$ and we take $r = 5$. The embedding degree with respect to r is $k = 2$ and we use $\mathbb{F}_{q^2} = \mathbb{F}_q(i)$ with $i^2 + 1 = 0$.

We consider $P = (17, 9) \in \mathbb{G}_1$ and $Q = (16, 16i) \in \mathbb{G}_2$. The Tate pairing of P and Q is $T_r(P, Q) = 7i + 3$ and the reduced Tate pairing is $t_r(P, Q) = 15i + 2$. We will now look at multiple ways to obtain $T_r(P, Q)^4$ respectively $t_r(P, Q)^4$ to see the effect of the final exponentiation:

- $T_r(P, Q)^4 = 3i + 7$ whereas $t_r(P, Q)^4 = 4i + 2$.
- $T_r(4P, Q) = 7i + 16$ whereas $t_r(4P, Q) = 4i + 2$.
- $T_r(P, 4Q) = 12i + 3$ whereas $t_r(P, 4Q) = 4i + 2$.
- $T_r(2P, 2Q) = 2i + 14$ whereas $t_r(2P, 2Q) = 4i + 2$.

Of course, the values obtained from T_r are all equivalent modulo r-th powers. The final exponentiation maps them to the same unique value in $\mu_r(\mathbb{F}_{q^k})$.

From now on we will always refer to the reduced Tate pairing in the Type 3 setting when talking about the Tate pairing.

5.3.3. Ate Pairing

The Ate pairing is a variant Tate pairing that exchanges the role of its arguments and uses properties from $\mathbb{G}_2$ to reduce the involved orders of the Miller functions. It was first introduced by Hess, Smart and Vercauteren [HSV06]. We will show how to derive the Ate pairing from the Tate pairing.

We need the following Lemma to derive the Ate pairing:

Lemma 5.19. *Let E be an elliptic curve defined over K. Let $Q \in E(\overline{K})$ and $a, b \in \mathbb{Z}$. Then we can obtain a Miller function $f_{ab,Q}$ as*

$$f_{ab,Q} = f_{a,Q}^b f_{b,aQ}.$$

Now we consider the order r Tate pairing where we swap the role of $P \in \mathcal{G}_1$ and $Q \in \mathcal{G}_2$ and raise it to some power m:

$$\left(f_{r,Q}(P)^{\frac{q^k-1}{r}}\right)^m = f_{r,Q}(P)^{\frac{m(q^k-1)}{r}} = \frac{f_{mr,Q}(P)^{\frac{q^k-1}{r}}}{f_{m,rQ}(P)^{\frac{q^k-1}{r}}} = f_{mr,Q}(P)^{\frac{q^k-1}{r}} \tag{5.1}$$

where the last two equalities follow from Lemma 5.19 and $rQ = \mathcal{O}$. Since the Tate pairing is a bilinear pairing,

$$f_{mr,Q}(P)^{\frac{q^k-1}{r}}$$

also gives rise to bilinear pairing for any $m \in \mathbb{Z}$ with $r \nmid m$.

The idea of the Ate pairing and its variants is to find suitable m such that the evaluation of $f_{mr,Q}(P)$ can be written as power of the evaluation of a simpler function $f_{\lambda,Q}(P)$. We can achieve this by exploiting the fact that the Frobenius endomorphism acts as multiplication by q on $\mathcal{G}_2$ and leaves $\mathcal{G}_1$ invariant. Also note that multiplication by q on $\mathcal{G}_2$ is the same as multiplication by λ if $\lambda \equiv q \mod r$.

So let $\lambda \in \mathbb{N}$ such that $\lambda \equiv q \mod r$. From $r \mid (q^k - 1)$ we also have that $r \mid (\lambda^k - 1)$. Now we define

$$m = \frac{\lambda^k - 1}{r}.$$

By Equation 5.1 we have

$$f_{mr,Q}(P)^{\frac{q^k-1}{r}} = f_{\lambda^k-1,Q}(P)^{\frac{q^k-1}{r}} = f_{\lambda^k,Q}(P)^{\frac{q^k-1}{r}}.$$

From repeatedly applying Lemma 5.19 and using the equality $\lambda^i Q = q^i Q$ for all $i \in \mathbb{N}$ we obtain

$$f_{\lambda^k,Q} = \prod_{i=0}^{k-1} f_{\lambda,q^iQ}^{\lambda^{k-1-i}}.$$

Next we exploit the action of the Frobenius endomorphism on both $\mathcal{G}_1$ and $\mathcal{G}_2$ and obtain

$$f_{\lambda^k,Q}(P) = f_{\lambda,Q}(P)^{\sum_{i=0}^{k-1} \lambda^{k-1-i} q^i}.$$

We are now able to define the Ate pairing:

Definition 5.20. Let $\lambda \equiv q \mod r$ and $m = \frac{\lambda^k-1}{r}$. The *(reduced) Ate pairing* is defined as

$$a_\lambda : \begin{cases} \mathcal{G}_1 \times \mathcal{G}_2 & \to \mu_r \\ (P, Q) & \mapsto f_{\lambda,Q}(P)^{\frac{q^k-1}{r}} \end{cases}.$$

Since a_λ corresponds to a fixed power of the Tate pairing, the Ate pairing is again a bilinear pairing:

Theorem 5.21. *If $r \nmid m$, then a_λ is a bilinear pairing.*

Proof. This result follows directly from Theorem 5.15. □

5.4. Miller's Algorithm

Miller's algorithm allows us to compute Miller functions efficiently. The algorithm was first described by Miller in 1986 [Mil86a]. Before looking at Miller's idea, we investigate the naive approach to compute Miller functions and see why this approach is infeasible. Let $m, n \in \mathbb{Z}$ and $P \in E[r]$. We denote by $\ell_{mP,nP}$ the equation of the line through mP and nP respectively the tangent at mP if $mP = nP$ and by $\nu_{(m+n)P}$ the equation of the vertical line through $(m+n)P$. Then the divisor of $f_{m+n,P}$ satisfies the equation

$$(f_{m+n,P}) = (f_{m,P}) + (f_{n,P}) + (\ell_{mP,nP}) - (\nu_{(m+n)P}).$$

By setting $n = 1$ the equation becomes

$$\begin{aligned}(f_{m+1,P}) &= (f_{m,P}) + (f_{1,P}) + (\ell_{mP,P}) - (\nu_{(m+1)P})\\ &= (f_{m,P}) + (\ell_{mP,P}) - (\nu_{(m+1)P}).\end{aligned}$$

From this equation we are able to construct a Miller function $f_{r,P}$ from any $f_{2,P}$ iteratively by setting

$$f_{m+1,P} = f_{m,P}\frac{\ell_{mP,P}}{\nu_{(m+1)P}}$$

for $3 \leq m < r$. Note that for the last step when $m = r - 1$ we have

$$(f_{r,P}) = r(P) - r(\mathcal{O}) \text{ and } (f_{r-1,P}) = (r-1)(P) - ((r-1)P) - (r-1)(\mathcal{O}).$$

Hence the required divisor is $(P) + ((r-1)P) - 2(\mathcal{O})$ which corresponds to the multiplication by the vertical line $\nu_{(r-1)P} = \nu_{-P} = \nu_P$. This is the same vertical line that appears on the denominator of $\frac{\ell_{(r-2)P,P}}{\nu_{(r-1)P}}$ and thus the function $f_{r,P}$ can be computed as the product

$$f_{r,P} = \ell_{(r-2)P,P}\prod_{i=1}^{r-3}\frac{\ell_{iP,P}}{\nu_{(i+1)P}}.$$

As it can be seen from this product, evaluating $f_{r,P}$ with this method requires to evaluate $\ell_{iP,P}$ and $\nu_{(i+1)P}$. However, the amount of functions that need to be evaluated is linear in r. So for exponentially large r, the naive method has exponential time complexity. This makes the naive method unusable for large r that we usually have.

Miller constructed $f_{r,P}$ differently using a double-and-add like approach to reduce the complexity. Instead of adding one zero and one pole via multiplying $f_{m,P}$ by linear functions, it is possible to double the number of zeros at P and the number of poles at $\mathcal{O}$ by squaring $f_{m,P}$. Note that

$$(f_{m,P}^2) = 2(f_{m,P}) = 2m(P) - 2(mP) - 2(m-1)(\mathcal{O}).$$

This divisor is almost the same as the divisor of $f_{2m,P}$ which is

$$(f_{2m,P}) = 2m(P) - (2mP) - (2m-1)(\mathcal{O}).$$

The difference between the two divisors $(f_{2m,P})$ and $(f_{m,P}^2)$ is

$$(f_{2m,P}) - (f_{m,P}^2) = 2(mP) - (2mP) - (\mathcal{O}).$$

So to advance from $f_{m,P}^2$ to $f_{2m,P}$ we need to find a function with two zeros at mP and a pole at $2mP$ as well as $\mathcal{O}$. The divisor of the quotient $\frac{\ell_{mP,mP}}{\nu_{2mP}}$ has exactly this form. Hence it is possible to advance from $f_{m,P}$ to $f_{2m,P}$ by setting

$$f_{2m,P} = f_{m,P}^2 \frac{\ell_{mP,mP}}{\nu_{mP}}.$$

We are now able to advance from any m to $f_{(m+1)P,P}$ or $f_{2m,P}$ quickly which gives rise to a double-and-add style algorithm. It is thus possible to reach $f_{r,P}$ in $\mathcal{O}(\log(r))$ steps.

Note that the degree of $f_{m,P}$ still grows linear in the size of m. So as m approaches r the function $f_{m,P}$ becomes too large to store explicitly. Thus Miller's algorithm does not store $f_{m,P}$ at every stage but evaluates $f_{m,P}$ at the given divisor D, $f_{m,P}(D) \in \mathbb{F}_{p^k}$. Algorithm 3 lists the full algorithm to evaluate $f_{r,P}$ at D_Q.

Algorithm 3 Miller's algorithm to evaluate $f_{r,P}$

```
Input: $P \in E(\mathbb{F}_{q^k})[r], D_Q \sim (Q) - (\mathcal{O})$ with support disjoint from $(f_{r,P})$ and $r = (r_{n-1}, \ldots, r_0)_2$ with $r_{n-1} = 1$.
Output: $f_{r,P}(D_Q)$
  $R \leftarrow P$.
  $f \leftarrow 1$.
  for $i = n-2, \ldots, 0$ do
      Compute the line functions $\ell_{R,R}$ and $\nu_{2R}$.
      $R \leftarrow 2R$.
      $f \leftarrow f^2 \frac{\ell_{R,R}}{\nu_{2R}}(D_Q)$.
      if $r_i = 1$ then
          Compute the line functions $\ell_{R,P}$ and $\nu_{R+P}$.
          $R \leftarrow R + P$.
          $f \leftarrow f \frac{\ell_{R,P}}{\nu_{R+P}}(D_Q)$.
      end if
  end for
  return $f$
```

Example 5.22. We use Miller's algorithm to compute the reduced Tate pairing. Let $E : Y^2 = X^3 + 21X + 15$ be defined over $\mathbb{F}_{47}$. The elliptic curve E consists of 51 $\mathbb{F}_{47}$-rational points. We take $r = 17$ and the embedding degree with respect to r is $k = 4$, so we take $\mathbb{F}_{47^4} = \mathbb{F}_{47}$ with $u^4 - 4u^2 + 5 = 0$.

A point of order 17 is $P = (45, 23)$. It is contained in $\mathbb{G}_1$. A point in $\mathbb{G}_2$ is given by $Q = (31u^2 + 29, 35u^3 + 11u)$. We now illustrate Miller's algorithm to compute $f_{r,P}(D_Q)$. Take $D_Q = (2Q) - (Q)$ which has disjoint support to $(f_{r,P})$ and is equivalent to $(Q) - (\mathcal{O})$. The following table shows the steps of Miller's algorithm and the immediate values.

i	r_i	R	update $\frac{\ell}{\nu}$	update at Q	f
		$(45, 23)$			1
3	0	$(12, 16)$	$\frac{y+33x+43}{x+35}$	$41u^3 + 32u^2 + 2u + 21$	$41u^3 + 32u^2 + 2u + 21$
2	0	$(27, 14)$	$\frac{y+2x+7}{x+20}$	$4u^3 + 5u^2 + 28u + 17$	$22u^3 + 27u^2 + 30u + 33$
1	0	$(18, 31)$	$\frac{y+42x+27}{x+29}$	$6u^3 + 13u^2 + 33u + 28$	$36u^3 + 2u^2 + 21u + 37$
0	1	$(45, 24)$	$\frac{y+9x+42}{x+2}$	$46u^3 + 45u^2 + u + 20$	$10u^3 + 21u^2 + 40u + 25$
		$\mathcal{O}$	$x + 2$	$6u^2 + 43$	$17u^3 + 6u^2 + 10u + 22$

So $f_{r,P}(D_Q) = 17u^3 + 6u^2 + 10u + 22$. To compute the reduced Tate pairing of P and Q this value now needs to be raised to $\frac{47^k-1}{r}$:

$$t_r(P, Q) = f_{r,P}(D_Q)^{\frac{47^k-1}{r}} = (17u^3 + 6u^2 + 10u + 22)^{287040} = 33u^3 + 43u^2 + 45u + 39$$

5.5. Optimal Pairings

Early optimizations of bilinear pairings focused on reducing the number of iterations in Miller's algorithm. We now discuss optimal pairings that reduce the number of iterations to a minimum.

Definition 5.23. Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a bilinear pairing with $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| = r$ where $\mathbb{G}_T$ is a subgroup of $\mathbb{F}_{q^k}^{\times}$. If e can be computed in

$$\frac{\log_2 r}{\phi(k)} + \epsilon(k) \text{ basic Miller iterations}$$

where $\epsilon(k) \leq \log_2 k$, then e is called *optimal pairing.*

This definition does not specify that the pairing e should be computed as the evaluation of one Miller function, but also allows combinations of Miller functions as long as all of them can be computed in $\frac{\log_2 r}{\phi(k)} + \epsilon(k)$ Miller iterations. The central idea for loop reduction in Miller's algorithm is to exploit efficiently computable endomorphisms such as powers of the Frobenius endomorphism. This can be achieved by decomposing a multiple of r as sum of these endomorphisms. The bound is the best one that is obtainable by using powers of the Frobenius endomorphism. Vercauteren also conjectured that if powers of the Frobenius endomorphism are the only efficiently computable endomorphisms on an elliptic curve, then the best possible lower bound for the number of basic Miller iterations is $(1 - \epsilon)\frac{\log_2 r}{\phi(k)}$ for some $0 < \epsilon < \frac{1}{4}$:

Conjecture (Optimality Conjecture)**.** *A bilinear pairing on an elliptic curve without efficiently computable endomorphisms different from powers of the Frobenius endomorphism requires at least*

$$(1-\epsilon)\frac{\log_2 r}{\phi(k)}$$

basic Miller iterations for some $0 < \epsilon < \frac{1}{4}$.

Optimal Ate pairings can be constructed by repeatedly applying Equation 5.1 for a $\lambda = mr$ that has a q-adic expansion $\lambda = \sum_{i=0}^{n} c_i q^i$ with small coefficients. Theorem 5.24 shows the that the maps obtained in that way are pairings.

Theorem 5.24. *Let* $\lambda = mr$ *with* $r \nmid m$ *and* $\lambda = \sum_{i=0}^{n} c_i q^i$. *If*

$$mkq^{k-1} \not\equiv \frac{q^k-1}{r} \sum_{i=0}^{n} ic_i q^{i-1} \mod r,$$

then the map

$$a_{[c_0,\ldots,c_n]} : \begin{cases} \mathcal{G}_1 \times \mathcal{G}_2 & \to \mu_r \\ (P,Q) & \mapsto \left(\prod_{i=0}^{n} f_{c_i,Q}^{q^i}(P) \prod_{i=0}^{n-1} \frac{\ell_{s_{i+1}Q, c_i q^i Q}(P)}{\nu_{s_i Q}(P)} \right)^{\frac{q^k-1}{r}} \end{cases}$$

with $s_i = \sum_{j=i}^{n} c_j q^j$ *defines a bilinear pairing.*

Proof. We refer to [Ver08, Theorem 1] for a proof. □

Note that in the computation of the line functions $\ell_{s_{i+1}Q, c_i q^i Q}(P)$ it is possible to replace all multiplications of Q by q^i with a power of the Frobenius endomorphism, i.e. $q^i Q = \pi_q^i(Q)$.

5.6. Building Type 2 from Type 3 Pairings

While we have seen multiple examples of Type 3 pairings and one Type 1 pairing, we have not discussed any Type 2 pairings so. Fortunately, Type 2 pairings can easily be constructed from a Type 3 pairings [KP05, CM09].

Let E be an elliptic curve defined over $\mathbb{F}_q$ and $e_3 : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a Type 3 pairing defined over E with order r. Let k be the embedding degree of E with respect to r. If we take any point $P_2' \in E[r]$ such that $P_2' \notin \mathbb{G}_1$ and $P_2' \notin \mathbb{G}_2$, then the group $\mathbb{G}_2' = \langle P_2' \rangle$ is a subgroup of $E(\mathbb{F}_{q^k})$ of order r. Since $\mathbb{G}_2' \neq \mathbb{G}_2$, we know from Proposition 3.18 that the trace map Tr acts non-trivially on $\mathbb{G}_2'$ and thus induces an efficiently-computable isomorphism from $\mathbb{G}_2'$ to $\mathbb{G}_1$. So any bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2' \to \mathbb{G}_T$ is a Type 2 pairing.

The following lemma ensures that we can build a Type 2 pairing from e_3:

Lemma 5.25. *The map*

$$e_2 : \begin{cases} \mathbb{G}_1 \times \mathbb{G}_2' & \to \mathbb{G}_T \\ (P, Q) & \mapsto e_3(P, Q - \pi_q^{k/2}(Q)) \end{cases}$$

is a bilinear pairing.

Proof. For a proof we refer to [CM09, Lemma 1]. □

Now define the points $P_1 = \frac{1}{k}\operatorname{Tr}(P_2')$ and $P_2 = \frac{1}{c}(P_2' - P_1)$ for some $c \in \mathbb{Z}/r\mathbb{Z}^\times$. Then the maps

$$\psi : \begin{cases} \mathbb{G}_2' & \to \mathbb{G}_1 \\ Q & \mapsto \frac{1}{k}\operatorname{Tr}(Q) \end{cases} \text{ and } \rho : \begin{cases} \mathbb{G}_2' & \to \mathbb{G}_2 \\ Q & \mapsto Q - \psi(Q) \end{cases}$$

are efficiently computable isomorphism with $\psi(P_2') = P_1$ and $\rho(P_2') = cP_2$. Using these two isomorphisms we can now represent each point $Q \in \mathbb{G}_2'$ by two unique points $Q_1 \in \mathbb{G}_1$ and $\mathbb{G}_2$ such that $Q = Q_1 + Q_2$ by setting $Q_1 = \psi(Q)$ and $Q_2 = \rho(Q)$. So we obtain a subgroup $\mathbb{G}_2'' \subset \mathbb{G}_1 \times \mathbb{G}_2$ that is isomorphic to $\mathbb{G}_2'$. The isomorphism between $\mathbb{G}_2'$ and $\mathbb{G}_2''$ is induced by $Q \mapsto (\psi(Q), \rho(Q))$.

Recall from Section 3.6 that if E has a degree-d twist E', $\mathbb{G}_2$ is isomorphic to $E'(\mathbb{F}_{q^{k/d}})[r]$. While this isomorphism allows points in $\mathbb{G}_2$ to be represented using coordinates from $\mathbb{F}_{q^{k/d}}$ instead of $\mathbb{F}_{q^k}$, we can also use it to represent points in $\mathbb{G}_2'$ using only coordinates from $\mathbb{F}_q$ and $\mathbb{F}_{q^{k/d}}$. This representation is stiller larger than the one obtained for $\mathbb{G}_2$, but is far better than using $\mathbb{F}_{q^k}$ coordinates. Similarly, the cost of the arithmetic in $\mathbb{G}_2'$ can be reduced, but is not as efficient as in $\mathbb{G}_2$.

5.7. Application of Bilinear Pairings

Since the publication of a one-round Diffie-Hellman protocol involving three parties by Joux in 2000 [Jou00], the use of pairings in cryptography has developed at an extraordinary pace. For example, bilinear pairings have been used in in identity-based encryption schemes [BF01], blind signature schemes [Bol03, FHS15], group signature schemes [BBS04] and structure-preserving signatures [AFG+10]. We will present two applications of pairings:

1. the MOV algorithm to reduce the ECDLP to a DLP in a multiplicative subgroup of a finite field, and

2. the BLS signature scheme.

5.7.1. MOV Algorithm

One of the applications of the Weil pairing is to mount an attack on the ECDLP on supersingular curves. The attack was first published by Menezes, Okamato and Vanstone [MVO91] in 1991 and is named MOV after its authors. It was the first cryptographic application of a bilinear pairing. In this attack, the Weil pairing is used to convert the discrete logarithm problem in $E(\mathbb{F}_q)$ to one in $\mathbb{F}_{q^k}^\times$. As long as the field $\mathbb{F}_{q^k}^\times$ is not much larger than $\mathbb{F}_q$, i.e. the embedding degree k is small, the DLP in $\mathbb{F}_{q^k}^\times$ can be solved much faster than the ECDLP in $E(\mathbb{F}_q)$. For supersingular curves defined over fields prime characteristic the embedding degree is usually 1 or 2.

Let E be a supersingular curve defined over $\mathbb{F}_q$. We take a point $P \in E[r]$ of prime order $r \geq 3$. We assume that r and q are coprime. Let $Q \in E[r]$ be a point that is contained in the subgroup generated by P. Recall that if k is the embedding degree with respect to r, then $P, Q \in E(\mathbb{F}_{q^k})$.

We assume that $Q = aP$. The idea of the algorithm is to find an third point $T \in E(\mathbb{F}_{p^k})$ such that $\alpha = w_r(P, T)$ is a primitive r-th root of unity. Then one computes $\beta = w_r(Q, T)$ and computes the discrete logarithm of β to the base α. We denote this discrete logarithm by b. Hence we have

$$\alpha^b = \beta = w_r(Q, T) = w_r(aP, T) = w_r(P, T)^a = \alpha^a.$$

Thus $\alpha^{b-a} = 1$. Since α is primitive r-th root, this implies that $b \equiv a \mod r$, hence $Q = bP$ and b solves the ECDLP.

The existence of such a T is guaranteed by the following proposition:

Proposition 5.26. *Let $3 \leq r \in \mathbb{P}$ and E be an elliptic curve. Let $P, T \in E[r]$ and consider $E[r] \simeq \mathbb{F}_r \times \mathbb{F}_r$ as two dimensional vector space over $\mathbb{F}_r$. The following statements are equivalent:*

1. *P and T are a $\mathbb{F}_r$-vector space basis of $E[r]$.*
2. *$w_r(P, T)$ is a primitive r-th root of unity.*
3. *$w_r(P, T) \neq 1$.*

Proof. For a proof see [HPS08, Proposition 5.49]. □

Algorithm 4 lists the full MOV algorithm to solve the ECDLP.

Algorithm 4 The MOV algorithm

```
Input: $P, Q \in E[r]$, $\mathrm{ord}(P) = r$ and $3 \leq r \in \mathbb{P}$.
Output: $Q = bP$
  repeat
      Pick a random point $T \in E(\mathbb{F}_{p^k})$.
      $\alpha \leftarrow w_r(P, T)$.
  until $\alpha \neq 1$
  $\beta \leftarrow w_r(Q, T)$.
  Compute $b \in \mathbb{N}_0$ such that $\beta = \alpha^b$.
  return $b$
```

5.7.2. BLS Signature Scheme

Boneh, Lynn and Shacham [BLS01] presented a signature scheme in 2001 that is based on the Diffie-Hellman problem and uses a bilinear pairing to verify signatures. Originally, the signature scheme was using Type 1 and Type 2 pairings, but it was later adopted to the Type 3 setting [CHKM09]. This signature scheme allows short signatures since a signature consists of a single field element of the field of definition of the elliptic curve.

The setup of the signature scheme is the following: we fix a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ on an elliptic curve E defined over $\mathbb{F}_q$ and denote by P a generator of $\mathbb{G}_1$ and by Q a generator of $\mathbb{G}_2$. Let $p \in \mathbb{P}$ be the order of P and let $h : \{0,1\}^* \to \mathbb{G}_1$ be hash function mapping bit strings to points on the elliptic curve. Key generation, signing and verification is now performed in the following way:

- Key generation: Pick a random $x \in [1, \dots, p-1]$ and compute $V = xQ$. The public key is V and the secret key is x.
- Signing: Given a secret key x and a message $M \in \{0,1\}^*$, first compute $H = h(M)$. Then compute $\sigma = xH$. The signature on M is σ.
- Signature verification: Given a public key V, a message $M \in \{0,1\}^*$, and a signature $\sigma \in E(\mathbb{F}_q)$, compute $H = h(M)$. Then verify if $e(\sigma, Q) = e(H, V)$ and accept the signature if and only if the equation holds.

Expanding the equation $e(\sigma, Q) = e(H, V)$ demonstrates how the properties of a bilinear pairing are used in the scheme. For valid message-signature pair the following holds:

$$e(\sigma, Q) = e(xH, Q) = e(H, Q)^x = e(H, xQ) = e(H, V)$$

This signature scheme is proven to be secure in the random oracle model [BR93]. But note that for the proof to hold, we require a hash function where the discrete logarithm of its image is unknown. Constructing h from another hash function $h' : \{0,1\} \to \mathbb{Z}/p\mathbb{Z}$ naively as $h(M) = h'(M)G$ for some fixed point $G \in \mathbb{G}_1$ renders the signature scheme insecure [Tib12].

Instead of using the full point σ as signature, Boneh et al. only used the x-coordinate of σ as signature on M. This reduces the size of the signature by half, but requires additional computation and checks in the signature verification. First one needs to check if the points with the given x-coordinate exist on the elliptic curve. Then, if σ' is a point with the correct x-coordinate, one needs to check if either $e(\sigma', Q) = e(H, V)$ or $e(\sigma, Q)^{-1} = e(H, V)$ since the only other point with the same x-coordinate as σ' is $-\sigma'$. So the signature length can be reduced to $\lceil \log_2 q \rceil$.

The bilinearity of the pairing also enables the aggregation [BGLS03] of signatures. Suppose we have n distinct messages $M_1, \dots M_n \in \{0,1\}^*$ and corresponding signatures $\sigma_1, \dots, \sigma_n \in \mathbb{G}_1$. Let $V_i \in \mathbb{G}_2$ be the public keys of the signer i. The n signatures can be aggregated into one short signature by computing their sum and setting $s = \sum_{i=1}^{n} \sigma_i$. Given the public keys $V_1, \dots, V_n$ and the aggregated signature

σ, it is possible to verify that all messages $M_1, \dots M_n$ have been signed by the signer i by checking that messages are all distinct and checking whether

$$e(\sigma, Q) = \prod_{i=1}^{n} e(h(M_i), V_i)$$

holds. This approach requires less pairing evaluations than checking each signature individually. Also note that the aggregation can happen incrementally and can be performed by anyone knowing the messages and the signatures.

Batch verification of signatures is another possible extension which is made possible by the bilinear pairing. For batch verification one can use the small exponent test [BGR98] in the following way [CHP07]: given $M_1, \dots, M_n \in \{0,1\}^*$ distinct messages, signatures $\sigma_1, \dots, \sigma_n \in \mathbb{G}_1$ and public keys $V_1, \dots, V_n \in \mathbb{G}_2$ checking whether all signatures are valid is achieved by testing whether

$$e\left(\sum_{i=1}^{n} \delta_i \sigma_i, Q\right) = \prod_{i=1}^{n} e(h(M_i), V_i)^{\delta_i},$$

where the $\delta_1, \dots, \delta_n \in \mathbb{Z}/p\mathbb{Z}$ are picked randomly hand have bit length ℓ. The error probability of incorrectly accepting the signatures is controlled via ℓ and is at most $\frac{1}{\ell}$. If there is only a single signer with public key V, then the verification equation can be simplified to

$$e\left(\sum_{i=1}^{n} \delta_i \sigma_i, Q\right) = e\left(\prod_{i=1}^{n} \delta_i h(M_i), V\right).$$

6. Pairing-friendly Elliptic Curves

So far we have discussed the definition of pairings and algorithms to compute them. In this chapter we will discuss the selection of suitable elliptic curves. We will focus on ordinary elliptic curves and will shortly discuss a general method to find curves without going into much detail. We will then switch the focus to the family of Barreto-Naehrig curves and present the Optimal Ate pairing for Barreto-Naehrig curves.

The discussion of pairing-friendly curves follows [FST10, BN06, PSNB10, Ver08].

6.1. Constructing Ordinary Pairing-Friendly Curves

One method to construct pairing-friendly curves is called the *complex multiplication method* (CM method). This method is based on the following theorem:

Theorem 6.1 (Deuring Lifting Theorem)**.** *Let $p \in \mathbb{P}$ and $D, t, f \in \mathbb{Z}$ with D being square-free. If $4p = t - Df^2$, then there exists an elliptic curve E defined over $\mathbb{F}_p$ with $|E(\mathbb{F}_p)| = p + 1 - t$.*

Proof. For a proof we refer to [Lan87, Theorems 13.12, 13.13 and 13.14]. □

The value D appearing in the theorem is called *complex multiplication discriminant.* Based on this theorem, Atkin and Morain [AM93] developed an algorithm to find elliptic curves which is now known as *complex multiplication method.* The algorithm works given p and the number of desired points provided that the discriminant is not too large. Atkin and Morain used this method to find curves for primality testing. In 2001, Miyaji, Nakabayashi and Takano gave the first construction using this technique for pairing-friendly elliptic curves [MNT01]. For some special cases, they used the fact that if k is the desired embedding degree, then $r \mid p^k - 1$ implies $r|\Phi_k(p)$ where Φ_k is the k-th cyclotomic polynomial. By writing the trace of the Frobenius, the prime order of the elliptic curve and the size of the underlying prime field as polynomials $t, r, q \in \mathbb{Z}[X]$, Miyaji et al. obtained a parameterized families of pairing-friendly curves for embedding degrees $k = 3, 4, 6$. They also showed that for these embedding degrees the only possible choices are

- $t = -1 \pm 6X$ and $q = 12X^2 - 1$ for $k = 3$,
- $t = -X$ or $t = X + 1$ and $q = X^2 + X + 1$ for $k = 4$, and
- $t = 1 \pm 2X$ and $q = 4X^2 + 1$ for $k = 6$.

This approach has been generalized by many works after the initial paper by Miyaji et al. An overview of the various construction methods and a classification can be found in [FST10]. We will give the definition of parameterized families used there:

Definition 6.2. 1. A polynomial $f \in \mathbb{Q}[X]$ is called *integer-valued* if $f(\mathbb{Z}) \subset \mathbb{Z}$.

2. A polynomial $f \in \mathbb{Q}[X]$ is said to be *representing primes* if the following conditions are satisfied:

   a) The polynomial f is irreducible and has a positive leading coefficient.

   b) There exists a $x \in \mathbb{Z}$ such that $f(x) \in \mathbb{Z}$.

   c) The set
   $$\{f(x) \mid x \in \mathbb{Z}, f(x) \in \mathbb{Z}\}$$
   has a greatest common divisor equal to 1.

3. Let $t, r, q \in \mathbb{Q}[X]$ be non-zero polynomials, $k \in \mathbb{N}$ and $D \in \mathbb{Z}$ be square-free. The triples (t, r, q) *parameterize a family of elliptic curves with embedding degree k and discriminant D* if the following conditions are satisfied:

   a) There exists a $p \in \mathbb{Q}[X]$ representing primes and $d \in \mathbb{N}$ such that $q = p^d$.

   b) The polynomial r is irreducible, integer-valued and has a positive leading coefficient.

   c) The polynomials r, q and t satisfy
   $$r \mid q + 1 - t \text{ and } r \mid \Phi_k(t-1).$$

   d) The equation
   $$Dy^2 = 4q(x) - t(x)^2$$
   has infinitely many solutions $(x, y) \in \mathbb{Z}^2$.

   An elliptic curve E defined over $\mathbb{F}_{q(x)}$ with Frobenius trace $t(x)$ for some $x \in \mathbb{Z}$ is a *curve in the family* (t, r, q).

Example 6.3 shows two examples of parameterized families. In the following sections we will focus on a specific family, namely the family of Barreto-Naehrig curves.

Example 6.3. 1. For $k = 10$ and $D \equiv 43 \mod 120$ or $D \equiv 67 \mod 120$ there is family by Freeman [Fre06] given by

$$\begin{aligned} t &= 10X^2 + 5X + 3, \\ r &= 25X^4 + 25X^3 + 15X^2 + 5X + 1, \text{ and} \\ q &= 25X^4 + 25X^3 + 25X^2 + 10X + 3. \end{aligned}$$

2. For $k = 6$ and almost arbitrary D there is a family found by Scott and Barreto [SB04] using

$$\begin{aligned} t &= -4X^2 + 4X + 2, \\ r &= 16X^4 - 32X^3 + 12X^2 + 4X + 1, \text{ and} \\ q &= 4X^5 - 8X^4 + 3X^3 - 3X^2 + \tfrac{17}{4}X + 1. \end{aligned}$$

6.2. Barreto-Naehrig Curves

Barreto and Naehrig described their method to construct pairing-friendly elliptic curves over a prime field $\mathbb{F}_p$ in 2006 [BN06]. Barreto-Naehrig curves are a family obtained from applying the CM method to obtain curves with embedding degree 12 and this family is described by the following polynomials:

$$\begin{aligned} q &= 36X^4 + 36X^3 + 24X^2 + 6X + 1 \in \mathbb{Z}[X] \\ r &= 36X^4 + 36X^3 + 18X^2 + 6X + 1 \in \mathbb{Z}[X] \\ t &= 6X^2 + 1 \in \mathbb{Z}[X] \end{aligned}$$

Note that the polynomials satisfy $r = q + 1 - t$.

Definition 6.4. Let $x \in \mathbb{Z}$ be such that $q(x) \in \mathbb{P}$ and $r(x) \in \mathbb{P}$. An elliptic curve E defined over $\mathbb{F}_{q(x)}$ is called *Barreto-Naehrig curve* if

1. it of the form $Y^2 = X^3 + b$, and
2. satisfies $\left|E(\mathbb{F}_{q(x)})\right| = r(x)$.

We will refer to the parameter $x \in \mathbb{Z}$ as *Barreto-Naehrig parameter.*

From the definition it is immediately clear that for Barreto-Naehrig curves E the group of $\mathbb{F}_{q(x)}$-rational points always has prime order. Barreto and Naehrig proved that such curves exist and are efficiently constructible:

Theorem 6.5. *Barreto-Naehrig curves exists and have embedding degree* 12. *Furthermore, there exists an efficient algorithm to construct a Barreto-Naehrig curve.*

Proof. For a proof we refer to [BN06, Theorem 1] □

The algorithm to construct Barreto-Naehrig curves is very simple and consists of two steps:

1. It starts with a large enough $x \in \mathbb{Z}$ such that $q(x)$ has the desired bit length and then increments x until an x is found where $q(x)$ and $r(x)$ or $q(-x)$ and $r(-x)$ are prime.
2. Once an x is selected, the algorithm finds a suitable b by testing whether $b+1$ is a quadratic residue modulo p. For each suitable b, it is checked whether the point $(1, \sqrt{b+1})$ has order $r(x)$.

Algorithm 5 Constructing a curve of prime order with $k = 12$ [BN06, Algorithm 1]

```
Input: approximate desired size $m$ of the curve oder (in bits)
Output: parameters $p, n, b, y$ such that the curve $Y^2 = X^3 + b$ has order $n$ over $\mathbb{F}_p$
  and the point $P = (1, y)$ is a generator of the curve
  Compute the smallest $x \approx 2^{m/4}$ such that $\lceil \log_2 q(-x) \rceil = m$.
  loop
      $p \leftarrow q(-x)$
      $n \leftarrow r(-x)$
      if $p$ and $n$ are prime then
          break
      end if
      $p \leftarrow q(x)$
      $n \leftarrow r(x)$
      if $p$ and $n$ are prime then
          break
      end if
      $x \leftarrow x + 1$
  end loop
  $b \leftarrow 0$
  repeat
      repeat
          $b \leftarrow b + 1$
      until $b + 1$ is a quadratic residue modulo $p$
      Compute $y$ such that $y^2 \equiv b + 1 \mod p$
      $P \leftarrow (1, y)$.
  until $nP = \mathcal{O}$
  return $p, n, b, y$
```

The full algorithm can be found in Algorithm 5. Example 6.6 gives an example of Barreto-Naehrig curve constructed from a given parameter.

Example 6.6. A Barreto-Naehrig curve with a bit length of 256 bits is given by

$$x = 6953557824660308035$$

and we obtain

$$\begin{aligned} p = \ & 8416485564362346561058801833553559677775 \cdot 10^{38} + \\ & 30301461415811439712641988306731283611 \\ n = \ & 8416485564362346561058801833553559677772 \cdot 10^{38} + \\ & 40189662890443868617734158020217916261 \\ t = \ & 29011179852536757109490783028651336735 1. \end{aligned}$$

Both p and n are prime. A possible choice of b is 3, since $3 + 1 = 4$ is a quadratic residue mod p. So we have the Barreto-Naehrig curve

$$E : Y^2 = X^3 + 3 \text{ defined over } \mathbb{F}_p$$

and $E(\mathbb{F}_p)$ has order n. Using a small b like 3 allows the efficient implementation of operations involving b. For example the multiplication with $b = 3$ when doubling a point can be replaced by a left-shift and an addition.

6.3. Twists of Barreto-Naehrig Curves

Since Barreto-Naehrig curves have the form $Y^2 = X^3 + b$ with a non-zero b, the j-invariant of these curves is always 0. From Table 3.1 we know that the only possible twist degrees are 3 and 6. In fact, for Barreto-Naehrig curves there always exists a twist of degree 6. The construction of the twist is based on the following lemma:

Lemma 6.7. *If* $p \equiv 1 \mod 6$*, then there exists a* $\zeta \in \mathbb{F}_{p^2}^{\times}$ *such that* $X^6 - \zeta$ *is irreducible over* $\mathbb{F}_{p^2}[X]$.

Proof. For a proof we refer to [BN06, Lemma 1]. □

Now let $E : Y^2 = X^3 + b$ defined over $\mathbb{F}_p$ be a Barreto-Naehrig curve with order $n = |E(\mathbb{F}_p)|$. Due to the choice of the prime, the conditions of this lemma are alway fulfilled. Now any $\zeta \in \mathbb{F}_{p^2}$ provided by this lemma can be used to construct $\mathbb{F}_{p^{12}}$ as $\mathbb{F}_{p^2}[X]/(X^6 - \zeta)\mathbb{F}_{p^2}[X]$. The sextic twist is then obtained as either

$$E' : Y^2 = X^3 + \tfrac{b}{\zeta} \text{ defined over } \mathbb{F}_{p^2}$$

or

$$E' : Y^2 = X^3 + \tfrac{b}{\zeta^5} \text{ defined over } \mathbb{F}_{p^2}.$$

The desired order of the twist is $|E'(\mathbb{F}_{p^2})| = n(2p-n)$ and one of the two possible twists has this order. So it needs to be check which twist has the desired order. To obtain ζ one can choose $\lambda \in \mathbb{F}_p$ and $\mu \in \mathbb{F}_{p^2}$ such that λ is a non-cube and μ is a non-square and then set $\zeta = \frac{1}{\lambda^2\mu^3}$.

The isomorphism between E' and E is given by

$$\psi : \begin{cases} E'(\overline{\mathbb{F}_{p^2}}) & \to E(\overline{\mathbb{F}_p}) \\ (x,y) & \mapsto (z^2x, z^3y) \end{cases},$$

where $z \in \mathbb{F}_{p^{12}}$ is a root of $X^6 - \zeta \in \mathbb{F}_{p^2}$. Since this isomorphism induces a group isomorphism $E'(\mathbb{F}_{p^2})[n] \to \mathcal{G}_2$, instead of working in $\mathcal{G}_2 \subset E(\mathbb{F}_{p^{12}})$ it is possible to work with points on the twist which only require $\mathbb{F}_{p^2}$-arithmetic instead of $\mathbb{F}_{p^{12}}$-arithmetic.

Example 6.8. We continue from Example 6.6. We construct $\mathbb{F}_{p^2}$ as $\mathbb{F}_p[i]$ with $i^2+1=0$. We choose $\zeta' = 1+i$ and set $\zeta = \frac{1}{\zeta'}$. The desired sextic twist of E is then given by

$$E' : Y^2 = X^3 + 3(1+i) \text{ defined over } \mathbb{F}_{p^2}.$$

6.4. A Subfamily of Barreto-Naehrig Curves with an Explicit Description of Twist parameters

Although Barreto and Naehrig noted the existence of the sextic twist, Algorithm 5 only considers the Barreto-Naehrig curve but not the twist. Pereira et al. [PSNB10] later described another method to construct Barreto-Naehrig curves which has the benefit that also generators of sextic twists are known. We will give a short overview of this method.

We define the following subfamily of Barreto-Naehrig curves:

Definition 6.9. A Barreto-Naehrig curve $E : Y^2 = X^3 + b$ over $\mathbb{F}_p$ is called *friendly* if

1. $p \equiv 3 \mod 4$, and
2. there exist $c, d \in \mathbb{F}_p^\times$ such that either $b = c^4 + d^6$ or $b = c^6 + 4d^4$.

Friendly Barreto-Naehrig curves have nice properties that make it easy to describe multiple parameters in terms of c and d. Since $p \equiv 3 \mod 4$, -1 is a quadratic non-residue modulo p and we can represent $\mathbb{F}_{p^2}$ as $\mathbb{F}_p[i]/(i^2+1)$. To derive the other properties, we need the following lemmas:

Lemma 6.10. *Let $\zeta \in \mathbb{F}_{p^e}^\times$ and $b = \mathcal{N}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(\zeta) \in \mathbb{F}_p$. If the elliptic curve $E : Y^2 = X^3 + b$ has order $n = |E(\mathbb{F}_p)|$ with $2 \nmid n$ and $3 \nmid n$, then ζ is neither a square nor a cube in $\mathbb{F}_{p^e}$.*

Proof. For a proof we refer to [PSNB10, Lemma 2]. □

Lemma 6.11. *Let $p \in \mathbb{P}$ with $p \equiv 1 \mod 3$ and $\zeta \in \mathbb{F}_{p^2}$ with $b = \mathcal{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\zeta) \in \mathbb{F}_p$. Then $\frac{b}{\zeta^5}$ is a cube.*

Proof. For a proof we refer to [PSNB10, Lemma 3]. □

Recall that one way to choose ζ is to find $\lambda \in \mathbb{F}_p$ and $\mu \in \mathbb{F}_{p^2}$ such that λ is a non-cube and μ is a non-square and then set $\zeta = \frac{1}{\lambda^2\mu^3}$. Lemma 6.10 makes it possible to find ζ without first finding non-cubes and non-squares in $\mathbb{F}_p$ respectively $\mathbb{F}_{p^2}$.

After finding ζ it is still necessary to check whether ζ or ζ^5 gives the correct twist by checking its order. Lemma 6.11 ensures that ζ already gives the correct twist, so checking the order becomes unnecessary. The following theorem now puts everything together:

Theorem 6.12. *Let $E : Y^2 = X^3 + b$ be a Barreto-Naehrig curve with $b = \mathcal{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\zeta)$ for some $\zeta \in \mathbb{F}_{p^2}$. Let $E' : Y^2 = X^3 + \overline{\zeta}$ be defined over $\mathbb{F}_{p^2}$. Then E' is a sextic twist of E and the order of $E(\mathbb{F}_p)$ divides the order of $E'(\mathbb{F}_{p^2})$.*

Proof. For a proof we refer to [PSNB10, Theorem 1]. □

The parameters c and d of a friendly Barreto-Naehrig curve provide $\zeta \in \mathbb{F}_{p^2}$ with $b = \mathcal{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\zeta)$ for free. It is given by

$$\zeta = \begin{cases} c^2 + d^3 i, & \text{if } b = c^4 + d^6 \\ c^3 + 2d^2 i, & \text{if } b = c^6 + 4d^4 \end{cases}.$$

From Theorem 6.12 we obtain the sextic twist E' as

$$E' : Y^2 = X^3 + \overline{\zeta}.$$

A generator P of $E(\mathbb{F}_p)$ can be easily obtained by solving the curve equation with $-d^2$ respectively $-c^2$ as x-coordinate. We obtain

$$P = \begin{cases} (-d^2, c^2), & \text{if } b = c^4 + d^6 \\ (-c^2, 2d^2), & \text{if } b = c^6 + 4d^4 \end{cases}.$$

Similarly we can find a generator of $E'(\mathbb{F}_{p^2})[n]$ as hP' where $h = 2p - n$ and

$$P' = \begin{cases} (-di, c), & \text{if } b = c^4 + d^6 \\ (-c, d(1-i)), & \text{if } b = c^6 + 4d^4 \end{cases}.$$

Algorithm 6 now merges the idea of Algorithm 5 with the concept of friendly Barreto-Naehrig curves. Example 6.13 gives an example of a friendly Barreto-Naehrig curve.

Algorithm 6 Constructing a curve of prime order with $k = 12$

Input: approximate desired size m of the curve oder (in bits)

Output: parameters p, n, b, P, ζ, P' such that the curve $E : Y^2 = X^3 + b$ has order n over $\mathbb{F}_p$, the point P is a generator of the curve, $E' : Y^2 = X^3 + \overline{\zeta}$ defined over $\mathbb{F}_{p^2}$ is the twist of E and P' the generator of the order n subgroup.

```
Compute the smallest $x \approx 2^{m/4}$ such that $\lceil \log_2 q(-x) \rceil = m$.
loop
    $p \leftarrow q(-x)$
    $n \leftarrow r(-x)$
    if $p$ and $n$ are prime then
        break
    end if
    $p \leftarrow q(x)$
    $n \leftarrow r(x)$
    if $p$ and $n$ are prime then
        break
    end if
    $x \leftarrow x + 1$
end loop
for $(c, d) \in \mathbb{F}_p^2$ do
    $b \leftarrow c^4 + d^6$
    $P \leftarrow (-d^2, c^2)$
    if $nP = \mathcal{O}$ then
        $\zeta \leftarrow c^2 + d^3 i$
        $P' \leftarrow (-di, c)$
        return $p, n, b, P, \zeta, P'$
    end if
    $b \leftarrow c^6 + 4d^4$
    $P \leftarrow (-c^2, 2d^2)$
    if $nP = \mathcal{O}$ then
        $\zeta \leftarrow c^3 + 2d^2 i$
        $P' \leftarrow (-c, d(1 - i))$
        return $p, n, b, P, \zeta, P'$
    end if
end for
```

Example 6.13. We now look at a Barreto-Naehrig curve with bit length of 254. We take

$$x = -4647714815446351873$$

and obtain

$$\begin{aligned} p =\ & 16798108731015832284940804142231733909 8 \cdot 10^{38} + \\ & 89187121439069848933715426072753864723 \\ n =\ & 16798108731015832284940804142231733909 7 \cdot 10^{38} + \\ & 59579603404752749028378864165570215949 \\ t =\ & 1296075180343170999053365619071836487 75. \end{aligned}$$

We can find $b = 2$ of the form $b = c^4 + d^6$ where $c = 1$ and $d = 1$. So we have $\zeta = c^2 + d^3 i = 1 + i$ and the sextic twist defined over $\mathbb{F}_{p^2}$ is given by

$$E' : Y^2 = X^3 + 1 - i.$$

6.5. Optimal Ate Pairing on Barreto-Naehrig Curves

For pairing-friendly families Vercauteren proposed a method to derive q-adic compositions to obtain optimal bilinear pairings. We will demonstrate this method by applying it to Barreto-Naehrig curves.

Since we have $r \mid \Phi_k(q)$ and in view of the condition in Theorem 5.24, it suffices to consider powers q^i for $i = 0, \ldots, \phi(k) - 1$. From Theorem 5.24 we obtain the necessary condition that the absolute values of the coefficients c_i may not exceed $r^{\frac{1}{\phi(k)}}$. Such small c_i can be obtained in general by finding short vectors in the $\phi(k)$-dimension lattice spanned by

$$L = \begin{pmatrix} r & 0 & 0 & \ldots & 0 \\ -q & 1 & 0 & \ldots & 0 \\ -q^2 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & & \ddots & \\ -q^{\phi(k)-1} & 0 & \ldots & 0 & 1 \end{pmatrix}.$$

The volume of L is r, so there exists a short vector in L that satisfies

$$\|V\|_\infty \leq r^{\frac{1}{\phi(k)}}$$

by Minkowski's theorem [Min10]. By this observation, any pairing-friendly family satisfies the necessary condition for the existence of an optimal pairing. Vercauteren's method tries to find short vectors in L where only one coefficient c_i is of size $r^{\frac{1}{\phi(k)}}$. If such a vector can be found it is possible to construct an optimal pairing.

For Barreto-Naehrig curves the shortest vectors in the lattice L for the Euclidean norm are given by

$$(x+1, x, x, -2x), \text{ and } (2x, x+1, -x, x).$$

Both vectors give possibilities for optimal Ate pairings. However, we can look for short vectors with a minimal number of coefficients of size x and obtain

$$W = (6x+2, 1, -1, 1).$$

We will use this vector for the optimal Ate pairing on Barreto-Naehrig curves:

Definition 6.14. For $x \in \mathbb{Z}$ parameterizing a Barreto-Naehrig curve, the *optimal Ate pairing* is defined as

$$a_W : \begin{cases} \mathcal{G}_1 \times \mathcal{G}_2 & \to \mu_r \\ (P, Q) & \mapsto a_{(6x+2,1,-1,1)}(P, Q) \end{cases}.$$

This choice allows us to rewrite the optimal Ate pairing in the following way and eliminate all but one Miller function:

$$\begin{aligned} a_W(P,Q) = &\left(f_{6x+2,Q}(P) \cdot f_{1,Q}^{q}(P) \cdot f_{-1,Q}^{q^2}(P) \cdot f_{1,Q}^{q^3}(P)\right)^{\frac{q^k-1}{r}} \cdot \\ &\left(\ell_{Q_3,-Q_2}(P) \cdot \ell_{-Q_2+Q_3,-Q_1}(P) \cdot \ell_{Q_1-Q_2+Q_3,(6x+2)Q}(P)\right)^{\frac{q^k-1}{r}} \end{aligned}$$

where $Q_i = Q^{q^i}$. Since we have $f_{1,Q} = 1$ and $f_{-1,Q}$ satisfies

$$f_{-1,Q} = \frac{\nu_Q}{f_{1,Q}},$$

we obtain

$$\begin{aligned} a_W(P,Q) = \; &\left(f_{6x+2,Q}(P) \cdot \nu_Q^{q^2}(P) \cdot \ell_{Q_3,-Q_2}(P)\right)^{q^k-1} \cdot \\ &\left(\ell_{-Q_2+Q_3,-Q_1}(P) \cdot \ell_{Q_1-Q_2+Q_3,(6x+2)Q}(P)\right)^{\frac{q^k-1}{r}}. \end{aligned}$$

We will see in Section 7.4 we can also eliminate ν_Q from the computation.

6.6. Hashing to Barreto-Naehrig Curves

Hashing to an elliptic curve group E is required in many elliptic curve-based cryptography protocols. They involve hash functions $H : \{0,1\}^* \to E(\mathbb{F}_p)$ that map arbitrary values to points on elliptic curves.

Various methods have been proposed to create hash functions. The first generic construction for hashing to elliptic curves is called "try-and-increment" and was

Algorithm 7 "Try-and-increment" algorithm for an elliptic curve $E : Y^2 = f(X)$ over $\mathbb{F}_p$ with security parameter k and a hash function h to $\mathbb{F}_p$

```
Input: message $M$
Output: $H \in E(\mathbb{F}_p)$
  for $c = 0, \ldots, k$ do
    $x \leftarrow h(Mc)$
    if $f(x)$ is a quadratic residue in $\mathbb{F}_p$ then
      return $\left(x, \sqrt{f(x)}\right)$
    end if
  end for
```

introduced by Boneh, Lynn and Shacham [BLS01]. It is based on a hash function h to the base field of the elliptic curve. Basically, one takes the message m and concatenates it with a counter c. If the digest values $h(mc)$ is the x-coordinate of a point on the elliptic curve, $H(m)$ is set to the point. Otherwise, c is incremented until a point is found. Algorithm 7 gives a sketch of the algorithm.

Although it can be shown that this construction is secure provided the counter size is large enough, it has the drawback that it may take multiple iterations to find a point on the curve. Since the length of the computation depends on the input, side-channel attacks are possible.

Starting with the work of Icart [Ica09], constant-time methods have been proposed [BCI$^+$09, FT10, KLR10]. However, none of efficient methods are suitable for Barreto-Naehrig curves. For example, some involve taking various cube roots and thus require $p \equiv 2 \mod 3$, which makes them unusable for Barreto-Naehrig curves.

Shallue and van de Woestijne [SvdW06] presented a general encoding function in 2006. Fouque and Tibouchi [FT12] then showed, that by specializing this construction to Barreto-Naehrig curves, it is possible to obtain an encoding function that can be used to implement a hash function securely and efficiently.

Let $E : Y^2 = X^3 + b$ be a Barreto-Naehrig curve defined over $\mathbb{F}_p$. Set $f = X^3 + b$ and define the algebraic threefold V by the equation

$$V : Y^2 = f(X_1)f(X_2)f(X_3).$$

If $(x_1, x_2, x_3, y) \in V$ is a $\mathbb{F}_p$-rational point, then one of the x_i is the x-coordinate of a point in $E(\mathbb{F}_p)$. Now we only need to find a map $\phi : \mathbb{F}_p^\times \to V$ and can use it to hash onto the Barreto-Naehrig curve. For a given $t \in \mathbb{F}_p^\times$ and $f(t) = (x_1, x_2, x_3, y)$, the smallest index $i \in \{1, 2, 3\}$ such that $f(x_i)$ is a square then determines the point on the curve E.

To obtain ϕ, we let $t \in \mathbb{F}_p^\times$ and define

$$w = \frac{\sqrt{-3}t}{1 + b + t^2}.$$

Using w, the potential x-coordinates can be computed as

$$\begin{aligned} x_1 &= \frac{-1+\sqrt{-3}}{2} - tw \\ x_2 &= -1 - x_1 \text{ and} \\ x_3 &= 1 + \frac{1}{w^2}. \end{aligned}$$

From these three definites we can compute y and have a map $\mathbb{F}_p^\times \to V$.

Algorithm 8 gives the full algorithm to obtain the Shallue-van de Woestijne encoding. Note that this algorithms also includes blinding to prevent side-channel attacks.

Algorithm 8 Shallue-van de Woestijne encoding to a Barreto-Naehrig curve $E : Y^2 = X^3 + b$ over $\mathbb{F}_p$

```
Input: $t \in \mathbb{F}_p^\times$
Output: $H \in E(\mathbb{F}_p)$
  $w \leftarrow \frac{\sqrt{-3}t}{1+b+t^2}$
  $x_1 \leftarrow \frac{-1+\sqrt{-3}}{2} - tw$
  $x_2 \leftarrow -1 - x_1$
  $x_3 \leftarrow 1 + \frac{1}{w^2}$
  Pick random $r_1, r_2, r_3 \in \mathbb{F}_p^\times$.
  $\alpha \leftarrow \chi_p(r_1^2(x_1^3 + b))$
  $\beta \leftarrow \chi_p(r_2^2(x_2^3 + b))$
  $i \leftarrow ((\alpha - 1)\beta \mod 3) + 1$
  return $\left(x_i, \chi_p(r_3^2 t)\sqrt{x_i^3 + b}\right)$
```

From the algorithm it can be seen that no step relies on the fact that the base field is a prime field. Thus the algorithm can be adopted to work over $\mathbb{F}_q$ for a prime power q as long as there is an efficient implementation to compute square roots in $\mathbb{F}_q$. Also, an efficient implementation of the quadratic character of $\mathbb{F}_q$ is required. So the algorithm is suitable for hashing to both $\mathbb{G}_1$ and $\mathbb{G}_2$.

Part III.

Implementation of Pairings

7. Techniques to Speed up Pairing Computations

Many of the operations involved in the evaluation of a pairing are considerably more expansive than arithmetic on the prime field and group operations on an elliptic curve defined over a prime field. This chapter describes various state-of-the-art techniques to improve the performance of a pairing evaluation. The discussion of this techniques is based on [AKL$^+$10, BDM$^+$10, Sco07, Kar10, BKLS02, SBC$^+$08].

7.1. Towered Extension Fields and Finite Field Arithmetic

The arithmetic in the full extension field is more expensive than in any of its proper subfields. Hence the performance of a pairing evaluation heavily depends on the complexity of the associated extension field arithmetic. This section describes tower-friendly fields which allow a nice construction using binomials. We will also look at the Frobenius automorphism for degree 12 extensions and at compressed squaring algorithms for the cyclotomic subgroup.

Let p be a prime and $k \in \mathbb{N}$. To implement the arithmetic in $\mathbb{F}_{p^k}$ we can always use a representation of the form $\mathbb{F}_p[X]/f\mathbb{F}_p[X]$ for some monic irreducible polynomial f of degree k. However, when considering the particular nature of the finite field extension that we have seen so far, it is possible to construct $\mathbb{F}_{p^k}$ as a tower of field extension:

$$\begin{tikzcd}
\mathbb{F}_{p^k} = \mathbb{F}_{p^{k_{n-1}}}[X]/f_{n_1}\mathbb{F}_{p^{k_{n-1}}}[X] \arrow[d, dotted, no head] \\
\mathbb{F}_{p^{k_i}} = \mathbb{F}_{p^{k_{i-1}}}[X]/f_{k_i}\mathbb{F}_{p^{k_{i-1}}}[X] \arrow[d, dotted, no head] \\
\mathbb{F}_{p^{k_1}} = \mathbb{F}_p[X]/f_1\mathbb{F}_p[X] \arrow[d, no head] \\
\mathbb{F}_p
\end{tikzcd}$$

where $k = k_1 \cdots k_{n-1}$ and the polynomials f_i are of the form $f_i = X^{k_i} - \beta_i$ with suitable $\beta_i \in \mathbb{F}_{p^{k_{i-1}}}$. Of course, a construction like this using monic irreducible polynomials is always possible, but in the general case it might not be possible to find f_is that are binomials. However, when considering friendly Barreto-Naehrig curves Theorem 6.12 or more general Theorem 7.1 ensure the existence of f_i that are binomials. We will refer to fields that allow such a construction *tower-friendly fields.*

Theorem 7.1. *If* $p \equiv 1 \mod 12$, $k = 2^i 3^j$ *for some* $i, j \in \mathbb{N}$ *and* $\beta \in \mathbb{F}_p$ *is neither a square nor a cube, then* $X^k - \beta$ *is irreducible over* $\mathbb{F}_p$.

So if k has this form, we can construct $\mathbb{F}_{p^k}$ using a binomial of degree k or we can simply construct by adjoining a square or a cube root of such a β to $\mathbb{F}_p$ and then continue by adjoining cube or square roots of the previous root until the desired extension degree has been reached. Example 7.2 demonstrates the construction of extension fields as a tower of extensions.

Example 7.2. We consider a prime p coming from a friendly Barreto-Naehrig curve and let $k = 2^2 3$. We have already seen that we can obtain $\mathbb{F}_{p^2}$ from $\mathbb{F}_p$ by adjoining a square root of -1, i.e. $\mathbb{F}_{p^2} = \mathbb{F}_p[i]$ with $i^2 + 1 = 0$.

Recall that from a friendly Barreto-Naehrig curve we obtain a $\zeta \in \mathbb{F}_{p^2}$ for free that is neither a square nor a cube. So it is possible to construct $\mathbb{F}_{p^{12}}$ from $\mathbb{F}_{p^2}$ directly as degree six extension using $X^6 - \zeta$ or by first adjoining a square root of ζ and then a cubic root respectively the other way around:

$$\begin{tikzcd}
 & \begin{array}{c} \mathbb{F}_{p^{12}} = \mathbb{F}_{p^2}[U]/(U^6 - \zeta)\mathbb{F}_{p^2}[U] \simeq \\ \mathbb{F}_{p^4}[V]/(V^3 - \zeta)\mathbb{F}_{p^4}[V] \simeq \\ \mathbb{F}_{p^6}[W]/(W^2 - \zeta)\mathbb{F}_{p^6}[W] \end{array} \arrow[dl, dash] \arrow[dr, dash] & \\
\begin{array}{c} \mathbb{F}_{p^6} = \\ \mathbb{F}_{p^2}[T]/(T^3 - \zeta)\mathbb{F}_{p^2}[T] \end{array} \arrow[dr, dash] & & \begin{array}{c} \mathbb{F}_{p^4} = \\ \mathbb{F}_{p^2}[S]/(S^2 - \zeta)\mathbb{F}_{p^2}[S] \end{array} \arrow[dl, dash] \\
 & \mathbb{F}_{p^2} = \mathbb{F}_p[i] \arrow[d, dash] & \\
 & \mathbb{F}_p &
\end{tikzcd}$$

Note that in this construction it is very easy to switch between the three representations of $\mathbb{F}_{p^{12}}$ without the need to perform any computations. We have the following relations

$$\begin{gathered} a_0 + a_1 U + a_2 U^2 + a_3 U^3 + a_4 U^4 + a_5 U^5 \leftrightarrow \\ (a_0 + a_3 S) + (a_1 + a_4 S)V + (a_2 + a_5 S)V^2 \leftrightarrow \\ (a_0 + a_2 T + a_4 T^2) + (a_1 + a_3 T + a_5 T^2)W \end{gathered}$$

for all $a_0, \ldots, a_5 \in \mathbb{F}_{p^2}$.

Since tower-friendly fields and extensions of degree $2^i 3^j$ for some $i, j \in \mathbb{N}$ allow the representation by only using degree 2 and degree 3 extensions, it is possible to implement higher degree extension fields simply by implementing degree 2 and degree 3 extensions. While the implementation of the addition is straightforward, the choice of algorithms used to perform multiplications has been discussed extensively in [BDM$^+$10, AKL$^+$10, Sco07, BS09, DÓSD06]. Instead of discussing the implementation of the basic arithmetic any further, we will now focus on the implementation of the Frobenius isomorphism in $\mathbb{F}_{p^{12}}$ and squaring in the cyclotomic subgroup of $\mathbb{F}_{p^{12}}^{\times}$ since they play an important role in the final exponentiation of the pairing evaluation.

7.2. Frobenius isomorphism in $\mathbb{F}_{p^{12}}$

Raising elements of $f \in \mathbb{F}_{p^{12}}$ to a p-th power can always be replaced by an application of the Frobenius automorphism. We will demonstrate how compute the Frobenius automorphism without computing p-th powers.

We start with elements in $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$. In quadratic extension fields raising to a p-th power comes essentially for free. So let $f = g + h\alpha \in \mathbb{F}_{p^2}$, then we have

$$f^p = g^p + h^p\alpha^p = g + h\alpha^p.$$

The value α^p can be pre-computed, but if α's minimal polynomial is of the form $X^2 - \beta \in \mathbb{F}_p[X]$, then we have $\alpha^p = -\alpha$ and simply obtain

$$f^p = g - h\alpha.$$

Now we assume that we have a representation of $\mathbb{F}_{p^{12}}$ as

$$\mathbb{F}_{p^{12}} \simeq \mathbb{F}_{p^6}[U]/(U^2 - u)\mathbb{F}_{p^6}[U] \text{ and } \mathbb{F}_{p^{12}} \simeq \mathbb{F}_{p^2}[W]/(W^6 - w)\mathbb{F}_{p^2}[W].$$

As seen in the Section 7.1, we can represent any element $f = g + hU \in \mathbb{F}_{p^{12}}$ with $g = g_0 + g_1u + g_2u^2, h = h_0 + h_1u + h_2u^2 \in \mathbb{F}_{p^6}$ where $g_i, h_i \in \mathbb{F}_{p^2}$ for all $i = 1, 2, 3$. But we can also represent the same element as $g = g_0 + h_0W + g_1W^2 + h_1W^3 + g_2W^4 + h_2W^5$. For f^p we now obtain

$$\begin{aligned} f^p &= (g_0 + h_0W + g_1W^2 + h_1W^3 + g_2W^4 + h_2W^5)^p \\ &= \overline{g_0} + \overline{h_0}W^p + \overline{g_1}W^{2p} + \overline{h_1}W^{3p} + \overline{g_2}W^{4p} + \overline{h_2}W^{5p} \\ &= \overline{g_0} + \overline{h_0}\gamma_{1,1}W + \overline{g_1}\gamma_{1,2}W^2 + \overline{h_1}\gamma_{1,3}W^3 + \gamma_{1,4}W^4 + \overline{h_2}\gamma_{1,5}W^5 \end{aligned}$$

by using the identity $W^p = w^{(p-1)/6}W$ and by writing $(W^i)^p = \gamma_{1,i}W^i$ with $\gamma_{1,i} = w^{i(p-1)/6}$. This equation has a computational cost of 5 multiplications in $\mathbb{F}_p$ and 5 conjugations in $\mathbb{F}_{p^2}$. The values $\gamma_{1,i}, \ldots, \gamma_{1,5}$ need to be computed only once and can be reused. Similarly, we can derive formulas for f^{p^2} and f^{p^3} using constants $\gamma_{2,i} = \gamma_{1,i}\overline{\gamma_{1,i}}$ and $\gamma_{3,i} = \gamma_{1,i}\gamma_{2,i}$ for $i = 1, \ldots, 5$.

Algorithm 9 demonstrates the computation of the Frobenius automorphism using this formula.

Algorithm 9 Computation of the Frobenius automorphism in $\mathbb{F}_{p^{12}}$

```
Input: $f \in \mathbb{F}_{p^{12}}$ where $\mathbb{F}_{p^{12}} \simeq \mathbb{F}_{p^6}[U]/(U^2 - u)\mathbb{F}_{p^6}[U]$ and $\mathbb{F}_{p^{12}} \simeq \mathbb{F}_{p^2}[W]/(W^6 - w)\mathbb{F}_{p^2}[W]$, $i \in \{1, 2, 3\}$, and pre-computed $\gamma_{1,j} = u^{j(p-1)/6}$, $\gamma_{2,j} = \gamma_{1,j}\overline{\gamma_{1,j}}$, and $\gamma_{3,j} = \gamma_{1,j}\gamma_{2,j}$ for $j = 1, \dots, 5$.
Output: $f^{p^i} \in \mathbb{F}_{p^{12}}$
  if $i = 2$ then
    $t_1 \leftarrow g_0$
    $t_2 \leftarrow h_0$
    $t_3 \leftarrow g_1$
    $t_4 \leftarrow h_1$
    $t_5 \leftarrow g_2$
    $t_6 \leftarrow h_2$
  else
    $t_1 \leftarrow \overline{g_0}$
    $t_2 \leftarrow \overline{h_0}$
    $t_3 \leftarrow \overline{g_1}$
    $t_4 \leftarrow \overline{h_1}$
    $t_5 \leftarrow \overline{g_2}$
    $t_6 \leftarrow \overline{h_2}$
  end if
  $t_2 \leftarrow t_2\gamma_{i,1}$
  $t_3 \leftarrow t_3\gamma_{i,2}$
  $t_4 \leftarrow t_4\gamma_{i,3}$
  $t_5 \leftarrow t_5\gamma_{i,4}$
  $t_6 \leftarrow t_6\gamma_{i,5}$
  $c_0 \leftarrow t_1 + t_3u + t_5u^2$
  $c_1 \leftarrow t_2 + t_4u + t_6u^2$
  return $c_0 + c_1U$
```

7.3. Cyclotomic subgroups

Cyclotomic subgroups are subgroups of the multiplicative group of a finite field with an order coming from a cyclotomic polynomial. These subgroups allows one to implement fast squaring algorithms and thus faster exponentiations algorithms.

Definition 7.3. Let Φ_k be the k-th cyclotomic polynomial and let q be a prime power. The order $\Phi_k(q)$ *cyclotomic subgroup* of $\mathbb{F}_{q^k}$ is defined as

$$G_{\Phi_k(q)} = \left\{ x \in \mathbb{F}_{q^k}^{\times} \mid x^{\Phi_k(q)} = 1 \right\}.$$

We will discuss the squaring and multiplication formulas from Karabina [Kar10] which are based on compressed representation of elements contained in the cyclotomic subgroup of order $\Phi_6(q) = q^2 - q + 1$. This subgroup is the most interesting cyclotomic subgroup with respect to the final exponentiation for bilinear pairings on Barreto-Naehrig curves.

Let q be a prime power with $q \equiv 1 \mod 6$. We assume that we have $\mathbb{F}_{q^2} = \mathbb{F}_q(w)$ with $w^2 = c$ for some sextic non-residue $c \in \mathbb{F}_q$ and $\mathbb{F}_{q^6} = \mathbb{F}_{q^2}(\sigma)$ where $\sigma^3 = w$. Every element $g \in \mathbb{F}_{q^6}$ can then be represented as

$$g = (g_0 + g_1 w) + (g_2 + g_3 w)\sigma + (g_4 + g_5 w)\sigma^2$$

for some $g_0, \dots, g_5 \in \mathbb{F}_q$. However, for $g \in G_{\Phi_6(q)}$, we only need 4 $\mathbb{F}_q$ elements to represent it instead of the 6 $\mathbb{F}_q$ elements. This reduced representation of elements in the cyclotomic subgroup allows the implementation of a faster squaring algorithm.

We first define the compression and decompression of elements contained in $G_{\Phi_k(q)}$.

Definition 7.4. Let q be a prime power with $q \equiv 1 \mod 6$ and $\mathbb{F}_{q^2} = \mathbb{F}_q(w)$ with $w^2 = c$ for some sextic non-residue $c \in \mathbb{F}_q$ and $\mathbb{F}_{q^6} = \mathbb{F}_{q^2}(\sigma)$ where $\sigma^3 = w$.

1. Let $g = (g_0 + g_1 w) + (g_2 + g_3) w\sigma + (g_4 + g_5 w)\sigma^2 \in G_{\Phi_6(q)} \setminus \{1\}$. We define the *compression function* $\mathcal{C}$ as

$$\mathcal{C}(g) = (g_2, g_3, g_4, g_5).$$

2. For $(g_2, g_3, g_4, g_5) \in \mathbb{F}_q^4$ the *decompression function* $\mathcal{D}$ is defined as

$$\mathcal{D}((g_2, g_3, g_4, g_5)) = (g_0 + g_1 w) + (g_2 + g_3 w)\sigma + (g_4 + g_5 w)\sigma^2$$

where

$$\begin{cases} g_1 = \frac{g_5^2 c + 3g_4^2 - 2g_3}{4g_2}, g_0 = (2g_1^2 + g_2 g_5 - 3g_3 g_4)c + 1, & \text{if } g_2 \neq 0 \\ g_1 = \frac{2g_4 g_5}{g_3}, g_0 = (2g_1^2 - 3g_3 g_4)c + 1, & \text{if } g_2 = 0 \end{cases}.$$

Note that $g_2 = 0$ and $g_3 = 0$ can not appear at the same time as this would imply that $g = 1$. The next theorem ensures that the compression and decompression function are well-defined.

Theorem 7.5. *Let q, $\mathcal{C}$ and $\mathcal{D}$ be as in Definition* 7.4. *Then*

1. *$\mathcal{D}$ is well-defined for all $\mathcal{C}(g)$ with $g \in G_{\Phi_6(q)} \setminus \{1\}$, and*
2. *$\mathcal{D}(\mathcal{C}(g)) = g$ for all $g \in G_{\Phi_6(q)} \setminus \{1\}$.*

Proof. For a proof we refer to [Kar10, Theorem 3.1]. □

This theorem ensures that every element of the cyclotomic subgroup of order $\Phi_6(q)$ is uniquely determined by its image under $\mathcal{C}$. Karabina used the compressed representation to derive a squaring formula. The next theorem shows how the squaring formula looks like and ensures its correctness.

Theorem 7.6. *Let q, $\mathcal{C}$, $\mathcal{D}$, c, w and σ be as in Definition* 7.4. *Let $g, h \in G_{\Psi_6(q)}$ be such that $h = g^2$ and $\mathcal{C}(g) = (g_2, g_3, g_4, g_5)$. Then*

$$\mathcal{C}(g^2) = (h_2, h_3, h_4, h_5)$$

where

$$\begin{aligned} h_2 &= 2(g_2 + 3cB_{4,5}), \\ h_3 &= 3(A_{4,5} - (c+1)B_{4,5}) - 2g_3, \\ h_4 &= 3(A_{2,3} - (c+1)B_{2,3}) - 2g_4, \\ h_5 &= 2(g_5 + 3B_{2,3}), \\ A_{i,j} &= (g_i + g_j)(g_i + cg_j), \\ B_{i,j} &= g_i g_j \end{aligned}$$

and

$$h = \mathcal{D}((h_2, h_3, h_4, h_5)).$$

Proof. For a proof we refer to [Kar10, Theorem 3.2]. □

From this squaring formula we can derive an exponentiation algorithm easily. Let $e = (e_{r-1}, \ldots, e_0)_2$ with $e_{r-1} = 1$ be the exponent and $g \in G_{\Phi_6(q)} \setminus \{1\}$. Then we can compute g^e in the following way:

$$g^e = \prod_{i=0}^{r-1} g^{2^i} = g^{e_0} \prod_{i=1, e_i=1}^{r-1} \mathcal{D}\left(\mathcal{C}\left(g^{2^i}\right)\right).$$

Note that the $\mathcal{C}\left(g^{2^i}\right)$ can be computed by repeated squaring without the need to decompress the intermediate values. Each decompression requires one $\mathbb{F}_q$ inversion, but this can be reduced to only one inversion in total by using Montgomery's simultaneous inversion trick [Har08]. Let $(g_{i,2}, g_{i,3}, g_{i,4}, g_{i,5}) = \mathcal{C}(g^{2^i})$. For $i \neq 0$ with $e_i = 1$ we set

$$\begin{aligned} x_i &= g_{i,5}^2 c + 3g_{i,4}^2 - 2g_{i,3}, \\ y_i &= 4g_{i,2}, \\ g_{i,0} &= (2g_{i,1}^2 + g_{i,2}g_{i,5} - 3g_{i,3}g_{i,4})c + 1 \end{aligned} \tag{7.1}$$

if $g_2 \neq 0$ and

$$\begin{aligned} x_i &= 2g_{i,4}g_{i,5}, \\ y_i &= g_{i,3}, \\ g_{i,0} &= (2g_{i,1}^2 - 3g_{i,3}g_{i,4})c + 1 \end{aligned} \tag{7.2}$$

if $g_2 = 0$. Whenever we are interested in the decompressed value of $\mathcal{C}(g^{2^i})$ we can compute $\frac{x_i}{y_i}$ to obtain $g_{i,1}$. Then we have

$$\mathcal{D}(\mathcal{C}(g^{2^i})) = (g_{i,0} + g_{i,1}w) + (g_{i,2}, g_{i,3}w)\sigma + (g_4 + g_5w)\sigma^2.$$

We end up with a cost that is dominated by $4(r-1)$ $\mathbb{F}_q$ multiplications and n $\mathbb{F}_{q^6}$ multiplications. Algorithm 10 shows the complete algorithm to compute powers of any non-trivial element in the cyclotomic subgroup.

Algorithm 10 Exponentiation using compressed squaring

```
Input: $g \in G_{\Phi_6(q)} \setminus \{1\}$, $e = (e_{r-1}, \ldots, e_0)$ with $e_r = 1$.
Output: $g^e$
  for $i = 1, \ldots r - 1$ do
      Compute $\mathcal{C}(g^{2^i})$ from $\mathcal{C}(g^{2^{i-1}})$ using Theorem 7.6.
      if $e_i = 1$ then
          Compute $x_i$, $y_i$ and $g_{i,0}$ from $\mathcal{C}(g^{2^i})$ using (7.1) respectively (7.2) and store
  $x_i$, $y_i$, $g_{i,0}$, $g_{i,2}, \ldots, g_{i,5}$.
      end if
  end for
  Compute $g_{i,1} = \frac{x_i}{y_i}$ for all $i$ with $e_i = 1$ simultaneously.
  return $g^{e_0} \prod_{i=1,e_i=1}^{r-1} ((g_{i,0} + g_{i,1}w) + (g_{i,2}, g_{i,3}w)\sigma + (g_4 + g_5w)\sigma^2)$
```

Another useful property of the cyclotomic subgroup is, that the inversion can be replaced by a conjugation. If $x \in G_{\Phi_6(q)}$, then we have

$$x^{-1} = x^{q^6}$$

since $\Phi_6(q)$ divides $q^6 + 1$ and thus

$$xx^{q^6} = x^{q^6+1} = 1.$$

7.4. Denominator Elimination

Denominator elimination is an important technique to reduce the amount of factors that need to be computed during the evaluation of the Tate pairing. It also applies to any pairing that is derived from the Tate pairing and uses the same final exponentiation. The technique is based on work by Barreto, Kim, Lynn and Scott [BKLS02] and also Galbraith, Harrison and Soldera [GHS02].

Let E be an elliptic curve defined over $\mathbb{F}_q$. Let $r \mid E(\mathbb{F}_q)$ and k be the embedding degree with respect to r. Since we consider the Tate pairing, we may assume $k > 1$. Recall that if we want evaluate the Tate pairing for two points $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$, we need to calculate

$$f_{r,P}(D_Q)^{(q^k-1)/r}$$

where D_Q is a divisor equivalent to $(D) - (\mathcal{O})$ which has disjoint support to $(f_{r,P})$. Corollary 4.20 ensures that $D_Q = (R) - (S)$ for two points $R, S \in E(\mathbb{F}_{q^k})$. So we can compute the Tate pairing as

$$f_{r,P}(D_Q)^{(q^k-1)/r} = \left(\frac{f_{r,P}(R)}{f_{r,P}(S)}\right)^{(q^k-1)/r}.$$

This computation involves an expensive division in $\mathbb{F}_{q^k}$. The first optimization gets rid of this division and is based on the following theorem:

Theorem 7.7. *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let $r \mid E(\mathbb{F}_q)$ and assume that k, the embedding degree with respect to r, is larger than 1. Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$ and $D_Q \sim (D) - (\mathcal{O})$ be a divisor with disjoint support to $(f_{r,P})$. If P and Q are linearly independent, then*

$$f_{r,P}(D_Q)^{(q^k-1)/r} = f_{r,P}(Q)^{(q^k-1)/r}$$

Proof. For a proof we refer to [BKLS02, Theorem 1]. □

First of all this result makes it unnecessary to find a divisor that is equivalent to $(Q) - (\mathcal{O})$ having disjoint support to $(f_{r,P})$. It also ensures that we only need to evaluate $f_{r,P}$ at one point instead of two points. Hence it saves us from performing a costly division in $\mathbb{F}_{q^k}$.

Example 7.8. We use the same values as in Example 5.22. The following table shows the evaluation of Tate pairing using Miller's algorithm, but the updates are computed using Q instead of D_Q.

i	r_i	R	update $\frac{\ell}{\nu}$	update at Q	f
		$(45, 23)$			1
3	0	$(12, 16)$	$\frac{y+33x+43}{x+35}$	$6u^3 + 19u^2 + 36u + 33$	$6u^3 + 19u^2 + 36u + 33$
2	0	$(27, 14)$	$\frac{y+2x+7}{x+20}$	$39u^3 + 8u^2 + 20u + 18$	$11u^3 + 17u^2 + 24u + 4$
1	0	$(18, 31)$	$\frac{y+42x+27}{x+29}$	$18u^3 + 32u^2 + 41u + 30$	$22u^3 + 34u^2 + 5u + 10$
0	1	$(45, 24)$	$\frac{y+9x+42}{x+2}$	$21u^3 + 26u^2 + 25u + 20$	$8u^3 + 22u^2 + 5u + 27$
		$\mathcal{O}$	$x + 2$	$31u^2 + 31$	$32u^3 + 17u^2 + 43u + 12$

Note that $f_{r,P}(Q)$ differs from $f_{r,P}(D_Q)$ computed in Example 5.22. However, the final exponentiation maps both values to the same element in μ_{17}:

$$f_{r,P}(Q)^{\frac{47^k-1}{r}} = (32u^3 + 17u^2 + 43u + 12)^{287040} = 33u^3 + 43u^2 + 45u + 39$$

In Miller's algorithm the update always involves an evaluation of a line running through R and $-R$ for some intermediate point R and then dividing by this value. But this division can also be removed using the following observations.

Observe that $q-1 \mid \frac{q^k-1}{r}$ whenever $k > 1$. Since if otherwise $r \mid q-1$, then $k = 1$ (see [BKLS02, Lemma 1]). This allows us to write the final exponent as

$$\frac{q^k-1}{r} = (q-1)c$$

for some $c \in \mathbb{N}$, which gives

$$f_{r,P}(Q)^{(q^k-1)/r} = \left(f_{r,P}(Q)^{(q-1)}\right)^c .$$

Now recall that raising elements of $\mathbb{F}_q$ to the $q-1$-th power always gives 1. Thus we can freely multiply $f_{r,P}(Q)$ with any element of $\mathbb{F}_q$, since they will all be mapped to 1 by the final exponentiation.

First assume that E is a supersingular curve with $k = 2$. In this case the x-coordinate of Q is defined over $\mathbb{F}_q$. Also note that the vertical lines appearing in the denominators of Miller's algorithm only depend on $P \in E(\mathbb{F}_q)[r]$, and so they are defined over $\mathbb{F}_q$. These lines also only take the x-coordinate into account, so the value when evaluated at Q is still contained in $\mathbb{F}_q$. Hence the vertical lines only contribute factors in $\mathbb{F}_q$ which are eliminated by the final exponentiation, so we can entirely omit them without changing the value of the pairing.

For ordinary curves with $k > 2$, the x-coordinate of Q will no longer be in the base field. But when employing a twist of E, we can perform the same trick. We need the following result that generalizes the observation that $q-1 \mid \frac{q^k-1}{r}$ which follows directly from Proposition 3.9:

Lemma 7.9. *Let $e, k \in \mathbb{N}$ with $k \geq 2$ such that $e < k$ and $e \mid k$, then*

$$q^e - 1 \mid \frac{q^k-1}{r}.$$

So if the twist has degree d, then we set $e = \frac{k}{d}$. The x-coordinate of Q is then contained in the proper subfield $\mathbb{F}_{q^e}$ of $\mathbb{F}_{q^k}$. Thus the vertical line only contributes factors in $\mathbb{F}_{q^e}$. But since $q^e - 1 \mid \frac{q^k-1}{r}$, we can write the final exponent as

$$\frac{q^k-1}{r} = (q^e-1)c$$

and obtain

$$f_{r,P}(Q)^{(q^k-1)/r} = \left(f_{r,P}(Q)^{(q^e-1)}\right)^c .$$

So we can again ignore all contributions from the vertical line and simply drop it from Miller's algorithm.

Example 7.10. We use the same values as in Example 5.22 and Example 7.8. The following table shows the evaluation of Tate pairing using Miller's algorithm with denominator elimination.

i	r_i	R	update ℓ	update at Q	f
		$(45, 23)$			1
3	0	$(12, 16)$	$y + 33x + 43$	$35u^3 + 36u^2 + 11u + 13$	$35u^3 + 36u^2 + 11u + 13$
2	0	$(27, 14)$	$y + 2x + 7$	$35u^3 + 15u^2 + 11u + 18$	$44u^3 + 34u^2 + 3u + 44$
1	0	$(18, 31)$	$y + 42x + 27$	$35u^3 + 33u^2 + 11u + 23$	$5u^3 + 24u^2 + 21u + 24$
0	1	$(45, 24)$ $\mathcal{O}$	$y + 9x + 42$ $x + 2$	$35u^3 + 44u^2 + 11u + 21$ $31u^2 + 31$	$21u^3 + 36u^2 + 9u + 25$ $9u^3 + 10u^2 + 32u + 36$

As before, the final exponentiation maps the computed value to the same pairing value as before:

$$f_{r,P}(Q)^{\frac{47^k-1}{r}} = (9u^3 + 10u^2 + 32u + 36)^{287040} = 33u^3 + 43u^2 + 45u + 39$$

After applying these optimizations to Miller's algorithm, it is often referred to as BKLS-GHS version of Miller's algorithm. Algorithm 11 lists this version of Miller's algorithm. Example 7.11 shows how the same trick can be used to remove the last occurrence of the vertical line function from the optimal Ate pairing for Barreto-Naehrig curves.

Algorithm 11 BKLS-GHS version Miller's algorithm for the Tate pairing

```
Input: $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$ (Type 3) and $r = (r_{n-1}, \ldots, r_0)_2$ with $r_{n-1} = 1$.
Output: $f_{r,P}(Q)^{(q^k-1)/r}$
  $R \leftarrow P$.
  $f \leftarrow 1$.
  for $i = n - 2, \ldots, 0$ do
      Compute the line function $\ell_{R,R}$.
      $R \leftarrow 2R$.
      $f \leftarrow f^2 \cdot \ell_{R,R}(Q)$.
      if $r_i = 1$ then
          Compute the line function $\ell_{R,P}$.
          $R \leftarrow R + P$.
          $f \leftarrow f \cdot \ell_{R,P}(Q)$.
      end if
  end for
  $f \leftarrow f^{(q^k-1)/r}$
  return $f$
```

Example 7.11. Recall that we have

$$\begin{aligned} a_W(P, Q) = \ & \left(f_{6x+2,Q}(P) \cdot \nu_Q^{q^2}(P) \cdot \ell_{Q_3,-Q_2}(P)\right)^{q^k-1} \cdot \\ & \left(\ell_{-Q_2+Q_3,-Q_1}(P) \cdot \ell_{Q_1-Q_2+Q_3,(6x+2)Q}(P)\right)^{\frac{q^k-1}{r}} . \end{aligned}$$

with $Q_i = Q^{q^i}$ for the Optimal Ate pairing for Barreto-Naehrig curves with Barreto-Naehrig parameter $x \in \mathbb{Z}$. Since Q is a point on the sextic twist, $\nu_Q^{q^2}$ has coefficients in $\mathbb{F}_{p^2}$. By Lemma 7.9 we have $p^2 - 1 \mid \frac{p^{12}-1}{r}$ and thus obtain

$$\nu_Q^{q^2}(P)^{\frac{q^k-1}{r}} = \left(\nu_Q^{q^2}(P)^{q^2-1}\right)^c = 1^c = 1$$

for $c \in \mathbb{N}$ such that $c(p^2-1) = \frac{p^{12}-1}{r}$.

7.5. Curve Arithmetic in Miller's algorithm

In this section we will discuss methods to optimize the curve arithmetic in Miller's algorithm. We will present the formulas derived by Aranha et al. [AKL+10].

Similar to the previous section, we want to get rid of as many inversions as possible. Recall from Section 3.1, that when using affine coordinates to represent curve points calculating the slope always involves an inversion. However, when using projective coordinates, this inversion can be avoided, since the denominator can be eliminated. Even better results can be achieved when using Jacobian coordinates. We will apply the same trick to compute the line function. Furthermore, since the addition of two points implicitly involves the computation of the line function, we will derive explicit formulas to compute the line function and the sum of the points at the same time.

We will start with formulas for points in Jacobian coordinates since they are often used to implement efficient curve arithmetic. Let E be a Barreto-Naehrig curve defined over $\mathbb{F}_p$ and let $T = (X_1 : Y_1 : Z_1), R = (X_2 : Y_2 : Z_2) \in E$ be two points in Jacobian coordinates. Formulas for the sum can be derived similar as detailed in Section 3.1. When $T \neq R$, we obtain for $T + R = (X_3 : Y_3 : Z_3)$

$$\begin{aligned}
\nu &= Y_2 Z_1^3 - Y_1 \\
\lambda &= X_2 Z_1^2 - X_1 \\
X_3 &= \nu^2 - 2X_1\lambda 2 - \lambda^3 \\
Y_3 &= \theta(3X_1\lambda^2 - \nu^2 + \lambda^3) \\
Z_3 &= Z_1\lambda
\end{aligned}$$

The associated line intersecting E in T and R can then simply be computed as

$$\ell : Z_3 Y - \nu X + (\nu X_2 - Y_2 Z_3)$$

If $T = R$, then the formulas can be derived in the same way and become

$$\begin{aligned}
X_3 &= \frac{9X_1^4}{4} - 2X_1Y_1^2 \\
Y_3 &= \frac{3X_1^2}{2}(X_1Y_1^2 - X_3) - Y_1^4 \\
Z_3 &= Y_1 Z_1
\end{aligned}$$

and for the line function we obtain

$$\ell : Z_3 Z_1^2 Y - \frac{3X_1^2 Z_1^2 X}{2} + \frac{3X_1^3}{2} - Y_1^2.$$

Castello et al. [CLN10, Section 9] proposed to use projective coordinates to perform the curve arithmetic entirely on the twist. When using projective coordinates, it is possible to remove the inversion incurred by the group isomorphism since the factors vanish in the final exponentiation.

Now let $E' : Y^2 = X^3 + b' \in \mathbb{F}_{p^2}$ be the twist of E'. We use a similar description of $\mathbb{F}_{p^{12}}$ to the one in Section 7.2: $\mathbb{F}_{p^{12}} \simeq \mathbb{F}_{p^6}[w]/(w^2 - v)\mathbb{F}_{p^6}[w]$ and $\mathbb{F}_{p^{12}} \simeq \mathbb{F}_{p^2}[X]/(X^6 - \zeta)\mathbb{F}_{p^2}[X]$.

Then the addition formulas can be derived as

$$\begin{aligned} \nu &= Y_2 Z_1^3 - Y_1 \\ \lambda &= X_2 Z_1^2 - X_1 \\ X_3 &= \nu^2 - 2X_1 \lambda 2 - \lambda^3 \\ Y_3 &= \theta(3X_1 \lambda^2 - \nu^2 + \lambda^3) \\ Z_3 &= Z_1 \lambda \end{aligned}$$

and the line function becomes

$$\ell : -\lambda Y - \nu X v^2 + \zeta(\nu X_2 - \lambda Y_2) v w.$$

For the doubling formulas we obtain

$$\begin{aligned} X_3 &= \frac{X_1 Y_1}{2}(Y_1^2 - 9b' Z_1^2) \\ Y_3 &= \left(\frac{1}{2}(Y_1^2 + 9b' Z_1^2)\right) \\ Z_3 &= 2Y_1^3 Z_1 \end{aligned}$$

and

$$\ell : -2Y_1 Z_1 Y v w + 3X_1^2 X v^2 + \zeta(3b' Z_1^2 - Y_1^2)$$

Algorithms 12 and 13 demonstrate the algorithms implementing these formulas.

7.6. Final Exponentiation

So far we have only looked at optimizations that apply to Miller's algorithm. For larger field sizes, the cost of the final exponentiation also increases and becomes the bottleneck of the pairing evaluation. Around the 128-bit security level the cost of the final exponentiation overtakes the cost of Miller's algorithm. So for increasing security levels optimizing the final exponentiation as it is the most time-consuming part of the pairing computation. In this section we will discuss Scott et al.'s technique to compute the final exponentiation [SBC$^+$08].

Algorithm 12 Simultaneous point addition and line function evaluation in projective coordinates

```
Input: $T = (X_1 : Y_1 : Z_1), R = (X_2 : Y_2 : Z_2) \in E'(\mathbb{F}_{p^2})$ with $T \neq R$ and
    $P = (x_P, y_P) \in E(\mathbb{F}_p)$
Output: $T + R = (X_3 : Y_3 : Z_3)$ and the line $\ell \in \mathbb{F}_{p^{12}}$ running through $T$ and $R$
  $t_1 \leftarrow X_1 - Z_1 X_2$
  $t_2 \leftarrow Y_1 - Z_1 Y_2$
  $t_3 \leftarrow t_1^2$
  $X_3 \leftarrow t_3 X_1$
  $t_3 \leftarrow t_1 t_3$
  $t_4 \leftarrow t_3 + t_2^2 Z_1 - 2X_3$
  $X_3 \leftarrow X_3 - t_4$
  $Y_3 \leftarrow t_2 X_3 - t_3 Y_1$
  $X_3 \leftarrow t_1 t_4$
  $Z_3 \leftarrow t_3 Z_1$
  $l_{0,2} \leftarrow -t_2 x_P$
  $l_{0,0} \leftarrow \zeta(t_2 X_2 - t_1 Y_2)$
  $l_{1,1} \leftarrow -t_1 y_P$
  return $T + R = (X_3 : Y_3 : Z_3)$ and $\ell = (l_0, l_1)$
```

Algorithm 13 Simultaneous point doubling and line function evaluation in projective coordinates

```
Input: $T = (X_1 : Y_1 : Z_1) \in E'(\mathbb{F}_{p^2})$ and $P = (x_P, y_P) \in E(\mathbb{F}_p)$
Output: $2T = (X_3 : Y_3 : Z_3)$ and the tangent line $\ell \in \mathbb{F}_{p^{12}}$ to $T$
  $t_0 \leftarrow Z_1^2$
  $t_1 \leftarrow Y_1^2$
  $t_2 \leftarrow 3bt_0$
  $t_3 \leftarrow 3t_2$
  $l_{0,2} \leftarrow 3X_1^2$
  $X_3 \leftarrow \frac{(t_1 - t_3)X_1 Y_1}{2}$
  $T_0 \leftarrow \left(\frac{t_1 + t_3}{2}\right)^2$
  $t_3 \leftarrow (Y_1 + Z_1)^2 - (t_0 + t_1)$
  $Y_3 \leftarrow T_0 - 3t_2^2$
  $Z_3 \leftarrow t_1 t_3$
  $l_{0,0} \leftarrow \zeta t_2 t_1$
  $l_{0,2} \leftarrow l_{0,2} x_P$
  $l_{1,1} \leftarrow -t_3 y_P$
  return $2T = (X_3 : Y_3 : Z_3)$ and $\ell = (l_0, l_1)$
```

We assume that the embedding degree k is even and let $d = \frac{k}{2}$. We start by splitting the final exponent into three components:

$$\frac{q^k - 1}{r} = \left(q^d - 1\right)\left(\frac{q^d + 1}{\Phi_k(q)}\right)\frac{\Phi_k(q)}{r}.$$

Exponentiating by the first two factors is the easy part of the final exponentiation. They only involve raising elements of $\mathbb{F}_{q^k}$ by powers of q and some inversions. But raising elements in $\mathbb{F}_{q^k}$ to a power of q can be done by applying the Frobenius isomorphism and comes almost for free. Raising to the third factor is the hard part, as it does not reduce to such a simple form. A straightforward idea to improve raising by the third factor is to express $\frac{\Phi_k(q)}{r}$ as a sum of powers of q:

$$\frac{\Phi_k(q)}{r} = \sum_{i=0}^{n} \lambda_i q^i.$$

So raising $m \in \mathbb{F}_{q^k}$ to $\frac{\Phi_k(q)}{r}$ would then become

$$m^{\frac{\Phi_k(q)}{r}} = \prod_{i=0}^{n}\left(m^{q^i}\right)^{\lambda_i}$$

Again the m^{q^i} come almost for free by using the Frobenius isomorphism and the hard part becomes exponentiating by the λ_i.

Example 7.12. We consider a Barreto-Naehrig curve. Recall that $q = 36X^4+36X^3+24X^2+6X+1 \in \mathbb{Z}[X]$ and $r = 36X^4+36X^3+18X^2+6X+1 \in \mathbb{Z}[X]$. We can write the final exponent as

$$\begin{aligned}\frac{q^{12}-1}{r} &= \left(q^6 - 1\right)\left(\frac{q^6+1}{q^4-p^2+1}\right)\frac{q^4-q^2+1}{r}\\ &= \left(q^6 - 1\right)\left(q^2+1\right)\frac{q^4-q^2+1}{r}.\end{aligned}$$

From this factorization it is clear that after raising by the easy part, the hard part can be computed in the cyclotomic subgroup of order $\Phi_6(q^2)$. The hard part can be further expressed in base p in the following way:

$$\frac{q^4-q^2+1}{r} = \lambda_3 q^3 + \lambda_2 q^2 + \lambda_1 q + \lambda_0$$

where the polynomials $\lambda_0, \ldots, \lambda_3$ are given by

$$\begin{aligned}\lambda_3 &= 1 \in \mathbb{Z}[X],\\ \lambda_2 &= 6X^2 + 1 \in \mathbb{Z}[X],\\ \lambda_1 &= -36X^3 - 18X^2 - 12X + 1 \in \mathbb{Z}[X], \text{ and}\\ \lambda_0 &= -36X^3 - 30X^2 - 18X - 2 \in \mathbb{Z}[X].\end{aligned}$$

Scott et al.'s technique now goes a step further and tries to find an optimal way to rearrange the factors in the q-adic representation to end up with a minimal number of multiplications and hard exponentiations. Although the technique works for all families, we will focus our discussion on Barreto-Naehrig curves. As seen in Example 7.12 we can write the hard part of the final exponentiation as

$$\frac{q^4 - q^2 + 1}{r} = \lambda_3 q^3 + \lambda_2 q^2 + \lambda_1 q + \lambda_0$$

with

$$\begin{aligned}
&\lambda_3 = 1 \in \mathbb{Z}[X], \\
&\lambda_2 = 6X^2 + 1 \in \mathbb{Z}[X], \\
&\lambda_1 = -36X^3 - 18X^2 - 12X + 1 \in \mathbb{Z}[X], \text{ and} \\
&\lambda_0 = -36X^3 - 30X^2 - 18X - 2 \in \mathbb{Z}[X].
\end{aligned}$$

We now fix a Barreto-Naehrig parameter $x \in \mathbb{Z}$ and let $p = q(x)$. For a unitary $m \in \mathbb{F}_{p^{12}}$ we can now rewrite the hard part as

$$\begin{gathered}
\left(m^p m^{p^2} m^{p^3}\right) \cdot \left(\frac{1}{m}\right)^2 \cdot \left(\left(m^{x^2}\right)^p\right)^6 \cdot \left(\left(\frac{1}{m^x}\right)^p\right)^{12} \cdot \\
\left(\frac{1}{m^x \left(m^{x^2}\right)^p}\right)^{18} \cdot \left(\frac{1}{m^{x^2}}\right)^{30} \cdot \left(\frac{1}{m^{x^3} \left(m^{x^3}\right)^p}\right)^{36} .
\end{gathered}$$

The individual parts inside the parenthesis can be computed as $m^{x^2} = (m^x)^x$ and $m^{x^3} = (m^{x^2})^x$. If x is chosen in such a way that it has low Hamming weight, then a minimal number of multiplications are required when computing these values with a square-and-multiply algorithm or the compressed exponentiation algorithm for $G_{\Phi_6(p^2)}$. Raising by p can again be replaced by an application of the Frobenius isomorphism. Since m is unity, all the inversions can be replaced by conjugations. So we end up with an expression of the form

$$y_0 y_1^2 y_2^6 y_3^{12} y_4^{18} y_5^{30} y_6^{36} .$$

Scott et al. applied an algorithm by Olivos [Oli81] to minimize the number of required multiplications to evaluate this expression. We need the following definition:

Definition 7.13. A finite sequence $a_0, a_1, \ldots, a_r \in \mathbb{N}_0$ is called an *addition chain* if $a_0 = 1$ and for every $i \neq 0$ there exist elements in the list with indices $j < i$ and $k < i$ such that $a_i = a_j + a_k$.

First we need to find an addition sequence which is an addition chain that includes within in its elements the integers occurring as exponents. For our case, it is not hard to see that the optimal addition sequence is

$$(1, 2, 3, 6, 12, 18, 30, 36).$$

Only 3 does not occur as exponent. Olivos' algorithm now turns this addition sequence into a vectorial addition chain:

$$
\begin{gathered}
(1,0,0,0,0,0,0)\\
(0,1,0,0,0,0,0)\\
(0,0,1,0,0,0,0)\\
(0,0,0,1,0,0,0)\\
(0,0,0,0,1,0,0)\\
(0,0,0,0,0,1,0)\\
(0,0,0,0,0,0,1)\\
(2,0,0,0,0,0,0)\\
(2,0,1,0,0,0,0)\\
(2,1,1,0,0,0,0)\\
(0,1,1,0,0,0,0)\\
(2,2,1,1,0,0,0)\\
(2,1,1,0,1,0,0)\\
(4,4,2,2,0,0,0)\\
(6,5,3,2,1,0,0)\\
(12,10,6,4,2,0,0)\\
(12,10,6,5,2,1,0)\\
(12,10,6,4,2,0,1)\\
(24,20,12,8,4,2,0)\\
(36,30,18,12,6,2,1)
\end{gathered}
$$

This vertical addition chain can now be used to derive an algorithm which only requires 9 multiplications and 4 squaring computations to compute the hard part from $y_0, \ldots, y_6$. The algorithm is given in Algorithm 14.

Algorithm 14 Scott et al.'s method to compute the final exponentiation

```
Input: $y_0, \ldots, y_6 \in \mathbb{F}_{p^{12}}$.
Output: $y_0 y_1^2 y_2^6 y_3^{12} y_4^{18} y_5^{30} y_6^{36}$
  $T_0 \leftarrow y_6^2$
  $T_0 \leftarrow T_0 y_4$
  $T_0 \leftarrow T_0 y_5$
  $T_1 \leftarrow y_3 y_5$
  $T_1 \leftarrow T_1 T_0$
  $T_0 \leftarrow T_0 y_2$
  $T_1 \leftarrow T_1^2$
  $T_1 \leftarrow T_1 T_0$
  $T_1 \leftarrow T_1^2$
  $T_0 \leftarrow T_1 y_1$
  $T_0 \leftarrow T_0^2$
  $T_0 \leftarrow T_0 T_1$
  return $T_0$
```

8. Implementation in ECCelerate

The IAIK ECCelerate™ [HR15] library for the Java™ platform is a library providing protocols based on elliptic curve cryptography. The implemented protocols include

- Elliptic Curve Digital Signature Algorithm (ECDSA),
- Elliptic Curve Diffie Hellman (ECDH),
- Elliptic Curve Integrated Encryption Scheme (ECIES), and optionally
- Elliptic Curve Menezes-Qu-Vanstone protocol for authenticated key agreement (ECMQV).

Since version 3.0, support for Type 2 and Type 3 bilinear pairings on Barreto-Naehrig curves has been added. The Optimal Ate pairing as defined in Definition 6.14 is implemented using the techniques described in Chapter 7:

- Denominator elimination (Section 7.4) is applied wherever possible and the BKLS-GHS version of Miller's algorithm (Algorithm 11) is used to evaluate the Optimal Ate pairing. Also, the non-adjacent form representation of the order is used to further reduce the number of point additions and line function evaluations [EEAA13].
- The elliptic curve operations in Miller's algorithm are all performed on the twist. Point addition respectively point doubling and the line function computation are performed simultaneously (Algorithms 12 and 13).
- The final exponentiation is implemented using Scott et al.'s technique for the hard part of the final exponentiation (Algorithm 14). Furthermore the exponentiation algorithm using compressed squarings for elements of the cyclotomic subgroup is used to improve the performance of the final exponentiation (Algorithm 10). Also, the Frobenius automorphism is evaluated using explicit formulas involving only conjugations and multiplications without any exponentiations (Algorithm 9).

The construction detailed in Section 5.6 is used to build an efficient Type 2 pairing on top of the Optimal Ate pairing implementation and to provide efficient arithmetic in $\mathbb{G}_2$.

Beside the pairing evaluation, the implementation also features the following useful methods:

- Efficient hashing of messages to points on both $\mathbb{G}_1$ and $\mathbb{G}_2$ is implemented using Shallue-van de Woestijne encoding (Algorithm 8).

- Methods to generate parameters for both Barreto-Naehrig curves and friendly Barreto-Naehrig curves are provided (Algorithms 5 and 6).

There exist other implementations of bilinear pairings which are mainly implemented in the C and C++ programming languages. These libraries include

- the RELIC toolkit [AG14],
- the PBC library [Lyn13], and
- ate-pairing library [MT14].

Implementations for the Java™ platform include BNPairings [Per12], an implementation of the Optimal Ate pairing for Barreto-Naehrig curves in Java™. The implementations of the RELIC toolkit, ate-pairing and BNPairings focus on a fixed set of Barreto-Naehrig parameters and have hard-coded values for specific pre-selected curves. While IAIK ECCelerate™ also supports these particular curves, it also enables the investigation of other Barreto-Naehrig curves by implementing Algorithms 5 and 6 and providing methods to generate parameters for suitable elliptic curves.

Methods for hashing of messages to points are also implemented in BNPairings and the RELIC toolkit. While BNPairings features Shallue-van de Woestijne encoding, it only provides hashing to $\mathbb{G}_1$. Hashing to $\mathbb{G}_2$ is not provided at all. The RELIC toolkit provides hashing to both $\mathbb{G}_1$ and $\mathbb{G}_2$, but relies on the "try-and-increment"-method (Algorithm 7). To the best of our knowledge, IAIK ECCelerate™ is the only library also supporting efficient and secure hashing to $\mathbb{G}_2$.

Tables 8.1 and Table 8.2 contain a comparison of the two pure Java™ implementations. The benchmarks presented in these tables have been performed using Java™ 8 on a Intel® Core™ i7-4790 CPU with 16 GiB RAM running Ubuntu 15.04. The Barreto-Naehrig curves defined in BNPairings have been used in the benchmarks.

Tables 8.1 contains a comparison of the number of pairing evaluations per second that can be achieved using IAIK ECCelerate™ and BNPairings. The improvement that can be seen in this benchmark is largely based on improved implementations of finite fields and the elliptic curve arithmetic in Miller's algorithm.

When multiple pairings evaluations are performed for a fixed point in $\mathbb{G}_2$, it is possible to compute multiple pairings all at once by storing respectively precomputing the line functions involved in Miller's algorithm. IAIK ECCelerate™ implements the possibility to evaluate multiple pairings of this kind at the same time. This approach also allows the evaluation of the line functions and the final exponentiation to be parallelized. Table 8.2 shows the improvement that can be obtained per pairing when evaluating multiple pairings at the same time. The data in this table also highlights the importance of an efficient implementation of finite field arithmetic and in particular of the final exponentiation. In this case, all the elliptic curve arithmetic is performed only once and the performance is mainly affected by the evaluation of the line functions at the points in $\mathbb{G}_1$, the multiplication of the intermediate values and the final exponentiation.

Bit length	ECCelerate	BNPairings	improvement
254	154.316 ± 1.421 ops/s	122.847 ± 4.510 ops/s	25.62%
256	132.836 ± 2.711 ops/s	111.372 ± 1.981 ops/s	19.27%
408	59.280 ± 0.437 ops/s	46.450 ± 0.599 ops/s	27.62%
512	38.536 ± 0.187 ops/s	31.498 ± 1.301 ops/s	23.34%

Table 8.1.: Pairing evaluations per second for two randomly chosen points using IAIK ECCelerate™ and BNPairings

Bit length	ECCelerate	BNPairings	improvement
254	178.200 ± 1.682 ops/s	124.767 ± 4.459 ops/s	42.83%
256	153.259 ± 1.999 ops/s	111.150 ± 1.852 ops/s	37.89%
408	67.897 ± 0.682 ops/s	46.474 ± 0.527 ops/s	46.10%
512	44.593 ± 0.276 ops/s	31.475 ± 1.298 ops/s	41.67%

Table 8.2.: Pairing evaluations per second for a random point in $\mathbb{G}_1$ and a fixed point in $\mathbb{G}_2$ using IAIK ECCelerate™ and BNPairings

Part IV.

Conclusion

9. Conclusion

In this thesis we discussed the construction and efficient implementation of bilinear pairings on elliptic curves.

Part I covered the preliminaries. It reviewed some concepts from algebra and algebraic geometry and gave a short overview of elliptic curves and their properties.

Part II focused on the construction of bilinear pairings on elliptic curves and was divided in to three parts: divisors, bilinear pairings and pairing-friendly curves. At first, divisors were introduced as they are an essential building block in the construction of pairings. We also discussed the unique connection between divisors and points that is special to elliptic curves. The focus then switched to the definition of pairings and presented the definitions of the Weil, Tate and Ate pairings. After the first definitions, Miller's algorithm was presented and we argued why such an algorithm is necessary to make bilinear pairings a feasible primitive. Since Miller's algorithm allows first optimizations by reducing the number of iterations, we presented an optimality conjecture which is believed to give a lower bound for the number iterations required to evaluate pairings on elliptic curves. Together with this optimality conjecture, we also outlined the construction of Optimal Ate pairings to achieve the conjectured lower bound. The final part discussed the family of Barreto-Naehrig curves. The structure of this family and algorithms for parameter finding were discussed. We also detailed the Optimal Ate pairing on Barreto-Naehrig curves where we made use of the curves twist.

Part III was concerned with the efficient implementation of the finite field and elliptic curve arithmetic involved in the computation of bilinear pairings. We started with the description of tower-friendly fields which turned out to be very beneficial to derive algorithms to compute the Frobenius automorphism in extension fields. For the final exponentiation we also discussed the cyclotomic subgroup which enables the implementation of faster squaring and exponentiation algorithms. Then we considered techniques to remove unnecessary factors that appear in evaluation of pairings and were mainly focused on removing undesirable inversions. The last optimization technique targets the hard part of the final exponentiation.

Part II and III together demonstrate how the polynomial time algorithm used to evaluate pairings can be further optimized by using the special structure of the chosen elliptic curve family and properties of the pairing itself. These performance improvements are made possible by the existence of curve twists and efficiently computable endomorphisms as well as the properties of the cyclotomic subgroup in extension fields.

Finally, we also presented the implementation of the Optimal Ate pairing on Barreto-Naehrig curves in the IAIK ECCelerate™ library in Part III. We compared it to other existing pure Java™ implementations and demonstrated that IAIK

ECCelerate™ performs around 25 % up to 46 % better per pairing evaluation. IAIK ECCelerate™ is also the only library providing efficient Type 2 pairings, efficient and secure hashing to both the Barreto-Naehrig curve and its twist as well as algorithms for finding friendly Barreto-Naehrig curves.

The pairing libraries fully implemented in Java™ all use generic multi-precision integer implementations to perform the finite field arithmetic. It would be interesting to see whether switching to a fixed-width big integer implementation as used by libraries implemented in other languages provides any performance gains. Also, this switch would allow for some level of protection against side-channel attacks, since the generic multi-precision integer implementations complete operations as early as possible and may leak the length of the involved values.

Appendices

List of Symbols

(f)	the divisor of a function f
$[L : K]$	degree of the field extension L over K
aTr	the anti trace map on an elliptic curve
$\mathbb{C}$	field or complex numbers
$\lvert S \rvert$	the cardinality of a set S
$\mathrm{char}(K)$	characteristic of a field K
χ_p	quadratic character over $\mathbb{F}_p$
$\mathrm{Deg}(D)$	degree of a divisor D
$\deg(f)$	degree of a polynomial f
$\Delta(E)$	discriminant of the elliptic curve E
$\mathrm{Div}(E)$	divisor group of an elliptic curve E
$\mathrm{Div}^0(E)$	the subgroup of degree-zero divisors
$\epsilon(D)$	the effective part of a divisor D
$\mathbb{F}_q$	finite field of q elements
$\langle g \rangle$	group generated by the element g
$\left(\frac{a}{p}\right)$	Legendre symbol of $a \in \mathbb{Z}$ and $p \in \mathbb{P}$
$\mathbb{A}^n(K)$	affine space of dimension n over the field K
$\mathbb{P}^n(K)$	projective space of dimension n over the field K
$\mathcal{N}_{L/K}$	field norm of L over K
$\mu_r(K)$	r-th roots of unity of a field K
$\mathbb{N}$	set of natural numbers
$\mathbb{N}_0$	set of natural numbers and 0
$\overline{K}$	algebraic closure of a field K

$\overline{x}$	conjugate of a $x \in \mathbb{F}_q$
$\mathrm{ord}_P(f)$	the order of a function f over an elliptic curve E at point $P \in E(\overline{K})$
ϕ	Euler's totient function
Φ_n	the n-th cyclotomic polynomial
π_q	Frobenius map of $\mathbb{F}_q$
$\mathrm{Pic}^0(E)$	the divisor class group of E
$\mathrm{Prin}(E)$	the subgroup of principal divisors
$\mathbb{Q}$	field of rational numbers
$\mathbb{R}$	field or real number
$\mathrm{supp}(D)$	support of a divisor D
Tr	the trace map on an elliptic curve
$\mathbb{Z}$	ring of integers
$A \hookrightarrow B$	a map $A \to B$ that is injective
$a \| b$	a strictly divides b, i.e. a divides b but a^2 does not divide b
a_λ	(reduced) Ate pairing
$G_{\Phi_k(q)}$	order $\Phi_k(q)$ cyclotomic subgroup of $\mathbb{F}_{q^k}$
$j(E)$	j-invariant of the elliptic curve E
R/qR	quotient ring of R modulo q
$R^\bullet$	set of all non-zero elements of a ring R
t_r	(reduced) Tate pairing of order r
w_r	Weil pairing of order r

Bibliography

[ABLR14] Diego F. Aranha, Paulo S. L. M. Barreto, Patrick Longa, and Jefferson E. Ricardini. The realm of the pairings. In Tanja Lange, Kristin Lauter, and Petr Lisonek, editors, *SAC 2013: 20th Annual International Workshop on Selected Areas in Cryptography*, volume 8282 of *Lecture Notes in Computer Science*, pages 3–25, Burnaby, BC, Canada, August 14–16, 2014. Springer, Heidelberg, Germany.

[AFG$^+$10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 209–236, Santa Barbara, CA, USA, August 15–19, 2010. Springer, Heidelberg, Germany.

[AG14] Diego F. Aranha and Conrado P. L. Gouvêa. *RELIC toolkit version 0.4.0*, 2014. `https://github.com/relic-toolkit/relic`.

[AKL$^+$10] Diego F. Aranha, Koray Karabina, Patrick Longa, Catherine H. Gebotys, and Julio López. Faster explicit formulas for computing pairings over ordinary curves. Cryptology ePrint Archive, Report 2010/526, 2010. `http://eprint.iacr.org/2010/526`.

[ALNR09] Christophe Arene, Tanja Lange, Michael Naehrig, and Christophe Ritzenthaler. Faster computation of the tate pairing. Cryptology ePrint Archive, Report 2009/155, 2009. `http://eprint.iacr.org/2009/155`.

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp*, 61:29–68, 1993.

[AR12] Gora Adj and Francisco Rodríguez-Henríquez. Square root computation over even extension fields. Cryptology ePrint Archive, Report 2012/685, 2012. `http://eprint.iacr.org/2012/685`.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55, Santa Barbara, CA, USA, August 15–19, 2004. Springer, Heidelberg, Germany.

[BCI$^+$09] Eric Brier, Jean-Sebastien Coron, Thomas Icart, David Madore, Hugues Randriam, and Mehdi Tibouchi. Efficient indifferentiable hashing into ordinary elliptic curves. Cryptology ePrint Archive, Report 2009/340, 2009. http://eprint.iacr.org/2009/340.

[BDM+10] Jean-Luc Beuchat, Jorge Enrique González Díaz, Shigeo Mitsunari, Eiji Okamoto, Francisco Rodríguez-Henríquez, and Tadanori Teruya. High-speed software implementation of the optimal ate pairing over Barreto-Naehrig curves. Cryptology ePrint Archive, Report 2010/354, 2010. http://eprint.iacr.org/2010/354.

[BF01] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229, Santa Barbara, CA, USA, August 19–23, 2001. Springer, Heidelberg, Germany.

[BGLS03] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432, Warsaw, Poland, May 4–8, 2003. Springer, Heidelberg, Germany.

[BGÓS04] Paulo S. L. M. Barreto, Steven Galbraith, Colm Ó hÉigeartaigh, and Michael Scott. Efficient pairing computation on supersingular abelian varieties. Cryptology ePrint Archive, Report 2004/375, 2004. http://eprint.iacr.org/2004/375.

[BGR98] Mihir Bellare, Juan A. Garay, and Tal Rabin. Fast batch verification for modular exponentiation and digital signatures. Cryptology ePrint Archive, Report 1998/007, 1998. http://eprint.iacr.org/1998/007.

[BKLS02] Paulo S. L. M. Barreto, Hae Yong Kim, Ben Lynn, and Michael Scott. Efficient algorithms for pairing-based cryptosystems. In Moti Yung, editor, *Advances in Cryptology – CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 354–368, Santa Barbara, CA, USA, August 18–22, 2002. Springer, Heidelberg, Germany.

[BLS01] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532, Gold Coast, Australia, December 9–13, 2001. Springer, Heidelberg, Germany.

[BLS02] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. Cryptology ePrint Archive, Report 2002/088, 2002. http://eprint.iacr.org/2002/088.

[BN06] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In Bart Preneel and Stafford Tavares, editors, *SAC 2005: 12th Annual International Workshop on Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331, Kingston, Ontario, Canada, August 11–12, 2006. Springer, Heidelberg, Germany.

[Bol03] Alexandra Boldyreva. Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme. In Yvo Desmedt, editor, *PKC 2003: 6th International Workshop on Theory and Practice in Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 31–46, Miami, USA, January 6–8, 2003. Springer, Heidelberg, Germany.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *ACM CCS 93: 1st Conference on Computer and Communications Security*, pages 62–73, Fairfax, Virginia, USA, November 3–5, 1993. ACM Press.

[BS09] Naomi Benger and Michael Scott. Constructing tower extensions for the implementation of pairing-based cryptography. Cryptology ePrint Archive, Report 2009/556, 2009. `http://eprint.iacr.org/2009/556`.

[BSS99] I.F. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography.* Lecture note series. Cambridge University Press, 1999.

[CCS06] L. Chen, Z. Cheng, and N.P. Smart. Identity-based key agreement protocols from pairings. Cryptology ePrint Archive, Report 2006/199, 2006. `http://eprint.iacr.org/2006/199`.

[CHKM09] Sanjit Chatterjee, Darrel Hankerson, Edward Knapp, and Alfred Menezes. Comparing two pairing-based aggregate signature schemes. Cryptology ePrint Archive, Report 2009/060, 2009. `http://eprint.iacr.org/2009/060`.

[CHP07] Jan Camenisch, Susan Hohenberger, and Michael Østergaard Pedersen. Batch verification of short signatures. Cryptology ePrint Archive, Report 2007/172, 2007. `http://eprint.iacr.org/2007/172`.

[CLN10] Craig Costello, Tanja Lange, and Michael Naehrig. Faster pairing computations on curves with high-degree twists. In Phong Q. Nguyen and David Pointcheval, editors, *PKC 2010: 13th International Conference on Theory and Practice of Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 224–242, Paris, France, May 26–28, 2010. Springer, Heidelberg, Germany.

[CM09] Sanjit Chatterjee and Alfred Menezes. On cryptographic protocols employing asymmetric pairings – the role of ψ revisited. Cryptology ePrint Archive, Report 2009/480, 2009. `http://eprint.iacr.org/2009/480`.

[Cos12] Craig Costello. Pairings for beginners, 2012. `http://craigcostello.com.au/pairings/PairingsForBeginners.pdf`.

[DÓSD06] Augusto Jun 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/2006/471`.

[DSD07] Augusto Jun Devegili, Michael Scott, and Ricardo Dahab. Implementing cryptographic pairings over Barreto-Naehrig curves. Cryptology ePrint Archive, Report 2007/390, 2007. `http://eprint.iacr.org/2007/390`.

[EEAA13] Siham Ezzouak, Mohammed El Amrani, and Abdelmalek Azizi. Improving miller's algorithm using the naf and the window naf. In Vincent Gramoli and Rachid Guerraoui, editors, *Networked Systems*, volume 7853 of *Lecture Notes in Computer Science*, pages 279–283. Springer Berlin Heidelberg, 2013.

[Eng13] Andreas Enge. Bilinear pairings on elliptic curves. *ArXiv e-prints*, January 2013. `http://arxiv.org/abs/1301.5520`.

[FHS15] Georg Fuchsbauer, Christian Hanser, and Daniel Slamanig. Practical round-optimal blind signatures in the standard model. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 233–253, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[FKR12] Laura Fuentes-Castañeda, Edward Knapp, and Francisco Rodríguez-Henríquez. Faster hashing to $\mathbb{G}_2$. In Ali Miri and Serge Vaudenay, editors, *SAC 2011: 18th Annual International Workshop on Selected Areas in Cryptography*, volume 7118 of *Lecture Notes in Computer Science*, pages 412–430, Toronto, Ontario, Canada, August 11–12, 2012. Springer, Heidelberg, Germany.

[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):pp. 865–874, 1994.

[Fre06] David Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. Cryptology ePrint Archive, Report 2006/026, 2006. `http://eprint.iacr.org/2006/026`.

[FST10] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology*, 23(2):224–280, April 2010.

[FT10] Pierre-Alain Fouque and Mehdi Tibouchi. Deterministic encoding and hashing to odd hyperelliptic curves. In Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors, *PAIRING 2010: 4th International Conference on Pairing-based Cryptography*, volume 6487 of *Lecture Notes in Computer Science*, pages 265–277, Yamanaka Hot Spring, Japan, December 13–15, 2010. Springer, Heidelberg, Germany.

[FT12] Pierre-Alain Fouque and Mehdi Tibouchi. Indifferentiable hashing to Barreto-Naehrig curves. In Alejandro Hevia and Gregory Neven, editors, *Progress in Cryptology - LATINCRYPT 2012: 2nd International Conference on Cryptology and Information Security in Latin America*, volume 7533 of *Lecture Notes in Computer Science*, pages 1–17, Santiago, Chile, October 7–10, 2012. Springer, Heidelberg, Germany.

[Gal05] Steven D. Galbraith. Pairings. In *Advances in elliptic curve cryptography*, London Mathematical Society Lecture Note Series, pages 183–213. Cambridge University Press, 2005.

[GHS02] Steven D. Galbraith, Keith Harrison, and David Soldera. Implementing the Tate pairing. In *Algorithmic number theory*, pages 324–337. Springer Berlin Heidelberg, 2002.

[GLS09] Steven D. Galbraith, Xibin Lin, and Michael Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. In Antoine Joux, editor, *Advances in Cryptology – EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Computer Science*, pages 518–535, Cologne, Germany, April 26–30, 2009. Springer, Heidelberg, Germany.

[GPS06] R. Granger, D. Page, and N.P. Smart. High security pairing-based cryptography revisited. Cryptology ePrint Archive, Report 2006/059, 2006. `http://eprint.iacr.org/2006/059`.

[GS09] Robert Granger and Michael Scott. Faster squaring in the cyclotomic subgroup of sixth degree extensions. Cryptology ePrint Archive, Report 2009/565, 2009. `http://eprint.iacr.org/2009/565`.

[Har08] David G. Harris. Simultaneous field divisions: an extension of montgomery's trick. Cryptology ePrint Archive, Report 2008/199, 2008. `http://eprint.iacr.org/2008/199`.

[HPS08] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography.* Undergraduate Texts in Mathematics. Springer, 2008.

[HR15] Christian Hanser and Sebastian Ramacher. *IAIK ECCelerate™ version 3.0*, 2015. `https://jce.iaik.tugraz.at/sic/Products/Core_Crypto_Toolkits/ECCelerate`.

[HSV06] F. Hess, N.P. Smart, and F. Vercauteren. The eta pairing revisited. Cryptology ePrint Archive, Report 2006/110, 2006. `http://eprint.iacr.org/2006/110`.

[Hun03] Thomas W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2003.

[Ica09] Thomas Icart. How to hash into elliptic curves. Cryptology ePrint Archive, Report 2009/226, 2009. `http://eprint.iacr.org/2009/226`.

[Jou00] Antoine Joux. A one round protocol for tripartite diffie-hellman. In *Proceedings of the 4th International Symposium on Algorithmic Number Theory*, ANTS-IV, pages 385–394, London, UK, UK, 2000. Springer-Verlag.

[Kar10] Koray Karabina. Squaring in cyclotomic subgroups. Cryptology ePrint Archive, Report 2010/542, 2010. `http://eprint.iacr.org/2010/542`.

[KKM08] Ann Hibner Koblitz, Neal Koblitz, and Alfred Menezes. Elliptic curve cryptography: The serpentine course of a paradigm shift. Cryptology ePrint Archive, Report 2008/390, 2008. `http://eprint.iacr.org/2008/390`.

[KLR10] Jean-Gabriel Kammerer, Reynald Lercier, and Guénaël Renault. Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time. In Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors, *PAIRING 2010: 4th International Conference on Pairing-based Cryptography*, volume 6487 of *Lecture Notes in Computer Science*, pages 278–297, Yamanaka Hot Spring, Japan, December 13–15, 2010. Springer, Heidelberg, Germany.

[KM05] Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels. Cryptology ePrint Archive, Report 2005/076, 2005. `http://eprint.iacr.org/2005/076`.

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, January 1987.

[KP05] Bo Gyeong Kang and Je Hong Park. On the relationship between squared pairings and plain pairings. Cryptology ePrint Archive, Report 2005/112, 2005. `http://eprint.iacr.org/2005/112`.

[Lan87] Serge Lang. *Elliptic Functions*. Graduate texts in mathematics. Springer, 1987.

[Lan02] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2002.

[Lic69] Stephen Lichtenbaum. Duality theorems for curves over p-adic fields. *Inventiones mathematicae*, 7(2):120–136, 1969.

[Lyn13] Ben Lynn. *PBC library version 0.5.14*, 2013. `https://crypto.stanford.edu/pbc/`.

[Men05] Alfred Menezes. An introduction to pairing-based cryptography. *Department of Combinatorics and Optimization*, 2005.

[Mil86a] Victor S. Miller. Short programs for functions on curves. In *IBM Thomas J. Watson Resarch Center*, 1986. unpublished.

[Mil86b] Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *Advances in Cryptology – CRYPTO'85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426, Santa Barbara, CA, USA, August 18–22, 1986. Springer, Heidelberg, Germany.

[Mil04] Victor S. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, September 2004.

[Min10] Hermann Minkowski. *Geometrie der Zahlen*. Number v. 1 in Geometrie der Zahlen. B.G. Teubner, 1910.

[MNT01] A. Miyaji, M. Nakabayashi, and S. Takano. New Explicit Conditions of Elliptic Curve Traces for FR-Reduction, 2001.

[MT14] Shigeo Mitsunari and Tadanori Teruya. *ate-pairing version 2014-06-15*, 2014. `https://github.com/herumi/ate-pairing`.

[MVO91] Alfred Menezes, Scott A. Vanstone, and Tatsuaki Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *23rd Annual ACM Symposium on Theory of Computing*, pages 80–89, New Orleans, Louisiana, USA, May 6–8, 1991. ACM Press.

[Oli81] Jorge Olivos. On vectorial addition chains. *Journal of Algorithms*, 2(1):13–21, 1981.

[Per12] Geovandro C.F.F. Pereira. *BNPairings version 1.2*, 2012. `https://code.google.com/p/bnpairings/`.

[PSNB10] Geovandro C. C. F. Pereira, Marcos A. Simplício Jr., Michael Naehrig, and Paulo S. L. M. Barreto. A family of implementation-friendly BN elliptic curves. Cryptology ePrint Archive, Report 2010/429, 2010. `http://eprint.iacr.org/2010/429`.

[SB04] Michael Scott and Paulo S.L.M Barreto. Generating more MNT elliptic curves. Cryptology ePrint Archive, Report 2004/058, 2004. `http://eprint.iacr.org/2004/058`.

[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`.

[SBC$^+$09] Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa. Fast hashing to g_2 on pairing-friendly curves. In Hovav Shacham and Brent Waters, editors, *PAIRING 2009: 3rd International Conference on Pairing-based Cryptography*, volume 5671 of *Lecture Notes in Computer Science*, pages 102–113, Palo Alto, CA, USA, August 12–14, 2009. Springer, Heidelberg, Germany.

[Sco07] Michael Scott. Implementing cryptographic pairings. *Lecture Notes in Computer Science*, 4575:177, 2007.

[Sha84] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology – CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53, Santa Barbara, CA, USA, August 19–23, 1984. Springer, Heidelberg, Germany.

[Sil09] Jospeh H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2009.

[SOK00] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems based on pairing. In *SCIS 2000*, Okinawa, Japan, January 2000.

[Sti09] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Graduate Texts in Mathematics. Springer, 2009.

[SvdW06] Andrew Shallue and Christiaan E. van de Woestijne. Construction of rational points on elliptic curves over finite fields. In *Proceedings of the 7th International Conference on Algorithmic Number Theory*, ANTS'06, pages 510–524, Berlin, Heidelberg, 2006. Springer-Verlag.

[Tat58] John Tate. WC-groups over p-adic fields. *Séminaire Bourbaki*, 4:265–277, 1956-1958.

[Tat63] John Tate. Duality theorems in Galois cohomology over number fields. Proc. Int. Congr. Math. 1962, 288-295 (1963)., 1963.

[Tib12] Mehdi Tibouchi. A note on hashing to bn curves. In *SCIS 2012*, Kanazawa, Japan, January 2012.

[Ver08] F. Vercauteren. Optimal pairings. Cryptology ePrint Archive, Report 2008/096, 2008. `http://eprint.iacr.org/2008/096`.

[Was08] Lawrence C. Washington. *Elliptic Curves - Number Theory and Cryptography*. Chapman & Hall/CRC, 2nd edition, 2008.

[Wei40] André Weil. Sur les fonctions algébriques à corps de constantes fini. Les Comptes rendus de l'Académie des sciences, pages 592–594, 1940.

[WP06] André Weimerskirch and Christof Paar. Generalizations of the karatsuba algorithm for efficient implementations. Cryptology ePrint Archive, Report 2006/224, 2006. `http://eprint.iacr.org/2006/224`.