THE UNIVERSITY OF CALGARY

# Taxonomy of Cryptographic Pairings

by

SARAH CHISHOLM

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF MATHEMATICS AND STATISTICS

CALGARY, ALBERTA

September, 2008

# THE UNIVERSITY OF CALGARY

# FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Taxonomy of Cryptographic Pairings" submitted by SARAH CHISHOLM in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE.

Mark L. Bauer

Supervisor, Dr. Mark Bauer
Department of Mathematics and Statistics

Co-supervisor, Dr. Hugh C. Williams
Department of Mathematics and Statistics

Dr. Matthew Greenberg
Department of Mathematics and Statistics

P.

Dr. Philipp Woelfel
Department of Computer Science

Sept. 16, 2008

Date

# Acknowledgments

Many thanks to my supervisor, Mark Bauer. I couldn't have asked for a better supervisor; I didn't know they made supervisors like that. Thanks to my co-supervisor Hugh Williams, and my defense committee members Matthew Greenberg and Phillip Woelfel for several valuable suggestions on the later drafts of this thesis. Thank you to everyone in the Mathematics Department who helped me along the way. In particular, thanks to Alan Silvester for all of the technical support, Kjell Wooding for comments on earlier drafts of this thesis, Matt Musson for loaning me several of his books and Kristine Bauer for many helpful suggestions. Thanks to Rentate Scheidler for rather useful ideas and her many books. Thanks to Clifton Cunningham for helping me to develop the structure of the thesis. Finally, thanks to my best friend Jonny Dodd for encouragement and support.

# Table of Contents


Approval Page ii

Acknowledgments iii

Table of Contents iv

**1 Introduction** **1**
- 1.1 Applications of Cryptographic Pairings . . . . . 2
- 1.2 The Motivation and Organization . . . . . 4

**2 Preliminaries for Pairings** **6**
- 2.1 Affine and Projective Space . . . . . 6
- 2.2 Divisors . . . . . 10
- 2.3 Elliptic Curves . . . . . 13
- 2.4 Divisors for Pairings . . . . . 17

**3 The Weil pairing** **22**
- 3.1 The Definition of the Weil Pairing . . . . . 22
- 3.2 Properties of the Weil Pairing . . . . . 24
- 3.3 The Computational Description . . . . . 29
- 3.4 The Squared Weil Pairing . . . . . 30
  - 3.4.1 Computing the Squared Weil Pairing . . . . . 33

**4 The Tate Pairing** **35**
- 4.1 Definition of the Tate Pairing . . . . . 35
- 4.2 Properties of the Tate Pairing . . . . . 40
- 4.3 The Squared Tate Pairing . . . . . 43
  - 4.3.1 Computing the Squared Tate Pairing . . . . . 44

**5 The Eta pairing** **45**
- 5.1 Supersingular Elliptic Curves . . . . . 45
- 5.2 Defining the Eta Pairing . . . . . 46
- 5.3 Relating the Eta Pairing to the Tate Pairing . . . . . 47

**6 The Ate Pairing** **50**
- 6.1 Defining the Ate Pairing . . . . . 50
- 6.2 A Different Approach for the Ate Pairing . . . . . 56
- 6.3 The Optimised Ate Pairing . . . . . 58

6.4 The Ate$_i$ Pairing . . . . . 59

**7 The Twisted Ate pairing** **61**
7.1 Preliminaries for Twists . . . . . 61
7.2 Definition of the Twisted Ate Pairing . . . . . 64
7.3 The Optimised Twisted Ate Pairing . . . . . 67
7.4 The Twisted Ate$_i$ Pairing . . . . . 67

**8 The R-ate pairing** **69**
8.1 Defining the R-ate Pairing . . . . . 69
8.2 Optimizing the R-ate Pairing . . . . . 72

**9 Miller's Algorithm** **75**
9.1 Overview . . . . . 75
9.2 Miller's Algorithm . . . . . 77
9.3 Example of the Algorithm . . . . . 78
9.4 Miller's Algorithm in Practice . . . . . 80

**10 Efficiency Comparison** **82**
10.1 Minimum Security Requirements . . . . . 82
10.2 The Cost of Computing the Weil Pairing . . . . . 83
10.2.1 Projective Coordinates . . . . . 85
10.2.2 Affine Coordinates . . . . . 88
10.3 The Cost of Computing the Tate Pairing . . . . . 89
10.3.1 Projective Coordinates . . . . . 89
10.3.2 Affine Coordinates . . . . . 90
10.4 The Cost of Computing the Squared Weil Pairing . . . . . 91
10.5 The Cost of Computing the Squared Tate Pairing . . . . . 92
10.6 Computing the Variants of the Tate Pairing . . . . . 93
10.7 Conclusion . . . . . 97

**Bibliography** **99**

# Chapter 1

# Introduction

For groups $G_1$, $G_2$ and $G_3$, a pairing is a map of the form $\phi : G_1 \times G_2 \longrightarrow G_3$. Typically, $G_1$ and $G_2$ are written additively, while $G_3$ is written multiplicatively. In elliptic curve cryptography, a pairing maps a pair of points on an elliptic curve into the multiplicative group of a finite field.

For cryptographic applications, it is desirable for the pairing to have additional properties. In particular, pairings that are bilinear, non-degenerate and efficiently computable [BF03] may be used in several different ways. A pairing is *bilinear* if for all points $P_1, P_2 \in G_1$ and $Q_1, Q_2 \in G_2$,

$$\phi(P_1 + P_2, Q_1) = \phi(P_1, Q_1)\phi(P_2, Q_1)$$

$$\phi(P_1, Q_1 + Q_2) = \phi(P_1, Q_1)\phi(P_1, Q_2)$$

which implies that $\phi(aP_1, bP_2) = \phi(P_1, P_2)^{ab}$ for integers $a$ and $b$. A pairing is *non-degenerate* if for every nonzero point $P_1 \in G_1$ there exists a point $P_2 \in G_2$ such that $\phi(P_1, P_2) \neq 1$ and likewise, for every nonzero point $P_2 \in G_2$ there exists a point $P_1 \in G_1$ such that $\phi(P_1, P_2) \neq 1$. An *efficiently computable* pairing simply means that there must be an efficient algorithm to compute $\phi(P_1, P_2)$ for $P_1 \in G_1$ and $P_2 \in G_2$.

It is also desirable that the selected groups have large prime order. Furthermore, the groups must be selected so that the discrete logarithm problem, DLP, is sufficiently hard in each of the groups. The DLP is given elements $a$ and $b$, find $k \in \mathbb{Z}$

such that $a^k = b$.

## 1.1 Applications of Cryptographic Pairings

There are numerous instances in which pairings can be applied to elliptic curve cryptography. Some of the earlier inspirational work is given by the MOV attack [MOV93], the Tripartite Key Exchange [Jou00], and most notably, the Identity Based Encryption scheme [BF03]. For a more extensive list of applications using pairings, see [BKLS02].

In 1993, the first application of a pairing used in cryptography was given by the MOV attack, named after its creators Alfred Menezes, Tatsuaki Okamoto, and Scott Vanstone. This attack converts an elliptic curve discrete logarithm problem, ECDLP, into a DLP in a finite field. The ECDLP is stated as follows: let $P$ be a point on an elliptic curve of order $m$ and $R$ an additional point on the curve where $m$, $P$ and $R$ are publicly known. Find an integer $\ell$ such that $0 \leq \ell \leq m-1$ and $R = \ell P$, provided it exists. The MOV attack is accomplished by way of an isomorphism between a subgroup of an elliptic curve of order $m$ generated by $P$ and the set of $m^{th}$ roots of unity. This map is given by the Weil pairing $e_m$. Let $Q$ be a point of order dividing $m$ such that the Weil pairing applied to $S \in \langle P \rangle$ and $Q$, $e_m(S, Q)$, is an $m^{th}$ root of unity. This isomorphism, denoted by $f$, is defined as

$$\begin{aligned} f : \langle P \rangle &\longrightarrow \mu_m \\ S &\mapsto e_m(S, Q). \end{aligned}$$

The general idea is to solve $e_m(R, Q) = e_m(P, Q)^\ell$ for $\ell \pmod m$. Note that under certain conditions $\mu_m$ is a subset of the multiplicative group of a finite field and so the

ECDLP becomes a DLP. This attack can be applied to supersingular elliptic curves due to the fact that $\mu_m$ is embedded into a relatively small field that is a subset of or equal to $\mathbb{F}_{q^k}$; see Chapter 10 for further discussion. It is unknown if this attack will be effective as the size of the field $\mu_m$ is embedded into tends to infinity [MOV93]. In particular, this attack can be avoided by choosing non-supersingular curves (these curves have fewer restrictions on the value $k$, as $k$ can be at most 6 for a supersingular curve) such that the field that $\mu_m$ is embedded into is large enough so that the DLP is infeasible. The advantage of using this attack is that it is easier to solve the DLP than it is to solve the ECLP as there are known attacks for the former form of the logarithm problem that have running times that are subexponential [MOV93].

The first constructive application of a pairing was with the Tripartite Key Exchange, created by Antoine Joux in 2000. This allows three parties to exchange a key in one round of communication so that they can all participate in a secure exchange of information. Since the exchange is done in only one step, the process is faster and less demanding of the communication channel. For the key exchange, the parties agree upon an elliptic curve $E$ defined over a finite field $\mathbb{F}_q$ such that the discrete logarithm problem in $E(\mathbb{F}_q)$ is sufficiently difficult. Also, two linearly independent points, $P$ and $Q$, are chosen with large prime order. Each party has a secret integer, $a$, $b$ and $c$ and computes $aP, aQ$, $bP, bQ$ and $cP, cQ$ respectively; these values are made public. Using a pairing, each party computes $\phi(bP, cQ)^a = \phi(cP, bQ)^a$, $\phi(aP, cQ)^b = \phi(cP, aQ)^b$ and $\phi(aP, bQ)^c = \phi(bP, aQ)^c$. By the bilinearity property, each of these values is equal to $\phi(P, Q)^{abc}$, the shared secret key. What is significant about this application is that all previously developed protocols for key exchange between three parties require at least two rounds of communication for exchanging

keys.

Arguably the most useful application was to due Dan Boneh and Michael Franklin in 2003 with their identity based-encryption scheme. This enables one to attach an identity along with an encryption that is efficient and secure. Although there have been several identity-based encryption schemes presented in the literature, they have all required certain restrictions [BF03], making them less desirable. The identity-based encryption scheme given by Boneh and Franklin manages to avoid problematic stipulations and is therefore a much more functional system. In fact, before 2003, finding such a system was considered an open problem.

## 1.2 The Motivation and Organization

In a given application that makes use of a cryptographic pairing, computing the pairing is often the computational bottleneck. In an attempt to expedite this computation, numerous pairings have been developed and improved. This thesis serves as a dictionary for these pairings which, to the best of my knowledge, does not currently exist in the literature. Also, for the sake of simplicity, an attempt to obtain consistnet notation among each of the pairings has been provided to make comprehending and comparing the pairings more feasible. As well, my analysis of the cryptographic pairings has been included.

First, the background for cryptographic pairings is covered in Chapter 2. This is followed by a description of each of the pairings in Chapters 3-8, beginning with the first pairing that was applied to cryptography, the Weil pairing. This is followed by the Tate pairing, and then each of the variants of the Tate pairing are introduced

in the order in which they were developed. In Chapter 9, the basic algorithm that is used to compute the pairings is outlined. Finally, a discussion on the efficiency of each of the pairings is given in Chapter 10.

# Chapter 2

# Preliminaries for Pairings

This chapter begins by introducing the space in which an elliptic curve is defined and builds up to the formal definition of a curve. This is followed by a discussion on divisors which are fundamental for cryptographic pairings. Finally, an elliptic curve is defined and the chapter concludes with pairing specific definitions.

## 2.1 Affine and Projective Space

Let $K$ be a perfect field. *Affine n-space over* $K$ is defined to be the set of $n-$tuples

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{P = (x_1, \ldots, x_n) \mid x_i \in \overline{K}\}.$$

The set of points $\mathbb{A}^n(K) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n(\overline{K}) \mid x_i \in K\}$ is called the set of $K-$*rational points in* $\mathbb{A}^n$. In a similar manner, *projective n-space* can be defined over $K$ as the set of $(n+1)-$tuples as follows,

$$\mathbb{P}^n = \mathbb{P}^n(\overline{K}) = \{P = (x_0, \ldots, x_n) \in \mathbb{A}^{n+1} \mid \exists\ i \text{ such that } x_i \neq 0\}/\sim .$$

The equivalence relation is given by $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ if there is an element $\lambda \in \overline{K}^*$ such that for every $i$, $x_i = \lambda y_i$. The equivalence is denoted by $[x_0, \ldots, x_n]$. The coordinates of $[x_0, \ldots, x_n]$ are called the homogeneous coordinates for the corresponding point in $\mathbb{P}^n$. Again, the set of $K-$*rational points in* $\mathbb{P}^n$ is given by $\mathbb{P}^n(K) = \{P = [x_0, \ldots x_n] \in \mathbb{P}^n(\overline{K}) \mid x_i \in K\}$. It may be the case that not each

of the $x_i \in K$ for $P = [x_0, \ldots x_n] \in \mathbb{P}^n(\overline{K})$, it is just required that some non-zero coordinate $x_i$ can be chosen such that $x_j/x_i \in K$.

The relationship between projective and affine space, roughly speaking, is that projective space can be thought of as affine space with points at infinity added. Projective $n-$space contains many copies of affine $n-$space. One particular way to illustrate this notion is to consider the map $\phi_i$ for $0 \leq i \leq n$ such that

$$\begin{aligned} \phi_i : \mathbb{A}^n &\longrightarrow \mathbb{P}^n \\ (x_1, \ldots, x_n) &\mapsto [x_1, \ldots, x_i, 1, x_{i+1}, \ldots, x_n]. \end{aligned}$$

Each $i$ gives a distinct copy of $\mathbb{A}^n$ in $\mathbb{P}^n$.

Let $\overline{K}[X]$ denote the ring of polynomials in $n$ variables, $\overline{K}[X_1, \ldots, X_n]$ with coefficients in $\overline{K}$. A polynomial $f \in \overline{K}[X]$ is called *homogeneous of degree d* if

$$f(\lambda X_1, \ldots, \lambda X_n) = \lambda^d f(X_1, \ldots, X_n)$$

for every $\lambda \in \overline{K}$. For example, let $f(X_1, X_2, X_3, X_4) \in \overline{K}[X]$ such that

$$f(X_1, X_2, X_3, X_4) = X_1^2 X_4^2 + X_2^4 + X_3 X_4^3$$

and $\lambda \in \overline{K}$. Note that

$$\begin{aligned} f(\lambda X_1, \ldots, \lambda X_4) &= (\lambda X_1)^2 (\lambda X_4)^2 + (\lambda X_2)^4 + (\lambda X_3)(\lambda X_4)^3 \\ &= \lambda^4 (X_1^2 X_4^2 + X_2^4 + X_3 X_4^3) \\ &= \lambda^4 f(X_1, \ldots, X_4), \end{aligned}$$

and so $f$ is a homogeneous polynomial of degree 4.

An ideal $J \subset \overline{K}[X]$ is called a *homogeneous ideal* if it is generated by homogeneous polynomials. The set of zeros of the homogeneous polynomials in a homogeneous ideal $J$ is called a *(projective) algebraic set* and is denoted as

$$V(J) = \{P \in \mathbb{P}^n \mid f(P) = 0 \ \forall \ \textit{homogeneous} \ f \in J\}.$$

The *homogeneous ideal of* $V(J)$ is denoted by $I(V(J)) \subset \overline{K}[X]$ and it is generated by homogeneous polynomials $f \in \overline{K}[X]$ such that $f(P) = 0$ for all points $P \in V(J)$. If the polynomials that generate $I(V(J))$ are strictly in $K[X]$, then $V(J)$ is said to be defined over $K$ which is denoted as $V(J)/K$ and its ideal is denoted as $I(V(J)/K)$. In affine space the notions of an *affine algebraic set,* the variety $V(J)$ *defined over* $K$ and the *ideal of V(J)* hold except that polynomials need not be homogeneous.

If $V(J)$ is an algebraic set defined over $K$ then the set of *$K$-rational points of* $V(J)$ is

$$(V(J))(K) = \begin{cases} V(J) \cap \mathbb{A}^n(K) & \text{in affine space, and} \\ V(J) \cap \mathbb{P}^n(K) & \text{in projective space.} \end{cases}$$

The projective algebraic set $V(J)$ is called a *(projective) variety* if the homogeneous ideal of $V(J)$, $I(V(J))$, is prime in $\overline{K}[X]$. Likewise, an *(affine) variety* is defined in the same way, except that $I(V(J))$ need not be homogeneous.

Let $V(J)$ be a variety defined over $K$. The *affine coordinate ring* of $V(J)/K$ is defined by

$$K[V(J)] = \frac{K[X]}{I(V(J)/K)}.$$

The quotient field of $K[V(J)]$ is denoted as $K(V(J))$ and is called the *function field of* $V(J)/K$. Similarly, the affine coordinate ring for $\overline{K}$ is defined as $\overline{K}[V(J)] = \overline{K}[X]/I(V(J))$ and its function field is $\overline{K}(V(J))$. In projective space, the function

field $K(V(J))$ of $V(J)$ defined over $K$ is given by the function field of $V(J) \cap \mathbb{A}^n$. $\overline{K}(V(J))$ may be defined in the same manner.

A subset $\{\ell_1, \ldots, \ell_n\}$ of a field $L$ that is an extension over $F$ is called *algebraically independent* if there does not exist a non-zero polynomial $f \in F[X]$ such that $f(\ell_1, \ldots, \ell_n) = 0$. The *transcendence base* for the extension $L$ over $F$ is a maximal subset, with respect to inclusion, of $L$ that is algebraically independent over $F$. The *transcendence degree* of the extension $L$ over $F$ is the cardinality of the transcendence base. For an affine variety $V(J)$ the transcendence degree of the extension $\overline{K}(V(J))$ over $\overline{K}$ is called the *dimension of* $V(J)$, which is denoted as $\dim(V(J))$. In projective space, if $\mathbb{A}^n \subset \mathbb{P}^n$ is chosen so that $V(J) \cap \mathbb{A}^n \neq \emptyset$ for $V(J)$ defined over $K$, then the dimension of $V(J)$ is given by $\dim(V(J) \cap \mathbb{A}^n)$.

**Definition 2.1.1.** *(An algebraic curve) A projective variety of dimension one is called* an algebraic curve.

Finally, consider the following map between the algebraic varieties $V(J)_1, V(J)_2$ in $\mathbb{A}^n$. A map $\phi$ is called a *rational map from* $V(J)_1$ *to* $V(J)_2$ if

$$\phi : V(J)_1 \to V(J)_2,$$

$$\phi = (f_0, \ldots, f_n),$$

where $f_i \in \overline{K}(V(J)_1)$ and for every point $P \in V(J)_1$, each of the $f_i$'s are defined, i.e. $\phi(P) = (f_0(P), \ldots, f_n(P)) \in V(J)_2$. The rational map $\phi$ is *defined over* $K$ if there is an element $\lambda \in \overline{K}^*$ such that $\lambda f_0, \ldots, \lambda f_n \in K(V(J)_1)$. Note that $(f_0, \ldots, f_n)$ and $(\lambda f_0, \ldots, \lambda f_n)$ give the same map on points.

Consider two curves $C_1$ and $C_2$ and a non-constant rational map $\phi : C_1 \longrightarrow C_2$ defined over $K$. Then $\phi$ induces an injection of function fields that fixes $K$ as follows,

$$\begin{aligned} \phi^* : K(C_2) &\hookrightarrow K(C_1) \\ f &\mapsto \phi^*(f) = f \circ \phi. \end{aligned} \tag{2.1}$$

The *degree of* $\phi$, $\deg \phi$, is defined to be zero if $\phi$ is constant, otherwise the degree is said to be *finite* and is given by

$$\deg \phi = [K(C_1) : \phi^*(K(C_2))].$$

Furthermore, the map $\phi$ induces another map

$$\begin{aligned} \phi_* : K(C_1) &\longrightarrow K(C_2) \\ f &\mapsto (\phi^*)^{-1} \circ N_{K(C_1)/\phi^*(K(C_2))}(f) \end{aligned} \tag{2.2}$$

where $N_{K(C_1)/\phi^*(K(C_2))}$ is the norm map [DF99] relative to the inclusion of $K(C_2)$ into $K(C_1)$ under $\phi^*$.

## 2.2 Divisors

The free abelian group of a curve $C$, generated by the points on the curve is called the *divisor group* of $C$ which is denoted by $\mathrm{Div}(C)$. A *divisor* $D$ in $\mathrm{Div}(C)$ is written as the formal sum

$$D = \sum_{P \in C} n_P(P)$$

where $n_P \in \mathbb{Z}$, and $n_P = 0$ for all but a finite number of points $P$ on $C$. The *degree of* $D$ is defined to be

$$\deg D = \sum_{P \in C} n_P.$$

The *divisors of degree 0,* which are denoted

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) \mid \deg D = 0\},$$

form a subgroup of $\mathrm{Div}(C)$. The *support* of $D$, $\mathrm{supp}(D)$, is the set of points $P$ such that $n_P \neq 0$.

For example, let $C$ be a curve and $S, T, U$ be points on $C$. A divisor $D \in \mathrm{Div}(C)$ could take the form

$$D = 3(S) + 4(T) - 7(U). \tag{2.3}$$

In this case, $\deg D = 3 + 4 - 7 = 0$, hence $D \in \mathrm{Div}^0(C)$. Also, $\mathrm{supp}(D) = \{S, T, U\}$.

Let $C$ be a smooth curve and $f \in \overline{K}(C)^*$. A divisor can be associated to $f$, called $\mathrm{div}(f)$, which is given by

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P)$$

where $\mathrm{ord}_P(f) \in \mathbb{Z}$ counts the multiplicity of a zero or a pole[1] at a point $P \in C$.

To illustrate this notion, consider a curve $C = \mathbb{P}^1$ and identify $\mathbb{P}^1$ with $\mathbb{A}^1 \cup \{\mathcal{O}\}$. Let $f$ be a function in $\mathbb{P}^1$ restricted to an affine set such that

$$f = \frac{(x-P)^2(x-Q)^3}{(x-R)^5}. \tag{2.4}$$

The divisor of $f$ is given by $\mathrm{div}(f) = 2(P) + 3(Q) - 5(R)$.

A divisor $D \in \mathrm{Div}(C)$ is called *principal* if $D = \mathrm{div}(f)$ for some $f \in \overline{K}(C)^*$; let $\mathrm{Prin}(C)$ describe the set of principal divisors. An equivalence relation of divisors $D$ and $D'$ is defined by the property that if $D - D'$ is principal then $D \sim D'$. The

[1]Note that if $\mathrm{ord}_P(f) > 0$ then $P$ is a zero, and if $ord_P(f) < 0$ then $P$ is a pole.

*Picard group* or the *divisor class group* of $C$ called $\mathrm{Pic}(C)$ is defined as

$$\mathrm{Pic}(C) = \frac{\mathrm{Div}(C)}{\mathrm{Prin}(C)}.$$

The subgroup of $\mathrm{Pic}(C)$ which is fixed by $G_{\overline{K}/K}$ is written as $\mathrm{Pic}_K(C)$. $\mathrm{Pic}^0(C)$ refers to the quotient of $\mathrm{Div}^0(C)$ by $\mathrm{Prin}(C)$ and is called the *degree 0 part of the divisor class group of C.*

Once again, consider the non-constant map of smooth curves $\phi : C_1 \to C_2$. This map also induces a map on divisor groups,

$$\begin{aligned} \phi^* : \mathrm{Div}(C_2) &\to \mathrm{Div}(C_1) \\ (Q) &\mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) \end{aligned} \tag{2.5}$$

which can be extended additively to arbitrary divisors. The term $e_\phi(P)$ is called the *ramification index of $\phi$ at $P$* which is defined as

$$e_\phi(P) = \mathrm{ord}_P(\phi^*(t_{\phi(P)}))$$

where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at the point $\phi(P)$. A *uniformizer* for a curve at a given point $P$ is defined as a function $t \in \overline{K}(C)$ such that $\mathrm{ord}_P(t) = 1$.

**Proposition 2.2.1.** *Consider the non-constant map of smooth curves $\phi : C_1 \to C_2$, then for all $f \in \overline{K}(C_2)^*$,*

$$\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f)).$$

*Proof.*

$$\begin{aligned}
\phi^*(\mathrm{div}(f)) &= \phi^*\left(\sum_{P\in C} \mathrm{ord}_P(f)(P)\right) \\
&= \sum_{P\in C} \mathrm{ord}_P(f)\phi^*(P) \\
&= \sum_{P\in C} \mathrm{ord}_P(f) \sum_{Q\in\phi^{-1}(P)} e_\phi(Q)(Q) \\
&= \sum_{P\in C} \sum_{Q\in\phi^{-1}(P)} \mathrm{ord}_P(f)e_\phi(Q)(Q) \\
&= \sum_{P\in C} \sum_{Q\in\phi^{-1}(P)} \mathrm{ord}_Q(\phi^*(f))(Q) \\
&= \sum_{Q\in\phi^{-1}(P)} \mathrm{ord}_Q(\phi^*(f))(Q) \\
&= \mathrm{div}(\phi^*(f))
\end{aligned}$$

Note that the fifth equality comes from [Sil86, Ex.2.2] and the second to last equality is due to the fact that every point is counted exactly once. □

The previous proposition indicates that the map $\phi^*$ takes divisors of degree zero to divisors of degree zero and also principal divisors to principal divisors, hence inducing the map

$$\phi^* : \mathrm{Pic}^0(C_2) \to \mathrm{Pic}^0(C_1).$$

## 2.3 Elliptic Curves

**Definition 2.3.1.** *(Elliptic Curve) An* elliptic curve *is a curve given by the* Weierstraß *equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*The elliptic curve is non-singular i.e., there are no points of the curve satisfying both the partial derivative with respect to* $y$

$$2y + a_1x + a_3 = 0,$$

*and the partial derivative with respect to* $x$

$$3x^2 + 2a_2x + a_4 - a_1y = 0.$$

$E$ *is said to be defined over* $K$ *if* $a_i \in K$ *for all* $i$. *If the points* $(x, y)$ *on* $E$ *are in* $L \times L$ *for some extension* $L$ *of* $K$, *this set is denoted by*

$$E(L) = \{(x, y) \in L \times L \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

*where* $\mathcal{O}$ *represents a special point at infinity. If the* $\mathrm{char}(K) \neq 2, 3$ *then the Weierstraß equation can be written in the reduced form*

$$y^2 = x^3 + Ax + B.$$

*This equation is non-singular if the discriminant [DF99]* $-16(4A^3+27B^2)$ *is nonzero [Sil86].*

For a more theoretical definition of an elliptic curve see [Sil86, III].

Consider an elliptic curve of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Points $P \in E$ are of the form $(x, y)$ along with the point $\mathcal{O}$ at infinity. Recall that $E$ is a subset of $\mathbb{P}^2$. Since the degree of $E$ is 3, then a line $L$ in $\mathbb{P}^2$ intersects $E$ in three places, which need not be distinct. Two points $P, Q \in E$ are added using

the *Composition Law:* Let $L$ be the secant line of $P$ and $Q$ (or the tangent line if $P = Q$) and denote $R$ as the third point of intersection of $L$ with $E$. Let $V$ denote the vertical line through $R$ and $\mathcal{O}$. The third point of intersection of $V$ with $E$ is defined to be $P + Q$.

**Proposition 2.3.2.** *The Composition Law on $E$ has the following properties.*

1. *Consider the line $L$ that intersects $E$ at the points $P, Q, R$, then* $(P + Q) + R = \mathcal{O}$.
2. *For every point $P \in E$, $P + \mathcal{O} = P$.*
3. *For all points $P, Q \in E$, $P + Q = Q + P$.*
4. *Every point $P$ in $E$ has an inverse which is denoted as $-P$.*
5. *For all points $P, Q, R \in E$, addition is associative, i.e.* $(P + Q) + R = P + (Q + R)$.

Note that $E$ together with the Composition Law forms an abelian group.

*Proof.* 1. Clear from the Composition Law.

2. Let $Q = \mathcal{O}$, then the lines $L$ and $V$ in the Composition Law are the same line. Since $L$ intersects $E$ at points $P, \mathcal{O}, R$ and $V$ intersects $E$ at points $R, \mathcal{O} + P, \mathcal{O}$ then $P = \mathcal{O} + P$.
3. Clear from the Composition Law.
4. Let $L$ be the line that intersects $E$ at points $P, \mathcal{O}, R$. The vertical line $V$ through $R$ and $\mathcal{O}$ intersects $E$ at $P + \mathcal{O} = P$. Thus $\mathcal{O} = (P + \mathcal{O}) + R = P + R$ implying that $R$ is the inverse of $P$.

5. Using the Group Law given in Definition 2.3.3, this can be proved by working each case out explicitly.

□

Not only can points on $E$ be added together, but they can also be scaled. Multiplying a point $P$ by an integer is given by the *multiplication by m map*, $[m]$, where

$$\begin{aligned} [m] : E &\longrightarrow E \\ P &\mapsto [m]P \end{aligned}$$

where $[m]P = P + \cdots + P$ ($m$ terms) for $m > 0$.

The following definition gives explicit formulae for computing the addition of points on an elliptic curve.

**Definition 2.3.3.** *(The Group Law) Consider the elliptic curve $E$ given by*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

*with points $P_i = (x_i, y_i) \in E$ for $1 \leq i \leq 3$, and $P_3 = P_1 + P_2$.*

1. *The point $-P_1$ is given by $(x_1, -y_1 - a_1x_1 - a_3)$.*
2. *If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 + P_2 = \mathcal{O}$.*
3. *If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 \neq 0$, then $P_1 + P_2$ is given by*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \quad y_3 = -(\lambda + a_1)x_3 - b - a_3$$

*where $L = \lambda x + b$ and*

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad b = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

4. *If* $x_1 \neq x_2$ *then* $P_3 = P_1 + P_2$ *is again given by*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \quad y_3 = -(\lambda + a_1)x_3 - b - a_3$$

*where* $L = \lambda x + b$ *and*

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \; b = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

The possible values for the number of points on an elliptic curve is given in the following theorem.

**Theorem 2.3.4.** *Let* $N = q + 1 - t$ *where* $q = p^n$ *for a prime* $p$ *and* $t$ *is called the* trace of Frobenius *[Was03]. For an elliptic curve* $E$ *defined over* $\mathbb{F}_q$, $\#E(\mathbb{F}_q) = N$ *if and only if* $|t| \leq 2\sqrt{q}$ *and one of the following holds:*

1. $\gcd(t, p) = 1$,
2. $n$ *is even and* $t = \pm 2\sqrt{q}$,
3. $n$ *is even,* $p \not\equiv 1 \pmod 3$ *and* $t = \pm\sqrt{q}$,
4. $n$ *is odd,* $p = 2$ *or* $3$, *and* $t = \pm p^{(n+1)/2}$
5. $n$ *is even,* $p \not\equiv 1 \pmod 4$ *and* $t = 0$,
6. $n$ *is odd and* $t = 0$.

## 2.4 Divisors for Pairings

The following definitions are standard in most cryptographic pairings. Let $D = \sum_{P \in E} n_P(P)$ be a divisor such that

$$D \sim (P) - (\mathcal{O})$$

for points $P, \mathcal{O} \in E$. Let $f_{i,D}$ be a rational function on $E$ with divisor

$$\mathrm{div}(f_{i,D}) = iD - D_i$$

where $D_i = ([i]P) - (\mathcal{O})$. If $D = (P) - (\mathcal{O})$ then the function $f_{i,D}$ is also written as $f_{i,P}$ with divisor

$$\mathrm{div}(f_{i,P}) = i(P) - i(\mathcal{O}) - ([i]P) + (\mathcal{O}).$$

For any function $f$, the evaluation of $f$ at a divisor $D = \sum_{P \in E} n_P(P)$ is given by

$$f(D) = \prod_P f(P)^{n_P}.$$

For example, consider the divisor $D = 3(S) + 4(T) - 7(U)$ given in (2.3) and function $f = (x - P)^2(x - Q)^3/(x - R)^5$ defined in (2.4). Then

$$f(D) = \left[\frac{(S-P)^2(S-Q)^3}{(S-R)^5}\right]^3 \cdot \left[\frac{(T-P)^2(T-Q)^3}{(T-R)^5}\right]^4 \cdot \left[\frac{(U-P)^2(U-Q)^3}{(U-R)^5}\right]^7.$$

A standard requirement for most pairings is that the function $f_{i,D}$ is normalized by a uniformizer at the point $\mathcal{O}$ so that the pole at $\mathcal{O}$ is removed. Thus, the product of $f_{i,D}$ with the uniformizer evaluates to 1 at the point $\mathcal{O}$. From here on, it will always be assumed that $f_{i,D}$ is normalized at $\mathcal{O}$.

An important property of principal divisors is given in the next proposition.

**Proposition 2.4.1.** *For $f \in \overline{K}(E)^*$, $\deg(\mathrm{div}(f)) = 0$.*

For a proof see [Sil86, II.3]. A property that is often used for determining whether a divisor is principal is given by the following theorem.

Let $\sigma$ define the following surjective map that takes a degree zero divisor $D$ to

the following sum

$$\begin{aligned} \sigma : \mathrm{Div}^0(E) &\longrightarrow E \\ D &\mapsto \sum_{P\in E}[n_P]P. \end{aligned}$$

**Theorem 2.4.2.** *Consider an elliptic curve $E$ and a divisor $D = \sum_{P\in E} n_P(P) \in \mathrm{Div}^0(E)$. Then*

$$D \text{ is principal} \iff \sum_{P\in E}[n_P]P = \mathcal{O}.$$

*Proof.* In order to simplify the proof, it is necessary to show that the general form of $D$ is

$$D = (S) - (T) + \mathrm{div}(\ell)$$

for points $S, T \in E$ and a function $\ell$. Consider the points $P$, $Q$ and $R$ on $E$ that also lie on the line $ax+by+c = 0$. then these points are zeros of the line $f(x, y) = ax+by+c$. If $b \neq 0$[†] then $f$ has a triple pole at the point $\mathcal{O}$. Note that

$$\begin{aligned} \mathrm{div}(f) &= (P) + (Q) + (R) - 3(\mathcal{O}) \\ &= (P) + (Q) + (-(P+Q)) - 3(\mathcal{O}) \end{aligned} \tag{2.6}$$

where the last equality holds by Proposition 2.3.2. Suppose that the points $R$ and $-R$ lie on the vertical line $x + d = 0$, then the function $g(x) = x + d$ has zeros at $R$ and $-R$. This implies that $g$ has a double pole at $\mathcal{O}$ and the divisor of $g$ is given by

$$\begin{aligned} \mathrm{div}(g) &= (R) + (-R) - 2(\mathcal{O}) \\ &= (-(P+R)) + (P+R) - 2(\mathcal{O}) \end{aligned} \tag{2.7}$$

[†]If $b = 0$ then $x = -c/a$ is a vertical line.

and again, the last equality follows from Proposition 2.3.2. Subtracting (2.7) from (2.6) yields the following,

$$\operatorname{div}(f) - \operatorname{div}(g) = \operatorname{div}(f/g) = (P) + (Q) - (P+Q) - (\mathcal{O}). \tag{2.8}$$

Equation (2.8) can be rewritten as $(P) + (Q) = (P+Q) + (\mathcal{O}) + \operatorname{div}(f/g)$ which shows that for a divisor $D$ on $E$, the sum of any two terms with positive coefficients is equal to a single positive term, say $(S)$, plus a multiple of $(\mathcal{O})$ plus the divisor of a function. This is analogous for the sum of any two terms of $D$ with negative coefficients, which gives the following general form for $D$,

$$D = (S) - (T) + i(\mathcal{O}) + \operatorname{div}(\ell)$$

for some points $S, T \in E$, $i \in \mathbb{Z}$ and a function $\ell$. For the map $\sigma$ defined in equation (2.8) note that

$$\sigma(\operatorname{div}(f/g)) = P + Q - P - Q - \mathcal{O} = \mathcal{O}$$

and so the function $\ell$ is the product of functions of the form $f/g$ which implies that

$$\sigma(\operatorname{div}(\ell)) = \mathcal{O} \tag{2.9}$$

as well.

By supposition, $\deg D = 0$, therefore

$$0 = \deg D = 1 - 1 + i + 0 = i,$$

that is, $i = 0$[††], and

$$D = (S) - (T) + \operatorname{div}(\ell)$$

[††]Note that by Proposition 2.4.1, $\deg(\operatorname{div}(\ell)) = 0$.

gives the simplified general form for $D$.

Applying the map $\sigma$ to $D$ shows that

$$\sigma(D) = S - T + \mathcal{O} = S + T.$$

($\Leftarrow$) : Suppose that $\sigma(D) = \sum_{P \in E}[n_P]P = \mathcal{O}$, then $S - T = \mathcal{O}$, i.e. $S = T$, and $D = \mathrm{div}(\ell)$ is principal.

($\Rightarrow$) : On the other hand, let $D = \mathrm{div}(k)$ for some function $k$. Using (2.9),

$$\sigma(D) = \sigma(\mathrm{div}(k)) = \mathcal{O}$$

that is $\sum_{P \in E}[n_P]P = \mathcal{O}$ as desired. □

By Theorem 2.4.2, the kernel of $\sigma$ is $\mathrm{Prin}(E)$. Using the $1^{st}$ Isomorphism Theorem note that

$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Prin}(E) \cong \mathrm{Im}(\sigma) = \sigma(\mathrm{Div}^0(E)) = E$$

where the last equality holds since $\sigma$ is surjective. Therefore, $\sigma$ also induces an isomorphism, which is again denoted by $\sigma$,

$$\begin{aligned} \sigma : \mathrm{Pic}^0(E) &\longrightarrow E \\ [(P) - (\mathcal{O})] &\mapsto P \end{aligned} \tag{2.10}$$

where $[(P) - (\mathcal{O})]$ represents the equivalence class of the divisor $(P) - (\mathcal{O})$.

Finally, two special types of divisors that are required for pairings are defined as follows. A *semi-reduced divisor* is a divisor of the form $D = \sum_{P \in E} n_P(P) - \sum_{P \in E} n_P(\mathcal{O})$ where $n_P \geq 0$ and the points $P$ are finite points such that when $P \in \mathrm{supp}(D)$ then $-P \notin \mathrm{supp}(D)$. Let $D = \sum_{P \in E} n_P(P) - \sum_{P \in E} n_P(\mathcal{O})$ be a semi-reduced divisor. For an elliptic curve, if $\sum_{P \in E} n_P \leq 1$ then $D$ is a called a *reduced divisor.*

# Chapter 3

# The Weil pairing

André Weil introduced this pairing in his proof of the Riemann Hypothesis for function-fields [Wei46] in 1946. Almost fifty years later, Menezes et al. [MOV93] first made use of the Weil pairing in cryptography in 1993 with the MOV attack. The Weil pairing is significant as it was the first pairing used in cryptography; however, in practice it is no longer favoured because it takes more than double the time required to compute than other types of pairings, such as the Tate Pairing [Gal05]. This is due largely to the fact that it requires computing the Tate pairing twice. It has been argued that asymptotically this pairing would be more efficient to compute at high security levels [KM05]. However, in [GPS06] it is stated that at security levels of cryptographic relevance, the Tate pairing is always more efficient than the Weil pairing.

## 3.1 The Definition of the Weil Pairing

For an elliptic curve $E$ defined over a field $K$ the set of *m-torsion points* of $E$ for $m \in \mathbb{Z}^+$ is defined to be

$$E[m] = \{P \in E(\overline{K}) \mid [m]P = \mathcal{O}\}.$$

Let $T \in E[m]$. By Theorem 2.4.2 there exists a function $f \in \overline{K}(E)$ such that $\mathrm{div}(f) = m(T) - m(\mathcal{O})$. Let $T' \in E$ such that $[m]T' = T$. Similarly, there exists a function $g \in \overline{K}(E)$ such that

$$\begin{aligned} \operatorname{div}(g) &= [m]^*(T) - [m]^*(\mathcal{O}) \\ &= \sum_{R \in E[m]} (T' + R) - (R), \end{aligned} \tag{3.1}$$

where $[m]^*$ is an automorphism induced by $[m]$ on $\operatorname{Div}(E)$ given by $[m]^*(Q) = \sum_{P \in [m]^{-1}(Q)} e_\phi(P)(P)$.

Since $f \circ [m]$ and $g^m$ have the same divisor, then up to a scalar multiple in $\overline{K}^*$,

$$f \circ [m] = g^m. \tag{3.2}$$

For all points $X \in E$ and a point $S \in E[m]$ the following holds,

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m. \tag{3.3}$$

Thus $g(X+S)^m / g(X)^m = 1$, and hence $g(X+S)/g(X) \in \mu_m$ where $\mu_m$ is the set of $m^{th}$ roots of unity.

From these properties it is possible to give the classical definition of the Weil pairing [Sil86].

**Definition 3.1.1.** *Let $E$ be an elliptic curve defined over a field $K$. Let $m \in \mathbb{Z}$ such that $m \geq 2$ and relatively prime to* $\operatorname{char}(K) > 0$. *Let $T, S \in E[m]$. For a function $g$ as defined in (3.1) the* Weil pairing $e_m$ *is defined to be*

$$\begin{aligned} e_m : E[m] \times E[m] &\longrightarrow \mu_m \\ (S, T) &\mapsto g(X+S)/g(X) \end{aligned}$$

*for any point $X \in E$ such that $g(X+S)$ and $g(X)$ are defined and nonzero.*

Note that although $g$ is only defined up to a scalar multiple $c \in \overline{K}^*$, the pairing is independent of this choice of $c$.

## 3.2 Properties of the Weil Pairing

The Weil pairing has several nice properties that are particularly useful in applications. For example, the bilinearity property is an integral component of A. Joux's Tripartite key exchange [Jou00]. The following is a list of the relevant properties.

**Theorem 3.2.1.** *The Weil pairing has the following properties:*

1. *(Bilinearity) For all points* $S_1$, $S_2$, $S$, $T_1$, $T_2$, $T \in E[m]$,

$$(a.)\ e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$$

$$(b.)\ e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2).$$

2. *(Alternating) For any point* $T \in E[m]$, $e_m(T, T) = 1$. *This implies that for any points* $S, T \in E[m]$

$$e_m(S, T) = e_m(T, S)^{-1}.$$

3. *(Non-degeneracy) For any point* $S \in E[m]$, *if* $e_m(S, T) = 1$ *for all* $T \in E[m]$ *then* $S = \mathcal{O}$.

4. *(Galois invariance) If* $E$ *is defined over* $K$ *and* $\sigma \in \mathrm{Gal}(\overline{K}/K)$ *then for all points* $S, T \in E[m]$

$$e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma).$$

5. *(Compatibility) If* $P \in E[mn]$ *and* $Q \in E[m]$, *then*

$$e_{mn}(P, Q) = e_m([n]P, Q).$$

*Proof.* 1. Bilinearity: (a.)

$$\begin{aligned} e_m(S_1+S_2,T) &= \frac{g(X+S_1+S_2)}{g(X)}\cdot\frac{g(X+S_1)}{g(X+S_1)} \\ &= e_m(S_1,T)\cdot\frac{g(X+S_1+S_2)}{g(X+S_1)} \\ &= e_m(S_1,T)\cdot\frac{g(Y+S_2)}{g(Y)} \\ &= e_m(S_1,T)\cdot e_m(S_2,T). \end{aligned}$$

(b.) Let $f_1, f_2, f_3, g_1, g_2, g_3$ be functions such that for $i = 1,2,3$, $T_i \in E[m]$ and $f_i \in \overline{K}(E)$ such that $\operatorname{div}(f_i) = m(T_i) - m(\mathcal{O})$. Let $T_i' \in E$ such that $[m]T_i' = T_i$ and define $g_i \in \overline{K}(E)$ such that $\operatorname{div}(g_i) = [m]^*(T_i) - [m]^*(\mathcal{O})$. As in (3.2), up to a constant in $\overline{K}^*$, $f_i \circ [m] = g_i^m$. Let $T_3 = T_1 + T_2$, and $h \in \overline{K}(E)$ such that $\operatorname{div}(h) = (T_1+T_2) - (T_1) - (T_2) + (\mathcal{O})$. Consequently

$$\begin{aligned} \operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) &= \operatorname{div}(f_3) - \operatorname{div}(f_1) - \operatorname{div}(f_2) \\ &= m(T_1+T_2) - m(\mathcal{O}) - (m(T_1) - m(\mathcal{O})) - (m(T_2) - m(\mathcal{O})) \\ &= m[(T_1+T_2) - (T_1) - (T_2)' + (\mathcal{O})] \\ &= \operatorname{div}(h)\cdot m \\ &= \operatorname{div}(h^m) \end{aligned}$$

and hence $f_3 = c f_1 f_2 h^m$ for some constant $c \in \overline{K}^*$. Therefore

$$\begin{aligned} g_3^m = f_3 \circ [m] &= (c f_1 f_2 h^m) \circ [m] \\ &= c(f_1 \circ [m])(f_2 \circ [m])(h^m \circ [m]) \\ &= c g_1^m g_2^m (h \circ [m])^m, \end{aligned}$$

and $g_3 = c' g_1 g_2 (h \circ [m])$. Evaluating the pairing by substituting for $g_3$ yields

$$\begin{aligned} e_m(S, T_1 + T_2) = \frac{g_3(X+S)}{g_3(X)} &= \frac{g_1(X+S)g_2(X+S)h([m]X + [m]S)}{g_1(X)g_2(X)h([m]X)} \\ &= e_m(S,T_1)e_m(S,T_2)\frac{h([m]X)}{h([m]X)} \\ &= e_m(S,T_1)e_m(S,T_2) \end{aligned}$$

as desired.

2. Alternating: By the bilinearity property,

$$e_m(S+T, S+T) = e_m(S,S)e_m(S,T)e_m(T,S)e_m(T,T).$$

If for all $T \in E[m]$, $e_m(T,T) = 1$ then

$$e_m(S+T, S+T) = e_m(S,T)e_m(T,S) = 1$$

and the desired result would be obtained. Consider the *translation by* $P$ map $\tau_P$ where

$$\begin{aligned} \tau_P : E &\longrightarrow E \\ R &\mapsto R + P. \end{aligned}$$

The translation by $P$ map induces the map $\tau_P^*$ on $\mathrm{Div}(E)$ as follows,

$$\begin{aligned} \tau_P^* : \mathrm{Div}(E) &\longrightarrow \mathrm{Div}(E) \\ (T) &\mapsto \sum_{Q \in \tau_P^{-1}(T)} e_\tau(Q)(Q). \end{aligned}$$

Hence, $\tau_P^*$ takes $(T)$ to the sum of points that are in the preimage of $T$ under the map $\tau_P$ counting appropriate multiplicity. It is worth noting that this is a

rather simple map with no multiplicity and that there are only single points in the preimage. For example, observe that

$$\begin{aligned}\operatorname{div}(f \circ \tau_{[i]T}) &= \operatorname{div}(\tau^*_{[i]T}(f)) \\ &= m(\tau^*_{[i]T}(T)) - m(\tau^*_{[i]T}(\mathcal{O})) \\ &= m(\tau^{-1}_{[i]T}(T)) - m(\tau^{-1}_{[i]T}(\mathcal{O})).\end{aligned}$$

Let $Q$ be a point that gets mapped to $T$ under $\tau_{[i]T}$. Then

$$T = \tau_{[i]T}(Q) = Q + i[T],$$

and solving for $Q$,

$$Q = [1-i]T.$$

Therefore,

$$\operatorname{div}(f \circ \tau_{[i]T}) = m([1-i]T) - m([-i](T)),$$

and hence

$$\operatorname{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}\right) = m\sum_{i=0}^{m-1}([1-i]T) - ([-i]T) = 0.$$

This implies that $\prod_{i=0}^{m-1}(f \circ \tau_{[i]T})$ is constant.

Composing $f$ first with the function $[m]$ gives $\prod_{i=0}^{m-1}(f \circ [m] \circ \tau_{[i]T})$ which is still a constant function. Raising the product of functions $\prod_{i=0}^{m-1}(g \circ \tau_{[i]T'})$ to the $m^{th}$ power gives

$$\prod_{i=0}^{m-1}(g \circ \tau_{[i]T'})^m = \prod_{i=0}^{m-1}(g^m \circ \tau^m_{[i]T'}) = \prod_{i=0}^{m-1}(g^m \circ \tau_{[i]T})$$

where the latter equality holds, as $\tau^m_{[i]T'}(P) = P + [m][i]T' = P + [i]T = \tau_{[i]T}(P)$. Observe that $\prod_{i=0}^{m-1}(g^m \circ \tau_{[i]T}) = \prod_{i=0}^{m-1}(f \circ [m] \circ \tau_{[i]T})$ by the property that $f \circ [m] = g^m$ and so $\prod_{i=0}^{m-1}(g \circ \tau_{[i]T'})$ is constant.

Thus, evaluating this function at the two points $X$ and $X+T'$ produces the same result, i.e.

$$\prod_{i=0}^{m-1} g(X+[i]T') = \prod_{i=0}^{m-1} g(X+[i+1]T').$$

Cancellation gives

$$g(X) = g(X+[m]T') = g(X+T)$$

and so

$$e_m(T,T) = \frac{g(X+T)}{g(X)} = 1.$$

3. Non-degeneracy: Suppose that for all $S \in E[m]$, $e_m(S,T) = 1$. Since $e_m(S,T) = g(X+S)/g(X)$ then $g(X+S) = g(X)$ for all $S \in E[m]$. By [III.4.10.b Silv] there exists a function $h \in \overline{K}(E)$ such that $g = h \circ [m]$. Then

$$f \circ [m] = g^m = (h \circ [m])^m = h^m \circ [m].$$

Therefore $h^m = f$, and so $m \cdot \mathrm{div}(h) = \mathrm{div}(f) = m(T) - m(\mathcal{O})$, giving that $\mathrm{div}(h) = (T) - (\mathcal{O})$. Finally, [Sil86, III.3.3] states that if $(T) \sim (\mathcal{O})$ then $T = \mathcal{O}$.

4. Galois invariance: Let $\sigma \in G_{\overline{K}/K}$. If $f, g$ are functions for $T$ as above, then $f^\sigma, g^\sigma$ are the corresponding functions for $T^\sigma$. Evaluating the pairing yields

$$e_m(S^\sigma, T^\sigma) = \frac{g^\sigma(X^\sigma + S^\sigma)}{g^\sigma(X^\sigma)} = \left[\frac{g(X+S)}{g(X)}\right]^\sigma = e_m(S,T)^\sigma$$

5. Compatibility: Taking the functions $f$ and $g$ as above,

$$\mathrm{div}(f^n) = nm(T) - nm(\mathcal{O})$$

and

$$(g \circ [n])^{mn} = (f \circ [mn])^n.$$

Therefore,

$$e_{mn}(S,T) = \frac{g \circ [n](X+S)}{g \circ [n](X)} = \frac{g(Y+[n]S)}{g(Y)} = e_m([n]S,T).$$

□

## 3.3 The Computational Description

It is possible to give an alternate, more explicit definition for the Weil pairing. This definition is better suited for computations and facilitates comparisons to other pairings.

**Theorem 3.3.1.** *Let $P, Q \in E[m]$. Let $D$ and $D'$ be divisors of degree zero with disjoint support such that $D \sim (P) - (\mathcal{O})$ and $D' \sim (Q) - (\mathcal{O})$. Let $f_{m,D}$ and $f_{m,D'}$ be functions as defined in § 2.4. Namely,* $\mathrm{div}(f_{m,D}) = mD - D_m$ *and* $\mathrm{div}(f_{m,D'}) = mD' - D'_m$. *The* Weil pairing, $e_m(P,Q)$, *is defined as*

$$\begin{aligned} e_m : E[m] \times E[m] &\longrightarrow \mu_m \\ (P,Q) &\mapsto f_{m,D}(D')/f_{m,D'}(D). \end{aligned} \tag{3.4}$$

For a proof of the equivalence this description of the Weil pairing to the definition of the pairing given by Definition 3.1.1 see [How96]. Note that $D$ and $D'$ are typically chosen to be $D = (P) - (\mathcal{O})$, and $D' = (Q+R) - (R)$, where $R$ is an arbitrarily chosen point on the curve. In a cryptographic setting, the points $P$ and $Q$ are usually taken from the groups $E(\mathbb{F}_q)$ and $E(\mathbb{F}_{q^k})$ respectively. This pairing, like many of the other pairings, is computed using Miller's algorithm which will be described later in Chapter 9.

The following proposition gives yet another description of the Weil pairing. In this case, the functions $f_{m,P}$ and $f_{m,Q}$ are evaluated at points rather than divisors. Other types of pairings are often evaluated in this way, and thus this particular description makes it easier to compare each of the different pairings.

**Proposition 3.3.2.** *Let $E$ be an elliptic curve defined over $\mathbb{F}_q$. Consider the points $P, Q \in E[m]$ such that $P \neq Q$. Then*

$$e_m(P,Q) = (-1)^m \frac{f_{m,P}(Q)}{f_{m,Q}(P)}.$$

For a proof see [Mil04, CC90]. It is interesting to note that in the literature this version of the Weil pairing is often given incorrectly— without the $(-1)^m$ factor.

## 3.4 The Squared Weil Pairing

This pairing was developed by Kirsten Eisenträger, Kristen Lauter, and Peter L. Montgomery [ELM04] in 2004. Although it provides an improvement to the Weil pairing, which will be discused further in Chapter 10, it is still not superior to the Tate pairing or its variants. However, the concepts used in the Squared Tate pairing may be applied to the Tate pairing giving an improvement of the efficiency there.

**Definition 3.4.1.** *The Squared Weil pairing is the composite*

$$\begin{aligned} e_m^2 : E[m] \times E[m] &\xrightarrow{e_m} \quad \mu_m \xrightarrow{\bullet^2} \quad \mu_m \\ (P,Q) &\mapsto \quad e_m(P,Q) \mapsto \quad e_m(P,Q)^2. \end{aligned}$$

**Theorem 3.4.2.** *Let $m \in \mathbb{Z}^+$. Let $P, Q \in E[m]$ such that $P, Q \neq \mathcal{O}$ and $P \neq \pm Q$.*

*Then the Squared Weil pairing admits the following formula*

$$\frac{f_{m,P}(Q)f_{m,Q}(-P)}{f_{m,P}(-Q)f_{m,Q}(P)} = (-1)^m e_m(P,Q)^2.$$

*Proof.* Let $R_1, R_2 \in E$ such that the divisors $D = (P + R_1) - (R_1)$ and $D' = (Q + R_2) - (R_2)$ have disjoint support. Let $D'' = (-Q + R_2) - (R_2)$. Note that the functions $f_{m,D}, f_{m,D'}$ have divisors

$$\mathrm{div}(f_{m,D}) = mD - ([m]P) - (\mathcal{O}) = mD$$

and

$$\mathrm{div}(f_{m,D'}) = mD' - ([m]Q) - (\mathcal{O}) = mD'.$$

From Theorem 3.3.1,

$$e_m(P,Q) = \frac{f_{m,D}((Q + R_2) - (R_2))}{f_{m,D'}((P + R_1) - (R_1))} = \frac{f_{m,D}(Q + R_2)f_{m,D'}(R_1)}{f_{m,D'}(P + R_1)f_{m,D}(R_2)}.$$

Let $g(X) = f_{m,P}(X - R_1)$. Then

$$\mathrm{div}(g) = m(P + R_1) - m(R_1) = mD = \mathrm{div}(f_{m,D}).$$

Therefore $g = cf_{m,D}$ for some constant $c \in \overline{\mathbb{F}}_q^*$ and hence

$$\frac{f_{m,D}(Q + R_2)}{f_{m,D}(R_2)} = \frac{g(Q + R_2)}{g(R_2)} = \frac{f_{m,P}(Q + R_2 - R_1)}{f_{m,P}(R_2 - R_1)}.$$

Likewise,

$$\frac{f_{m,D'}(R_1)}{f_{m,D'}(P + R_1)} = \frac{f_{m,Q}(R_1 - R_1)}{f_{m,Q}(P + R_1 - R_2)}.$$

Substituting into the Weil pairing gives

$$e_m(P,Q) = \frac{f_{m,D}(D')}{f_{m,D'}(D)} = \frac{f_{m,P}(Q + R_2 - R_1)}{f_{m,P}(R_2 - R_1)} \cdot \frac{f_{m,Q}(R_1 - R_2)}{f_{m,Q}(P + R_1 - R_2)}.$$

Similarly for $P, -Q$ :

$$e_m(P,-Q) = \frac{f_{m,P}(-Q+R_2-R_1)}{f_{m,P}(R_2-R_1)} \cdot \frac{f_{m,-Q}(R_1-R_2)}{f_{m,-Q}(P+R_1-R_2)}$$

which reduces to

$$e_m(P,-Q) = \frac{f_{m,P}(-Q+R_2-R_1)}{f_{m,P}(R_2-R_1)} \cdot \frac{f_{m,Q}(-R_1+R_2)}{f_{m,Q}(-P-R_1+R_2)}.$$

Therefore $e_m(P,Q)^2$ can be simplified to

$$\frac{e_m(P,Q)}{e_m(P,-Q)} = \frac{f_{m,P}(Q+R_2-R_1)f_{m,Q}(R_1-R_2)f_{m,Q}(-P-R_1+R_2)}{f_{m,P}(-Q+R_2-R_1)f_{m,Q}(-(R_1-R_2))f_{m,Q}(P+R_1-R_2)}.$$

Letting $R = R_2 - R_1$ gives

$$e_m(P,Q)^2 = \frac{f_{m,P}(Q+R)f_{m,Q}(R)f_{m,Q}(-P+R)}{f_{m,P}(-Q+R)f_{m,Q}(-R)f_{m,Q}(P-R)}. \tag{3.5}$$

Let $P, Q \in E[m]$ such that $P$ is not a multiple of $Q$. Equation (3.5) is a rational function in $R$, call it $\ell(R)$. Since the zeros and poles of $f_{m,P}$ are at $P$ and $\mathcal{O}$ respectively and similarly at $Q$ and $\mathcal{O}$ for $f_{m,Q}$, then $\ell(R)$ can only have zeros and poles at $R \in \{P, Q, -Q, P+Q, P-Q, \mathcal{O}\}$. Although at each of these points the function $\ell$ cannot be evaluated at $R$, there is an equivalent function that behaves like $\ell$ at every other place, except that it has these singularities at $R$ removed. Since $\ell(R) = e_m(P,Q)^2$ for the values of $R$ where $\ell$ does not have a zero or a pole, then this must hold for all values of $R$.

Now, let $f : E \longrightarrow \mathbb{F}_q$ be a rational function on $E$ with a zero of order $m$ at $\mathcal{O}$. Consider the rational function $h(X) = x(X)/y(X)$ that has only a zero of order 1 at $X = \mathcal{O}$. Then the function

$$k = \frac{f}{h^m} = \frac{f}{(x/y)^m} = \frac{fy^m}{x^m}$$

has neither a pole nor a zero at $X = \mathcal{O}$ since $f$ has a zero of order $m$ at $\mathcal{O}$. Then $k(\mathcal{O})$ is finite and nonzero. Consider the function $\phi(X) = h(X)/h(-X)$. Since this function has no zeros or poles on $E$, it is constant. Computing $\phi(X)$ at a finite point $X = (x, y)$ on $E$ with nonzero coordinates gives $\phi = -1$. Let

$$\begin{aligned} g : E &\longrightarrow \mathbb{F}_q \\ X &\mapsto f(X)/f(-X). \end{aligned}$$

Thus

$$g(X) = \frac{f(X)}{f(-X)} = \frac{k(X)h^m(X)}{k(X)h^m(-X)} = \frac{\phi(X)^m k(X)}{k(-X)} = (-1)^m \frac{k(X)}{k(-X)}.$$

This gives that $g(\mathcal{O}) = (-1)^m$ and so

$$\frac{f_{m,Q}(R_1 - R_2)}{f_{m,Q}(-(R_1 - R_2))} = (-1)^m$$

for $R = \mathcal{O}$, i.e. $R_1 = R_2$. By assumption, $f_{m,P}$ has no zeros or poles at $Q$ and similarly, $f_{m,Q}$ has no zeros or poles at $P$ which gives the following simplification

$$e_m(P, Q)^2 = (-1)^m \frac{f_{m,P}(Q) f_{m,Q}(-P)}{f_{m,P}(-Q) f_{m,Q}(P)}.$$

□

### 3.4.1 Computing the Squared Weil Pairing

The Squared Weil pairing is computed using a modified version of Miller's algorithm [Mil86], also Chapter 9, except that the functions are built up and evaluated as follows, to account for the squaring.

$$\begin{aligned} \frac{f_{j+k,P}(Q)/f_{j+k,P}(-Q)}{f_{j+k,Q}(P)/f_{j+k,Q}(-P)} = \frac{f_{j,P}(Q)/f_{j,P}(-Q)}{f_{j,Q}(P)/f_{j,Q}(-P)} \cdot \frac{f_{k,P}(Q)/f_{k,P}(-Q)}{f_{k,Q}(P)/f_{k,Q}(-P)} \\ \cdot \frac{g_{[j]P,[k]P}(Q)/g_{[j]P,[k]P}(-Q)}{g_{[j]Q,[k]Q}(P)/g_{[j]Q,[k]Q}(-P)}. \end{aligned}$$

Because the pairing is a quotient of the Weil pairing evaluated at a point over Weil pairing evaluated at the negative of the point there is cancellation with the secant line terms that is not obtained with the standard Weil pairing. Therefore, there are two less fractions in the Squared Weil pairing than in the Weil pairing which will be more evident in Chapter 10.

# Chapter 4

# The Tate Pairing

Despite some early debate [KM05], it is now commonly accepted that the Tate pairing is more efficient to compute in a general cryptographic setting than the Weil pairing, [GPS06]. John Tate introduced this pairing in *Applications of Galois Cohomology in Algebraic Geometry* [Tat59] in 1959. Stephen Lichtenbaum, a former student of Tate, modified this pairing for computational purposes [Lic69] in 1969. In 1994, Gerhard Frey and Hans-Georg Rück first made use of the Tate pairing in cryptography by expanding upon the MOV attack [FR94]. Five years later, Gerhard Frey and Michael Müller along with Hans-Georg Rück proposed the idea of using the Tate pairing as part of an elliptic curve cryptographic protocol [FMR99]. Note that in the literature the names Tate pairing and Tate-Lichtenbaum pairing are often used interchangeably.

## 4.1 Definition of the Tate Pairing

Let $E$ be an elliptic curve defined over $\mathbb{F}_q$, with $q = p^n$ for some prime $p$. Choose $m$ such that $\gcd(m, q) = 1$. Let $k$ be the unique integer such that $\mathbb{F}_{q^k} = \mathbb{F}_q(\mu_m)$ where $\mu_m$ is the set of $m^{th}$ roots of unity in $\overline{\mathbb{F}}_q^*$. The value $k$ is called the embedding degree and it is the least positive integer such that $m \mid (q^k - 1)$ and unless specified, it is assumed that $k > 1$. Consider the sets $E(\mathbb{F}_{q^k})[m] = \{P \in E(\mathbb{F}_{q^k}) \mid [m]P = \mathcal{O}\}$ and $mE(\mathbb{F}_{q^k}) = \{[m]P \mid P \in E(\mathbb{F}_{q^k})\}$. Let $P \in E(\mathbb{F}_{q^k})[m]$, and $Q \in E(\mathbb{F}_{q^k})$.

**Definition 4.1.1.** *Let $D$ and $D'$ be divisors with disjoint support such that $D = (P) - (\mathcal{O})$ and $D' = (Q + R) - (R)$, for some $R \in E(\mathbb{F}_{q^k})$. As defined in § 2.4, let $f_{i,P}$ be a function (normalized at $\mathcal{O}$) such that* $\mathrm{div}(f_{i,P}) = i(P) - i(\mathcal{O}) - ([i]P) + (\mathcal{O})$ *for $i \in \mathbb{Z}$. The* Tate pairing *is defined as*

$$\begin{aligned} \langle \cdot, \cdot \rangle_m : E(\mathbb{F}_{q^k})[m] \times E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k}) &\longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^m \\ (P, Q) &\mapsto f_{m,P}(D') \pmod{(\mathbb{F}_{q^k}^*)^m}. \end{aligned} \tag{4.1}$$

Note that the element $Q$ is of the form $Q + mE(\mathbb{F}_{q^k})$. However, for a point $S \in mE(\mathbb{F}_{q^k})$,

$$\langle P, Q + mS \rangle_m = \langle P, Q \rangle_m \cdot \langle P, S \rangle_m^m \equiv \langle P, Q \rangle_m \pmod{(\mathbb{F}_{q^k}^*)^m}$$

by bilinearity of the pairing, § 4.2. For simplicity, the element $Q + mE(\mathbb{F}_{q^k})$ will be always written as $Q$.

Alternatively, by the isomorphism $\mathrm{Pic}^0(E) \cong E$ from (2.10), this map can be defined as follows [FR94], which can be used to extend the Tate pairing to hyperelliptic curves. Let $[D]$ and $[D']$ represent equivalence classes in $\mathrm{Pic}^0(E)[m]$ and $\mathrm{Pic}^0(E)$ respectively. Let $D = (P) - (\mathcal{O})$, $D' \sim (Q) - (\mathcal{O})$ and let $f_{m,D}$ be defined as in § 2.4, i.e. with divisor $\mathrm{div}(f_{m,D}) = mD - D_m = mD$. Then

$$\begin{aligned} \langle \cdot, \cdot \rangle_m : \mathrm{Pic}^0_{\mathbb{F}_{q^k}}(E)[m] \times \mathrm{Pic}^0_{\mathbb{F}_{q^k}}(E)/m\,\mathrm{Pic}^0_{\mathbb{F}_{q^k}}(E) &\longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^m \\ ([D], [D']) &\mapsto f_{m,D}(D') \pmod{(\mathbb{F}_{q^k}^*)^m}. \end{aligned} \tag{4.2}$$

Proposition 4.1.3 states that the choice of divisors for the Tate pairing in the divisor equivalence classes is irrelevant. In order to prove this proposition, the following property is required.

**Lemma 4.1.2.** *(Weil Reciprocity law) Let $C$ be a non-singular curve, $K$ a field and $f, g \in \overline{K}(C)^*$ functions such that* $\mathrm{supp}(f) \cap \mathrm{supp}(g) = \emptyset$. *Then*

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)).$$

*Proof.* **Case 1:** Suppose that $C = \mathbb{P}^1$. Let $\mathbb{P}^1$ be identified with $\mathbb{A}^1 \cup \{\mathcal{O}\}$. Looking at the restriction of functions $f$ and $g$ in $\mathbb{P}^1$ to an affine set, these functions are of the form

$$f = \prod_{i=0}^{m} (x - P_i)^{\mathrm{ord}_{P_i}(f)},$$

$$g = \prod_{i=0}^{n} (x - Q_i)^{\mathrm{ord}_{Q_i}(g)}$$

where the divisors of these functions are given by

$$\mathrm{div}(f) = \sum_{i=0}^{m} \mathrm{ord}_{P_i}(f)(P_i),$$

$$\mathrm{div}(g) = \sum_{i=0}^{n} \mathrm{ord}_{Q_i}(g)(Q_i).$$

Suppose that $f$ and $g$ have disjoint support and that their support does not contain the point $\mathcal{O}$. Notice that

$$\begin{aligned} f(\mathrm{div}(g)) = \prod_{i=0}^{n} f(Q_i)^{\mathrm{ord}_{Q_i}(g)} &= \prod_{i=0}^{n}\prod_{i=0}^{m} (Q_i - P_i)^{\mathrm{ord}_{Q_i}(g)\,\mathrm{ord}_{P_i}(f)} \\ &= (-1)^{\sum \mathrm{ord}_{Q_i}(g) \sum \mathrm{ord}_{P_i}(f)} \prod_{i=0}^{n}\prod_{i=0}^{m} (P_i - Q_i)^{\mathrm{ord}_{Q_i}(g)\,\mathrm{ord}_{P_i}(f)} \\ &= \prod_{i=0}^{n}\prod_{i=0}^{m} (P_i - Q_i)^{\mathrm{ord}_{Q_i}(g)\,\mathrm{ord}_{P_i}(f)} \\ &= \prod_{i=0}^{m} g(P_i)^{\mathrm{ord}_{P_i}(f)} = g(\mathrm{div}(f)) \end{aligned}$$

where the fourth equality holds by Proposition 2.4.1. If $\mathcal{O} \in \text{supp}(f)$ or $\mathcal{O} \in \text{supp}(g)$, then $(\mathcal{O} - P_i)/(\mathcal{O} - P_j)$ is defined to be 1 and the proof still holds.

**Case 2:** Let $C$ be an arbitrary curve and $id \in \mathbb{P}^1$ be the identity function. Note that $\text{div}(id) = (0) - (\mathcal{O})$. Using Proposition 2.2.1,

$$\begin{aligned} g^*(\text{div}(id)) &= \text{div}(g^*(id)) \\ &= \text{div}(g \circ id) \\ &= div(g) \end{aligned}$$

where $g^*$ is the map on funtion fields and divisor groups defined in equations (2.1) and (2.5) respectively. Thus, $f(\text{div}(g)) = f(g^*(\text{div}(id))) = (g_*(f))(\text{div}(id))$, where the former equality holds by [Sil86, Ex.2.10] and $g_*$ is the map on function fields defined in equation (2.2). The function $g_*(f)$ is defined on $\mathbb{P}^1$ and by the Weil reciprocity law on $\mathbb{P}^1$ given in Case 1,

$$\begin{aligned} (g_*(f))(\text{div}(id)) &= id(\text{div}(g_* \circ f)) \\ &= (g^*(id))(\text{div}(f)) \\ &= (g \circ id)(\text{div}(f)) \\ &= g(\text{div}(f)). \end{aligned}$$

□

**Proposition 4.1.3.** *In the evaluation of the Tate pairing, the divisors $D$ and $D'$ may be replaced with any divisors $C$ and $C'$ from the equivalence classes $[D]$ and $[D']$ respectively, provided that the support of $C$ is disjoint from that of $C'$.*

*Proof.* Consider $C \in [D]$ and $C' \in [D']$. Note that $C = D + \text{div}(g)$ and $C' = D' + \text{div}(h)$ for some functions $g, h$ defined over $\mathbb{F}_{q^k}$. Let $f'_{m,C}$ be a function such that

$\mathrm{div}(f'_{m,C}) = mC - C_m = mC$ as in § 2.4, and such that $\mathrm{supp}(h) \cap \mathrm{supp}(f'_{m,C}) = \emptyset$. Also, assume that $\mathrm{supp}(C) \cap \mathrm{supp}(g, h, f'_{m,C}) = \emptyset$. Note that

$$\begin{aligned}\mathrm{div}(f'_{m,C}) &= mC \\ &= mD + m\ \mathrm{div}(g) \\ &= \mathrm{div}(f_{m,P}) + \mathrm{div}(g^m).\end{aligned}$$

Then up to a constant in $\mathbb{F}_{q^k}^*$, the equality $f'_{m,C} = f_{m,P} \cdot g^m$ holds. Consider

$$\begin{aligned}f'_{m,C}(C') &= f_{m,P}(C')g(C')^m \\ &= f_{m,P}(D' + \mathrm{div}(h))g(C')^m \\ &= f_{m,P}(D')f_{m,P}(\mathrm{div}(h))g(C')^m \\ &= f_{m,P}(D')h(\mathrm{div}(f_{m,P}))g(C')^m \\ &= f_{m,P}(D')h(D)^m g(C')^m \\ &= f_{m,P}(D') \pmod{(\mathbb{F}_{q^k}^*)^m}.\end{aligned}$$

The fourth equality holds by the Lemma 4.1.2. Therefore, the choice of divisors in the divisor classes $[D]$ and $[D']$ in the Tate pairing is irrelevant. □

A variant, $e$, of the Tate pairing often called the *reduced Tate pairing* [HSV06] is defined as

$$\begin{aligned}e : E(\mathbb{F}_{q^k})[m] \times E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k}) &\longrightarrow \mu_m. \\ (P, Q) &\mapsto \langle P, Q\rangle_m^{(q^k-1)/m}.\end{aligned}$$

Like the Weil pairing, in practice the point $P$ is chosen from the group $E(\mathbb{F}_q)$ and $Q$ from the group $E(\mathbb{F}_{q^k})$. This pairing is better suited to computations as it does not

involve cosets in the codomain, but rather a unique value in $(\mathbb{F}_{q^k}^*)^{(q^k-1)/m}$. Again, by the isomorphism $\mathrm{Pic}^0(E) \cong E$, the reduced Tate pairing can be represented as $\langle D, D' \rangle_m^{(q^k-1)/m}$.

Since by (4.2) the Tate pairing can be expressed as $\langle P, Q \rangle_m = f_{m,D}(D')$ and by (3.4) the Weil pairing as $e_m(P,Q) = f_{m,D}(D')/f_{m,D'}(D)$, the relationship between these two pairings is given by

$$e_m(P,Q) = \frac{\langle P, Q \rangle_m}{\langle Q, P \rangle_m} . \tag{4.3}$$

Note that computing the Weil or Tate pairing reduces to finding the value of the function $f_{m,D}$ (and also $f_{m,D'}$ in the case of the Weil pairing) evaluated at $D'$ ($D$) such that $\mathrm{div}(f_{m,D}) = mD - D_m$ ($\mathrm{div}(f_{m,D'}) = mD' - D'_m$). Miller's algorithm, described more fully in Chapter 9, can be used to compute the value of the necessary function at a given divisor.

## 4.2 Properties of the Tate Pairing

Much like the Weil pairing, the Tate pairing has the following properties.

1. (Bilinearity) For all points $P, P_1, P_2 \in E(\mathbb{F}_{q^k})[m]$, and $Q, Q_1, Q_2 \in E(\mathbb{F}_{q^k})$,

$$\langle P_1 + P_2, Q \rangle_m = \langle P_1, Q \rangle_m \langle P_2, Q \rangle_m ,$$

$$\langle P, Q_1 + Q_2 \rangle_m = \langle P, Q_1 \rangle_m \langle P, Q_2 \rangle_m .$$

2. (Non-degeneracy) For any point $P \in E(\mathbb{F}_{q^k})[m]$, such that $P \neq \mathcal{O}$, there exists a point $Q \in E(\mathbb{F}_{q^k})$ such that $\langle P, Q \rangle_m \neq 1$. Similarly, for any point $Q \in E(\mathbb{F}_{q^k})$ such that $Q \notin mE(\mathbb{F}_{q^k})$ there exists a point $P \in E(\mathbb{F}_{q^k})[m]$ such that $\langle P, Q \rangle_m \neq 1$.

3. (Galois invariance) If $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_{q^k}/\mathbb{F}_q)$ then $\sigma(\langle P, Q\rangle_m) = \langle \sigma(P), \sigma(Q)\rangle_m$.

These properties can be proved using techniques that are similar to those used for the Weil pairing in §3.2. For a more detailed description, see [Gal05, IX.4].

Another property of the Tate pairing that is useful for relating it to its variants is given by the following Theorem.

**Theorem 4.2.1.** *Consider an elliptic curve $E$ defined over $\mathbb{F}_q$. Let $m \mid \#E(\mathbb{F}_q)$ and $k$ be the embedding degree. Suppose that $N = hm$, for some $h \in \mathbb{Z}$ such that $N \mid (q^k - 1)$. Choose $P \in E(\mathbb{F}_q)$ to have order $m$ and $Q \in E(\mathbb{F}_{q^k})$. Then*

$$\langle P, Q\rangle_N^{(q^k-1)/N} = \langle P, Q\rangle_m^{(q^k-1)/m}.$$

*Proof.* Let $D \sim (Q) - (\mathcal{O})$ and $g$ be a function over $\mathbb{F}_q$ such that $\mathrm{div}(g) = m(P) - m(\mathcal{O})$. Then $\mathrm{div}(g^h) = N(P) - N(\mathcal{O})$ and hence

$$\langle P, Q\rangle_N^{(q^k-1)/N} = g^h(D)^{(q^k-1)/N} = g(D)^{(q^k-1)/m} = \langle P, Q\rangle_m^{(q^k-1)/m}.$$

□

The function $f_{m,P}$ in the Tate pairing can be evaluated at a point rather than at a divisor; this is commonly used in the variants of the pairing. The following lemma and theorem show how this may be accomplished.

**Lemma 4.2.2.** *Let $d$ be a divisor of $k$ such that $d < k$. Then the value $q^d - 1$ is a factor of $(q^k - 1)/m$ if $m$ is prime.*

*Proof.* Note that $q^k - 1$ can be factored as

$$q^k - 1 = (q^d - 1) \cdot \sum_{i=0}^{\frac{k}{d}-1} q^{id}.$$

Since the embedding degree $k$ is greater than 1, $m \mid (q^k-1)$ and $m \nmid q^d-1$. Therefore, $m \mid \sum_{i=0}^{\frac{k}{d}-1} q^{id}$ and so $q^d-1$ is a factor of $(q^k-1)/m$. □

**Theorem 4.2.3.** *Let $P \in E(\mathbb{F}_q)[m]$, $Q \in E(\mathbb{F}_{q^k})$ be linearly independent points, and $k > 1$. Then*

$$e(P,Q) = f_{m,P}(Q)^{(q^k-1)/m}.$$

*Proof.* Choose a point $R \in E(\mathbb{F}_q)$ such that $R \notin \{\mathcal{O}, -P, Q, Q-P\}$. Let $C$ be a divisor such that $C = (P+R)-(R)$. Consider a function $f'_{m,C}$ such that $\mathrm{div}(f'_{m,C}) = mC - C_m = m(P+R) - m(P) - ([m]P) + (\mathcal{O}) = m(P+R) - m(P)$. Since $C = (P+R)-(R) \sim (P)-(\mathcal{O}) = D$, this gives that $C = (P)-(\mathcal{O}) + \mathrm{div}(g)$ for some rational function $g$. In the proof of Proposition 4.1.3, the equality $f'_{m,C} = f_{m,P} \cdot g^m$ was demonstrated. Due to the restrictions imposed on the point $R$, the function $f'_{m,C}$ has neither a zero nor a pole at $Q$ or $\mathcal{O}$. Again, by Proposition 4.1.3, the function $f_{m,P}$ in the Tate pairing can be evaluated at any divisor in the divisor class $[D']$ provided that its support is disjoint from the support of $C$. Since $(Q)-(\mathcal{O})$ satisfies this property,

$$e(P,Q) = f'_{m,C}((Q)-(\mathcal{O}))^{(q^k-1)/m} = \frac{f'_{m,C}(Q)^{(q^k-1)/m}}{f'_{m,C}(\mathcal{O})^{(q^k-1)/m}}.$$

Because the points $P+R, R \in E(\mathbb{F}_q)$, $f'_{m,C}$ may be chosen so that $f'_{m,C} \in \mathbb{F}_q(E)$ which implies $f'_{m,C}(\mathcal{O}) \in \mathbb{F}_q^*$. By Lemma 4.2.2, $(q-1) \mid (q^k-1)/m$ and hence

$$f'_{m,C}(\mathcal{O})^{(q^k-1)/m} = (f'_{m,C}(\mathcal{O})^{q-1})^{(q^k-1)/m(q-1)} = 1.$$

Therefore $e(P,Q) = f'_{m,C}(Q)^{(q^k-1)/m}$. Note that $g(Q) \in \mathbb{F}_{q^k}^*$ and so

$$f'_{m,C}(Q)^{(q^k-1)/m} = f_{m,P}(Q)^{(q^k-1)/m} \cdot g(Q)^{q^k-1} = f_{m,P}(Q)^{(q^k-1)/m}.$$

□

## 4.3 The Squared Tate Pairing

This pairing was created in 2003 by Eisenträger et al. [ELM04], the same authors who created the Squared Weil pairing, in an effort to improve the efficiency of the Tate pairing. Under certain circumstances, less operations are required for computing the Squared Tate pairing versus Tate pairing, as will be described further in Chapter 10. The Squared Tate pairing is based upon the same principles used for the Squared Weil pairing.

**Definition 4.3.1.** *The Squared Tate pairing is the composite*

$$\begin{aligned} v_m = e^2 : E(\mathbb{F}_{q^k})[m] \times E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k}) \xrightarrow{e} \quad & \mu_m \xrightarrow{\bullet^2} \quad \mu_m \\ (P,Q) \mapsto \quad & e(P,Q) \mapsto \quad e(P,Q)^2 \end{aligned}$$

*where e is the reduced Tate pairing.*

**Theorem 4.3.2.** *Let $m \in \mathbb{Z}$, let $E$ be an elliptic curve defined over $\mathbb{F}_q$ such that $m \mid (q^k - 1)$. Consider points $P \in E(\mathbb{F}_{q^k})[m]$ and $Q \in E(\mathbb{F}_{q^k})$ such that $P, Q \neq \mathcal{O}$ and are linearly independent. Consider the divisor $D \sim (P) - (\mathcal{O})$ and the function $f_{m,P}$ on $E$ such that $\mathrm{div}(f_{m,P}) = m(P) - m(\mathcal{O}) - ([m]P) + (\mathcal{O})$. The Squared Tate pairing admits the following formula*

$$v_m(P,Q) = \left(\frac{f_{m,P}(Q)}{f_{m,P}(-Q)}\right)^{(q^k-1)/m}.$$

Note that this proof is analogous to the proof of the Squared Weil pairing except that there is no $(-1)^m$ factor involved.

*Proof.* Let $R_1, R_2 \in E$ such that the divisors $D = (P + R_1) - (R_1)$, $D' = (Q + R_2) - (R_2)$ have disjoint support. Let $D'' = (-Q + R_2) - (R_2)$. The proof follows from

the proof of the Squared Weil pairing, except that the term $f_{m,D'}(D)$ need not be computed. This gives that

$$\langle P,Q\rangle_m^2 = \frac{\langle P,Q\rangle_m}{\langle P,-Q\rangle_m^2} = \frac{f_{m,P}(Q+R_2-R_1)}{f_{m,P}(-Q+R_2-R_1)}.$$

Using the same reasoning as in the Weil case, $R_2$ can be chosen to equal $R_1$. Raising to the appropriate exponent gives the desired result, namely

$$e(P,Q)^2 = \left(\frac{f_{m,P}(Q)}{f_{m,P}(-Q)}\right)^{(q^k-1)/m} = v_m(P,Q).$$

□

### 4.3.1 Computing the Squared Tate Pairing

The method used for computing the Squared Tate pairing is similar to the approach for the Squared Weil pairing, which in turn uses the same principles as Miller's algorithm (Chapter 9). The functions are built up and evaluated as follows,

$$\frac{f_{j+k,P}(Q)}{f_{j+k,P}(-Q)} = \frac{f_{j,P}(Q)}{f_{j,P}(-Q)} \cdot \frac{f_{k,P}(Q)}{f_{k,P}(-Q)} \cdot \frac{g_{[j]P,[k]P}(Q)}{g_{[j]P,[k]P}(-Q)}.$$

Again, like the Squared Weil pairing, there is cancellation with the functions $g_{[j+k]P}(Q)$ and $g_{[j+k],P}(-Q)$, as the vertical lines through $[j+k]P$ evaluated at $Q$ and $-Q$ are equal.

# Chapter 5

# The Eta pairing

The Eta pairing is a generalization of the ideas originally presented by Iwan Duursma and Hyang-Sook Lee [DL03] in 2003 on a specific hyperelliptic curve. In 2007, Paulo S. L. M. Barreto, Steven Galbraith, Colm Ó'hÉigeartaigh and Michael Scott [BGOS07] developed the Eta pairing which extends the ideas of Duursma and Lee to more supersingular elliptic and hyperelliptic curves. To date, it is the only pairing that has been designed explicitly for such curves. Due to erroneous statements about their efficiency, misconceptions about their security and their seemingly simple form[1], supersingular elliptic curves have not been popular choices for uses in cryptography [KM05]. This is likely due to the fact that in cryptographic settings that do not involve pairings, supersingular curves are typically avoided [FST06]. However, making use of these curves provides a greater selection for pairing based cryptosystems and some of the most efficient pairing computations to date have utilized supersingular hyperelliptic curves [BGOS07].

## 5.1 Supersingular Elliptic Curves

The Eta pairing requires the elliptic curve $E$ to be supersingular. A supersingular curve can be defined as follows.

[1] An example of a simplistic supersingular elliptic curve is $E : y^2 = x^3 - 1$ defined over $\mathbb{F}_q$ with $q \equiv -1 \pmod 6$.

**Definition 5.1.1.** *Let $E$ be an elliptic curve defined over $\mathbb{F}_q$, where $q = p^n$ for some $n \in \mathbb{Z}$ and a prime $p$. $E$ is said to be supersingular if one of the following (equivalent) conditions holds.*

1. $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$ *in which case* $p \mid t$ *where* $\#E(\mathbb{F}_q) = q + 1 - t$.
2. $E(\overline{\mathbb{F}}_q)[p] = \{\mathcal{O}\}$.
3. *The ring of endomorphisms of $E$ defined over $\overline{\mathbb{F}}_q$ is non-commutative.*

For a proof of the equivalence of these conditions, see [Sil86, V.3].

Define a *distortion map* as an endomorphism that maps a point from $E(\mathbb{F}_q)$ to $E(\mathbb{F}_{q^k})$. Making use of such a map, another property of supersingular curves is given by the following theorem.

**Theorem 5.1.2.** *Let $E$ be an elliptic curve defined over $\mathbb{F}_q$. If $E$ has a distortion map then it is supersingular.*

*Proof.* Consider a point $P \in E(\mathbb{F}_q)$, then $\pi_q(P) = P$, where $\pi_q$ is the $q^{th}$ power Frobenius map. Let $\phi$ be a distortion map such that $\phi(P) \notin E(\mathbb{F}_q)$. Note that $\phi(\pi_q(P)) = \phi(P) \neq \pi_q(\phi(P))$. Since both $\pi_q, \phi \in \mathrm{End}(E)$, $\mathrm{End}(E)$ is non-commutative, and hence $E$ is supersingular by the third condition in Definition 5.1.1. □

Finally, another interesting property of supersingular curves is that the embedding degree is always less than or equal to 6 [MOV93].

## 5.2 Defining the Eta Pairing

Let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_q$ with $q$ a power of a prime such that the embedding degree is even. Let $\phi$ be a distortion map that allows

denominator elimination; that is if $P \in E(\mathbb{F}_q)$ then the $x-$coordinate of $\phi(P)$ is defined over $\mathbb{F}_{q^{k/2}}$.

**Definition 5.2.1.** *(The Eta pairing) Choose $N \in \mathbb{Z}$ such that $m \mid N \mid (q^k - 1)$. Let $D$, $D'$ be reduced divisors on $E$ that represent divisor classes of order dividing $N$; that is, $[D], [D'] \in \mathrm{Pic}^0(E)[N]$ and let $D = (P) - (\mathcal{O})$. As defined in 2.4, let $f_{i,P}$ be a function such that $\mathrm{div}(f_{i,P}) = i(P) - i(\mathcal{O}) - ([i]P) + (\mathcal{O})$[†]. For any integer $T$ the Eta pairing is defined as*

$$\begin{aligned} \eta_T : \mathrm{Pic}^0(E)[N] \times \mathrm{Pic}^0(E)/N\,\mathrm{Pic}^0(E) &\longrightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^N \\ ([D], [D']) &\mapsto f_{T,P}(\phi(D')). \end{aligned}$$

*The Eta pairing on points $P, Q$ is defined as*

$$\eta_T(P, Q) = \eta_T((P) - (\mathcal{O}), (Q) - (\mathcal{O})).$$

A special case of this pairing, when $T = q$, gives the pairing defined by I. Duursma and H. Lee [DL03] for a specific class of supersingular hyperelliptic curves; this was the motivation for the development of the Eta pairing. P. Barreto, S. Galbraith, C. Ó'hÉigeartaigh and M. Scott [BGOS07] improved the Eta pairing's efficiency by taking $T = q - N$.

## 5.3 Relating the Eta Pairing to the Tate Pairing

The following theorem relates the Eta pairing to the Tate pairing and hence shows that the Eta pairing is both non-degenerate and bilinear.

[†] *If $i < 0$ then $iD$ is written as $(-i)(-D)$ and* $\mathrm{div}(f_{i,P}) = (-i)(-P) - (-i)(\mathcal{O}) - ([-i](-P)) + (\mathcal{O})$.

**Theorem 5.3.1.** *Let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_q$ with even embedding degree $k \geq 2$ and distortion map $\phi$. Let $D$ be a divisor on $E$ defined over $\mathbb{F}_q$ with order dividing $N \in \mathbb{N}$. Choose $T \in \mathbb{Z}$ such that*

1. *$TD \sim \gamma(D)$ in the divisor class group where $\gamma$ is an automorphism of $E$ which is defined over $\mathbb{F}_q$.*
2. *$\gamma$ and $\phi$ satisfy the condition that $\gamma\phi^q(Q) = \phi(Q)$ for all points $Q \in E(\mathbb{F}_q)$.*
3. *$T^a + 1 = LN$ for some $a \in \mathbb{N}$ and $L \in \mathbb{Z}$.*
4. *$T = q + cN$ for some $c \in \mathbb{Z}$.*

*Then*

$$(\langle D, \phi(D')\rangle_N^{(q^k-1)/N})^L = (\eta_T(D, D')^{(q^k-1)/N})^{aT^{a-1}}.$$

In Chapter 6 it will be shown that this pairing is simply a version of the Ate pairing[2]. For this reason, the proof of this theorem will be omitted until that time. The Eta pairing can be defined in a much simpler way [HSV06] as

$$\begin{aligned} \eta_T : G_1 \times G_2 &\longrightarrow \mu_m \\ (P, Q) &\mapsto f_{T,P}(Q), \end{aligned}$$

where the definition of the groups $G_1$ and $G_2$ will be given in § 6.2. The relation between the Tate and Eta pairing is given as

$$e(P, Q)^L = f_{T,P}(Q)^{c(q^k-1)/M}$$

[2]The original version of this proof contains unnecessary details that the authors of [HSV06] manage to work around. In particular, the use of the automorphism $\gamma$ is avoided altogether.

where $M = \gcd(q^k - 1, T^k - 1)$, $L = (T^k - 1)/M$ and

$$c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \pmod{m}.$$

Although Theorem 5.3.1 relates the Eta pairing to the Tate pairing, a further exponentiation is required to obtain the correct value for the exponent of the reduced Tate pairing; the authors of [BGOS07] indicate that as an alternative, a cryptosystem could be designed around the Eta pairing which would alleviate this requirement. However, since it may not be desirable to work with a non-standard pairing, converting the Eta pairing to the Tate pairing may be required. Despite this additional step, the Eta pairing is still more efficient to compute than the Tate pairing for the supersingular curves defined over finite fields of characteristic 2 and 3 examined in [BGOS07].

Another advantage of the Eta pairing is in the case where it is desirable for points $P$ and $Q$ to be linearly dependent. Most pairings are degenerate in this case. For instance, if $Q = [\ell]P$ for some $\ell \in \mathbb{Z}$, then

$$e(P, Q) = (P, [\ell]P) = e(P, P)^\ell = 1^\ell = 1.$$

Using a supersingular curve, a distortion map $\phi$ can be used so that $\phi(P) \notin \langle P \rangle$ and so the Eta pairing applied to linearly dependent points need not be degenerate.

# Chapter 6

# The Ate Pairing

The Ate pairing is a generalized version of the Eta pairing and can be extended to ordinary curves as well as supersingular curves. This pairing was created by Florian Heß, Nigel Smart, and Frederik Vercauteren [HSV06] in 2006. The name was chosen based upon the fact that this pairing is very much like the Tate pairing, but under certain circumstances it is more efficient, see Chapter 10, so removing the 'T' from the name represents the accelerated computation. Since it is also like the Eta pairing in various ways, except that the arguments for the pairing are reversed, then noting that Ate is Eta spelled backwards is also rather fitting.

## 6.1 Defining the Ate Pairing

Typically the Tate pairing is defined on $G_1 \times G_2$ with the groups $G_1 = E(\mathbb{F}_{q^k})[m]$ and $G_2 = E(\mathbb{F}_{q^k})/mE(\mathbb{F}_{q^k})$. In practice however, subgroups of the form

$$G_1 = E[m] \cap \mathrm{Ker}(\pi_q - [1]), \tag{6.1}$$

$$G_2 = E[m] \cap \mathrm{Ker}(\pi_q - [q]) \tag{6.2}$$

are often used to speed up the computations where

$$\begin{aligned} \pi_q - [1] : E &\longrightarrow E \\ (x, y) &\mapsto (x^q, y^q) - (x, y) \end{aligned}$$

and

$$\begin{aligned} \pi_q - [q] : E &\longrightarrow E \\ (x,y) &\mapsto (x^q, y^q) - [q](x,y). \end{aligned}$$

Computing the Tate pairing on the cross product $G_2 \times G_1$ is less complicated from a theoretical stand point, which will become more evident in § 6.2. It is with these ideas that the Ate pairing is defined.

**Definition 6.1.1.** *(Ate pairing) Let $E$ be an elliptic curve defined over $\mathbb{F}_q$ and $m$ be a large prime such that $m \mid \#E(\mathbb{F}_q)$. Define $t$ by $\#E(\mathbb{F}_q) = q + 1 - t$. The quantity $t$ is called the trace of Frobenius acting on $E(\overline{\mathbb{F}_q})$. Denote $T = t - 1$ and choose $Q \in G_2$, $P \in G_1$ for $G_2, G_1$ defined in (6.2) and (6.1), respectively. Let $f_{T,Q}$ be the function defined in § 2.4, such that* $\operatorname{div}(f_{T,Q}) = T(Q) - T(\mathcal{O}) - ([T]Q) + (\mathcal{O})$. *The Ate pairing, $a_T$, is defined as follows,*

$$\begin{aligned} a_T : G_2 \times G_1 &\longrightarrow \mu_m \\ (Q,P) &\mapsto f_{T,Q}(P). \end{aligned}$$

The following series of lemmata will be required for relating the Ate pairing to the Tate pairing.

Let $N \in \mathbb{Z}$ such that $N = \gcd(T^k - 1, q^k - 1)$ where $m \mid N$. Denote $(T^k - 1)/N$ by $L$.

**Lemma 6.1.2.** *The Ate pairing with parameter $T^k$ is related to the reduced Tate pairing by the equality,*

$$e(Q,P)^L = f_{T^k,Q}(P)^{(q^k-1)/N} = a_{T^k}(Q,P)^{(q^k-1)/N}.$$

*Proof.* By definition,

$$e(Q,P) = \langle Q,P\rangle_m^{(q^k-1)/m} = f_{m,Q}(P)^{(q^k-1)/m}.$$

Lemma 4.2.1 implies that

$$f_{m,Q}(P)^{(q^k-1)/m} = f_{N,Q}(P)^{(q^k-1)/N}$$

since $m \mid N \mid (q^k-1)$. The divisors of the functions $f_{N,Q}^L$ and $f_{LN,Q}$ are given by

$$\mathrm{div}(f_{N,Q}^L) = L(N(Q) - N(\mathcal{O}) - ([N]Q) + (\mathcal{O})) = \mathrm{div}(f_{N,D}^L),$$

$$\mathrm{div}(f_{LN,Q}) = LN(Q) - LN(\mathcal{O}) - ([LN]Q) + (\mathcal{O})) = \mathrm{div}(f_{LN,D})$$

for $D = (Q) - (\mathcal{O}) \in [D]$, where $[D] \in \mathrm{Pic}^0(E)[m]$. Since the order of $D$ divides $N$ then

$$N(Q) - N(\mathcal{O}) \sim 0 \sim (\mathcal{O}) - (\mathcal{O}).$$

By the isomorphism $\sigma : \mathrm{Pic}^0(E) \longrightarrow E$ from equation (2.10), $\sigma(N((Q) - (\mathcal{O}))) = [N]Q$ and $\sigma((\mathcal{O}) - (\mathcal{O})) = \mathcal{O}$. Since $N(Q) - N(\mathcal{O}) \sim (\mathcal{O}) - (\mathcal{O})$, then $[N]Q = \mathcal{O}$. Up to a constant in $\mathbb{F}_q^*$,

$$f_{N,Q}^L = f_{LN,Q}.$$

Consider

$$\begin{aligned} e(Q,P)^L &= f_{N,Q}(P)^{L(q^k-1)/N} \\ &= f_{LN,Q}(P)^{(q^k-1)/N} \\ &= f_{T^k-1,Q}(P)^{(q^k-1)/N} \end{aligned}$$

where the third equality holds by definition of $L$. Finally, all that remains to be shown is that the parameter $T^k - 1$ can be replaced with $T^k$. Since $T^k - 1 = LN$

and the order of $Q$ divides $m$ which in turn divides $N$, $[T^k - 1]Q = \mathcal{O}$ and so

$$\begin{aligned}\operatorname{div}(f_{T^k-1,Q}) &= (T^k - 1)(Q) - (T^k - 1)(\mathcal{O}) - ([T^k - 1]Q) + (\mathcal{O}) \\ &= (T^k)(Q) - (T^k)(\mathcal{O}) - (Q) + (\mathcal{O}).\end{aligned}$$

Observe that $[T^k]Q = [T^k - 1]Q + Q = Q$, hence

$$\begin{aligned}\operatorname{div}(f_{T^k,Q}) &= T^k(Q) - T^k(\mathcal{O}) - ([T^k]Q) + (\mathcal{O}) \\ &= T^k(Q) - T^k(\mathcal{O}) - (Q) + (\mathcal{O}) \\ &= \operatorname{div}(f_{T^k-1,Q}).\end{aligned}$$

This implies that up to a constant in $\mathbb{F}_q^*$, $f_{T^k-1,Q} = f_{T^k,Q}$ giving the desired result that

$$e(Q,P)^L = f_{T^k,Q}(P)^{(q^k-1)/N}.$$

□

**Lemma 6.1.3.** *For $T = t - 1$, where $t$ is the trace of Frobenius, the function $f_{T^k,Q}$ can be chosen such that*

$$f_{T^k,Q} = f_{T,Q}^{T^{k-1}} f_{T,[T]Q}^{T^{k-2}} \cdots f_{T,[T^{k-1}]Q}.$$

*Proof.* Observe that

$$\begin{aligned}\operatorname{div}(f_{T,Q}^{T^{k-1}} f_{T,[T]Q}^{T^{k-2}} \cdots f_{T,[T^{k-1}]Q}) &= T^k(Q) - T^k(\mathcal{O}) - T^{k-1}([T]Q) + T^{k-1}(\mathcal{O}) \\ &\quad + T^{k-1}([T]Q) - T^{k-1}(\mathcal{O}) - T^{k-2}([T^2]Q) + T^{k-2}(\mathcal{O}) \\ &\quad \vdots \\ &\quad + T([T^{k-1}]Q) - T(\mathcal{O}) - ([T^k]Q) + (\mathcal{O}) \\ &= \operatorname{div}(f_{T^k,Q})\end{aligned}$$

and so up to a constant in $\mathbb{F}_q^*$, $f_{T^k,Q} = f_{T,Q}^{T^{k-1}} f_{T,[T]Q}^{T^{k-2}} \cdots f_{T,[T^{k-1}]Q}$. □

**Lemma 6.1.4.** *For each point $Q$ in the group $G_2$,*

$$f_{T,\pi_q^i(Q)} = f_{T,Q}^{\sigma^i}$$

*where $\sigma$ is the $q^{th}$ power Frobenius endomorphism.*

*Proof.* For every point $Q \in G_2$, $\pi_q(Q) = [q]Q = [t-1]Q = [T]Q$, hence, $\pi_q^i(Q) = [T^i]Q$. With this property,

$$\begin{aligned}\operatorname{div}(f_{T,\pi_q^i(Q)}) &= T(\pi_q^i(Q)) - T(\mathcal{O}) - ([T](\pi_q^i(Q))) + (\mathcal{O}) \\ &= T(\pi_q^i(Q)) - T(\mathcal{O}) - (\pi_q^{i+1}(Q)) + (\mathcal{O}).\end{aligned}$$

Since $\pi_q$ is of degree $q$ and purely inseparable,

$$\begin{aligned}(\pi_q^i)^*(\operatorname{div}(f_{T,\pi_q^i(Q)})) &= \operatorname{div}((\pi_q^i)^*(f_{T,\pi_q^i(Q)})) \\ &= q^i T(Q) - q^i T(\mathcal{O}) - q^i(\pi_q(Q)) + q^i(\mathcal{O}) \\ &= \operatorname{div}(f_{T,Q}^{q^i})\end{aligned}$$

Also, by Theorem 2.2.1,

$$(\pi_q^i)^*(\operatorname{div}(f_{T,\pi_q^i(Q)})) = \operatorname{div}(f_{T,\pi_q^i(Q)} \circ \pi_q^i)$$

and hence up to a scalar multiple in $\mathbb{F}_q^*$

$$f_{T,\pi_q^i(Q)} \circ \pi_q^i = f_{T,Q}^{q^i}.$$

Note that $q^i$ can be interpreted as an action of Frobenius and thus $f_{T,Q}^{q^i}$ can be written as $f_{T,Q}^{\sigma^i} \circ \pi_q^i$ implying that $f_{T,\pi_q^i(Q)} \circ \pi_q^i = f_{T,Q}^{\sigma^i} \circ \pi_q^i$. The desired result, $f_{T,\pi_q^i(Q)} = f_{T,Q}^{\sigma^i}$, follows since $\pi_q^i$ is in the group of automorphisms of $E$ and hence the cancellation law holds. □

The following Theorem describes the conditions under which the Ate pairing is non-degenerate. Also, it relates the reduced Ate pairing to the reduced Tate pairing.

**Theorem 6.1.5.** *Let $E$ be an elliptic curve over $\mathbb{F}_q$, $m$ a large prime such that $m \mid \#E(\mathbb{F}_q)$, $k$ the embedding degree and $t$ the trace of Frobenius. For $T = t - 1$, $Q \in G_2 = E[m] \cap \mathrm{Ker}(\pi_q - [q])$ and $P \in G_1 = E[m] \cap \mathrm{Ker}(\pi_q - [1])$, the following hold.*

1. *$a_T(Q, P) = f_{T,Q}(P)$ is a bilinear pairing.*
2. *For $N = \gcd(T^k - 1, q^k - 1)$, $T^k - 1 = LN$,*

$$e(Q, P)^L = f_{T,Q}(P)^{c(q^k-1)/N}$$

*where $e$ is the reduced Tate pairing and*

$$c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \pmod{m}.$$

3. *If $m$ does not divide $L$ then the pairing is non-degenerate.*

*Proof.* Recall that

$$\begin{aligned} f_{T^k,Q}(P) &= f_{T,Q}(P)^{T^{k-1}} f_{T,[T]Q}(P)^{T^{k-2}} \cdots f_{T,[T^{k-1}]Q}(P) \quad (\textit{Lemma } 6.1.3) \\ &= f_{T,Q}(P)^{T^{k-1}} f_{T,\pi_q(Q)}(P)^{T^{k-2}} \cdots f_{T,\pi_q^{k-1}(Q)}(P) \\ &= f_{T,Q}(P)^{T^{k-1}} f_{T,Q}(P)^{T^{k-2}q} \cdots f_{T,Q}(P)^{q^{k-1}} \quad (\textit{Lemma } 6.1.4) \\ &= f_{T,Q}(P)^c \end{aligned}$$

where $c = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \pmod{m}$. In summary, $f_{T^k,Q}(P) = f_{T,Q}(P)^c$ and therefore Lemma 6.1.2 gives

$$e(Q, P)^L = f_{T^k,Q}(P)^{(q^k-1)/N} = f_{T,Q}(P)^{c(q^k-1)/N}.$$

This shows that the Ate pairing is bilinear. If $m$ does not divide $L$, the Ate pairing is a non-degenerate pairing since the reduced Tate pairing is non-degenerate. $\square$

Like the Tate pairing, the Ate paring can be given in a reduced form. By convention, $m$ is chosen so that $m^2 \nmid (q^k - 1)$ and hence $m^2 \nmid N$. Denoting $N = ms$ for some integer $s$, then $m \nmid s$. Also, in practice, $m$ is much larger than $k$ thus $m \nmid k$. Since $m \mid q^k - 1$, $m \nmid q$ and so $m \nmid c$ where $c \equiv kq^{k-1} \pmod{m}$. Denoting $M$ as $M \equiv Lsc^{-1} \pmod{m}$, the reduced Ate pairing can be defined as

$$e(Q,P)^M = e(Q,P)^{Ls/c} = f_{T,Q}(P)^{(q^k-1)/m}.$$

## 6.2 A Different Approach for the Ate Pairing

For a slightly more complicated procedure defining the Ate pairing, consider the pairing on $G_1 \times G_2$. The first step will be to give a different representation for the groups $G_1$ and $G_2$. Let $\hat{\pi}_q$ denote the dual isogeny of $\pi_q$, called the Verschiebung, where $\hat{\pi}_q \circ \pi_q = [q]$.

Note that for $P \in G_1 = E[m] \cap \mathrm{Ker}(\pi_q - [1])$,

$$[q]P = (\hat{\pi}_q \circ \pi_q)(P) = \hat{\pi}_q(P)$$

since $\pi_q(P) = P$. Hence another representation for $G_1$ is given by $G_1 = E[m] \cap \mathrm{Ker}(\hat{\pi}_q - [q])$.

Similarly, for $Q \in G_2 = \mathrm{Ker}(\pi_q - [q])$,

$$\pi_q(Q) = [q]Q = (\hat{\pi}_q \circ \pi_q)(Q) = \hat{\pi}_q(\pi_q(Q)). \tag{6.3}$$

For a point $Q \in G_2$ consider the subgroup $\langle Q \rangle$ of $G_2$;

$$\pi_q(Q) = [q]Q \in \langle Q \rangle \subseteq G_2$$

and since $Q$ was chosen arbitrarily, $\pi_q(G_2) = G_2$. Using (6.3), this implies that for a given point $Q$, $\hat{\pi}_q(Q) = Q$. Therefore, another representation for $G_2$ is given by $G_2 = E[m] \cap \mathrm{Ker}(\hat{\pi}_q - [1])$.

In order to define the Ate pairing on $G_1 \times G_2$ a few modifications are required. The properties of the Ate pairing given by Theorem 6.1.5 still holds in the case of the Ate pairing on $G_2 \times G_1$ except that Lemma 6.1.4 may require modification depending upon whether $E$ is a supersingular or an ordinary elliptic curve.

**Case 1:** Let $E$ be a supersingular elliptic curve. By definition [Sil86, V.3.1], $E[q^i] = \{\mathcal{O}\}$ and the map $\hat{\pi}_q^i$ is purely inseparable of degree $q^i$. Lemma 6.1.4 implies that

$$f_{T,\hat{\pi}_q^i(P)} \circ \hat{\pi}_q^i = f_{T,P}^{q^i}.$$

Since $\hat{\pi}_q(Q) = Q$ for $Q \in G_2$ then

$$(f_{T,\hat{\pi}_q^i(P)} \circ \hat{\pi}_q^i)(Q) = f_{T,\hat{\pi}_q^i(P)}(Q) = (f_{T,P}(Q))^{q^i}.$$

Finally, by Theorem 6.1.5,

$$e(P,Q)^L = f_{T,P}(Q)^{c(q^k-1)/N}$$

where $c = \sum_{i=0}^{k-i} T^{k-1-i} q^i = kq^{k-1} \pmod{m}$.

This particular case gives a lovely description of the *Eta pairing* that is more simplified in contrast to the definition of the pairing given in Chapter 5.

**Case 2:** Let $E$ be an ordinary elliptic curve. Then, by definition [Sil86, V.3.1], $E[q^i] \cong \mathbb{Z}/q^i\mathbb{Z}$ and the map $\hat{\pi}_q^i$ is separable. Note that $\mathrm{Ker}(\hat{\pi}_q^i) = E[q^i]$, and hence $\mathrm{Ker}(\hat{\pi}_q^i)$ is not equivalent to $\{\mathcal{O}\}$ as before, which makes it difficult to relate $f_{T,\hat{\pi}_q^i(P)} \circ \hat{\pi}_q^i$ to $f_{T,P}$ as is needed in the proof of Lemma 6.1.4 for the Ate pairing.

However, using a twist of the elliptic curve it is possible to get around this problem, which will be addressed in Chapter 7.

## 6.3 The Optimised Ate Pairing

This pairing is a generalized version of the Ate pairing where the parameter $T$ is replaced with any integer that is congruent to $q$ modulo $m$. The parameter is chosen to be of minimal absolute value, hence optimizing the Ate pairing in certain circumstances. In 2007, this pairings was developed by Florian Heß, Naoki Kanayama, Seiichi Matsuda, and Eiji Okamoto [HKMO07].

The following theorem gives a description of the Optimised Ate pairing and relates the pairing to the reduced Tate pairing.

**Theorem 6.3.1.** *Let $E$ be an elliptic curve defined over $\mathbb{F}_q$. Let $S \in \mathbb{Z}$ such that $S \equiv q \pmod{m}$. Let $N = \gcd(S^k - 1, q^k - 1) > 0$ and $L = (S^k - 1)/N$. Let $c_S = \sum_{i=0}^{k-i} S^{k-1-i} q^i \pmod{N}$. Then*

$$\begin{aligned} a_S : G_2 \times G_1 &\longrightarrow \mu_m \\ (Q, P) &\mapsto f_{S,Q}(P)^{c_S(q^k-1)/N} \end{aligned}$$

*is a bilinear pairing.*

*If $m$ does not divide $L$ then this pairing is non-degenerate.*

*The Optimised Ate pairing can be related to the reduced Tate pairing as follows*

$$a_S(Q, P) = e(Q, P)^L.$$

The proof of this theorem is analogous to the proof of Theorem 6.1.5 for the Ate pairing. The pairing also gives improvements to the Ate pairing for certain

embedding degrees and composite group orders which will be addressed in Chapter 10.

## 6.4 The Ate$_i$ Pairing

This pairing is like the Optimised Ate pairing in that it generalizes the Ate pairing, but does so in a different way. The parameter $T$ is now replaced with a power $i$ of $T$ modulo $m$ for an $i$ within a certain range and can be computed efficiently for curves with small trace values. This pairing was developed by Jiwu Huang, Fangguo Zhang and Chang-An Zhao in 2008 [HZZ08].

In a manner similar to § 6.3, the subsequent theorem gives a description of the Ate$_i$ pairing and provides the relationship that equates it to the Tate pairing.

**Theorem 6.4.1.** *Consider an elliptic curve $E$ defined over a finite field $\mathbb{F}_q$ with $q$ a power of a prime. Let $m$ be a large prime such that $m \mid \#E(\mathbb{F}_q)$, $t$ the trace of Frobenius, $k$ the embedding degree and $T = t-1$. Consider $T_i = T^i \equiv q^i \pmod{m}$ for $0 < i < k$. Choose $Q \in G_2 = E[m] \cap \mathrm{Ker}(\pi_q - [q])$ and $P \in G_1 = E[m] \cap \mathrm{Ker}(\pi_q - [1])$. Consider the following:*

1. *$a_{T_i}(Q,P) = f_{T_i,Q}(P)$ is a bilinear pairing.*
2. *Let $\ell$ be the least positive integer such that $(T_i)^\ell \equiv 1 \pmod{m}$. Let $N = \gcd(T_i^\ell - 1, q^k - 1)$ and $T_i^\ell - 1 = LN$, then*

$$e(Q,P)^L = f_{T_i,Q}(P)^{c(q^k-1)/N}$$

   *where $e$ is the reduced Tate pairing and $c \equiv \sum_{j=0}^{\ell-1} T_i^{\ell-1-j}(q^i)^j \pmod{N}$.*

3. *If $m$ does not divide $L$ this pairing is non-degenerate.*

The proof follows in an analogous fashion to the proof of Theorem 6.1.5 for the Ate pairing.

In optimizing the computation of this pairing, the idea is to compute $T_i = T^i \equiv q^i \pmod{m}$ for each $i \in \mathbb{Z}$ such that $0 < i < k$ and to select the $T_i$ parameter with the least number of bits. In general, this approach does not provide improvements over the Tate pairing, but for curves in which the trace of Frobenius value is small, there may in fact be a reduction in the Miller loop. This will be discussed further in Chapter 10.

# Chapter 7

# The Twisted Ate pairing

The Twisted Ate pairing is like the Ate pairing except that it reverses the order of the arguments. In order to define a map in this way, the theory of twists is required. This pairing was developed in 2006 along with the Ate pairing by Heßet al. [HSV06]. Given certain parameters, this pairing provides improved efficiency over the Tate pairing, which will be discussed further in Chapter 10.

## 7.1 Preliminaries for Twists

First, the background material that is specific to the Twisted Ate pairing will be discussed.

**Definition 7.1.1.** *Let $E, E'$ be elliptic curves defined over $\mathbb{F}_q$. If there exists an isomorphism*

$$\phi_d : E' \longrightarrow E$$

*defined over $\mathbb{F}_{q^d}$ where $d$ is minimal, then $E'$ is called a* twist of degree d *of $E$.*

Consider an elliptic curve $E$ of the form $E : y^2 = x^3 + Ax + B$ defined over $\mathbb{F}_q$ where $q = p^n$ for some prime $p$. From [Sil86, X.5.4], if $p \geq 5$ then the set of twists is canonically isomorphic to $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$ with

$$d = \begin{cases} 2 & \text{if } j(E) \neq 0, 1728, \\ 4 & \text{if } j(E) = 1728, \\ 6 & \text{if } j(E) = 0. \end{cases}$$

The term $j(E)$ is called the $j-$invariant of the elliptic curve which is a quantity defined by the coefficients and the discriminant of the curve [Sil86, III.1]. Note that all elliptic curves have at least degree 2 twists [FST06]. In the case when $d = 2$, which is usually the case, the unique twist $E'$ of $E$ is given by the equation $\zeta y^2 = x^3 + Ax + B$, for $\zeta \in \mathbb{F}_q^*/(\mathbb{F}_q^*)^2$.

For $d = 2, 4$ and 6, $\mathrm{Aut}(E) \cong \mu_d$, with $\mu_d$ the set of $d^{th}$ roots of unity [Sil86, III.10.2]. An isomorphism is given by

$$\begin{aligned} [\cdot] : \mu_d &\longrightarrow \mathrm{Aut}(E) \\ \xi &\mapsto [\xi] \end{aligned}$$

where $[\xi](x, y) = (\xi^2 x, \xi^3 y)$.

Note that the isomorphism defining the twist $E'$ of $E$ of degree $d$ induces the following ring isomorphism,

$$\begin{aligned} \Phi_d : \mathrm{End}(E') &\longrightarrow \mathrm{End}(E) \\ f &\mapsto \Phi_d(f) = \phi_d \circ f \circ \phi_d^{-1}. \end{aligned}$$

Let $\pi_q$ and $\pi_q'$ denote the Frobenius endomorphisms on $E$ and $E'$ respectively. Consider any rational map $g : E \longrightarrow E'$ and observe that $\pi_q' \circ g = g^\sigma \circ \pi_q$. Therefore,

$$\Phi_d(\pi_q') = \phi_d \circ \pi_q' \circ \phi_q^{-1} = \phi_d \circ (\phi_d^{-1})^\sigma \circ \pi_q.$$

The automorphism $\phi_d \circ (\phi_d^{-1})^\sigma \in \mathrm{Aut}(E)$ is of order $d$ [HSV06] and hence a primitive $d^{th}$ root of unity. By the isomorphism $[\cdot] : \mu_d \longrightarrow \mathrm{Aut}(E)$, the twists $E_i$ of degree dividing $d$ of $E$ can be labelled for $i = 0, \ldots d-1$ by

$$\Phi_i(\pi_{q,i}) = [\xi_d^i]\pi_q.$$

The value $\xi_d$ is a fixed primitive $d^{th}$ root of unity and $\pi_{q,i} : E_i \longrightarrow E_i$ is the usual Frobenius endomorphism. The map $\Phi_i$ is the ring isomorphism induced by the isomorphism $\phi_i : E_i \longrightarrow E$ defining the twist $E_i$ of degree dividing $d$ of $E$.

Notice that $E(\mathbb{F}_{q^d}) = \mathrm{Ker}(\pi_q^d - [1])$ and likewise $E_i(\mathbb{F}_q) = \mathrm{Ker}(\pi_{q,i} - [1])$. Mapping the Frobenius endomorphism of $E'$ into $E$ by $\Phi(\pi_{q,i}) = [\xi_d^i]\pi_q$ gives the following isomorphism

$$E_i(\mathbb{F}_q) \cong \mathrm{Ker}([\xi_d^i]\pi_q - [1]). \tag{7.1}$$

Recall that

$$G_1 = E[m] \cap \mathrm{Ker}(\pi_q - [1]) \quad \textit{and} \tag{7.2}$$

$$G_2 = E[m] \cap \mathrm{Ker}(\pi_q - [q]). \tag{7.3}$$

Using the previous analysis, let $E'$ be a twist of degree $d$ of $E$, $n = \gcd(k, d)$ and $e = k/n$. Then

$$E'(\mathbb{F}_{q^e}) \cong \mathrm{Ker}([\xi_n]\pi_q^e - [1]).$$

Hence, the isomorphism in (7.1) can be used to give the following alternative representation for $G_2$ for the twisted Ate pairing,

$$G_2 = E[m] \cap \mathrm{Ker}([\xi_n]\pi_q^e - [1]). \tag{7.4}$$

Working with $G_2$ in the form of (7.3) for $Q \in G_2$, $\pi_q$ acts as a multiplication by $q$ map. Using the alternate representation of $G_2$ given in (7.4), this implies that the map $[\xi_n]$ acts as a multiplication by $q^{-e}$. From [HSV06], $[\xi_n]$ acts as a multiplication by $q^e$ map on $G_1$ and so for $P \in G_1$, $[q^e]P = [T^e]P = [\xi_n]P$. These properties of $G_1$ and $G_2$ will be required for the Twisted Ate pairing.

## 7.2 Definition of the Twisted Ate Pairing

Suppose that $E$ admits a twist $E'$ of degree $d$. Let $n = \gcd(k, d)$, $e = k/n$ and

$$G_1 = E[m] \cap \mathrm{Ker}(\pi_q - [1]),$$

$$G_2 = E[m] \cap \mathrm{Ker}([\xi_n]\pi_q^e - [1]),$$

where $\xi_n$ is a primitive $\mathrm{n}^{th}$ root of unity.

**Definition 7.2.1.** *Let $E$ be an elliptic curve over $\mathbb{F}_q$, $m$ a large prime dividing $\#E(\mathbb{F}_q) = q + 1 - t$ where $t$ is the Trace of Frobenius. Set $T = t - 1$ and choose $P \in G_1$ and $Q \in G_2$. Let $f_{i,P}$ be a function as defined in § 2.4 such that* $\mathrm{div}(f_{i,P}) = i(P) - i(\mathcal{O}) - ([i]P) + (\mathcal{O})$. *Then the* twisted Ate pairing *is defined as follows,*

$$\begin{aligned} a_{T^e}^{twist} : G_1 \times G_2 &\longrightarrow \mu_m \\ (P, Q) &\mapsto f_{T^e,P}(Q)^{c(q^k-1)/N} \end{aligned}$$

*where $N = \gcd(T^k - 1, q^k - 1)$, $T^k - 1 = LN$, and*

$$c = \sum_{i=0}^{m-1} T^{e(m-1-i)} q^{ei} \equiv m q^{e(m-1)} \pmod{m}.$$

The *reduced twisted Ate pairing* is defined as $f_{T^e,P}(Q)^{(q^k-1)/m}$.

The Twisted Ate pairing can be related to the Tate pairing in a similar manner as the Ate pairing relates to the Tate pairing. The following theorem describes this relation and gives the conditions under which the Twisted ate pairing is non-degenerate.

**Theorem 7.2.2.** *Let $E$ be an elliptic curve defined over $\mathbb{F}_q$, $m$ a large prime such that $m \mid \#E(\mathbb{F}_q)$. Denote $t$ as the trace of Frobenius and set $T = t - 1$. For $P \in G_1 = E[m] \cap \mathrm{Ker}(\pi_q - [1])$ and $Q \in G_2 = E[m] \cap \mathrm{Ker}([\xi_n]\pi_q^e - [1])$ the following hold.*

1. *$f_{T^e,P}(Q)$ is a bilinear pairing.*
2. *For $N = \gcd(T^k - 1, q^k - 1)$, $T^k - 1 = LN$ and $c = \sum_{i=0}^{n-1} T^{e(n-1-i)} q^{ei} \equiv nq^{e(n-1)} \pmod{m}$,*

$$e(P,Q)^L = f_{T^e,P}(Q)^{c(q^k-1)/N}$$

   *where $e(P,Q)$ is the reduced Tate pairing.*

3. *If $m \nmid L$ then the pairing is non-degenerate.*

The proof parallels the proof of Theorem 6.1.5 for the Ate pairing except that Lemma 6.1.4 is replaced by the following lemma.

**Lemma 7.2.3.** *Let $P \in G_1$. Then*

$$f_{T^e,[\xi_n]P} \circ [\xi_n] = f_{T^e,P}.$$

*Proof.* Note that $[\xi_n]$ is an automorphism of $E$, has trivial kernel, and is separable

of degree 1. Consider

$$\begin{aligned}\operatorname{div}((f_{T^e,[\xi_n]P}) \circ [\xi_n]) &= [\xi_n]^* \operatorname{div}(f_{T^e,[\xi_n]P}) \\ &= [\xi_n]^* \left(T^e([\xi_n]P) - T^e(\mathcal{O}) - ([T^e]([\xi_n]P)) + (\mathcal{O})\right) \\ &= T^e(P) - T^e(\mathcal{O}) - ([T^e]P) + (\mathcal{O}) \\ &= \operatorname{div}(f_{T^e,P}).\end{aligned}$$

□

Also, precomposing with $\pi_q^e$ gives

$$f_{T^e,[\xi_n]P} \circ [\xi_n] \circ \pi_q^e = f_{T^e,P}^{q^e}$$

since $f_{T^e,P}$ is defined over $\mathbb{F}_q$. Thus for $Q \in G_2$

$$f_{T^e,[\xi_n]P}(Q) = f_{T^e,P}(Q)^{q^e}.$$

Following the remaining steps in the proof of Theorem 6.1.5 gives

$$e(P,Q)^L = f_{T^e,P}(Q)^{c(q^k-1)/N}$$

for $N = \gcd(T^k - 1, q^k - 1)$, $T^k - 1 = LN$, and

$$c = \sum_{i=0}^{m-1} T^{e(m-1-i)} q^e i \equiv m q^{e(m-1)} \pmod{m}.$$

The Twisted Ate pairing is only more efficient to compute than the Tate pairing when $|T^e| \leq m$, namely when the trace of Frobenius is relatively small compared to the value of $m$. It is also worth noting that in the case where $E = E'$ and $E$ is supersingular, this pairing coincides with the Eta pairing.

## 7.3 The Optimised Twisted Ate Pairing

Like the Optimised Ate pairing, the Optimised Twisted Ate pairing was developed by Heß et al. [HKMO07] in 2007. This pairing also gives improvements to the Twisted Ate pairing for certain embedding degrees and composite group orders.

**Theorem 7.3.1.** *Let $E$ be an elliptic curve defined over $\mathbb{F}_q$ that admits a twist of degree $d$. Let $S \in \mathbb{Z}$ such that $S \equiv q \pmod{m}$. Let $N = \gcd(S^k - 1, q^k - 1) > 0$ and $L = (S^k - 1)/N$. Let $c_S = \sum_{i=0}^{k-i} S^{k-1-i} q^i \pmod{N}$. For points $P \in G_1$ and $Q \in G_2$ as defined in § 7.2, a bilinear pairing called the* Optimised Twisted Ate pairing *is defined as*

$$\begin{aligned} a_S^{twist} : G_1 \times G_2 &\longrightarrow \mu_m \\ (P, Q) &\mapsto f_{S,P}(Q)^{c_S(q^k-1)/N}. \end{aligned}$$

*If $m$ does not divide $L$ then this pairing is non-degenerate.*

*The Optimised Twisted Ate pairing can be related to the reduced Tate pairing as follows.*

$$a_S^{twist}(P, Q) = e(P, Q)^L.$$

The proof of this theorem is analogous to the proof of the Twisted Ate pairing in § 6.1.5. See [HKMO07] for the slight change of details. This pairing provides a generalization of the Twisted Ate pairing.

## 7.4 The Twisted Ate$_i$ Pairing

The definitions of the Ate$_i$ and Twisted Ate pairings can be extended to define the Twisted Ate$_i$ pairing. This pairing was developed by Huang et al. [HZZ08] in 2008,

along with the Ate$_i$ pairing. The definition is as follows.

**Definition 7.4.1.** *(Twisted Ate$_i$ Pairing) Consider the elliptic curve $E$ defined over $\mathbb{F}_q$ with embedding degree $k$. Suppose that $E$ admits a twist $E'$ of degree $d$. Let $m$ be a large prime divisor of $\#E(\mathbb{F}_q)$, $T = t-1$ and $T_i = T^i \equiv q^i \pmod{m}$ for $0 < i < k$. For a function $f_{i,P}$ defined in § 2.4 and points $P \in G_1$ and $Q \in G_2$ as defined in § 7.2, the* Twisted Ate$_i$ pairing *is defined by*

$$\begin{aligned} a_{T_i^e}^{twist} : G_1 \times G_2 &\longrightarrow \mu_m \\ (P,Q) &\mapsto f_{T_i^e,P}(Q)^{c(q^k-1)/N} \end{aligned}$$

*where $N = \gcd(T^k - 1, q^k - 1)$, $T^k - 1 = LN$, and*

$$c = \sum_{i=0}^{m-1} T_i^{e(m-1-i)} q^{ei} \equiv mq^{e(m-1)} \pmod{m}.$$

Showing that this is a bilinear, non-degenerate pairing is similar to doing this for the cases of the Ate$_i$ and Twisted Ate pairings.

# Chapter 8

# The R-ate pairing

The R-ate pairing is a further generalization of the Ate pairing that incorporates the $\text{Ate}_i$ pairing as well. In addition, it offers faster computation over the $\text{Ate}_i$ pairing given certain parameters, which will be discussed further in Chapter 10. This pairing yields greater efficiency on certain curves than has been obtained with any other pairing. It was developed in 2008 by Eunjeong Lee, Hyang-Sook Lee and Cheol-Min Park [LLP08].

## 8.1 Defining the R-ate Pairing

As defined in §2.4, for $D \sim (P) - (\mathcal{O})$ let $f_{n,D}$ denote the function with divisor

$$\text{div}(f_{n,D}) = nD - D_n$$

and let $D_n$ denote the divisor

$$D_n = ([n]P) - (\mathcal{O}).$$

Note that a function $f_{n,D_n}$ has divisor $\text{div}(f_{n,D_n}) = nD_n - D_{n^2}$ and is also commonly denoted as $f_{n,nD}$ where $nD$ in this case does not refer to the divisor $D$ multiplied by the scalar $n$. If $D = (P) - (\mathcal{O})$, then $f_{n,D}$ can also be written as $f_{n,P}$ where

$$\text{div}(f_{n,P}) = n(P) - n(\mathcal{O}) - ([n]P) + (\mathcal{O}).$$

Denote by $G_{[j]P,[k]P}$ the function that is the quotient of the secant line through the points $[j]P$ and $[k]P$ over the vertical line through the point $[j+k]P$. Consequently,

$$\mathrm{div}(G_{[j]P,[k]P}) = ([j]P) + ([k]P) - ([j+k]P) - (\mathcal{O})$$

which is represented in Miller's algorithm as the function $g_{[j]P,[k]P}/g_{[j+k]P}$ in Chapter 9.

**Definition 8.1.1.** *Let $E$ be defined over $\mathbb{F}_q$. Let $[D], [D'] \in \mathrm{Pic}^0(E)[m]$ such that $D \sim (P) - (\mathcal{O})$ and $D' \sim (Q) - (\mathcal{O})$. Let $a, b, A, B \in \mathbb{Z}$ such that $A = aB + b$. The* R-ate pairing *is defined as follows*

$$R_{A,B}(D, D') = f_{a,D_B}(D') \cdot f_{b,D}(D') \cdot G_{[aB]P,[b]P}(D').$$

This pairing is bilinear and non-degenerate if the conditions in the subsequent theorem are satisfied. Additionally, this theorem relates the R-ate pairing to the reduced Tate pairing.

**Theorem 8.1.2.** *Let $E$ be defined over $\mathbb{F}_q$. Let $D, D'$ and $a, b, A, B$ be defined as in the definition of the R-ate pairing. Suppose $f_{A,D}(D')$ and $f_{B,D}(D')$ are Tate pairings and hence non-degenerate bilinear pairings*[1] *such that*

$$e(D, D')^{L_1} = f_{A,D}(D')^{M_1}, \quad e(D, D')^{L_2} = f_{B,D}(E)^{M_2}$$

*for $L_1, L_2, M_1, M_2 \in \mathbb{Z}$. Let $M = \mathrm{lcm}(M_1, M_2)$, $d_1 = M/M_1$, $d_2 = M/M_2$, and $L = d_1 L_1 - a d_2 L_2$. If $m$ does not divide $L$ then the R-ate pairing $R_{A,B}(D, D')$ is a non-degenerate bilinear pairing such that*

$$e(D, D')^L = R_{A,B}(D, D')^M.$$

[1] *Recall that by the properties of the Tate pairing given in § 4.2, the pairing is bilinear and non-degenerate.*

*Proof.* Let $D = (P) - (\mathcal{O})$. Note that

$$\begin{aligned}
\operatorname{div}(f_{aB,D}) &= aBD - D_{aB} \\
&= aB(P) - aB(\mathcal{O}) - ([aB]P) + (\mathcal{O}) \\
&= aB(P) - aB(\mathcal{O}) - (a([B]P) - a(\mathcal{O})) \\
&+ (a([B]P) - a(\mathcal{O})) - ([aB]P) + (\mathcal{O}) \\
&= a \cdot \operatorname{div}(f_{B,D}) + \operatorname{div}(f_{a,D_B}).
\end{aligned}$$

Up to a constant in $\mathbb{F}_q^*$, this implies

$$f_{aB,D} = f_{B,D}^a \cdot f_{a,D_B}.$$

Thus

$$\begin{aligned}
f_{A,D}(D') &= f_{aB+b,D}(D') \\
&= f_{aB,D}(D') \cdot f_{b,D}(D') \cdot G_{[aB]P,[b]P}(D') \\
&= f_{B,D}^a(D') \cdot f_{a,D_B}(D') \cdot f_{b,D}(D') \cdot G_{[aB]P,[b]P}(D') \\
&= f_{B,D}^a(D') \cdot R_{A,B}(D, D').
\end{aligned}$$

The second equality follows from Theorem 9.1.1. Since $f_{A,D}(D')$ and $f_{B,D}^a(D')$ are bilinear pairings then $R_{A,B}(D, D')$ is as well. Raising both sides to the exponent $M$ gives

$$f_{A,D}(D')^M = f_{B,D}(D')^{aM} \cdot R_{A,B}(D, D')^M.$$

Hence

$$e(D, D')^{d_1 L_1} = e(D, D')^{a d_2 L_2} \cdot R_{A,B}(D, D')^M.$$

Therefore $e(D, D')^L = R_{A,B}(D, D')^M$. In conclusion, the R-ate pairing is non-degenerate if $m$ does not divide $L$, as in the Ate pairing, Theorem 6.1.5.

□

## 8.2 Optimizing the R-ate Pairing

The functions $f_{a,D_B}$ and $f_{b,D}$ are defined with distinct divisors, namely $D_B$ and $D$. Using certain parameters for $A$ and $B$ (that are typically used for other pairings) the functions $f_{a,D_B}$ and $f_{b,D}$ can be defined in a more optimal way. One way to do this is to define the functions with the same divisor and therefore Miller's algorithm does not need to be computed twice. Another way to optimize the pairing is to eliminate one of the functions altogether.

**Corollary 8.2.1.** Let $E$ be a non-singular elliptic curve defined over $\mathbb{F}_q$. Let $k$ denote the embedding degree and consider a large prime $m$ such that $m \mid \#\mathrm{Pic}^0(E)(\mathbb{F}_q)$. As in the Ate pairing, choose $[D] \in G_1 = \mathrm{Pic}^0(E)[m] \cap \mathrm{Ker}(\pi_q - [1])$ and $[D'] \in G_2 = \mathrm{Pic}^0(E)[m] \cap \mathrm{Ker}(\pi_q - [q])$. Consider the following.

- $T_i = T^i \equiv q^i \pmod{m}$ for $0 < i < k$.
- $h_i$, the least positive integer such that $T_i^{h_i} \equiv 1 \pmod{m}$.
- $N_i = \gcd(T_i^{h_i} - 1, q^k - 1)$; $T_i^{h_i} - 1 = L_i N_i$.
- $c_i = \sum_{j=0}^{h_i - 1} T_i^{h_i - 1 - j}(q^i)^j \pmod{N_i}$.
- $M_i = (q^k - 1)/N_i$.

The R-ate pairing is related to the Tate pairing via the relation

$$e(D, D')^L = R_{A,B}(D, D')^M$$

for the following parameters (A,B) and exponents $L, M$.

1. $(A, B) = (q^i, m)$,
   $L = iq^{i-1}\frac{q^k-1}{m} - kq^{k-1}a$, $M = kq^{k-1}\frac{q^k-1}{m}$ .
2. $(A, B) = (q, T)$, for $q > T$,
   $L = M_1 - aL_1$, $M = c_1 M_1$ .
3. $(A, B) = (T_i, T_j)$,
   $L = d_i L_i - a d_j L_j$, $M = \mathrm{lcm}(c_i M_i, c_j M_j) = d_i c_i M_i = d_j c_j M_j$ .
4. $(A, B) = (m, T_j)$,
   $L = d_0 - a d_j L_j$, $M = \mathrm{lcm}((q^k - 1)/m, c_j M_j) = d_0 \frac{q^k-1}{m} = d_j c_j M_j$.

In each of these cases, the R-ate pairing is equal to:

1. $R_{q^i,m}(D, D') = f_{T_i,D}(D')$
2. $R_{q,T}(D, D') = f_{a,D}(D')^q \cdot f_{b,D}(D') \cdot G_{[aT]P,[b]P}(D')$
3. $R_{T_i,T_j}(D, D') = f_{a,D}(D')^{q^j} \cdot f_{b,D}(D') \cdot G_{[aT_j]P,[b]P}(D')$
4. $R_{m,T_j}(D, D') = f_{a,D}(D')^{q^j} \cdot f_{b,D}(D') \cdot G_{[aT_j]P,[b]P}(D')$.

Note that in the first case the R-ate pairing reduces to the $\mathrm{Ate}_i$ pairing.

*Proof.* For $A = q^i$, $B = m$, the R-ate pairing is defined as follows,

$$R_{q^i,m}(D, D') = f_{a,D_m}(D') \cdot f_{b,D}(D') \cdot G_{[am]P,[b]P}(D')$$

where $q^i = am + b$. Since $T_i \equiv q^i \pmod{m}$ this gives that $q^i = am + T_i$, i.e. $b = T_i$. Because $P \in E[m]$, the secant line through $[am]P = \mathcal{O}$ and $[T_i]P$ is equal to the vertical line through $[am + T_i]P = [am]P + [T_i]P = [T_i]P$. Additionally, note that

$D_m = ([m]P) - (\mathcal{O}) = 0$ and so $f_{a,D_m} = f_{a,0}$, that is, $f_{a,0}$ is a constant function; let $f_{a,0} = 1$. Therefore

$$R_{q^i,m}(D, D') = f_{T_i,D}(D').$$

The proofs for cases 2 through 4 are identical since $B$ is given as some power of $T$ in each of these situations. Although the parameters for $A$ are quite distinct, they only affect the value of $a$ and $b$ given by the relation $A = aB + b$ which does not alter the proof. For $B = T_j$, and $A$ is either $q$, $T_i$ or $m$ the R-ate pairing is defined as follows,

$$R_{A,T_j}(D, D') = f_{a,D_{T_j}}(D') \cdot f_{b,D}(D') \cdot G_{[aT_j]P,[b]P}(D').$$

Note that $[D'] \in \mathrm{Pic}^0(E) \cap \mathrm{Ker}(\pi_q - [1])$, and so $\pi_q(D') = D'$. Similarly, $[D] \in \mathrm{Pic}^0(E) \cap \mathrm{Ker}(\pi_q - [q])$, hence, $\pi_q(D) = [q]D = [T]D$. Since $T_j \equiv q^j \pmod{m}$, $\pi_q^j(D) = [T_j]D$. Consider

$$f_{a,D_{T_j}}(D') = f_{a,T_jD} = f_{a,\pi_q^j(D)}(D') = f_{a,D}^{q^j}(D')$$

where the third equality holds by Lemma 6.1.4. Whence

$$R_{A,T_j}(D, D') = f_{a,D}(D')^{q^j} \cdot f_{b,D}(D') \cdot G_{[aT_j]P,[b]P}(D').$$

For a proof of the choice of exponents, see [LLP08]. □

# Chapter 9

# Miller's Algorithm

Victor Miller [Mil86] created the first efficient algorithm for computing pairings on elliptic curves in 1986. At present, it is the algorithm of choice for computing the Weil pairing, the Tate pairing and several of its variants, namely the Eta, Ate and Twisted Ate pairings. The Squared Weil and Tate pairings and the R-ate pairing are computed using algorithms that are variations of Miller's algorithm. The goal of this algorithm is to compute the value of a function at a divisor (or a point) using properties of the group law. The idea is to begin with the constant function $f_{1,P}$ with divisor $\mathrm{div}(f_{1,P}) = 1(P)-1(\mathcal{O})-([1]P)+(\mathcal{O})$ and, using point addition and doubling, obtain the function $f_{m,P}$ with divisor $\mathrm{div}(f_{m,P}) = m(P) - m(\mathcal{O}) - ([m]P) + (\mathcal{O})$ evaluated at the divisor $D' \sim (Q) - (\mathcal{O})$ (or explicitly at the point $Q$ provided that the embedding degree is larger than 1). What makes this algorithm particularly efficient is that specific functions for $f_{i,P}$ in $x$ and $y$ need not be computed at each stage; rather, the evaluation of these functions at either the divisor or the point is all that is required.

## 9.1 Overview

Miller's algorithm applied to the Tate pairing and its variants[1] proceeds based upon the idea that if $f_{j,P}(D')$ and $f_{k,P}(D')$ have been computed then $f_{j+k,P}(D')$ can be

[1]Miller's algorithm for the Weil pairing is quite similar, but an explicit description will be omitted as computing it is far less efficient than computing the Tate pairing [GPS06].

computed[2] as follows.

**Theorem 9.1.1.** *Let $P \in E(\mathbb{F}_q)$, $Q \in E(\mathbb{F}_{q^k})$ and $f_{n,P}$ the function defined in the usual way where* $\mathrm{div}(f_{n,P}) = n(P) - n(\mathcal{O}) - ([n]P) + (\mathcal{O})$ *for $n \in \mathbb{Z}$. Choose divisors $D \sim (P) - (\mathcal{O})$ and $D' \sim (Q) - (\mathcal{O})$ with disjoint support, denote $g_{[j]P,[k]P}$ as the line through the points $[j]P$ and $[k]P$ and $g_{[j+k]P}$ as the vertical line through $[j+k]P$. Then for all $j, k \in \mathbb{Z}$*

$$f_{j+k,P}(D') = f_{j,P}(D') \cdot f_{k,P}(D') \cdot \frac{g_{[j]P,[k]P}(D')}{g_{[j+k]P}(D')}. \tag{9.1}$$

*Proof.* Note that

$$\mathrm{div}(g_{[j]P,[k]P}) = ([j]P) + ([k]P) + (-[j+k]P) - 3(\mathcal{O}),$$

$$\mathrm{div}(g_{[j+k]P}) = ([j+k]P) + (-[j+k]P) - 2(\mathcal{O}).$$

Thus,

$$\mathrm{div}(g_{[j]P,[k]P}) - \mathrm{div}(g_{[j+k]P}) = ([j]P) + ([k]P) - ([j+k]P) - (\mathcal{O}).$$

Using the above equality,

$$\begin{aligned}
\mathrm{div}(f_{j+k,P}) &= (j+k)(P) - (j+k)(\mathcal{O}) - ([j+k]P) + (\mathcal{O}) \\
&= j(P) - j(\mathcal{O}) - ([j]P) + (\mathcal{O}) \\
&\quad + k(P) - k(\mathcal{O}) - ([k]P) + (\mathcal{O}) \\
&\quad + ([j]P) + ([k]P) - ([j+k]P) - (\mathcal{O}). \\
&= \mathrm{div}(f_{j,P}) + \mathrm{div}(f_{k,P}) + \mathrm{div}(g_{[j]P,[k]P}) - \mathrm{div}(g_{[j+k]P})
\end{aligned}$$

[2]Equivalently given $f_{j,P}(Q)$ and $f_{k,P}(Q)$, then $f_{j+k,P}(Q)$ can be computed.

giving the desired result,

$$f_{j+k,P}(D') = f_{j,P}(D') \cdot f_{k,P}(D') \cdot \frac{g_{[j]P,[k]P}(D')}{g_{[j+k]P}(D')}.^{\dagger}$$

□

Computing the function $f_{j+k,P}$ is called a "Miller operation" [Mil04].

Analogously, for the Weil pairing:

$$\frac{f_{j+k,P}(D')}{f_{j+k,Q}(D)} = \frac{f_{j,P}(D')}{f_{j,Q}(D)} \cdot \frac{f_{k,P}(D')}{f_{k,Q}(D)} \cdot \frac{g_{[j]P,[k]P}(D')/g_{[j+k]P}(D')}{g_{[j]Q,[k]Q}(D)/g_{[j+k]Q}(D)}. \tag{9.2}$$

## 9.2 Miller's Algorithm

The following gives a description for computing the Tate pairing (hence also the Eta, Ate and Twisted Ate pairings) using Miller's algorithm. The Weil pairing is computed in a similar manner using the equality in (9.2). This algorithm uses the principles of the Right-to-Left Double-and-Add algorithm.

Let $P \in E(\mathbb{F}_q)[m]$, and let $Q \in E(\mathbb{F}_{q^k})$. Let $f_{n,P}$ be a function with divisor $\mathrm{div}(f_{n,P}) = n(P) - n(\mathcal{O}) - ([n]P) + (\mathcal{O})$ and consider the divisors $D \sim (P) - (\mathcal{O})$ and $D' \sim (Q) - (\mathcal{O})$ with disjoint support. Define $v_n = f_{n,P}(D')$ and let $f_{0,P}, f_{1,P} = 1$.

1. Set $i = m$, $j = 0$, $k = 1$, $v_0 = 1$, $v_1 = 1$.

2. If $i$ is even: replace $i$ with $\frac{i}{2}$. Compute

$$v_{2k} = f_{2k,P}(D') = f_{k,P}^2(D') \cdot \frac{g_{[k]P,[k]P}(D')}{g_{[2k]P}(D')}$$

[†]Note that $D'$ is a degree zero divisor and so the equality holds, not simply up to a scalar multiple.

which holds by Theorem 9.1.1. This term, $v_{2k}$, is computed by finding the tangent line at $[k]P$ and the vertical line at $[2k]P$. Change $k$ to $2k$. Save $v_k$ for the new value of $k$.

3. If $i$ is odd: replace $i$ with $i-1$. Compute

$$v_{j+k} = f_{j+k,P}(D') = f_{j,P}(D') \cdot f_{k,P}(D') \cdot \frac{g_{[j]P,[k]P}(D')}{g_{[j+k]P}(D')}$$

which again is due to Theorem 9.1.1. The term $v_{j+k}$ is computed by finding the secant line of $[k]P$ and $[j]P$, and the vertical line at $[j+k]P$. Change $j$ to $j+k$. Save $v_j$ for the new value of $j$.

4. If $i \neq 0$ go to step 2.

5. Output: $v_m = f_{m,P}(D')$.

## 9.3 Example of the Algorithm

Let $E : y^2 = x^3 + 2$ be an elliptic curve defined over $\mathbb{F}_7$. The value $m$ is chosen to be a large (typically prime) divisor of $\#E(\mathbb{F}_7) = 9$ so let $m = 3$. The least positive integer $k$ such that $3 \mid 7^k - 1$ is 1, so 1 is the embedding degree. Let $P = (3,6)$ and note that $P$ has order 3.

Suppose that the objective is to compute $\langle P, P \rangle_3$. Then $Q = P = (3,6)$.

Let $D = (3,6) - (\mathcal{O})$, $D' = (0,4) - (5,1)$ so that $D$ and $D'$ have no common points[3].

[3]Note that $(3,6) + (5,1) = (0,4)$.

Miller's algorithm is then used to compute $f_{m,P}(D')$ where $\mathrm{div}(f_{m,P}) = 3(3,6) - 3(\mathcal{O}) - ([3](3,6)) + (\mathcal{O}) = 3(3,6) - 3(\mathcal{O})$. Recall that both $f_{0,P}$ and $f_{1,P}$ are equal to 1.

1. Set $i = 3, j = 0, k = 1, v_0 = 1, v_1 = 1$.

2. $i = 3$ is odd, so $v_{j+k} = v_{0+1} = v_1$ must be computed. However, $v_1 = 1$ from step 1. The values are updated: $i = 2, j = 1, k = 1, v_1 = 1, v_1 = 1$.

3. $i = 2$ is even, so $v_{2k} = v_2$ must be computed. This is done by computing the tangent line at $[k]P = P$, which in turn is done using the group law to compute $[2]P = P + P$. The slope of the tangent line of $E$ at $P$ is 4 and so $[2]P = (3,1)$. The tangent line through $P$ is given by $y + 3x + 6 = 0$ and the vertical line through $[2]P$ is $x + 4 = 0$. Thus,

$$v_2 = v_1^2 \cdot \frac{(y + 3x + 6)/(x + 4)|_{(0,4)}}{(y + 3x + 6)/(x + 4)|_{(5,1)}} \equiv 5 \pmod 7.$$

   Finally, the values are updated: $i = 1, j = 1, k = 2, v_1 = 1, v_2 = 5$.

4. $i = 1$ is odd, so $v_{j+k} = v_{1+2} = v_3$ must be computed. This is done by computing the secant line of $[2]P$ and $P$. However, $[2]P + P = [3]P = \mathcal{O}$ which simplifies this step to requiring only the computation of the secant line through $[2]P$ and $P$, which is given by the vertical line $x + 4 = 0$. The term $v_3$ is given by

$$v_3 = v_1 \cdot v_2 \cdot \frac{(x + 4)|_{(0,4)}}{(x + 4)|_{(5,1)}} = 1 \cdot 5 \cdot 2 \equiv 3 \pmod 7.$$

   Therefore the Tate pairing for $m = 3$ at $P = Q = (3,6)$ is given by

$$\langle P, P \rangle_3 = v_3 = 3 \pmod{(\mathbb{F}_7^*)^3}$$

and the reduced Tate pairing value is

$$e(P,P) = \langle P,P\rangle_3^{(7-1)/3} = 3^2 \equiv 2 \pmod 7.$$

## 9.4 Miller's Algorithm in Practice

The description in § 9.2 gives a nice, illustrative version of Miller's algorithm. However, for the purpose of applications, this algorithm is typically implemented in a more efficient manner using the principles of the Left-to-Right Double-and-Add algorithm. This procedure is more desirable as it requires less storage.

The setup of the algorithm is similar to the Right-to-Left version. Choose $P \in E(\mathbb{F}_q)[m]$ and $Q \in E(\mathbb{F}_{q^k})$. Let $D \sim (P) - (\mathcal{O})$ and $D' \sim (Q) - (\mathcal{O})$ have disjoint support. The function $f_{m,P}$ with divisor $\mathrm{div}(f_{m,P}) = m(P) - m(\mathcal{O})$ which is evaluated at $D'$ is computed as follows.

Set $T = P$, $f = 1$ and $i = \lfloor \log_2(m) \rfloor - 1$. For $i \geq 0$, compute the following steps:

1. Calculate the tangent line $\ell$ at $T$ and the vertical line $v$ through $[2]T$.
2. $T \leftarrow [2]T$.
3. $f \leftarrow f^2 \cdot \ell(D')/v(D')$.
4. If the $i^{th}$ bit of $m$ is 1, then:
   (a) Calculate the secant line $\ell$ of $T$ and $P$ and the vertical line $v$ through $T + P$.
   (b) $T \leftarrow T + P$
   (c) $f \leftarrow f \cdot \ell(D')/v(D')$.

5. $i \leftarrow i - 1$.

Output: $f = f_{m,P}(D')$.

The example from § 9.3 using the Left-to-Right method is computed as follows. Recall that $E$ is defined over $\mathbb{F}_7$ and is given by $y^2 = x^3 + 2$, $m = 3$, $k = 1$, $P = Q = (3,6)$. The divisors $D$ and $D'$ are given by $(3,6) - (\mathcal{O})$ and $(0,4) - (5,1)$ respectively. The objective is to compute $f_{3,P}(D')$. Note that $3 = 11_2$.

Let $T = (3,6)$, $f = 1$ and $i = 0$. Since $i \geq 0$, the lines $\ell$ and $v$ must be computed.

1. The tangent line $\ell$ is given by $y+3x+6 = 0$ and the vertical line $v$ is $x+4 = 0$.

2. $T \leftarrow [2]T = (3,1)$.

3. Set
$$f \leftarrow f^2 \cdot \frac{(y+3x+6)/(x+4)|_{(0,4)}}{(y+3x+6)/(x+4)|_{(5,1)}} \equiv 5 \pmod 7.$$

4. Because the $0^{th}$ bit of 3 is 1:

   (a) The lines $\ell$ and $v$ must be computed for adding $P$ and $T$. Note that $P+T = [3](3,6) = \mathcal{O}$ and so $\ell = v$ and is given by $x+4 = 0$.

   (b) $T \leftarrow \mathcal{O}$.

   (c) Set
   $$f \leftarrow f \cdot \frac{(x+4)|_{(0,4)}}{(x+4)|_{(5,1)}} \equiv 3 \pmod 7.$$

5. $i \leftarrow -1$.

Output: $f = f_{3,P}(D') \equiv 3 \pmod 7$.

The remaining steps of the computation are identical to those given in § 9.2.

# Chapter 10

# Efficiency Comparison

With such a large selection of pairings, it may seem that choosing the appropriate pairing in a particular cryptographic setting may be a daunting task that no longer comes down to simply deciding between the Weil or Tate pairings. If the embedding degree is small and the curve is supersingular, it may be more advantageous to work with the Eta pairing. Alternatively, perhaps the curve is ordinary and the number of points on the curve is roughly the same size as the large prime $m$; in this case the Ate pairing may be more optimal. There are a multitude of factors that can be considered. The objective of this chapter is to determine whether or not it is worthwhile to consider such factors or to simply use the Tate pairing in all settings.

## 10.1 Minimum Security Requirements

Let $q = p^n$ for $n \in \mathbb{Z}$ and consider the field $\mathbb{F}_{q^k}$ where $k$ is the embedding degree. Although the pairing is computed over the field $\mathbb{F}_{q^k}$, this may not be the minimal field in which $\mu_m$ is embedded into [Hit07]. In fact, the minimal field in which $\mu_m$ is embedded into is $\mathbb{F}_{q^{k'}} = \mathbb{F}_{q^{\mathrm{ord}_m(p)/n}}$, where $m$ is the large prime divisor of $\#E(\mathbb{F}_q)$. Note that in the case where $q$ is a prime, i.e. $q = p^1$, then $\mathbb{F}_{q^{k'}} = \mathbb{F}_{q^k}$. For security purposes, a pairing-based cryptosystem requires that $q^{k'}$ is large enough so that the discrete logarithm problem is infeasible[1]. It is also necessary that $m$ is large enough

[1]Currently, the best known algorithms for solving discrete logs in a finite field is the index calculus attack [FST06].

Table 10.1: Security requirements for a given bit size.

| *Security Level* | 80 | 128 | 192 | 256 |
|---|---|---|---|---|
| $m$ | 160 | 256 | 384 | 512 |
| $\lvert\mathbb{F}_{q^k}\rvert$ | 1024 | 3072 | 8192 | 15360 |

so that the points of order $m$ are unaffected by the Pollard-rho attack. For $m = 2^\ell$, $\ell \in \mathbb{Z}$, the number of group operations required to compute the Pollard-rho attack is $\sqrt{m} = 2^{\ell/2}$. The value $\ell/2$ defines the security level of a cryptosystem in bits, which indicates the number of bits required to write down the number $2^{\ell/2}$. For instance, if $m = 2^{160}$, then $\sqrt{m} = 2^{80}$ group operations are required for the Pollard-rho algorithm and such a system would have an 80 bit security level. Given a specific security level, the minimum bit length size for $m$ and $\mathbb{F}_{q^k}$ are given in Table 10.1 [KM05].

Note that not just any elliptic curve can be used for pairing based cryptography. Curves with relatively small embedding degree and large prime divisor $m$ (as mentioned above) are required; these curves are called *pairing-friendly elliptic curves* [FST06].

## 10.2 The Cost of Computing the Weil Pairing

Although in practice it is undesirable to compute, as it requires roughly two Tate pairing computations, the Weil pairing is, nevertheless, worthwhile examining, as it gives insight into the computation of the other, more efficient pairings. By Proposition 3.3.2, computing the pairing requires obtaining the value

$$e_m(P, Q) = (-1)^m \frac{f_{m,P}(Q)}{f_{m,Q}(P)}.$$

The coordinates of the points $P$ and $Q$ are typically chosen from the fields $\mathbb{F}_q$ and $\mathbb{F}_{q^k}$ respectively. Therefore, computing $f_{m,P}(Q)$ is not equivalent to computing $f_{m,Q}(P)$ for embedding degree larger than one. In the literature the latter is referred to as a Miller-Lite operation, as it is faster to compute, where the former is called the Full-Miller operation. It was argued in [KM05] that for high security levels, exponentiating the Tate pairing would have such a significant cost that it would offset the cost of computing the Weil pairing. However, at that time, the extent to which the exponentiation could be computed efficiently was not known. There are techniques that are used for point exponentiation for elliptic curves such as the use of projective coordinates [Gal05], defined in [BSS99, IV.1] and the Sliding Windows method [Gal05, GPS06], defined in [BSS99, IV.2.3]. However, it was argued in [Gal05] that these techniques are not useful for the Tate pairing. In the case of the Tate pairing, the exponentiation can be computed efficiently by making use of the Frobenius endomorphism [Gal05]; hence, it was concluded that at relevant levels of security, the Tate pairing is in fact always faster than the Weil pairing [GPS06].

A consideration that must be made when computing a pairing is whether to use affine coordinates or projective coordinates. Depending upon the circumstances, either choice could be more advantageous. This decision depends upon the number of divisions that are required when using affine coordinates versus the number of extra multiplications required when using projective coordinates. The Weil pairing will be examined using both types of coordinates following the analyses given in [KM05] and [ELM04] with some additional details included.

### 10.2.1 Projective Coordinates

Recall that in affine space, the Weierstraß equation for an elliptic curve defined over $\mathbb{F}_q$ can be written as

$$E : y^2 = x^3 + Ax + B$$

if $\text{char}(\mathbb{F}_q) \neq 2, 3$. Using projective coordinates $E$ becomes

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3$$

where $(x, y) = (X/Z, Y/Z)$ for $Z \neq 0$. A special type of weighted projective coordinates are called Jacobian coordinates. These are given by the relation $(x, y) = (X/Z^2, Y/Z^3)$ for $Z \neq 0$ where $E$ takes the form

$$E : Y^2 = X^3 + AXZ^4 + BZ^6.$$

At each stage of Miller's algorithm the computation of

$$f_{j+k,P}(Q) = f_{j,P}(Q) \cdot f_{k,P}(Q) \cdot \frac{g_{[j]P,[k]P}(Q)}{g_{[j+k]P}(Q)}$$

is required for the Miller-Lite operation.

If $m$ is chosen to be a Solinas prime [Sol99] of the form $2^\alpha \pm 2^\beta \pm 1$, the Miller-Lite operation can be denoted as

$$\frac{f_1}{f_2} \longleftarrow \frac{f_1^2}{f_2^2} \cdot \frac{\ell_1(Q)/\ell_2}{v_1(Q)/v_2}.$$

In this case, building up to $[m]P = [2^\alpha \pm 2^\beta \pm 1]P = [2^\beta(2^{\alpha-\beta} \pm 1) \pm 1]P$ requires only 2 additions or subtractions and $\alpha$ doublings, which means that the number of required additions (or subtractions) is negligible. The terms $\ell$ and $v$ are the tangent and vertical lines at a point $T$ and $[2]T$, respectively, where $T$ represents $[2^i]P$ in

Miller's algorithm for some $i \in \mathbb{Z}$. Note that the divisions are not computed at each stage but rather at the end of the computation and so the value $f_{j+k,P}(Q)$ is represented as a fraction. This computation is also done for $f_{m,Q}(P)$.

Let $T = (X, Y, Z)$ be a point given in Jacobian coordinates. The formula for doubling $T$ is given by $[2]T = (X_3, Y_3, Z_3)$ where

$$X_3 = (3X^2 + AZ^4)^2 - 8XY^2$$
$$Y_3 = (3X^2 + AZ^4)(4XY^2 - X_3) - 8Y^4$$
$$Z_3 = 2YZ.$$

The vertical and tangent lines are given by

$$v(x) = v_1(x)/v_2 = (Z_3^2 x - X_3)/Z_3^2,$$
$$\ell(x, y) = \ell_1(x, y)/\ell_2 = (Z_3 Z^2 y - 2Y^2 - (3X^2 + aZ^4)(xZ^2 - X))/(Z_3 Z^2).$$

For the case when $k = 1$, let $E$ be an elliptic curve defined over $\mathbb{F}_q$ where $q > 2$ and $q = A^2 + 1$. If $4 \mid q$ let

$$E : y^2 = x^3 - x.$$

If $q \equiv 2 \pmod 4$ then take

$$E : y^2 = x^3 - 4x.$$

Computing a Miller operation requires the following step for each bit of $m$.

$$T \longleftarrow [2]T, \quad f_1 \longleftarrow f_1^2 v_2 \ell_1(Q), \quad f_2 \longleftarrow f_2^2 \ell_2 v_1(Q).$$

Denoting a squaring as $S_i$, a multiplication as $M_i$ and an inversion as $I_i$ in the field $\mathbb{F}_{q^i}$ this procedure requires $9S_1 + 12M_1$. Since the Weil pairing requires the

computation of both $f_{m,P}(Q)$ and $f_{m,Q}(P)$ the total operation count for this pairing is $18S_1 + 24M_1$.

Consider the case when $k \geq 2$ and $k$ is even. Let $E$ be defined over $\mathbb{F}_q$, for $q > 2$ and $E$ of the form

$$E : y^2 = x^3 - 3x + B.$$

In this case, there are several ways to make the pairing computation more efficient. Since $k$ is even, the field $\mathbb{F}_{q^{k/2}}$ can be used by choosing the point $Q$ with $x-$coordinate in $\mathbb{F}_{q^{k/2}}$ and $y-$coordinate of the form $\gamma\sqrt{\beta}$ where $\beta$ is a non-square in $\mathbb{F}_{q^{k/2}}$ [Sol99]. The terms $x$ and $y$ can be referred to as "real" and "imaginary" respectively [KM05].

The value $m$ is chosen to be a large and therefore odd prime, and has the property that $m \mid (q^k - 1)$ but $m \nmid (q^{k/2} - 1)$. Note that $m \mid (q^{k/2} + 1)$ which is an even value since $q > 2$. Rewriting the exponent $(q^k - 1)/m$ as $\left(\frac{q^{k/2}+1}{m}\right)(q^{k/2} - 1)$ shows that an element of the form $\gamma\sqrt{\beta}$ when raised to this power is squared by the term $(q^{k/2}+1)/m$ and hence lies in $\mathbb{F}_{q^{k/2}}$ and the term $(q^{k/2} - 1)$ ensures the resulting element is 1. Therefore, in the final exponentiation of the reduced Tate pairing, terms in $\mathbb{F}_{q^{k/2}}$ become trivial, and so do terms that are "purely imaginary," i.e. of the form $\gamma\sqrt{\beta}$.

When computing the Miller-Lite portion of the Weil pairing, $f_{m,P}(Q)$, the terms $v_1(x), v_2, \ell_2 \in \mathbb{F}_{q^{k/2}}$ and thus the computation of $f_1/f_2$ is reduced to

$$T \longleftarrow [2]T, \quad f_1 \longleftarrow f_1^2 \ell_1(Q).$$

In the computation of the Full-Miller part of the Weil pairing, $f_{m,Q}(P)$, the terms $v_1(x), v_2$ are in $\mathbb{F}_{q^{k/2}}$ and $\ell_2$ is "purely imaginary" which gives the same simplification as in the Miller-Lite operation

$$T \longleftarrow [2]T, \quad f_1 \longleftarrow f_1^2 \ell_1(P).$$

Computing the Full-Miller step requires $kM_1+4S_{k/2}+6M_{k/2}+S_k+M_k$ operations. The Miller-Lite step requires $4S_1+8M_1+S_2+M_2$ for $k=2$ and $4S_1+(k+7)M_1+S_k+M_k$ for $k \geq 4$ and $k$ even [KM05].

### 10.2.2 Affine Coordinates

Following the method in [ELM04] both the numerator and the denominator of the Weil pairing are computed together as $f_{m,P}(Q)/f_{m,Q}(P)$ which doesn't affect the efficiency, but is significant for computing the Squared Weil pairing, thus enabling a comparative analysis. This description was given in Chapter 9; recall that at each stage of Miller's algorithm for $D=(P)-(\mathcal{O})$ and $D'=(Q+R)-(R)$, the value $f_{j+k,D}(D')/f_{j+k,D'}(D)$ is computed from $f_{j,D}(D')/f_{j,D'}(D)$ and $f_{k,D}(D')/f_{k,D'}(D)$ as follows,

$$\begin{aligned}\frac{f_{j+k,D}(D')}{f_{j+k,D'}(D)} &= \frac{f_{j,D}(D')}{f_{j,D'}(D)} \cdot \frac{f_{k,D}(D')}{f_{k,D'}(D)} \cdot \frac{g_{[j]P,[k]P}(D')/g_{[j+k]P}(D')}{g_{[j]Q,[k]Q}(D)/g_{[j+k]Q}(D)} \\ &= \frac{f_{j,D}(Q+R)/f_{j,D}(R)}{f_{j,D'}(P)/f_{j,D'}(\mathcal{O})} \cdot \frac{f_{k,D}(Q+R)/f_{k,D}(R)}{f_{k,D'}(P)/f_{k,D'}(\mathcal{O})} \\ &\quad \cdot \frac{g_{[j]P,[k]P}(Q+R)}{g_{[j]P,[k]P}(R)} \cdot \frac{g_{[j+k]P}(R)}{g_{[j+k]P}(Q+R)} \cdot \frac{g_{[j]Q,[k]Q}(\mathcal{O})}{g_{[j]Q,[k]Q}(P)} \cdot \frac{g_{[j+k]Q}(P)}{g_{[j+k]Q}(\mathcal{O})} \end{aligned} \tag{10.1}$$

where $g_{[j]P,[k]P}$ is the secant line through $[j]P$ and $[k]P$ and $g_{[j+k]P}$ is the vertical line through $[j+k]P$ (respectively for $Q$). Computing $[j]P+[k]P$ costs 1 field inversion and 2 field multiplications if the $x-$coordinates of $[j]P$ and $[k]P$ are distinct[2]. The secant line through $[j]P$ and $[k]P$ is given by $g_{[j]P,[k]P}(X)=y(X)-y([j]P)-\gamma(x(X)-x([j]P))$ where $\gamma$ is the slope. Hence, evaluating $g_{[j]P,[k]P}(D')$ requires 2 field multiplications. No further operations are required to compute $g_{[j+k]P}(D')$ since

[2]If $[j]P=[k]P$ with non-zero $y-$coordinate, then doubling $[j]P$ requires 2 addition field multiplications.

$g_{[j+k]P}(X) = x(X) - x([j+k]P)$. This procedure is repeated for point doubling and addition involving $Q$. Finally an additional 10 multiplications are required for multiplying the 6 fractions in (10.1) together. Thus for each bit of $m$, this procedure requires $18M_k + 2I_k$. In this particular case, an inversion is roughly equivalent to 5 multiplications, giving a total of $28M_k$.

## 10.3 The Cost of Computing the Tate Pairing

By analogy to the Weil pairing, an analysis of computing the Tate pairing in both projective and affine coordinates will be given.

### 10.3.1 Projective Coordinates

Computing the Tate pairing requires the evaluation of

$$\langle P, Q \rangle_m = f_{m,P}(D').$$

As in the similar case of the Weil pairing, at each stage of Miller's algorithm, $f_{j+k,P}(D')$ must be computed; this can also be represented as

$$\frac{f_1}{f_2} \longleftarrow \frac{f_1^2}{f_2^2} \cdot \frac{\ell_1(Q+R)/\ell_1(Q)}{v_1(Q+R)/v_1(R)}$$

where $\ell$ and $v$ are the tangent lines and vertical lines respectively defined in § 10.2.1 and $D' = (Q+R)-(R)$. Let $R = (0,0)$. For the case of $k = 1$ and hence $P, Q, R \in \mathbb{F}_q$ the following Miller operations must be computed for each bit of $m$

$$T \longleftarrow [2]T, \quad f_1 \longleftarrow f_1^2 \ell_1(Q+R)v_1(R), \quad f_2 \longleftarrow f_2^2 \ell_1(R)v_1(Q+R) \qquad (10.2)$$

for points $T$ and $[2]T$ as defined in § 10.2.1. This operation requires $9S_1 + 13M_1$.

Now consider the case when $k \geq 2$ and $k$ is even. Let the points $P$ and $Q$ be defined as in § 10.2.1. As in the case of the Weil pairing, terms contained in a proper subfield of $\mathbb{F}_{q^k}$ can be ignored. By Lemma 4.2.3, the point $R$ can be ignored, and then computing the reduced Tate pairing amounts to calculating

$$e(P,Q) = \langle P,Q \rangle_m^{(q^k-1)/m} = f_{m,P}(Q)^{(q^k-1)/m}.$$

Since $Q \in \mathbb{F}_{q^{k/2}}$ then $v_1(Q) \in \mathbb{F}_{q^{k/2}}$, and so the denominator in (10.2) can be eliminated. Therefore, for each bit of $m$ the Miller operation is simplified to

$$T \longleftarrow [2]T, \quad f_1 \longleftarrow f_1^2 \ell_1(Q).$$

This requires $4S_1+8M_1+S_2+M_2$ operations for $k=2$ and $4S_1+(k+7)M_1+S_k+M_k$ for $k \geq 4$ and $k$ even.

### 10.3.2 Affine Coordinates

The analysis for the Tate pairing computation using affine coordinates is analogous to that of the Weil pairing. The notable difference being that the goal is to compute $f_{m,D}(D')$ versus $f_{m,D}(D')/f_{m,D'}(D)$ and so there are two less fractions to compute. For $D = (P) - (\mathcal{O})$, $D' = (Q+R) - (R)$, the value $f_{j+k,D}(D')$ is given by:

$$\begin{aligned} f_{j+k,D}(D') &= f_{j,D}(D') \cdot f_{k,D}(D') \cdot \frac{g_{[j]P,[k]P}(D')}{g_{[j+k]P}(D')} \\ &= \frac{f_{j,D}(Q+R)}{f_{j,D}(R)} \cdot \frac{f_{k,D}(Q+R)}{f_{k,D}(R)} \cdot \frac{g_{[j]P,[k]P}(Q+R)}{g_{[j]P,[k]P}(R)} \cdot \frac{g_{[j+k]P}(R)}{g_{[j+k]P}(Q+R)} \end{aligned} \quad (10.3)$$

which must be computed for each bit of $m$. Again, elliptic curve addition requires 2 multiplications and 1 inversion[3]. Another 2 multiplications are required to evaluate

[3]In the case of point doubling, only 1 additional multiplication is required.

the secant lines and no further operations are needed for the vertical lines. Finally, combining the 4 fractions in (10.3) requires 6 multiplications giving a total of 10 multiplications and 1 inversion. Since 1 inversion is roughly equal to the cost of 5 multiplications, this gives a total of $15M_k$ for each bit of $m$ for computing the Tate pairing.

## 10.4 The Cost of Computing the Squared Weil Pairing

The computation of the Squared Weil pairing is analogous to that of the Weil pairing except that the objective is to compute

$$\frac{f_{m,P}(Q)/f_{m,P}(-Q)}{f_{m,Q}(P)/f_{m,Q}(-P)}.$$

Consider

$$\begin{aligned}\frac{f_{j+k,P}(Q)/f_{j+k,P}(-Q)}{f_{j+k,Q}(P)/f_{j+k,Q}(-P)} &= \frac{f_{j,P}(Q)/f_{j,P}(-Q)}{f_{j,Q}(P)/f_{j,Q}(-P)} \cdot \frac{f_{k,P}(Q)/f_{k,P}(-Q)}{f_{k,Q}(P)/f_{k,Q}(-P)} \\ &\quad \cdot \frac{g_{[j]P,[k]P}(Q)}{g_{[j]P,[k]P}(-Q)} \cdot \frac{g_{[j+k]P}(-Q)}{g_{[j+k]P}(Q)} \cdot \frac{g_{[j]Q,[k]Q}(-P)}{g_{[j]Q,[k]Q}(P)} \cdot \frac{g_{[j+k]Q}(P)}{g_{[j+k]Q}(-P)} \\ &= \frac{f_{j,P}(Q)/f_{j,P}(-Q)}{f_{j,Q}(P)/f_{j,Q}(-P)} \cdot \frac{f_{k,P}(Q)/f_{k,P}(-Q)}{f_{k,Q}(P)/f_{k,Q}(-P)} \\ &\quad \cdot \frac{g_{[j]P,[k]P}(Q)}{g_{[j]P,[k]P}(-Q)} \cdot \frac{g_{[j]Q,[k]Q}(-P)}{g_{[j]Q,[k]Q}(P)}.\end{aligned}$$

This follows as the vertical lines through $[j+k]P$ evaluated at $x(Q)$ and $x(-Q)$ are equal (respectively for $[j+k]Q$) and hence allow for cancellation.

Like the Weil pairing, the elliptic curve addition requires 2 multiplications and 1 inversion[4]. Evaluating

$$\frac{g_{[j]P,[k]P}(Q)}{g_{[j]P,[k]P}(-Q)} = \frac{y(Q) - y([j]P) - \lambda(x(Q) - x([j]P))}{y(-Q) - y([j]P) - \lambda(x(-Q) - x([j]P))}$$

[4]An additional 2 multiplications are required for a point doubling, as in the case of the Weil pairing.

requires one multiplication[5]. Repeating this procedure for $g_{[j]Q,[k]Q}(P)/g_{[j]Q,[k]Q}(-P)$ requires a total of 6 multiplications and 2 inversions. Computing the product of the remaining four fractions requires an additional 6 multiplications, giving a total of $12M_k + 2I_k$ operations.

## 10.5 The Cost of Computing the Squared Tate Pairing

The cost of computing this pairing is analogous to that of the Squared Weil pairing except that there are two less terms required. The objective is to compute

$$\begin{aligned}\frac{f_{j+k,P}(Q)}{f_{j+k,P}(-Q)} &= \frac{f_{j,P}(Q)}{f_{j,P}(-Q)} \cdot \frac{f_{k,P}(Q)}{f_{k,P}(-Q)} \cdot \frac{g_{[j]P,[k]P}(Q)}{g_{[j]P,[k]P}(-Q)} \cdot \frac{g_{[j+k]P}(Q)}{g_{[j+k]P}(-Q)} \\ &= \frac{f_{j,P}(Q)}{f_{j,P}(-Q)} \cdot \frac{f_{k,P}(Q)}{f_{k,P}(-Q)} \cdot \frac{g_{[j]P,[k]P}(Q)}{g_{[j]P,[k]P}(-Q)}.\end{aligned}$$

Again, evaluating the vertical line at $x(Q)$ and $x(-Q)$ gives cancellation.

The elliptic curve addition requires 2 multiplications and 1 inversion, and 1 additional multiplication if a point doubling is required. Only one multiplication is required to evaluate $g_{[j]P,[k]P}(Q)/g_{[j]P,[k]P}(-Q)$. Combining the remaining three fractions requires 6 additional multiplications giving a total of $7M_K + I_k$ operations for each bit of $m$.

Table 10.2 summarizes the cost required to compute the Weil and Tate pairing in both affine and projective coordinates (which will be denoted by A and P respectively) and as well as the Squared Weil and Tate pairings. The operations in the field $\mathbb{F}_{q^k}$ can be done with $O((\lg|\mathbb{F}_{q^k}|)^2)$ bit operations [BS96]. Although it is more efficient to compute operations in smaller fields, by current standards, it is desirable to have an embedding degree $k \sim 6 - 10$ [Fre06].

[5]Note that $x(Q) = x(-Q)$.

Table 10.2: Efficiency Comparison Between the Weil and Tate Pairings[6]

| *Pairing:* | $k=1$ | $k=2$ | $k=4$, *even* |
|---|---|---|---|
| Weil $(P)$ | $18S_1+24M_1$ | $8S_1+16M_1$ $+2S_2+2M_2$ | $4S_1+(2k+7)M_1+4S_{k/2}$ $+6M_{k/2}+2S_k+2M_k$ |
| Weil $(A)$ | $18M_1+2I_1$ | $18M_2+2I_2$ | $18M_k+2I_k$ |
| Sq. Weil | $12M_1+2I_1$ | $12M_2+2I_2$ | $12M_k+2I_k$ |
| Tate $(P)$ | $9S_1+13M_1$ | $4S_1+8M_1$ $+S_2+M_2$ | $4S_1+(k+7)M_1$ $+S_k+M_k$ |
| Tate $(A)$ | $10M_1+I_1$ | $10M_2+I_2$ | $10M_k+I_k$ |
| Sq. Tate | $7M_1+I_1$ | $7M_2+I_2$ | $7M_k+I_k$ |

## 10.6 Computing the Variants of the Tate Pairing

Following the analysis in [KM05, GPS06, HSV06], consider a curve $E$ of the form

$$E: y^2 = x^3 + Ax + B.$$

Suppose that $E$ admits a twist of degree 2 and a twist of degree 6; then $A=-3$ and $A=0$ respectively. Let $C_{Lite}$ represent the cost of computing the Miller-Lite operation, $f_{N,P}(Q)$, $C^A_{Full}$ the Full-Miller operation, $f_{N,Q}(P)$, in affine coordinates and $C^P_{Full}$ the Full-Miller operation in projective coordinates. The cost of computing a pairing of the form $f_{N,P_1}(P_2)$ for point $P_1$ and $P_2$ is given in the following two cases.

*Case 1:* For $(d,A)=(2,-3)$,

$$C_{Lite} = [4S_1+(2e+7)M_1+S_k+M_k]\cdot\log_2(N)$$

$$C^A_{Full} = [4S_e+6M_e+2eM_1+S_k+M_k]\cdot\log_2(N)$$

$$C^P_{Full} = [2S_e+3M_e+I_e+eM_1+S_k+M_k]\cdot\log_2(N).$$

[6]Recall that $S_k$, $M_k$ and $I_k$ represent squaring, multiplication and inversion, respectively, in the field $\mathbb{F}_{q^k}$.

Table 10.3: Efficiency Comparison Between the Tate Pairing and its Variants

| *Pairing:* | *Defined on:* | *Evaluated as:* |
|---|---|---|
| Tate | $G_1 \times G_2$ | $f_{m,P}(Q)$ |
| Eta | $G_1 \times G_2$ | $f_{T,P}(Q)$ |
| Ate | $G_2 \times G_1$ | $f_{T,Q}(P)$ |
| Optimised Ate | $G_2 \times G_1$ | $f_{S,Q}(P)$ |
| Ate$_i$ | $G_2 \times G_1$ | $f_{T_i,Q}(P)$ |
| Twisted Ate | $G_1 \times G_2$ | $f_{T^e,P}(Q)$ |
| Optimised Twisted Ate | $G_1 \times G_2$ | $f_{S^e,P}(Q)$ |
| Twisted Ate$_i$ | $G_1 \times G_2$ | $f_{T_i^e,P}(Q)$ |

*Case 2:* For $(d, A) = (6, 0)$,

$$C_{Lite} = [5S_1 + (2e+6)M_1 + S_k + M_k] \cdot \log_2(N)$$

$$C^A_{Full} = [5S_e + 6M_e + 2eM_1 + S_k + M_k] \cdot \log_2(N)$$

$$C^P_{Full} = [2S_e + 3M_e + I_e + eM_1 + S_k + M_k] \cdot \log_2(N).$$

Substituting the parameter $N$ for the corresponding parameter in each of the pairings in Table 10.3 provides a comparison of the length of the loop in Miller's algorithm for each of the pairings. Recall that $T = t-1$, $S \equiv q \pmod m$, $T_i = T^i \equiv q^i \pmod m$ for $0 < i < k$ and $e = k/\gcd(k, d)$.

The following gives the specifications required for these pairings to be optimal, which is summarized in Table 10.4.

**The Eta and Ate pairings:** Although the Ate pairing requires a Full-Miller operation, it is still possible to decrease the loop length so that it is shorter than the loop in the Miller-Lite operation of the Tate pairing. In a standard implementation, the number of bits of $m$ is roughly equal to the number of bits of $q$. Typically, the

trace is approximately $\sqrt{q}$; however, it can be as small as $m^{1/\varphi(k)}$ [HSV06] where $\varphi$ is the Euler-phi function. The loop length in Miller's algorithm for the Eta and Ate pairings is roughly $\log_2(|t|)$ and is at most half of the loop length in the Tate pairing, which is roughly $\log_2(m)$, if $m \approx \#E(\mathbb{F}_q)$, and hence the trace must be small. This follows from Hasse's Theorem which states that for an elliptic curve $E$ defined over $\mathbb{F}_q$, the order of $E(\mathbb{F}_q)$ satisfies $|t| = |q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$. Taking the logarithm of both sides yields $\log_2(|t|) \leq \frac{1}{2}\log_2(q)$. Substituting $m$ for $q$ into the equality gives the desired result $\log_2(|t|) \leq \frac{1}{2}\log_2(m)$. On the other hand, the Tate pairing may be more efficient to compute than the Eta and the Ate pairings if $m \leq \frac{1}{2}\log_2(q)$ [HKMO07].

**The Twisted Ate pairing:** This pairing can only be more efficient than the Tate pairing when $|T^e| \leq m$ since both pairings require computing the Miller-Lite operation [HSV06].

**The Ate$_i$ and Twisted Ate$_i$ pairings:** These pairings have improvements over the Ate and Twisted Ate pairings when the number of bits of $T_i$ and $T_i^e$ are less then the number of bits in $T$ and $T^e$ respectively. Also, these pairing are more efficient when the number of bits of $m$ is significantly less than the number of bits of $q$ [HZZ08].

**The Optimised Ate and Twisted Ate pairings:** The loop lengths of the Optimised Ate and Twisted Ate pairings are always no larger than the loop length of the Tate pairing. There is a reduction in the length of the loops by a factor of $(\deg(m(x)) - 1)/(\deg(m(x)))$, where $m(x)$ refers to the single variable function used in the construction of the family of pairing friendly elliptic curves [FST06] evaluated at a particular prime, when $T \geq m$ for the Optimised Ate pairing and $T^e \geq m$ for

Table 10.4: Optimizing the Pairings

| *Pairing* | *Parameter Specification* |
|---|---|
| Eta | $m \approx \#E(\mathbb{F}_q)$, supersingular curves |
| Ate | $m \approx \#E(\mathbb{F}_q)$ |
| Twisted Ate | $\lvert T^e \rvert \leq m$ |
| Ate$_i$ | $\lfloor \lg(T_i) \rfloor \leq \lfloor \lg(T) \rfloor$ |
| Twisted Ate$_i$ | $\lfloor \lg(T_i^e) \rfloor \leq \lfloor \lg(T^e) \rfloor$ |
| Optimised Ate | $T \geq m$ |
| Optimised Twisted Ate | $T^e \geq m$ |
| R-ate | $\lfloor \lg((76cd/17) \cdot \min\{a,b\}) \rfloor \leq \lfloor \lg(T_i) \rfloor$ |

the Optimised Twisted Ate pairing [HKMO07].

The following pairings are excluded from Table 10.3 as they are not of the form $f_{N,P_1}(P_2)$.

**The Squared Tate pairing:** This pairing requires fewer multiplications than the Tate pairing when using affine coordinates with the advantage that there are no restrictions imposed upon the choice of $k$. However, this is not as significant of an improvement that can be obtained with other variants of the Tate pairing.

**The R-ate pairing:** Let $\max\{a,b\} = c \cdot \min\{a,b\} + d$ where $A = aB + b$ and $A, B$ are the parameters in the pairing $R_{A,B}(D, D')$. In order for the R-ate pairing to be more efficient than the Ate$_i$ pairing, the value

$$\frac{76}{17} \cdot c \cdot d \cdot \min\{a,b\}$$

must have fewer bits than the parameter $T_i$ [LLP08].

## 10.7 Conclusion

Although in each of the specific circumstances, described in § 10.6, advantages can be obtained for each of the pairings, it is unclear if it is justifiable to substitute the Tate pairing with one of its variants in a general cryptographical setting. In [GPS06, BGOS07, HSV06, HKMO07, LLP08] emperical data has been given with regard to the cost of computing the Tate pairing, the Eta pairing, the Ate and Twisted Ate pairings, The Optimised Ate and Twisted Ate pairings, and the $\text{Ate}_i$ and R-ate pairings respectively. For the most part, the data for the variants of the Tate pairing is given for the most optimal circumstances in which the pairing may be applied, and not in a general setting. However, the trials given in [HSV06] seem to compare the cost of the Tate pairing to the Ate and Twisted Ate pairings in a broader range of settings and indicate that on average the Tate pairing is superior to the other pairings and when it is not, it is not significantly less efficient than those other pairings. It would seem worthwhile to replace the Tate pairing with one of its variants only if a given cryptosystem happened to meet a specification required to optimize the pairing computation outlined in Table 10.4. It was, however, concluded that the Weil pairing is not more efficient to compute than the Tate pairing with the currently known computational methods [GPS06].

Each of the pairings presented here have also been extended to hyperelliptic curves. In some cases, such as the Eta pairing applied to hyperelliptic curves defined over fields of characterstic 3, the pairings can be computed more quickly. However, in general they do not provide an improvement over elliptic curves [GHV07] and so they have not been included in this thesis.

One potential idea with regard to further work in this area is to further examine the following parameters: the embedding degree $k$, the prime power $q$ and the large prime $m$ dividing the order of the elliptic curve group. Doing so may shed some light on how the number of iterations of the Miller loop can reach the lower bound of $m^{1/\varphi(k)}$.

# Bibliography


[BF03] Dan Boneh and Matthew Franklin. Identity-based encryption from the weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[BGOS07] Paulo S.L.M. Barreto, Steven D. Galbraith, Colm Ó'hÉigeartaigh, and Michael Scott. Efficient pairing computation on supersingular abelian varieties. *Des Codes Crypt*, 42:239–271, 2007.

[BKLS02] Paulo S. L. M. Barreto, Hae Yong Kim, Ben Lynn, and Michael Scott. Efficient algorithms for pairing-based cryptosystems. In *CRYPTO '02: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, pages 354–368, London, UK, 2002. Springer-Verlag.

[BS96] Eric Bach and Jeffrey Shallit. *Algorithmic Number Theory, Volume i: Efficient Algorithms.* The MIT Press, 1996.

[BSS99] Ian Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic Curves in Cryptography.* Cambridge University Press, 1999.

[CC90] Leonard S. Charlap and Raymond Coley. An elementary introduction to elliptic curves. Technical Report II, Center for Communications Research-Princeton, 1990. CCR Expository Report 34, available online at `http://www.idaccr.org/reports/reports.html`.

[DF99] David S. Dummit and Richard M. Foote. *Abstract Algebra.* Prentice Hall, 1999.

[DL03] Iwan Duursma and Hyang-Sook Lee. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. In *ASIACRYPT*, volume 2894 of *Lecture Notes in Computer Science*, pages 111–123. International Association for Cryptologic Research, 2003.

[ELM04] Kirsten Eisenträger, Kristen Lauter, and Peter L. Montgomery. Improved weil and tate pairings for elliptic and hyperelliptic curves. In *The 6th Algorithmic Number Theory Symposium 2004*, volume 3076 of *Lecture Notes in Computer Science*, pages 169–183. Springer-Verlag, 2004.

[FMR99] Gerhard Frey, Michael Müller, and Hans-Georg Rück. The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Transactions on Information Theory*, 45(5):1717–1719, 1999.

[FR94] Gerhard Frey and Hans-Georg Rück. A remark concerning $m$-divisibility and discrete logarithm problem in the divisor class group of curves. *Mathematics of Computation*, 62:865–874, 1994.

[Fre06] David Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. In Florian Heß Sebastian Pauli, and Michael Pohst, editors, *The 7th Algorithmic Number Theory Symposium 2006*, volume 4076 of *Lecture Notes in Computer Science*, pages 452–465. Springer-Verlag, 2006.

[FST06] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves, 2006. Available online at `http://eprint.iacr.org/2006/372.pdf`.

[Gal05] Steven Galbraith. Pairings. In Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, editors, *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*, pages 183–213. Cambridge University Press, 2005.

[GHV07] Steven D. Galbraith, Florian Heß and Frederik Vercauteren. Hyperelliptic pairings. In Tsuyoshi Takagi, Tatsuaki Okamoto, Eiji Okamoto, and Takeshi Okamoto, editors, *Pairing-Based Cryptography – Pairing 2007 (First International Conference, Tokyo, Japan, July 2-4, 2007.)*, volume 4575 of *Lecture Notes in Computer Science*, pages 108–131. Springer, 2007.

[GPS06] Robert Granger, Dan Page, and Nigle P. Smart. High security pairing-based cryptography revisited. In *The 7th Algorithmic Number Theory Symposium 2006*, volume 4076 of *Lecture Notes in Computer Science*, pages 480–494. Springer-Verlag, 2006.

[Hit07] Laura Hitt. On the minimal embedding field. In Eiji Okamoto and Takeshi Okamoto, editors, *Pairing-Based Cryptography—Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, pages 294–301. Springer-Verlag, 2007.

[HKMO07] Florian Heß Naoki Kanayama, Seiichi Matsuda, and Eiji Okamoto. Optimised versions of the ate and twisted ate pairings. In *The 11th IMA International Conference on Cryptography and Coding 2007*, volume 4887 of *Lecture Notes in Computer Science*, pages 302–312. Springer-Verlag,

2007.

[How96] Everett W. Howe. The weil pairing and the hilbert symbol. *Mathematische Annalen*, 305(2):387–392, 1996.

[HSV06] Florian Hess, Nigel Smart, and Frederik Vercauteren. The eta pairing revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006.

[HZZ08] Jiwu Huang, Fangguo Zhang, and Chang-An Zhao. A note on the ate pairing. *International Journal of Information Security*, 2008.

[Jou00] Antoine Joux. A one round protocol for tripartite diffie-hellman. In *The 4th Algorithmic Number Theory Symposium 2000*, volume 1838 of *Lecture Notes in Computer Science*, pages 385–393. Springer, 2000.

[KM05] Neal Koblitz and Alfred Menezes. Pairing-based cryptography at high security levels. In *The 10th IMA International Conference on Cryptography and Coding 2005*, volume 3796 of *Lecture Notes in Computer Science*, pages 13–36. Springer-Verlag, 2005.

[Lic69] Stephen Lichtenbaum. Duality theorems for curves over p-adic fields. *Inventiones Mathematicae*, 7(2):120–136, 1969.

[LLP08] Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park. Efficient and generalized pairing computation on abelian varieties, 2008. Preprint; available online at `http://eprint.iacr.org/2008/040.pdf`.

[Mil86] Victor Miller. Short programs for functions on curves, 1986. Unpublished manuscript; available online at `http://crypto.stanford.edu/miller/miller.pdf`.

[Mil04] Victor S. Miller. The weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, 2004.

[MOV93] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5), 1993.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1986.

[Sol99] Jerome A. Solinas. Generalized mersenne numbers. Technical Report CORR-39, Department of Combinatorics and Optimization, University of Waterloo, 1999. Available online at `http://www.cacr.math.uwaterloo.ca/`.

[Tat59] John Tate. Applications of galois cohomology in algebraic geometry. In *Topics in Cohomology of Groups*, volume 1625 of *Lecture Notes in Mathematics*, pages 188–215. Springer Berlin / Heidelberg, 1959.

[Was03] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography.* Chapman & Hall/CRC, New Jersey, 2003.

[Wei46] André Weil. *Foundations of Algebraic Geometry.* American Mathematical Society, 1946.