# ELLIPTIC CURVE PAIRING-BASED CRYPTOGRAPHY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

BARIŞ BÜLENT KIRLAR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

SEPTEMBER 2010

Approval of the thesis:

**ELLIPTIC CURVE PAIRING-BASED CRYPTOGRAPHY**

submitted by **BARIŞ BÜLENT KIRLAR** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Ersan Akyıldız ________________
Director, Graduate School of **Applied Mathematics**

Prof. Dr. Ferruh Özbudak ________________
Head of Department, **Cryptography**

Prof. Dr. Ersan Akyıldız ________________
Supervisor, **Department of Mathematics, METU**

**Examining Committee Members:**

Assoc. Prof. Dr. Ali Doğanaksoy ________________
Department of Mathematics, METU

Prof. Dr. Ersan Akyıldız ________________
Department of Mathematics, METU

Prof. Dr. A. Ceylan Çöken ________________
Department of Mathematics, Süleyman Demirel University

Prof. Dr. Ferruh Özbudak ________________
Department of Mathematics, METU

Dr. Hamdi Murat Yıldırım ________________
Department of Computer Technology and Information Systems, Bilkent University

**Date:** ________________

**I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.**

Name, Last Name: BARIŞ BÜLENT KIRLAR

Signature :

# ABSTRACT

ELLIPTIC CURVE PAIRING-BASED CRYPTOGRAPHY

Kırlar, Barış Bülent
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ersan Akyıldız

September 2010, 87 pages

In this thesis, we explore the pairing-based cryptography on elliptic curves from the theoretical and implementation point of view. In this respect, we first study so-called pairing-friendly elliptic curves used in pairing-based cryptography. We classify these curves according to their construction methods and study them in details.

Inspired of the work of Koblitz and Menezes, we study the elliptic curves in the form $y^2 = x^3 - c$ over the prime field $\mathbb{F}_q$ and compute explicitly the number of points $\#E(\mathbb{F}_q)$. In particular, we show that the elliptic curve $y^2 = x^3 - 1$ over $\mathbb{F}_q$ for the primes $q$ of the form $27A^2 + 1$ has an embedding degree $k = 1$ and belongs to Scott-Barreto families in our classification. Finally, we give examples of those primes $q$ for which the security level of the pairing-based cryptographic protocols on the curve $y^2 = x^3 - 1$ over $\mathbb{F}_q$ is equivalent to 128-, 192-, or 256-bit AES keys.

From the implementation point of view, it is well-known that one of the most important part of the pairing computation is final exponentiation. In this respect, we show explicitly how the final exponentiation is related to the linear recurrence relations. In particular, this correspondence gives that finding an algoritm to compute final exponentiation is equivalent to finding an algorithm to compute the *m*-th term of the associated linear recurrence relation. Furthermore, we list all those work studied in the literature so far and point out how the associated linear recurrence computed efficiently.

Keywords: Elliptic Curves, Pairing-Based Cryptography, Complex Multiplication, Linear Recurrence Relation

# ÖZ

ELİPTİK EĞRİ EŞLEME TABANLI KRİPTOGRAFİ

Kırlar, Barış Bülent
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ersan Akyıldız

Eylül 2010, 87 sayfa

Bu tezde, eliptik eğriler üzerindeki eşleme tabanlı kriptografiyi teorik ve uygulama açısından inceliyoruz. Bu bağlamda, ilk olarak eşleme tabanlı kriptografide kullanılan, adına eşlemeye uygun denilen elliptik eğrileri çalışıyoruz. Bu eğrileri oluşturulma yöntemlerine göre sınıflandırıyor ve detaylı olarak açıklıyoruz.

Koblitz ve Menezes'in yaptıkları çalışmadan esinlenerek, boyutu asal $q$ olan sonlu cisim $\mathbb{F}_q$ üzerinde tanımlı $y^2 = x^3 - c$ biçimindeki eliptik eğrileri çalışıyoruz ve bu eğrilerin $\mathbb{F}_q$ üzerindeki nokta sayılarını net olarak hesaplıyoruz. Bunun yanısıra, boyutu $q = 27A^2 + 1$ biçiminde olan $\mathbb{F}_q$ üzerinde tanımlı $y^2 = x^3 - 1$ eliptik eğrisinin gömme derecesinin $k = 1$ olduğunu ve yapmış olduğumuz sınıflandırmada bu eğrinin Scott-Barreto ailesinin bir üyesi olduğunu gösteriyoruz. Son olarak, eşleme tabanlı kriptografik protokollerde kullanılan $y^2 = x^3 - 1$ eğrisinin üzerinde tanımlı olduğu $\mathbb{F}_q$ cisminin boyutunu temsil eden $q = 27A^2 + 1$ biçimindeki asallara, güvenlik seviyesi 128-, 192- ya da 256-bitlik AES anahtarlarına denk olacak şekilde örnekler veriyoruz.

Uygulama açısından, eşleme hesaplamanın en önemli bölümlerinden birisi de son üs alma işlemidir. Bu bağlamda, son üs alma işeminin, lineer yineleme bağıntısıyla nasıl bağlantılı olduğunu gösteriyoruz. Bunun yanısıra, son üs almayı hesaplayan bir algoritma bulmanın, ilgili lineer yineleme bağıntısının genel terimini hesaplayan algoritmayı bulmaya karşılık geldiğini veriyoruz. Ayrıca, şimdiye kadar literatürde çalışılmış bütün işleri listeliyor ve ilgili lineer yineleme bağıntısının etkili bir biçimde nasıl hesaplandığını ifade ediyoruz.

Anahtar Kelimeler: Eliptik Eğriler, Eşleme Tabanlı Kriptografi, Karmaşık Çarpım, Lineer Yineleme Bağıntısı

*To my little princess, Irmak Ada*

# ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor and the scientific father Prof. Dr. Ersan Akyıldız for his precious guidance, encouragement and patience during my studies. My special thanks to him also for his many great advices for the life. It is an honour for me to study with him.

I would like to give a special thanks to my dear wife Burcu Kırlar for her undying love, enormous support and great patience. With her endless understanding and generous encouragement, I have been able to continue my career in a sweet and peaceful environment.

I would like to express my deepest gratitude to my parents: To my devoted mother Alime Kırlar and to my admirable father Osman Kırlar for their love, encouragement and generous support.

I deeply thank my dear brother Mahmut Kırlar, my dear uncle Hikmet Yanartaş and their families for their love and support.

I also would like to send my special thanks to all my close relatives and my parents-in-law, Güngör family.

I am indebted to all the members of the Institute of Applied Mathematics at Middle East Technical University for their friendship, understanding and help.

Many thanks go to all my colleagues and office mates at the Middle East Technical University. I also wish to thank all my close friends whose names I may have forgotten to mention here.

# TABLE OF CONTENTS

ABSTRACT . . . . . iv

ÖZ . . . . . vi

DEDICATION . . . . . viii

ACKNOWLEDGMENTS . . . . . ix

TABLE OF CONTENTS . . . . . x

LIST OF TABLES . . . . . xiii

CHAPTERS

1 INTRODUCTION . . . . . 1

2 MATHEMATICAL BACKGROUNDS . . . . . 4

2.1 Finite Fields . . . . . 4

2.2 The Density of Prime Numbers . . . . . 5

2.3 Trace and Norm . . . . . 7

2.4 Characters and Jacobi Sums . . . . . 7

2.5 Elliptic Curves over Finite Fields . . . . . 10

2.6 Torsion Points on Elliptic Curves . . . . . 13

2.7 The Embedding Degree . . . . . 13

2.8 Curve Endomorphisms . . . . . 14

2.9 The Elliptic Curve $y^2 = x^3 - c$ . . . . . 14

3 PAIRING-BASED CRYPTOGRAPHY . . . . . 16

3.1 Bilinear Pairings . . . . . 16

3.2 Security of Pairings . . . . . 17

3.3 Pairing-Based Cryptographic Protocols . . . . . 18

3.3.1 Joux's One Round Three Party Key Agreement Protocol . 18

3.3.2 Short Signatures . . . . . 18

3.3.3 Identity-Based Cryptosystems . . . . . . . . . . . . . . . . 19

3.4 Divisors on Elliptic Curves . . . . . . . . . . . . . . . . . . . . . . . . 20

3.5 Weil Pairing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 21

3.6 Simplified Weil Pairing . . . . . . . . . . . . . . . . . . . . . . . . . 24

3.7 Tate Pairing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 25

3.8 Simplified Tate Pairing . . . . . . . . . . . . . . . . . . . . . . . . . 28

3.9 Construction of One Variable Non-Degenerate Pairings . . . . . . . 28

3.9.1 Distortion Maps . . . . . . . . . . . . . . . . . . . . . . . . 28

3.9.2 Twist Curves . . . . . . . . . . . . . . . . . . . . . . . . . 29

3.10 Eta and Ate Pairing . . . . . . . . . . . . . . . . . . . . . . . . . . 29

4 PAIRING-FRIENDLY ELLIPTIC CURVES . . . . . . . . . . . . . . . . . 32

4.1 Complex Multiplication . . . . . . . . . . . . . . . . . . . . . . . . . 32

4.2 Generalized Pell Equation . . . . . . . . . . . . . . . . . . . . . . . . 34

4.3 Hilbert Polynomials . . . . . . . . . . . . . . . . . . . . . . . . . . . 34

4.4 Generating Pairing-Friendly Elliptic Curves . . . . . . . . . . . . . 36

4.4.1 Families of Pairing-Friendly Elliptic Curves . . . . . . . . 37

4.5 Supersingular Elliptic Curves . . . . . . . . . . . . . . . . . . . . . . 40

4.5.1 Embedding Degree $k = 1$ Curves . . . . . . . . . . . . . . . 41

4.5.2 Embedding Degree $k = 2$ Curves . . . . . . . . . . . . . . . 42

4.5.3 Embedding Degree $k = 3$ Curves . . . . . . . . . . . . . . . 43

4.5.4 Embedding Degree $k = 4$ Curves . . . . . . . . . . . . . . . 45

4.5.5 Embedding Degree $k = 6$ Curves . . . . . . . . . . . . . . . 46

4.6 Ordinary Elliptic Curves . . . . . . . . . . . . . . . . . . . . . . . . 46

4.6.1 The MNT Method . . . . . . . . . . . . . . . . . . . . . . 47

4.6.1.1 MNT Curves for $k = 3, 4, 6$ . . . . . . . . . . 47

4.6.1.2 Freeman Curves for $k = 10$ . . . . . . . . . . 48

4.6.2 Extensions of the MNT Method . . . . . . . . . . . . . . 49

4.6.3 The Cocks-Pinch Method . . . . . . . . . . . . . . . . . . . 49

4.6.4 Extensions of the Cocks-Pinch Method . . . . . . . . . . 50

4.6.4.1 Cyclotomic Families . . . . . . . . . . . . . . . 53

4.6.4.2 Sporadic Families of Brezing-Weng Curves . 56

4.6.4.3 Scott-Barreto Families . . . . . . . . . . . . 58

4.6.4.4 Variable Discriminants $D$ in Cyclotomic Families . . . . . . . . . . . . . . . . . . . . . 63

4.6.5 The Dupont-Enge-Morain Method . . . . . . . . . . . . 66

4.6.6 Extension of the Dupont-Enge-Morain Method . . . . . . 67

5 EFFICIENT EXPONENTIATION IN PAIRING-BASED CRYPTOGRAPHY 68

5.1 The Final Exponentiation . . . . . . . . . . . . . . . . . . . . . . . . 68

5.2 Compression in Finite Fields . . . . . . . . . . . . . . . . . . . . . 69

5.2.1 Compression Factor 2 . . . . . . . . . . . . . . . . . . . . . 71

5.2.2 Compression Factor 3/2 . . . . . . . . . . . . . . . . . . . 72

5.2.3 Compression Factor 3 . . . . . . . . . . . . . . . . . . . . . 73

5.2.4 Compression Factor 5/2 . . . . . . . . . . . . . . . . . . . 74

5.2.5 Compression Factor 4 and 6 . . . . . . . . . . . . . . . . . 74

5.2.6 Compression Factor 7/3 . . . . . . . . . . . . . . . . . . . 75

5.3 Compressed Pairings . . . . . . . . . . . . . . . . . . . . . . . . . . 77

6 CONCLUSION . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 79

REFERENCES . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 80

VITA . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 86

# LIST OF TABLES

TABLES

Table 4.1 Supersingular elliptic curves with $k = 1$ over $F_{2^n}$ for even $n$ . . . . . . . . . 41

Table 4.2 Supersingular elliptic curves with $k = 1$ over $F_{3^n}$ for even $n$ . . . . . . . . . 41

Table 4.3 Supersingular elliptic curves with $k = 2$ over $F_{2^n}$ . . . . . . . . . . . . . . . 42

Table 4.4 Supersingular elliptic curves with $k = 2$ over $F_{3^n}$ . . . . . . . . . . . . . . . 43

Table 4.5 Family of supersingular curves with embedding degree $k = 3$ . . . . . . . . 44

Table 4.6 Supersingular elliptic curves with $k = 3$ over $F_{2^n}$ for even $n$ . . . . . . . . . 44

Table 4.7 Supersingular elliptic curves with $k = 3$ over $F_{3^n}$ for even $n$ . . . . . . . . . 45

Table 4.8 Supersingular elliptic curves with $k = 4$ over $F_{2^n}$ for odd $n$ . . . . . . . . . 45

Table 4.9 Supersingular elliptic curves with $k = 6$ over $F_{3^n}$ for odd $n > 1$ . . . . . . . 46

Table 4.10 Representation of MNT curves . . . . . . . . . . . . . . . . . . . . . . . . 48

Table 4.11 Families with odd $k < 1000$ and $D = 1$ . . . . . . . . . . . . . . . . . . . . 54

Table 4.12 Families with $k < 1000$, $3 \mid k$, $l = \mathrm{lcm}(8, k)$ and $D = 2$ . . . . . . . . . . . . 54

Table 4.13 Families with $k \leq 1000$, $18 \nmid k$, $l = \mathrm{lcm}(6, k)$ and $D = 3$ . . . . . . . . . . . 55

Table 4.14 Minimum bit lengths of $r$ and $q$ . . . . . . . . . . . . . . . . . . . . . . . . 63

# CHAPTER 1

# INTRODUCTION

Over the last years, bilinear pairings, the Weil and Tate pairings derived from certain elliptic curves of embedding degree $k$ with $k \leq 50$, have been used widely to implement pairing-based cryptographic protocols. Although, the Weil pairing was initially proposed in [12] as a suitable construction for the realisation of such protocols, it is now usually accepted that the Tate pairing is preferable for its greater efficiency. Efficient computation of the Tate pairing on supersingular elliptic curves and certain ordinary curves that are equally suitable for pairing-based schemes have been suggested in [6, 4, 36]. In fact, ordinary curves offer more flexibility for the choice of security parameters [6, 74]. The Weil and Tate pairings are efficiently computed by using the Miller's algorithm [73].

More recently, the cryptography researchers are focused on shortening the loop length in Miller's algorithm, which was initiated by Duursma-Lee [28] and extended by Barreto et al. [3] to supersingular abelian varieties using the Eta pairing approach. The ate pairing, which is introduced in [44] for elliptic curves, is then generalized to hyperelliptic curves in [41]. Recently, several variants of the above pairings were introduced by shortening the loop length in Miller's algorithm. Those are so-called generalized pairings [96], optimized pairings [68], the R-ate pairing [63] and optimal pairings [90].

Elliptic curves with small embedding degree and large prime-order subgroup have a great interest for implementing pairing-based cryptographic systems. Such curves, which is so-called "pairing-friendly" are rare and thus require specific constructions. Cryptosystems such as one-round three party key exchange [49], identity-based encryption [12] and short signature schemes [13] require pairing-friendly elliptic curves. The interest in recent times is to explore various methods of constructing pairing-friendly curves with prescribed embedding degrees.

The first work for constructing pairing-friendly elliptic curves is described by Miyaji, Nakabayashi and Takano [74]. They constructed elliptic curves of prime order and embedding degree $k \in \{3, 4, 6\}$. Such curves are now called MNT curves and the size of the field $q$ is approximatelly the same as the subgroup order $r$. Extensions of the MNT method in the sense of constructing elliptic curves of near-prime order were investigated by Scott and Barreto [82] and more recently by Galbraith, McKee and Valença [37]. Later, several methods have been proposed to construct curves with arbitrary $k$ by Cocks and Pinch [22] and Dupont, Enge and Morain [26], respectively. In general, these methods only achieve $\rho = \log q / \log r \approx 2$. The Cocks-Pinch method is extented by Scott and Barreto [82] and independently Brezing and Weng [17] which is due originally the work of Barreto, Lynn and Scott [5].

The other component of pairing-based cryptography is so-called the final exponentiation. This is done by raising the output of pairing value to the power of $(q^k - 1)/r$ to get a unique value in the group of $r$-th roots of unity $G_{r,q,k}$ that is the subgroup of the cyclotomic subgroup $\Phi_k(q)$ in the extension fields $\mathbb{F}^*_{q^k}$. It is well-known that pairing-based cryptographic protocols require these components.

In recent years, there have been several studies on compressing the elements of certain subgroups of some field extensions. The compression methods fall into two categories in these work. They either use the trace representation of elements or a rational parametrization of algebraic torus. We only consider the trace representation in this work.

In 1994, the first proposal is given by Smith and Skinner using the Lucas sequences. They showed that the elements of a subgroup $G_{r,q,2}$ whose order $r$ divides $\Phi_2(q) = q + 1$ in $\mathbb{F}^*_{q^2}$ could be identified by their traces over $\mathbb{F}_q$. In other words, the elements of $G_{r,q,2}$ can be uniquely identified up to conjugation using the characteristic polynomials over $\mathbb{F}_q$. Morever, they showed that exponentiation in $G_{r,q,2}$ can be efficiently performed using the trace representation. Their construction provides a compression factor 2. Gong and Harn [40] showed that the elements of a subgroup $G_{r,q,3}$ whose order $r$ divides $\Phi_3(q) = q^2 + q + 1$ in $\mathbb{F}^*_{q^3}$ could be identified with a compression factor 3/2. They also obtained an efficient exponentiation for the compressed form of those elements. Brouwer, Pellikaan and Verheul [18] obtained a compression factor 3 by representing the elements of a subgroup $G_{r,q,6}$ whose order $r$ divides $\Phi_6(q) = q^2 - q + 1$ in $\mathbb{F}^*_{q^6}$. However, they did not give an algorithm to exponentiate the elements of $G_{r,q,6}$ in compressed form.

In 2000, Lenstra and Verheul [64] showed that the elements of subgroup $G_{r,q,6}$ whose order $r$ dividing $\Phi_6(q) = q^2 - q + 1$ in $\mathbb{F}^*_{q^6}$ can be uniquely represented by their traces over $\mathbb{F}_{q^2}$. They gave a very efficient exponentiation algorithm in $G_{r,q,6}$ with a compression factor 3. Verheul et al. in [16] obtained a precise formulation for representations of elements in extension fields of arbitrary degree. In 2004, Giuliani and Gong [38] obtained a compression factor 5/2 in a subgroup $G_{r,q,10}$ of order $r$ dividing $\Phi_{10}(q) = q^4 - q^3 + q^2 - q + 1$ in $\mathbb{F}^*_{q^{10}}$ using the fifth order characteristic sequences over $\mathbb{F}_{q^2}$. They obtained an algoritm to exponentiate the compressed form of elements in $G$ and also proposed more efficient algorithm in [39].

More recently, Shirase et al. [85] considered that the elements of subgroup $G_{r,q,6}$ whose order $r$ dividing $q - \sqrt{3q} + 1$ in $\mathbb{F}^*_{q^6}$ where $q = 3^t$ for some odd $t$ and they showed that those elements in $G_{r,q,6}$ can be uniquely represented (up to conjugation) with a compression factor 6 over $\mathbb{F}_q$. They also presented an algorithm for exponentiation of those elements. In 2009, using the same trick in [85], Karabina [54] observed that the elements of order dividing $q \pm \sqrt{3q} + 1$ in $\mathbb{F}^*_{q^6}$ where $q = 3^t$ for some odd $t$ and the elements of order dividing $q \pm \sqrt{2q} + 1$ in $\mathbb{F}^*_{q^4}$ where $q = 2^t$ for some odd $t$ can be uniquely represented by their traces over $\mathbb{F}_q$ with a compression factor 6 and 4, respectively. He presented five exponentiation algorithms for compression factor 4 and six exponentiation algorithms for compression factor 6. Morever, he compared those exponentiation algorithms.

This thesis is organized as follows. In Chapter 2, we review the mathematical backgrounds about finite fields and elliptic curves over finite fields. In Chapter 3, we discuss basic facts used in elliptic curve pairing based cryptography. In Chapter 4, we give the complex multiplication (CM) method and show how to use it to construct pairing friendly elliptic curves of varies embedding degree. In Chapter 5, we describe the final exponentiation and show how it is related to the linear recurrence relations. Moreover, we list all those work studied in the literature so far. We conclude and give some future work in Chapter 6.

# CHAPTER 2

# MATHEMATICAL BACKGROUNDS

In this chapter, we are going to give the mathematical backgrounds which is necessary for the rest of the thesis. In this respect, basic facts about finite fields and elliptic curves over finite fields have been given.

## 2.1 Finite Fields

For every prime $p$ and any positive integer $n$, there exists a unique (up to isomorphism) finite field with $p^n$ elements. This field is denoted by $\mathbb{F}_{p^n}$ and can be constructed as follows:

(1) $\mathbb{F}_p$ : For every prime $p$, a finite field with $p$ elements denoted by $\mathbb{F}_p$ may be identified by integers modulo $p$, that is, $\mathbb{F}_p \cong \mathbb{Z}/ < p >= \{0, 1 \cdots, p-1\}$. One can perform the operations (addition and multiplication) on $\mathbb{F}_p$ using the usual operation on integers, followed by reduction modulo $p$. On the other hand, inversion can be done using the extended Euclidean algorithm for integers.

(2) $\mathbb{F}_{p^n}$ : Given any prime $p$ and $n \in \mathbb{Z}^+$, there exists an irreducible monic polynomial $p(x)$ over $\mathbb{F}_p[x]$ of degree $n$ [65, Theorem 2.5]. Then a simple algebraic extension $\mathbb{F}_p[x]/ < p(x) >$ of $\mathbb{F}_p$ can be identified by $\mathbb{F}_p(\alpha) \subset \overline{\mathbb{F}_p}$, the algebraic closure of $\mathbb{F}_p$. This extension $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^n}$ has exactly $p^n$ elements and every element of the extension field $\mathbb{F}_{p^n}$ can be uniquely represented by the polynomial $\sum_{i=0}^{n-1} c_i\alpha^i$, where $c_i \in \mathbb{F}_p$. The operations on $\mathbb{F}_{p^n}$ are performed by using the polynomial operations with modulo $p(x)$ reduction. As in the prime field case, extended Euclidean algorithm for polynomials can be used to compute the inversion in $\mathbb{F}_{p^n}$. It is well-known that any finite field $F$ is isomorphic to $\mathbb{F}_{p^n}$ for some prime $p$ and $n \in \mathbb{Z}^+$, where $p$ is the characteristic of $F$ and

$n$ is the degree of $F$ over its prime subfield [65, Theorem 2.2].

## 2.2 The Density of Prime Numbers

In the literature, the density of prime numbers has a long history, going back to Gauss and Legendre. They first conjectured prime number theorem in the late 18th century, independently.

**Theorem 2.2.1 (Prime Number Theorem)** *Let $\pi(N)$ be the number of primes less than or equal to $N$. Then*

$$\pi(N) \sim \frac{N}{\log N}.$$

*That is, $\pi(N)$ is asymptotically equal to $N/\log N$ as $N \to \infty$.*

In particular, Gauss conjectured an equivalent form of the prime number theorem by defining the function

$$\mathrm{Li}(N) := \int_2^N \frac{dt}{\log t},$$

which was a good approximation to $\pi(N)$.

In the beginning of 20th century, Hardy and Littlewood [42] developed a number of conjectures, one of these, Conjecture F, concerned the density of prime numbers of the form $f(x) = ax^2 + bx + c$. This conjecture says that there are infinitely many primes of the form $f(x) = ax^2 + bx + c$ provided that $a \in \mathbb{Z}^+$, $b, c \in \mathbb{Z}$, $\gcd(a, b, c) = 1$, $a + b$ and $c$ are not both even, and the discriminant $D = b^2 - 4ac$ is not a square. Furthermore, it predicts the number of such primes less than or equal to $N$, which is asymptotically given by

$$\pi_{(f)}(N) \sim \frac{\epsilon \cdot C}{\sqrt{a}} \frac{\sqrt{N}}{\log N} \prod (\frac{p}{p-1}).$$

Here, the product is taken over the common odd prime divisors $p$ of $a$ and $b$, $\epsilon$ is 1 if $a + b$ is odd and 2 if $a + b$ is even, and

$$C = \prod_{\substack{prime\ l \geq 3 \\ l \nmid a}} (1 - \frac{\chi_2(D)}{l-1}),$$

where the quadratic character $\chi_2$ is a homomorphism from $\mathbb{F}_l^*$ to $\mathbb{C}^*$ such that $\chi_2^2 = 1$.

In the middle of 20th century, Bateman and Horn [8] has come up with another conjecture which generalizes the conjecture of Hardy and Littlewood. Namely, let $f_1, \cdots, f_k$ be polynomials in one variable with integral and positive leading coefficients. Let $h_1, \cdots, h_k$ be their degrees, respectively. Let $f$ be the product of these polynomials $f = f_1 \cdots f_k$. Suppose each of these polynomials is irreducible over the field of rational numbers and they are pairwise relatively prime. Let $\pi_{(f)}(N)$ denote the number of positive integers $n$ between 1 and $N$ such that $f_1(n), \cdots, f_k(n)$ are all primes. Then Bateman-Horn conjecture says that $\pi_{(f)}(N)$ is asymptotically given by

$$\pi_{(f)}(N) \sim \frac{C(f_1, \cdots, f_k)}{h_1 h_2 \cdots h_k} \int_2^N \frac{dt}{(\log t)^k},$$

where

$$C(f_1, \cdots, f_k) = \prod_p \left\{(1 - \frac{1}{p})(1 - \frac{N_{(f)}(p)}{p})\right\},$$

the product being taken over all primes and $N_{(f)}(p)$ being the number of solutions of the congruence

$$f(n) = f_1(n) f_2(n) \cdots f_k(n) \equiv 0 \pmod{p},$$

where $1 \leq n \leq N$.

The following example gives a conjectural density of prime numbers in the form $f(A) = 27A^2 + 1$ that we used in Section 4.6.4.3. In particular, it shows that there are infinitely many such primes.

**Example 2.2.2** *Let $\pi_{(f)}(N)$ denote the number of primes in the form $f(A) = 27A^2 + 1$ for $1 \leq A \leq N$. Bateman and Horn conjecture [8] indicates*

$$\pi_{(f)}(N) \sim \frac{1}{2} \prod_{\substack{prime\ l \\ l \nmid 3}} (1 - \frac{\chi_2(-3)}{l-1}) \int_2^N \frac{dA}{\log A}.$$

*By using the computation in [84, Table 2], it can be checked that*

$$\pi_{(f)}(N) \sim 0.560366375 \int_2^N \frac{dA}{\log A}.$$

*We would also like to note that according to Hardy and Littlewood [42, Conjecture F], this value $\pi(N)$ is asymptotically given by*

$$\pi_{(f)}(N) \sim 0.323527677 \frac{\sqrt{N}}{\log N}.$$

## 2.3 Trace and Norm

**Definition 2.3.1** *Let $q = p^n$ with prime $p$, and let $k$ be a positive integer. Let $\sigma$ be the Frobenius automorphism of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ defined by $\sigma(\alpha) = \alpha^q$ for $\alpha \in \mathbb{F}_{q^k}$. Then trace of $\alpha$ with respect to $\mathbb{F}_q$ is defined by*

$$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha) = \sum_{i=0}^{k-1} \sigma^i(\alpha) = \sum_{i=0}^{k-1} \alpha^{q^i}$$

*and norm of $\alpha$ with respect to $\mathbb{F}_q$ is defined by*

$$\mathrm{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(\alpha) = \prod_{i=0}^{k-1} \sigma^i(\alpha) = \prod_{i=0}^{k-1} \alpha^{q^i}.$$

## 2.4 Characters and Jacobi Sums

**Definition 2.4.1** *A multiplicative character $\chi$ on $\mathbb{F}_q$, where $q = p^n$, is a map from $\mathbb{F}_q^*$ to the nonzero complex numbers $\mathbb{C}^*$ that satisfies*

$$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta) \; for \; all \; \alpha, \beta \in \mathbb{F}_q^*.$$

The trivial character denoted by $\chi_{triv}$ is given by $\chi_{triv}(\alpha) = 1$ for all $\alpha \in \mathbb{F}_q^*$. Given a character $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$, $\chi^{-1}$ denote the inverse of $\chi$ in $\mathbb{F}_q^*$, which is also a character and in fact $\chi^{-1} = \overline{\chi}$; namely $\chi^{-1}(x) = \overline{\chi}(x)$ for all $x \in \mathbb{F}_q^*$. It is convenient to extend the domain of definition of a character $\chi$ from $\mathbb{F}_q^*$ to $\mathbb{F}_q$ by setting

$$\begin{cases} \chi(0) = 1, & if \; \chi \; is \; trivial \\ \chi(0) = 0, & if \; \chi \; is \; nontrivial \end{cases}$$

With this definition, it is clear that we have

$$\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) = \begin{cases} q, & if \; \chi \; is \; trivial \\ 0, & if \; \chi \; is \; nontrivial \end{cases}$$

**Definition 2.4.2** *Let $\chi$ and $\psi$ denote the multiplicative characters on $\mathbb{F}_q$. The Jacobi sum $J(\chi, \psi)$ is defined by*

$$J(\chi, \psi) = \sum_{\alpha \in F_q} \chi(\alpha)\psi(1 - \alpha).$$

Since $\alpha \longrightarrow 1-\alpha$ is a permutation on $\mathbb{F}_q$, we obtain that Jacobi sums have the symmetry property

$$J(\chi,\psi) = J(\psi,\chi).$$

For the rest of this section, we give some basic facts related to the characters and Jacobi sums that will be used in Section 4.6.4.3. The proof of the following can be found in [48, Theorem 8.3.1].

**Proposition 2.4.3** *Let $\chi_{triv}$ be trivial character on $\mathbb{F}_q$. Then for any character $\chi$, we have the following:*

*(a)* $J(\chi_{triv},\chi_{triv}) = q.$

*(b)* $J(\chi_{triv},\chi) = 0.$

*(c)* $J(\chi,\overline{\chi}) = -\chi(-1).$

In this thesis, we consider quadratic, cubic and sextic characters to compute the number of points $\#E(\mathbb{F}_q)$ of the elliptic curve $y^2 = x^3 - c$ over $\mathbb{F}_q$ with $q \equiv 1 \pmod 3$ in Section 4.6.4.3. We now give some facts about these characters.

Let $\chi_i : \mathbb{F}_q^* \to \mathbb{C}^*$ be characters for $i = 2, 3$ and 6, which are defined by

$$\chi_2(g^j) = (-1)^j, \ \chi_3(g^j) = \delta^j \text{ and } \chi_6(g^j) = (-\delta)^j$$

respectively, where $\mathbb{F}_q^* =< g >$ and $\delta = \frac{-1+i\sqrt{3}}{2}$.

We note that for the character $\chi_2$, we have

$$\chi_2(-1) = (-1)^{\frac{q-1}{2}} = \begin{cases} 1, & if \ \ q \equiv 1 \pmod{12} \\ -1, & if \ \ q \not\equiv 1 \pmod{12} \end{cases}$$

We need the following lemmas, where the proofs can be found in [92, Section 4.4].

**Lemma 2.4.4** *Let $q \equiv 1 \pmod 3$ be prime and let $x \in \mathbb{F}_q^*$. Then*

$$\#\{u \in \mathbb{F}_q^* \mid u^2 = x\} = \sum_{l=0}^{1} \chi_2(x)^l,$$

*and*

$$\#\{u \in \mathbb{F}_q^* \mid u^3 = x\} = \sum_{l=0}^{2} \chi_3(x)^l.$$

**Lemma 2.4.5** *Let* $q \equiv 1 \pmod 3$ *be prime. Then*

$$\sum_{\alpha\in\mathbb{F}_q} \chi_2(\alpha)^l = \begin{cases} q, & \text{if } l \equiv 0 \pmod 2 \\ 0, & \text{if } l \not\equiv 0 \pmod 2 \end{cases}$$

*and*

$$\sum_{\alpha\in\mathbb{F}_q} \chi_3(\alpha)^l = \begin{cases} q, & \text{if } l \equiv 0 \pmod 3 \\ 0, & \text{if } l \not\equiv 0 \pmod 3 \end{cases}$$

**Lemma 2.4.6** *Let* $S = \{(x,y) \mid x,y \in \mathbb{F}_q^*;\ x,y \neq 1;\ x \neq y\}$. *Then the map*

$$\sigma \ : \ (x,y) \rightarrow \Big(\frac{x}{y}, \frac{1-x}{1-y}\Big)$$

*is a permutation of* $S$.

This lemma helps us to prove the following fact.

**Proposition 2.4.7** $|J(\chi_3,\chi_3)|^2 = q$.

**Proof.**

$$\begin{aligned} |J(\chi_3,\chi_3)|^2 &= \sum_{a\neq 0,1} \chi_3(a)\chi_3(1-a)\overline{\sum_{b\neq 0,1} \chi_3(b)\chi_3(1-b)} \\ &= \sum_{a\neq 0,1}\sum_{b\neq 0,1} \chi_3(\frac{a}{b})\chi_3(\frac{1-a}{1-b}) \\ &= \sum_{a=b}\chi_3(\frac{a}{b})\chi_3(\frac{1-a}{1-b}) + \sum_{(a,b)\in S} \chi_3(\frac{a}{b})\chi_3(\frac{1-a}{1-b}) \\ &= (q-2) + \sum_{(c,d)\in S} \chi_3(c)\chi_3(d) \\ &= (q-2) + \sum_{d\neq 0,1} \chi_3(d)\Big(\sum_{c\in F_q^*} \chi_3(c) - \chi_3(1) - \chi_3(d)\Big) \\ &= (q-2) + \sum_{d\neq 0,1} \chi_3(d)(0 - 1 - \chi_3(d)) \\ &= (q-2) - \sum_{d\neq 0,1} \chi_3(d) - \sum_{d\neq 0,1} \chi_3(d)^2 \\ &= (q-2) + \chi_3(1) + \chi_3(1)^2 \\ &= q \end{aligned}$$

■

We need the following facts that the proofs can be found in [10, Chapter 2].

**Proposition 2.4.8** *Let $q > 2$. If $\chi$ is a nontrivial character on $\mathbb{F}_q$ and $\chi_2$ is the quadratic character on $\mathbb{F}_q$, then*

$$J(\chi, \chi_2) = \chi(4) J(\chi, \chi).$$

**Proposition 2.4.9** *Let $\chi_3$ be a cubic character on $\mathbb{F}_q$, where $q \equiv 1 \pmod 3$. Then $\chi_3(2) = 1$ if and only if $q = x^2 + 27y^2$ for some integers $x$ and $y$.*

Now, we will give an important fact which is proved in [48, Proposition 8.3.4].

**Proposition 2.4.10** *Let $q \equiv 1 \pmod 3$ be a prime. Then*

$$J(\chi_3, \chi_3) = -1 \pmod 3$$

*in the ring $\mathbb{Z}[\delta] = \mathbb{Z}[x]/ < x^2 + x + 1 >$, where $\delta = \frac{-1+i\sqrt{3}}{2}$ is the complex cube root of unity.*

## 2.5 Elliptic Curves over Finite Fields

Let $\mathbb{F}_q$ be a finite field with $q = p^n$. Then the algebraic closure of $\mathbb{F}_q$ is given by $\overline{\mathbb{F}_q} = \bigcup_{i \geq 1} \mathbb{F}_{q^i}$. An elliptic curve $E$ over $\mathbb{F}_q$, denoted by $E(\mathbb{F}_q)$, is defined to be the set of solutions in the projective plane $\mathbb{P}^2(\overline{\mathbb{F}_q})$ of a homogeneous fuction $F$ in the form

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,$$

where $a_1, a_2, a_3, a_4, a_6 \in \overline{\mathbb{F}_q}$. For the rest of the thesis, we take $E(\overline{\mathbb{F}_q}) = E$. We require the curve $E$ to be a non-singular. In other words, the partial derivatives $\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}$ and $\frac{\partial F}{\partial Z}$ shoud not vanish simultaneously at any point on the curve. The curve $E$ has exactly one point with coordinate $Z$ equal to zero, namely $(0 : 1 : 0)$. This point is so called *point at infinity* and denoted by $\infty$.

For convenience, by using the affine coordinates $x = X/Z$ and $y = Y/Z$, we get the affine version of the Weierstrass equation as follows

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

where the coefficients $a_i$ are in the field $\mathbb{F}_q$. Then, the elliptic curve is the set of points $(x, y) \in \mathbb{A}^2(\overline{\mathbb{F}_q}) = \overline{\mathbb{F}_q} \times \overline{\mathbb{F}_q}$ that satisfy the affine equation (2.1) together with $\infty$. The curve

$E$ has an additive group structure determined by the fact that $\infty$ is an identity element and $P, Q, R \in E : P + Q + R = \infty$ if and only if $R$ lies in the line joining $P$ to $Q$ in the projective space. The group operation in this group structure is usually called *chord-and-tangent rule*. It is clear from the definition that the set of $\mathbb{F}_{q^k}$-rational points of $E$ is a subgroup of $E$ for any $k \geq 1$. This subgroup is denoted by $E(\mathbb{F}_{q^k})$. In fact, $E(\mathbb{F}_{q^k})$ consists of all solutions of (2.1) in $\mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$ together with $\infty$.

Two elliptic curves $E_1(\mathbb{F}_q)$ and $E_2(\mathbb{F}_q)$ are isomorphic over $\mathbb{F}_q$, denoted by $E_1(\mathbb{F}_q) \cong E_2(\mathbb{F}_q)$, if there exist $u, r, s, t \in \mathbb{F}_q$, $u \neq 0$ such that the change of variables, so called admissible change of variables,

$$(x, y) \longmapsto (u^2x + r, u^3y + u^2sx + t)$$

transforms the equation $E_1$ into the equation $E_2$. If $E$ is an elliptic curve over $\mathbb{F}_q$ with characteristic $p > 3$, then it can be shown that this curve $E$ isomorphic to the curve given by so-called Weierstrass equation

$$E \; : \; y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q,$$

where $\Delta = -16(4a^3 + 27b^2) \neq 0$ in $\mathbb{F}_q$. By using the *chord-and-tangent rule*, we now give the explicit formula for the addition of two points in the curve $E$ defined over $\mathbb{F}_q$ of characteristic $p > 3$. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be the points on $E$ with $P, Q \neq \infty$ and $Q \neq -P$. Then

- If $P \neq Q$, then $P + Q = (x_3, y_3)$, where

$$\begin{cases} x_3 = (\dfrac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \\ y_3 = (\dfrac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) - y_1 \end{cases}$$

- If $P = Q$, then $2P = (x_3, y_3)$, where

$$\begin{cases} x_3 = (\dfrac{3x_1^2 - a}{2y_1})^2 - 2x_1 \\ y_3 = (\dfrac{3x_1^2 - a}{2y_1})(x_1 - x_3) - y_1 \end{cases}$$

Similarly, one can simplify the Weierstrass equation for curves over $\mathbb{F}_q$ of characteristic $p = 2, 3$ and get similar formula as above (see [86, Appendix A]).

Let $E$ be an elliptic curve defined over $\mathbb{F}_q$. The number of points in $E(\mathbb{F}_q)$, called the order of the elliptic curve over $\mathbb{F}_q$, is denoted by $\#E(\mathbb{F}_q)$. The trace of the Frobenius or simply trace of a curve is the value $t$ satisfying $\#E(\mathbb{F}_q) = q + 1 - t$. The elliptic curve $E(\mathbb{F}_q)$ is said to be supersingular if the characteristic $p$ of $\mathbb{F}_q$ divides $t$, otherwise it is called ordinary. In other words, the curve $E(\mathbb{F}_q)$ is supersingular if $t \equiv 0 \pmod{p}$. The following fact improves the above bound on the size of $E(\mathbb{F}_q)$, whose proof is given in [86, Chapter V].

**Theorem 2.5.1 (Hasse)** *Let E be an elliptic curve defined over* $\mathbb{F}_q$. *Then,*

$$|t| \leq 2\sqrt{q}.$$

We now give a useful result that enables one to compute $\#E(\mathbb{F}_{q^k})$ from $\#E(\mathbb{F}_q)$, that the proof can be found in [86, Chapter V].

**Theorem 2.5.2 (Weil)** *Let E be an elliptic curve over* $\mathbb{F}_q$, *and let* $t = q + 1 - \#E(\mathbb{F}_q)$. *Let* $\phi_q : E \to E$ *be the Frobenius map given by* $(x, y) \mapsto (x^q, y^q)$. *Write the characteristic polynomial of* $\phi_q$ *as* $x^2 - tx + q = (x - \alpha)(x - \beta)$ *in* $\mathbb{C}[x]$. *Then*

$$\#E(\mathbb{F}_{q^k}) = q^k + 1 - (\alpha^k + \beta^k)$$

*for all* $k \geq 1$.

The characteristic polynomial of the Frobenius map $x^2 - tx + q$ allows us to introduce the following recurrence relation $\{V_n\}$, which is so-called Lucas sequence [87],

$$V_n = tV_{n-1} - qV_{n-2}$$

with the initial condition $V_0 = 2$ and $V_1 = t = \alpha + \beta = q + 1 - \#E(\mathbb{F}_q)$. Then $V_k = \alpha^k + \beta^k$ and therefore $\#E(\mathbb{F}_{q^k}) = q^k + 1 - V_k$. The Lucas sequence $\{V_n\}$ can be efficiently computed in [50] depending on the relations

$$\begin{aligned} V_{n+m} &= V_n V_m - q^m V_{n-m} \\ V_{2n} &= V_n^2 - 2q^n \end{aligned}$$

for $n, m \in \mathbb{Z}$. We shall quote the algorithm from [50] and discuss comprehensively in Section 5.2.1.

**Example 2.5.3** *Let E be the elliptic curve given by*

$$y^2 = x^3 - 1$$

*over* $\mathbb{F}_{19}$*. There are* 28 *points which are listed as follows:*

| | | | | | | |
|---|---|---|---|---|---|---|
| $(1,0)$ | $(2,8)$ | $(2,11)$ | $(3,8)$ | $(3,11)$ | $(4,5)$ | $(4,14)$ |
| $(6,5)$ | $(6,14)$ | $(7,0)$ | $(8,6)$ | $(8,13)$ | $(9,5)$ | $(9,14)$ |
| $(10,7)$ | $(10,12)$ | $(11,0)$ | $(12,6)$ | $(12,13)$ | $(13,7)$ | $(13,12)$ |
| $(14,8)$ | $(14,11)$ | $(15,7)$ | $(15,12)$ | $(18,6)$ | $(18,13)$ | $\infty$ |

*Therefore, the trace of Frobenius* $t = V_1 = 19 + 1 - \#E(\mathbb{F}_{19}) = -8$*. We can easily compute the number of points of* $E$ *over* $\mathbb{F}_{19^2}$ *by using the Lucas sequence* $\{V_n\}$*, that is,*

$$\#E(\mathbb{F}_{19^2}) = 19^2 + 1 - V_2,$$

*where* $V_2 = V_1 \cdot V_1 - q \cdot V_0 = 28 \cdot 28 - 19 \cdot 2 = 26$*, thus we get* $\#E(\mathbb{F}_{19^2}) = 336$.

## 2.6 Torsion Points on Elliptic Curves

Let $E$ be an elliptic curve over $\mathbb{F}_q$ and for any integer $r > 0$, let $E[r] = \{P \in E \mid rP = \infty\}$. $E[r]$ is a subgroup of $E$ containing all $r$-torsion elements of $E$.

It is not difficult to show that there exists $k \in \mathbb{Z}^+$ such that $E[r] \subset E(\mathbb{F}_{q^k})$. The following theorem gives the group structure of $E[r]$ (see [92, Section 3.2]).

**Theorem 2.6.1** *Let* $E$ *be an elliptic curve over* $\mathbb{F}_q$ *of characteristic* $p$*, and let* $r \in \mathbb{Z}^+$*. If* $p \nmid r$*, then* $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$*. If* $p \mid r$*, write* $r = p^n r'$ *with* $p \nmid r'$*, then* $E[r] \cong \mathbb{Z}_{r'} \times \mathbb{Z}_{r'}$ *or* $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_{r'}$*.*

## 2.7 The Embedding Degree

**Theorem 2.7.1** (Balasubramanian-Koblitz[2]) *Let* $E$ *be an elliptic curve defined over* $\mathbb{F}_q$ *and suppose that* $E(\mathbb{F}_q)$ *has a subgroup* $< P >$ *of order* $r$ *with* $\gcd(r, q-1) = 1$*. Then* $E[r] \subset E(\mathbb{F}_{q^k})$ *if and only if* $r \mid q^k - 1$*.*

**Definition 2.7.2** *Let* $E$ *be an elliptic curve defined over* $\mathbb{F}_q$*. Let* $< P >$ *be a cyclic subgroup of* $E(\mathbb{F}_q)$ *of order* $r$*. Then the embedding degree of* $< P >$ *is the smallest positive integer* $k$ *such that* $E[r] \subset E(\mathbb{F}_{q^k})$*.*

**Remark 2.7.3** *If* $\gcd(r, q-1) = 1$*, then by Balasubramanian and Koblitz, the embedding degree $k$ is nothing but the smallest $k$ such that $r \mid q^k - 1$.*

When we talk about the embedding degree of a curve $E(\mathbb{F}_q)$, we mean the embedding degree of the subgroup of $E(\mathbb{F}_q)$ of order $r$, where $r$ is the largest prime divisor of $\#E(\mathbb{F}_q)$.

## 2.8 Curve Endomorphisms

Let $E$ be an elliptic curve over $\mathbb{F}_q$, with $q = p^n$. Then an *endomorphism* $\delta$ of $E$ over $\mathbb{F}_q$ is a rational map $\delta : E \to E$ in the sense of algebraic varieties and it is furthermore a group homomorphism. The characteristic polynomial of an endomorphism $\delta$ is defined to be the least degree monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\delta)(P) = \infty$ for all $P \in E$. The set of all endomorphisms of $E$ over $\mathbb{F}_q$, denoted by $\mathrm{End}(E)$, forms a ring under addition and multiplication (corresponds to composition), which is called the *endomorphism ring* of $E$ over $\mathbb{F}_q$ (see [30, Section 3.1]).

There is a special endomorphism of $E$ over $\mathbb{F}_q$, called the Frobenius map $\phi_q : E \to E$ which is defined by $\phi_q(x, y) = (x^q, y^q)$ and $\phi_q(\infty) = \infty$. The Frobenius endomorphism $\phi_q$ has the property that $\phi_q(E(\mathbb{F}_{q^m})) = E(\mathbb{F}_{q^m})$ for any $m \geq 1$ with $\phi_q^m = id_E$ on $E(\mathbb{F}_{q^m})$. It follows from Hasse's theorem that the characteristic polynomial of $\phi_q$ is given by

$$f(x) = x^2 - tx + q,$$

where $t = q + 1 - \#E(\mathbb{F}_q)$ is the trace of the Frobenius $\phi_q$ (see [92, Section 4.2]).

## 2.9 The Elliptic Curve $y^2 = x^3 - c$

We will now give some property of the elliptic curves $E : y^2 = x^3 - c$ over $\mathbb{F}_q$ with prime $q$, which help us to compute the explicit formula for the number of points $\#E(\mathbb{F}_q)$ when $q \equiv 1 \pmod 3$ in Section 4.6.4.3. It is well-known that $\#E(\mathbb{F}_q) = q + 1$, when $q \equiv 2 \pmod 3$ (see [92, Proposition 4.31]).

Let $E$ be the elliptic curve given by the equation

$$y^2 = x^3 - c$$

over $\mathbb{F}_q$ with $q \equiv 1 \pmod 3$. This curve has the endomorphism ring isomorphic to the ring $\mathbb{Z}[\delta] = \mathbb{Z}[x]/ < x^2 + x + 1 >$, where $\delta = \frac{-1+i\sqrt{3}}{2}$ is the complex cube root of unity. Morever, the corresponding generator of the endomorphism ring $\delta : E \to E$ is given by the map $(x, y) \mapsto \delta(x, y) = (\beta x, y)$, where $\beta$ is a primitive cube root of unity in $\mathbb{F}^*_{q^2}$.

The elements $\tau = a + b\delta$ in $\mathbb{Z}[\delta]$ with $a, b \in \mathbb{Z}$ are called *Eisenstein* integers, and $\overline{\tau}$ is ordinary complex conjugate of $\tau$. One can check that $\overline{\tau} = a + b\delta^2 = (a - b) - b\delta$ and $\mathrm{N}(\tau) = \tau\overline{\tau} = a^2 + b^2 - ab$, where $\mathrm{N} : \mathbb{Z}[\delta] \to \mathbb{Z}$ is the norm function. In fact, $\mathbb{Z}[\delta]$ is a Euclidean domain under this norm function [48, Proposition 1.4.2]. The units of $\mathbb{Z}[\delta]$ are $\mathbb{Z}[\delta]^* = \{\pm 1, \pm\delta, \pm\delta^2\} =< -\delta >\cong \mathbb{Z}_6$ (see [48, Proposition 9.1.1]).

In the isomorphism $\mathrm{End}(E) \cong \mathbb{Z}[\delta]$, the Frobenius endomorphism $\phi_q$ corresponds to the endomorphism $\ell_\tau$ determined by the left multiplication of $\tau = a + b\delta$ in $\mathbb{Z}[\delta]$. This $\tau$ is unique up to complex conjugation and $\ell_\tau$ has the characteristic polynomial $x^2 - (2a - b)x + (a^2 + b^2 - ab)$. It follows from Hasse's theorem $\#E(\mathbb{F}_q) = q + 1 - t$ that

$$\begin{aligned} t &= \mathrm{Tr}(\tau) = \tau + \overline{\tau} = 2a - b, \\ q &= \mathrm{N}(\tau) = \tau\overline{\tau} = a^2 + b^2 - ab. \end{aligned}$$

Since all representations of $q$ are in the form $q = \mathrm{N}(u\tau)$ and $q = \mathrm{N}(u\overline{\tau})$, where $u \in \mathbb{Z}[\delta]^*$, there is exactly 12-representations producing $q = a^2 + b^2 - ab$. Therefore, all possible traces corresponding to these representations of $q$ are the following:

$$\pm(2a - b),\ \pm(a - 2b),\ \pm(a + b)$$

Since $q = a^2 + b^2 - ab \equiv 1 \pmod 3$, we may restrict the congruences for $a$ and $b$ to six classes : $a \equiv 0 \pmod 3$ and $b \not\equiv 0 \pmod 3$, $a \equiv 1 \pmod 3$ and $b \not\equiv 2 \pmod 3$, $a \equiv 2 \pmod 3$ and $b \not\equiv 1 \pmod 3$. We also would like to note that there is an algorithm to compute $a, b \in \mathbb{Z}$ such that $q = a^2 + b^2 - ab = \mathrm{N}(\tau)$, where $\tau = a + b\delta \in \mathbb{Z}[\delta]$ (see [94]).

# CHAPTER 3

# PAIRING-BASED CRYPTOGRAPHY

In this chapter, we first discuss the basic facts used in pairing-based cryptosystems and then we focus ourselves on the elliptic curves and study the Weil and Tate pairings (and its derivatives) used in these systems. For a more detailed background, one can refer to the Chapter IX and X of [11].

## 3.1 Bilinear Pairings

**Definition 3.1.1** *Let $(G_1, +)$ and $(G_2, +)$ be abelian groups of order n. Let $(G_3, .)$ be a cyclic group of order n. A bilinear pairing is an efficiently computable map $e : G_1 \times G_2 \longrightarrow G_3$ which satisfies the following additional properties:*

1. *(bilinearity) For all $P, R \in G_1$ and all $Q, S \in G_2$, we have $e(P + R, Q) = e(P, Q)e(R, Q)$ and $e(P, Q + S) = e(P, Q)e(P, S)$.*
2. *(non-degeneracy) For all $P \in G_1$, with $P \neq Id_{G_1}$, there is some $Q \in G_2$ such that $e(P, Q) \neq Id_{G_3}$. For all $Q \in G_2$, with $Q \neq Id_{G_2}$, there is some $P \in G_1$ such that $e(P, Q) \neq Id_{G_3}$.*

The following fact which is related to the properties of bilinear pairings can be easily verified.

**Lemma 3.1.2** *Let $e : G_1 \times G_2 \longrightarrow G_3$ be a bilinear pairing. Let $P \in G_1$ and $Q \in G_2$. Then*

1. $e(P, Id_{G_2}) = e(Id_{G_1}, Q) = Id_{G_3}$
2. $e(-P, Q) = e(P, -Q) = e(P, Q)^{-1}$

*3.* $e(aP, bQ) = e(bP, aQ) = e(P, Q)^{ab}$ *for all* $a, b \in \mathbb{Z}$.

## 3.2 Security of Pairings

We now give the bilinear Diffie-Hellman problem (BDHP) that has been widely studied in recent years. Security of some applications of bilinear pairings in cryptography is based on the hardness of the BDHP, which was first stated in [12].

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order $n$. Let $P \in G_1$, $G_1 =< P >$ and $e : G_1 \times G_1 \to G_2$ be a bilinear map.

**Discrete Logarithm Problem (DLP):**
**On $G_1$:** Given $P$ in $G_1$, find $a \in \mathbb{Z}_n^*$ such that $Q = aP$ in $G_1$.
**On $G_2$:** Given $e(P, P)$ in $G_2$, find $a \in \mathbb{Z}_n^*$ such that $Q = e(P, P)^a$ in $G_2$.

**Diffie-Hellman Problem (DHP):**
**On $G_1$:** Given $P, aP, bP$ in $G_1$, for some (unknown) $a, b \in \mathbb{Z}_n^*$, compute $abP$ in $G_1$.
**On $G_2$:** Given $e(P, P), e(P, P)^a, e(P, P)^b$ in $G_2$, for some (unknown) $a, b \in \mathbb{Z}_n^*$, compute $e(P, P)^{ab}$ in $G_2$.

**Bilinear Diffie-Hellman Problem (BDHP):** Given $P, aP, bP, cP$ in $G_1$, for some (unknown) $a, b, c \in \mathbb{Z}_n^*$, compute $e(P, P)^{abc}$ in $G_2$.

The BDHP is no harder than the DHP on $G_1$ and $G_2$. Namely, if we can solve the DHP on $G_1$, we could find $abP$, and compute $e(abP, cP) = e(P, P)^{abc}$. Thus we would solve the BDHP. Similarly, if we can solve the DHP on $G_2$, we could apply this problem to $e(P, P)$, $e(P, P)^c$, and $e(P, P)^{ab}$, which would solve the BDHP.

The DHP on $G_1$ and $G_2$ can be reduced to the DLP on $G_1$ and $G_2$. It is also assumed that the DLP on $G_1$ and $G_2$ are hard to solve. The bilinear property has many applications and it was first used for DLP in [70]. For instance, choosing $G_1 = E(\mathbb{F}_q)$ and $G_2 \subset \mathbb{F}_{q^k}^*$ with $k$ an embedding degree, defines bilinear pairing which we discuss later.

In the literature, there are a lot of different cryptographic protocols based on bilinear pairings that the security of them depends on the BDHP and its versions [27]. However, we present three fundamental of those protocols.

## 3.3 Pairing-Based Cryptographic Protocols

### 3.3.1 Joux's One Round Three Party Key Agreement Protocol

Key agreement, one of the fundamental cryptographic primitives, is required when two or more parties want to share a message securely. Three party key agreement in a single round proposed by Joux [49] was the first application of bilinear pairings in cryptography.

*Protocol:*

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order $n$. Let $P \in G_1$, $G_1 =< P >$ and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map. Consider three parties $A, B, C$ with secret keys $a, b, c \in Z_n$

- $A$ broadcasts $aP$ to both $B, C$
- $B$ broadcasts $bP$ to both $A, C$
- $C$ broadcasts $cP$ to both $A, B$
- $A$ computes $e(bP, cP)^a$
- $B$ computes $e(aP, cP)^b$
- $C$ computes $e(aP, bP)^c$
- Common agreed key is $e(P, P)^{abc}$

### 3.3.2 Short Signatures

Digital signatures are the most important cryptographic primitive for the daily life. Short signatures are needed in environments with space and bandwidth constraints. So far, the best known shortest signature [13] is obtained by using the Digital Signature Algorithm (DSA) over a finite field $\mathbb{F}_q$. The length of the signature is approximately $2 \log q$. On the other hand, when the following pairing-based protocol is used, the length of the signature is about $\rho \log r$, where $\rho = \log q / \log r$ and $r$ is the largest prime divisor of the number of the points of the elliptic curve. For example, if one uses RSA signature 1024 bit modulus, ECDSA signature is 320 bit long for the same security level. However, short signature provides the same security level only for 160 bits for the best choice. This case corresponds finding a suitable elliptic curve $E(\mathbb{F}_q)$, for which $r$ is close to $q$ and it is a general problem to find such suitable elliptic curves having this property that we shall discuss in Chapter 4.

*Protocol:*

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order $n$. Let $P \in G_1$, $G_1 =< P >$ and $e : G_1 \times G_1 \to G_2$ be a bilinear map. Let $H : \{0, 1\}^* \to G_1^*$ be a cryptographic hash function.

- **Key Generation :** Pick a random $c \in \mathbb{Z}_n^*$ and compute $cP$. The secret key is $c$ and the public key is $cP$.
- **Sign :** Given a secret key $c$ and a message $m \in \{0, 1\}^*$, compute the signature $\sigma = cH(m) \in G_1$.
- **Verify :** Given a public key $cP$, a message $m$ and a signature $\sigma$, verify $e(P, \sigma) = e(cP, H(m))$.

### 3.3.3 Identity-Based Cryptosystems

This was firstly suggested by Shamir in [83] that a public key encryption scheme can be run with the identity of the receiver. In other words, for Identity-Based (ID-based) encryption provides the simplification of certificate management in e-mail systems. By this way, management of keys and certificates gets more and more easier. The most used ID-based cryptosystem was proposed by [12] in 2001. The main advantage of ID-based crytosystems is to eliminate the need for certificates. Moreover, ID-based cryptosystems remove the certificate lookup, lifecycle management and certificate revocation lists.

*Protocol:*

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order $n$. Let $P \in G_1$, $G_1 =< P >$ and $e : G_1 \times G_1 \to G_2$ be a bilinear map. Let $l$ be the length of the message $m$. Let $H_1 : \{0, 1\}^* \to G_1^*$ and $H_2 : G_2 \to \{0, 1\}^l$ be the cryptographic hash functions.

- **Key Generation :** Pick a random $s \in \mathbb{Z}_n^*$ and compute $sP$. For a given string $ID \in \{0, 1\}^*$, compute $sH_1(ID)$. The master key is $s$, the public key is $S = sP$ and the private key is $d = sH_1(ID)$.

- **Encrypt :** Choose a random $a \in \mathbb{Z}_n^*$, then the ciphertext for the message $m$ to be $C = \langle aP, m \oplus H_2(e(H_1(ID), S)^a)\rangle$.

- **Decrypt :** Compute $V \oplus H_2(e(d, U)) = m$ for given $C = \langle U, V\rangle$.

## 3.4 Divisors on Elliptic Curves

The divisor group of an elliptic curve $E$, denoted by $\mathrm{Div}(E)$, is the free abelian group generated by the points of $E$. Therefore, a divisor $D \in \mathrm{Div}(E)$ is a formal sum given by

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

with $n_P \in \mathbb{Z}$ and $n_P = 0$ except for finitely many $P \in E$. The *degree* of a divisor $D$ is defined by

$$\deg(D) = \sum_{P \in E} n_P.$$

The *support* of a divisor $D$, $\mathrm{supp}(D)$, is the set of points $P \in E$ for which $n_P \neq 0$.

The divisors of degree zero form a subgroup of $\mathrm{Div}(E)$, that is denoted by

$$\mathrm{Div}^0(E) = \{D \in \mathrm{Div}(E) \mid \deg(D) = 0\}.$$

Let $\overline{\mathbb{F}_q}(E)$ denote the field of rational functions on $E$. Let $f \in \overline{\mathbb{F}_q}(E)$ be non-zero. Then the divisor of the function $f$ is $div(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P)$, where $\mathrm{ord}_P(f)$ is the multiplicity of $f$ at $P$. It is a well-known fact that $\deg(\mathrm{div}(f)) = 0$. A divisor $D$ is called *principal* if $D = \mathrm{div}(f)$ for some non-zero $f \in \overline{\mathbb{F}_q}(E)$. This is denoted by

$$\mathrm{Prin}(E) = \{D \in \mathrm{Div}(E) \mid D = \mathrm{div}(f),\ f \neq 0,\ f \in \overline{\mathbb{F}_q}(E)\}.$$

$\mathrm{Prin}(E)$ is a subgroup of $\mathrm{Div}^0(E)$ since for all non-zero rational functions $f, g \in E$, $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$ and $\mathrm{div}(f/g) = \mathrm{div}(f) - \mathrm{div}(g)$.

Two divisors $D$ and $D^{'}$ are equivalent (denoted by $D \sim D^{'}$) if $D^{'} = D + \mathrm{div}(f)$ for some nonzero $f \in \overline{\mathbb{F}_q}(E)$.

**Theorem 3.4.1 [86, Corollary 3.3.5]** *Let $D = \sum_{P \in E} n_P(P)$ be a divisor. Then $D$ is principal if and only if* $\deg(D) = 0$ *and* $\sum_{P \in E} n_P P = \infty$.

The *divisor class group* (or *Picard group*) $\mathrm{Pic}^0(E)$ of $E$ is the quotient of the group of degree zero divisors $\mathrm{Div}^0(E)$ by the principal divisors $\mathrm{Prin}(E)$, i.e,

$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Prin}(E).$$

It is well-known that for every divisor $D \in \mathrm{Div}^0(E)$, there is a unique point $Q \in E$ such that $D \sim (Q) - (\infty)$ [86, Proposition 3.3.4]. This gives a one-to-one correspondence between $\mathrm{Pic}^0(E)$ and the group of points of $E$.

Let $P, Q \in E$. Suppose the line between $P$ and $Q$ (tangent line if $P = Q$) has an equation $L(x, y) = 0$. By Bezout's theorem, this line $L$ intersects $E$ at a third point $R = (x_R, y_R)$. Then the divisor of $L$ is $\mathrm{div}(L) = (P) + (Q) + (R) - 3(\infty)$. The vertical line $V(x) = (x - x_R)$ passes through the points $R$ and $S = P + Q$. Then $\mathrm{div}(V) = (R) + (S) - 2(\infty)$. Therefore, the equation $S = P + Q$ corresponds to $\mathrm{div}(L/V) = (P) + (Q) - (S) - (\infty)$.

If $D = \sum_{P \in E} n_P(P) \in \mathrm{Div}(E)$ and $f \in E$ is a non-zero rational function such that $\mathrm{supp}(D) \cap \mathrm{supp}(\mathrm{div}(f)) = \emptyset$, then the value of $f$ at $D$ is defined to be the following element in $\overline{\mathbb{F}_q}$:

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

**Theorem 3.4.2 (Weil reciprocity)** *Let $f$ and $g$ be nonzero functions on a curve $E$ over $\mathbb{F}_q$. Suppose that $supp(div(f)) \cap supp(div(g)) = \emptyset$. Then $f(div(g)) = g(div(f))$.*

## 3.5 Weil Pairing

Let E be an elliptic curve defined over $\mathbb{F}_q$ of characteristic $p$ with the identity element $\infty$. Let $r$ be a large prime satisfying $r \mid \#E(\mathbb{F}_q)$ which is coprime to $p$. Let $k$ the embedding degree, i.e., the smallest positive integer such that $r \mid q^k - 1$. Then $E[r] \subset E(\mathbb{F}_{q^k})$ when $k > 1$ and thus $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$.

Let $P, Q \in E[r]$ and let $R, S \in E(\mathbb{F}_{q^k})$ such that $S \notin \{R, P + R, P + R - Q, R - Q\}$. Let $D = (P + R) - (R)$ and $D^{'} = (Q + S) - (S)$. Then by Theorem 3.4.1, the divisors $rD$, $rD^{'}$ are in the form $rD = \mathrm{div}(f_P)$ and $rD^{'} = \mathrm{div}(f_Q)$ for some rational functions $f_P \neq 0$, $f_Q \neq 0$ on the curve $E$ over $\mathbb{F}_q$. Let $\mu_r$ be the group of *r-th* roots of unity in $\mathbb{F}^*_{q^k}$. Let

$$e_r : E[r] \times E[r] \rightarrow \mu_r \subset \mathbb{F}^*_{q^k}$$

be the map given by

$$e_r(P,Q) = \frac{f_P(D^{'})}{f_Q(D)} = \frac{f_P(Q+S)/f_P(S)}{f_Q(P+R)/f_Q(R)}.$$

This map so-called Weil pairing is well-defined and has the properties given below.

**Theorem 3.5.1** (Properties of Weil Pairing) *Let $E$ be an elliptic curve defined over $\mathbb{F}_q$. Then, the Weil pairing $e_r$ satisfies the following properties :*

1. *(identity) $e_r(S,S) = 1$ for all $S \in E[r]$*
2. *(alternation) $e_r(S,T) = e_r(T,S)^{-1}$ for all $S,T \in E[r]$*
3. *(bilinearity) $e_r$ is bilinear in each variable; $e_r(S+T,P) = e_r(S,P)e_r(T,P)$ and $e_r(S,T+P) = e_r(S,T)e_r(S,P)$ for all $S,T,P \in E[r]$*
4. *(non-degeneracy) If $e_r(S,T) = 1$ for all $S \in E[r]$ with $S \neq \infty$, then $T = \infty$ and if $e_r(S,T) = 1$ for all $T \in E[r]$ with $T \neq \infty$, then $S = \infty$*
5. *(compatibility) For all $S,T \in E[r]$, $e_r(\alpha(S),\alpha(T)) = e_r(S,T)^{\deg\alpha}$, for any nonzero endomorphism $\alpha : E \to E$*
6. *If $E[r] =< P > \oplus < R >$, then $e_r(P,R) = \xi$ is a primitive r-th root of unity.*

We now briefly outline Miller's algorithm (Algorithm 1) [72, 73] for computing the Weil pairing $e_r(P,Q)$ in a polynomial time, efficiently. This algorithm aims to construct rational functions $f$ and $g$ associated to the point $P$ and $Q$ and evaluate at divisors $D^{'} = (Q+S) - (S)$ and $D = (P+R) - (R)$, respectively. The functions $f_P$ and $f_Q$ can be efficiently computed by double and add procedure. This idea is to define function $f_i$, where $1 \leq i \leq r$ and $f_r = f_P$ or $f_Q$, recursively. These functions are computed by the following way :

$$f_1 = \frac{V_{P+R}}{L_{P,R}},\ f_{i+j} = f_i \cdot f_j \cdot \frac{L_{iP,jP}}{V_{iP+jP}},\ f_{2i} = f_i^2 \cdot \frac{T_{iP}}{V_{2iP}},$$

where $V_P$ is the vertical line at $P$, $T_R$ is the tangent line at $R$ and $L_{P,Q}$ is the line passing through the points $P$ and $Q$.

**Example 3.5.2** *Let $E$ be the elliptic curve given by*

$$y^2 = x^3 - 4$$

*over* $\mathbb{F}_5$. *Since* $5 \equiv 2 \pmod 3$, $\#E(\mathbb{F}_5) = 5 + 1 = 6$. *These points form an additive group structure, that is,* $E(\mathbb{F}_5) = \Big\{(0,1),(0,4),(2,2),(2,3),(4,0),\infty\Big\}$.

*Let* $< P = (0,1) >$ *be the subgroup of* $E(\mathbb{F}_5)$ *of order* $r = 3$. *Then* $< P >= E(\mathbb{F}_5)[3] = \Big\{P = (0,1), 2P = (0,4), 3P = \infty\Big\}$. *If we give these points as inputs to the Weil Pairing, the output will be 1 since they are linearly dependent. Therefore, we must find the other 3-torsion points to apply Weil pairing. Since this curve is a supersingular elliptic curve with embedding degree* $k = 2$ *that we shall discuss in Section 4.5.2,* $E(\mathbb{F}_{5^2})$ *contains all* $9$ *points of* $E[5]$. *Therefore, Weil pairing exist and nontrivial in the field extension* $\mathbb{F}_{5^2}$. *Note that* $\chi_2(-2) \neq 1$ *in* $\mathbb{F}_5$, *so we can write* $\mathbb{F}_{5^2} = \mathbb{F}_5[\alpha]$, *where* $\alpha^2 + 2 = 0$. *Although the distortion map of this curve is given by* $\delta(x,y) = (x,\alpha y)$, *this does not give us the other 3-torsion points in* $\mathbb{F}_{5^2}$. *However* $E[3] = \Big\{(0,1),(0,4),(1,2\alpha),(1,3\alpha),(2+\alpha,2\alpha),(2+\alpha,3\alpha),(2+4\alpha,2\alpha),(2+4\alpha,3\alpha),\infty\Big\}$. *We compute the Weil pairing* $e_3(P,Q) = e_3((0,1),(1,2\alpha))$. *In order to do this, we first randomly select the points* $R$ *and* $S$ *to be not in* $E[3]$. *Let* $R = (2,2)$ *and* $S = (3,\alpha)$. *Using the point addition formulas, we find* $P + R = (2,3)$ *and* $Q + S = (3,4\alpha)$. *We now comprehensively describe how Miller's algorithm works for* $f_P(Q+S)$ *and* $f_P(S)$:

1. *We compute* $f_1 = \dfrac{V_{P+R}}{L_{P,R}} = \dfrac{x-2}{x-2y+2}$ *at the point* $Q+S$ *and* $S$ *that gives us* $f_1(Q+S) = \alpha$ *and* $f_1(S) = 4\alpha$.
2. *We compute* $f_2 = f_1^2 \cdot \dfrac{T_P}{V_{2P}} = \Big(\dfrac{x-2}{x-2y+2}\Big)^2 \cdot \dfrac{y-1}{x}$ *at the point* $Q+S$ *and* $S$ *that gives us* $f_2(Q+S) = 4 + 4\alpha$ *and* $f_2(S) = 4 + \alpha$.
3. *We compute* $f_3 = f_1 \cdot f_2 \cdot \dfrac{L_{2P,P}}{V_{3P}}$ *at the point* $Q+S$ *and* $S$. *Since* $3P = \infty$ *and* $-2P = P$, *we discard the denominator and* $L_{2P,P} = V_P$ *in this case. Therefore,* $f_3 = f_1 \cdot f_2 \cdot V_P = \Big(\dfrac{x-2}{x-2y+2}\Big)^3 \cdot \dfrac{y-1}{x} \cdot x$ *and then* $f_3(Q+S) = 1 + 2\alpha$ *and* $f_3(S) = 1 + 3\alpha$.

*Thus we have found* $f_3(Q+S) = f_P(Q+S) = 1 + 2\alpha$ *and* $f_3(S) = f_P(S) = 1 + 3\alpha$, *simultaneously.*

*On the other hand,* $f_Q(P+R)$ *and* $f_Q(R)$ *are computed using the same procedure above. It can be verified that* $f_Q(P+R) = 3 + 4\alpha$ *and* $f_Q(R) = 3 + \alpha$. *Finally, we have*

$$e_3(P,Q) = \frac{f_P(Q+S)/f_P(S)}{f_Q(P+R)/f_Q(R)} = 2 + 4\alpha,$$

*that gives us* $(2+4\alpha)^3 = 1$ *as expected.*

**Algorithm 1:** Miller's algorithm for Weil pairing

```
  Input: $P \in E[r]$ and $r = (r_t \cdots r_0)_2$
  Output: $f_r(Q) = f_P(Q)$
  Step 1 : $f_1 \leftarrow V_{P+R}(Q)/L_{P,R}(Q)$
  Step 2 : $f \leftarrow f_1$
  Step 3 : $Z \leftarrow P$
  Step 4 : for $i \leftarrow t-1$ to $0$ do
  Step 5 :     $f \leftarrow f^2 \cdot T_Z(Q)/V_{2Z}(Q)$
  Step 6 :     $Z \leftarrow 2Z$
  Step 7 :     if $r_i = 1$ then
  Step 8 :         $f \leftarrow f \cdot f_1 \cdot L_{Z,P}(Q)/V_{Z+P}(Q)$
  Step 9 :         $Z \leftarrow Z + P$
 Step 10 :     end if
 Step 11 : end for
 Step 12 : return $f_P(Q)$
```

## 3.6 Simplified Weil Pairing

Lynn [67] simplifies the Weil pairing by setting $R = \infty$ or $S = \infty$. If we choose $R = \infty$, we can compute the Weil pairing as

$$e_r(P, Q) = \frac{f_P(Q + S)/f_P(S)}{f_Q(P)}$$

where $f_P$ and $f_Q$ are rational functions with $\mathrm{div}(f_P) = r(P) - r(\infty)$ and $\mathrm{div}(f_Q) = r(Q + S) - r(S)$, respectively. In this case, we are careful to build the fuction $f_Q$, since we never divide it by itself. Therefore, we have to choose the lines, tangents and verticals in the special form when we use each Miller's loop. For the equations of lines and tangents, we choose the unit coefficient of variable $y$. For the equation of verticals, we choose the unit coefficient of variable $x$. After doing this particular construction for the function $f_Q$, we can check that $f_Q(\infty) = 1$ so as to simplify the Weil pairing as claimed. If we choose $S = \infty$, we can compute the Weil pairing as

$$e_r(P, Q) = \frac{f_P(Q)}{f_Q(P + R)/f_Q(R)}$$

where $f_P$ and $f_Q$ are rational functions with $\mathrm{div}(f_P) = r(P+R)-r(R)$ and $\mathrm{div}(f_Q) = r(Q)-r(\infty)$, respectively. We apply the same procedure in the previous case to be able to obtain $f_P(\infty) = 1$.

On the other hand, Miller [73] gives the following fact by choosing $S = -R$ and $R = \infty$. An alternative proof of it can be found in [20].

**Theorem 3.6.1** *Let E be an elliptic curve over $\mathbb{F}_q$. Let $P, Q \in E[r]$ with $P, Q \neq \infty$, and let $P \neq Q$. Then*

$$e_r(P, Q) = (-1)^r \frac{f_P(Q)}{f_Q(P)}$$

## 3.7 Tate Pairing

Let E be an elliptic curve defined over $\mathbb{F}_q$ of characteristic $p$ with the identity element $\infty$. Let $r$ be a large prime satisfying $r \mid \#E(\mathbb{F}_q)$ which is coprime to $p$. Let $k$ be the embedding degree, i.e., the smallest positive integer such that $r \mid q^k - 1$. Then $E[r] \subset E(\mathbb{F}_{q^k})$ when $k > 1$ and thus $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$. For every $P \in E(\mathbb{F}_{q^k})$ and integer $s$, let $f_{s,P}$ be a function with divisor

$$\operatorname{div}(f_{s,P}) = s(P) - (sP) - (s-1)(\infty),$$

where the function $f_{s,P}$ is called a Miller function.

Let $P \in E(\mathbb{F}_{q^k})[r]$ and let $Q \in E(\mathbb{F}_{q^k})$. We think of $Q$ as representing an equivalence class in $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$. Consider the divisor $D = (Q + R) - (R)$ with a random point $R \in E(\mathbb{F}_{q^k})$ such that $R \notin \{\infty, P, -Q, P - Q\}$. Since $\operatorname{supp}(D) \cap \operatorname{supp}(\operatorname{div}(f_{r,P})) = \emptyset$ due to the choice of $R$, we have $f_{r,P}(D) \neq 0$, and so $f_{r,P}(D) \in \mathbb{F}^*_{q^k}$. Let

$$\langle \cdot, \cdot \rangle_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$$

be the map given by

$$\langle P, Q \rangle_r = f_{r,P}(D) = f_{r,P}(Q + R)/f_{r,P}(R).$$

This map so-called Tate pairing [35] is well-defined and has the properties given below:

**Theorem 3.7.1** (Properties of Tate Pairing) *Let E be an elliptic curve defined over $\mathbb{F}_q$ with characteristic p. Let r be a large prime satisfying $r \mid \#E(\mathbb{F}_q)$ which is coprime to p. Let k be the embedding degree. Then, the Tate pairing satisfies the following properties :*

1. *(bilinearity) For all $P, P_1, P_2 \in E(\mathbb{F}_{q^k})[r]$, and $Q, Q_1, Q_2 \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$,*

$$\begin{aligned}\langle P_1 + P_2, Q\rangle_r &= \langle P_1, Q\rangle_r \langle P_2, Q\rangle_r \\ \langle P, Q_1 + Q_2\rangle_r &= \langle P, Q_1\rangle_r \langle P, Q_2\rangle_r .\end{aligned}$$

2. *(non-degeneracy) For all $P \in E(\mathbb{F}_{q^k})[r]$ with $P \neq \infty$, there is some $Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ such that $\langle P, Q\rangle_r \neq 1$. Similarly, for all $Q \in E(\mathbb{F}_{q^k})$ with $Q \notin rE(\mathbb{F}_{q^k})$ there is some $P \in E(\mathbb{F}_{q^k})[r]$ such that $\langle P, Q\rangle_r \neq 1$.*

In the definition of the Tate pairing, the quotient group $\mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$ is the set of equivalence classes of elements of $\mathbb{F}^*_{q^k}$ where the relation is given by $a \equiv b$ if and only if there exists $c \in \mathbb{F}^*_{q^k}$ such that $a = bc^r$. This means that the Tate pairing is only defined up to a multiple by an $r$-th power in $\mathbb{F}^*_{q^k}$. However, for most applications in cryptography, it is necessary to get a unique element associated to this equivalence class. Since $r \mid q^k - 1$, it is not difficult to show that the map $\xi \mapsto \xi^{\frac{q^k-1}{r}}$ gives an isomorphism $\mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r \cong \mu_r$, where $\mu_r$ is the group of $r$-th roots of unity in $\mathbb{F}^*_{q^k}$. In particular,

$$\tau(P, Q) = f_{r,P}(D)^{(q^k-1)/r}$$

gives a unique element in $\mu_r$, and $\tau(P, Q)$ is called the reduced Tate pairing. Here, raising the output $f_{r,P}(D)$ to the power of $(q^k - 1)/r$ is known as the final exponentiation that we shall comprehensively discuss in Chapter 5.

We now briefly outline Miller's algorithm (Algorithm 2) for the Tate pairing in a polynomial time, efficiently. The Tate pairing is computed by a function $f_{r,P} = f_r$ at the divisor $D = (Q + R) - (R)$ using double and add method in the following way:

$$f_1 = 1,\ f_{i+1} = f_i \cdot \frac{L_{iP,P}}{V_{(i+1)P}},\ f_{2i} = f_i^2 \cdot \frac{T_{iP}}{V_{2iP}},$$

where $V_P$ is the vertical line at $P$, $T_R$ is the tangent line at $R$ and $L_{P,Q}$ is the line passing through the points $P$ and $Q$.

**Example 3.7.2** *Let $E$ be an elliptic curve given by*

$$y^2 = x^3 - 4$$

*over $\mathbb{F}_5$. As we discussed in Example 3.5.2, since $3 \mid 5^2 - 1$ and $E(\mathbb{F}_5)$ contains all $9$ points of $E[3]$, the Tate pairing exists and nontrivial in $\mathbb{F}_{5^2}$. We compute the Tate pairing $\langle P, Q\rangle_3 =$*

$\langle(0,1),(1,2\alpha)\rangle_3$. *In order to do this, we first choose the points* $R = Q = (1, 2\alpha)$ *such that the divisor* $D = (Q + R) - (R)$. *We now comprehensively describe how Miller's algorithm works for* $f_{3,P}(2Q)$ *and* $f_{3,P}(Q)$*:*

1. *We first set* $f_1 = 1$.
2. *We compute* $f_2 = f_1^2 \cdot \dfrac{T_P}{V_{2P}} = \dfrac{y-1}{x}$ *at the point* $2Q$ *and* $Q$ *that gives us* $f_2(2Q) = 4 + 3\alpha$ *and* $f_2(Q) = 4 + 2\alpha$.
3. *We compute* $f_3 = f_2 \cdot \dfrac{L_{2P,P}}{V_{3P}}$ *at the point* $2Q$ *and* $Q$*. Since* $3P = \infty$ *and* $-2P = P$*, we discard the denominator and* $L_{-P,P} = V_P$ *in this case. Therefore,* $f_3 = f_2 \cdot V_P = \dfrac{y-1}{x} \cdot x$ *and then* $f_3(2Q) = 4 + 3\alpha$ *and* $f_3(Q) = 4 + 2\alpha$.

*Thus we have found* $f_3(2Q) = f_{3,P}(2Q) = 4{+}3\alpha$ *and* $f_3(Q) = f_{3,P}(Q) = 4{+}2\alpha$*, simultaneously. Finally, we have*

$$\tau(P, Q) = \Big(\frac{f_{3,P}(2Q)}{f_{3,P}(Q)}\Big)^{(5^2-1)/3} = (2 + \alpha)^8 = 2 + 4\alpha,$$

*that gives us* $(2 + 4\alpha)^3 = 1$ *as expected.*

**Algorithm 2:** Miller's algorithm for Tate pairing

```
Input: $P \in E[r]$ and $r = (r_t \cdots r_0)_2$
Output: $f_r(Q) = f_{r,P}(Q)$
Step 1 : $f \leftarrow 1$
Step 2 : $Z \leftarrow P$
Step 3 : for $i \leftarrow t - 1$ to $0$ do
Step 4 :     $f \leftarrow f^2 \cdot T_Z(Q)/V_{2Z}(Q)$
Step 5 :     $Z \leftarrow 2Z$
Step 6 :     if $r_i = 1$ then
Step 7 :         $f \leftarrow f \cdot L_{Z,P}(Q)/V_{Z+P}(Q)$
Step 8 :         $Z \leftarrow Z + P$
Step 9 :     end if
Step 10 : end for
Step 11 : return $f_{r,P}(Q)$
```

## 3.8 Simplified Tate Pairing

The following theorem which is due to Barreto, Kim, Lynn and Scott [4, 6], Lynn [67] gives a simple form of the Tate pairing when the embedding degree $k > 1$.

**Theorem 3.8.1** *Let $E$ be an elliptic curve over $\mathbb{F}_q$. Let $P \in E(\mathbb{F}_q)$ be a point of order $r$. Let $k$ be the embedding degree. If $k > 1$, then*

$$\tau(P, Q) = f_{r,P}(Q)^{(q^k-1)/r}$$

*is a bilinear, non-degenerate map, where $f_{r,P}$ is a rational function with $div(f_{r,P}) = r(P) - r(\infty)$.*

## 3.9 Construction of One Variable Non-Degenerate Pairings

It is a problem how to get practical and useful one parameter non-degenerate bilinear map out of the Weil and Tate pairings. In this section, we shall give such constructions. Let $E$ be an elliptic curve defined over $\mathbb{F}_q$ of characteristic $p$ with the identity element $\infty$. Let $r$ be a large prime satisfying $r \mid \#E(\mathbb{F}_q)$ which is coprime to $p$. Let $k$ be the embedding degree. Then $E[r] \subset E(\mathbb{F}_{q^k})$ and thus $E[r] \cong \mathbb{Z}_r \times \mathbb{Z}_r$. Let $P \in E[r] \cap E(\mathbb{F}_q)$, and consider the cyclic group $G_1 =< P >\subset E(\mathbb{F}_q)[r]$. For the Weil and Tate pairings (and its derivatives), it is important how to choose $Q$ to be used in the second component $G_2$. There are two methods for such choices, so far: Distortion maps and twist curves.

### 3.9.1 Distortion Maps

For supersingular curves, there is always so-called a distortion map, $\phi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^k})$, which is easy to compute. This allows us to choose $G_1 =< P >$, $G_2 = \phi(P) = Q$ together with Weil/Tate pairing to produce a non-degenerate bilinear map $e : G_1 \times G_2 \to G_3$ such that $e(P, Q) = f(P, \phi(Q))$. We note that distortion maps are all known for supersingular curves. Therefore, we can construct efficient pairing for supersingular curves.

**Example 3.9.1** *If $q = 3 \pmod 4$ and $E : y^2 = x^3 + ax$ for any $a \in \mathbb{F}_q^*$, then a distortion map is of the form $\phi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^2})$; $\phi(x, y) = (-x, iy)$, where $i$ is a square root of -1.*

**Example 3.9.2** *If $q = 2 \pmod 3$ and $E : y^2 = x^3 + b$ for any $b \in \mathbb{F}_q^*$, then a distortion map is of the form $\phi : E(\mathbb{F}_q) \to E(\mathbb{F}_{q^2})$, $\phi(x, y) = (\xi x, y)$, where $\xi$ is a primitive cube root of unity.*

### 3.9.2 Twist Curves

In the case of ordinary curves however, there is no distortion map. To produce such $G_2$, one looks at the twist $E^{'}$ of $E$ over $\mathbb{F}_q$. The twist $E^{'}$ can be constructed as follows : Let $E$ be an elliptic curve given by the equation

$$E \ : \ y^2 = x^3 + ax + b$$

over $\mathbb{F}_q$, where $q = p^n$ and $p > 3$. Let $v$ be a quadratic non-residue in $\mathbb{F}_q$. Then the twist of the curve is defined by the equation

$$E^{'} \ : \ y^2 = x^3 + v^2ax + v^3b$$

over $\mathbb{F}_q$. It is clear that $E^{'}$ is independent that the choice of quadratic non-residue $v$ up to isomorphism.

For the elliptic curve $E(\mathbb{F}_q)$ with embedding degree $k = 2d$, we can consider the twist $E^{'}(\mathbb{F}_{q^d})$ of $E(\mathbb{F}_{q^d})$, where $d \geq 1$ for $E[r] \subset E(\mathbb{F}_{q^k})$. It is easy to show that the map $\phi_d \, : \, E^{'}(\mathbb{F}_{q^d}) \to E(\mathbb{F}_{q^k})$; $\phi_d(x, y) = (v^{-1}x, v^{-3/2}y)$ is well-defined. This allows us to choose $G_2 = \phi_d(Q^{'}) = Q$ together with Weil/Tate pairing to produce a non-degenerate bilinear map $e : G_1 \times G_2 \to G_3$ such that $e(P, Q) = f(P, \phi_d(Q^{'}))$, where $Q^{'} \in E^{'}(\mathbb{F}_{q^d})$ of order multiple of $r$. So, if one has a suitable ordinary elliptic curve with even embedding degree, by this method scalar multiplication of input point can be performed in $\mathbb{F}_{q^d}$ instead of $\mathbb{F}_{q^k}$.

## 3.10 Eta and Ate Pairing

Eta and Ate pairings are the derivatives of the Tate pairing. The Eta Pairing was introduced in the supersingular curves by Barreto et al. in [3]. The Ate pairing was introduced by Hess, Smart and Vercauteren [44]. They also carried out the concept of the Eta pairing to ordinary curves and call it the twisted Ate pairing. In this case, the conditions stated in [3, Theorem 1] are in fact automatically satisfied.

Let $E$ be an elliptic curve defined over $\mathbb{F}_q$ of characteristic $p$ with the identity element $\infty$. Let $r$ be a large prime satisfying $r \mid \#E(\mathbb{F}_q)$ which is coprime to $p$. Let $k$ be the embedding degree. Let $P \in E(\mathbb{F}_q)[r]$ and $Q \in E(\mathbb{F}_{q^k})[r]$ but $Q \notin E(\mathbb{F}_q)[r]$. Let $G_1 =< P >\subseteq E(\mathbb{F}_q)[r]$ and $G_2 =< Q >\subseteq E(\mathbb{F}_{q^k})[r]$. Let $E^{'}$ be the twist curve of $E$ over an extension field of $\mathbb{F}_q$ of degree $d$. Then we may choose the point $Q$ arising from the isomorphism $\phi_d \ : \ E^{'} \rightarrow E$, that is, $Q = \phi_d(Q^{'})$, where $Q^{'}$ is an $\mathbb{F}_{q^{k/d}}$-rational point of order $r$ on the twist curve $E^{'}$. Let $T = t-1$, where $t$ is the trace of Fobenius and $\lambda = (t-1)^{k/d} \pmod r$, where $\lambda$ is a primitive $d$-th root of of unity modulo $r$. Let $\mu_r$ be the group of $r$-$th$ roots of unity in $\mathbb{F}^*_{q^k}$.

For every $P \in E(\mathbb{F}_{q^k})$ and integer $s$, let $f_{s,P}$ be a rational fuction with divisor

$$\mathrm{div}(f_{s,P}) = s(P) - (sP) - (s-1)(\infty),$$

where the function $f_{s,P}$ is called a Miller function. For $s = \lambda$,

$$\begin{aligned} \eta : G_1 \times G_2 &\rightarrow \mu_r \\ (P, Q) &\mapsto \eta(P, Q) = f_{\lambda,P}(Q)^{(q^k-1)/r} \end{aligned}$$

defines a well-defined, bilinear, non-degenerate pairing which is called the reduced Eta pairing. For $s = T$,

$$\begin{aligned} \alpha : G_1 \times G_2 &\rightarrow \mu_r \\ (P, Q) &\mapsto \alpha(P, Q) = f_{T,P}(Q)^{(q^k-1)/r} \end{aligned}$$

defines a well-defined, bilinear, non-degenerate pairing which is called the reduced Ate pairing.

Recently, the variants of the Eta and Ate pairings have been suggested which shorten the loop length in Miller's algorithm. Those are so-called generalized pairings [96], optimized pairings [68], the R-ate pairing [63] and optimal pairings [90].

We now consider the generalized versions of the Eta and Ate pairings by Zhao, Zhang and Huang [96]:

- generalized Eta pairing: $\eta_c(P, Q) = f_{\lambda^c \bmod r,P}(Q)^{(q^k-1)/r}, \ o < c < k,$
- generalized Ate pairing: $\alpha_c(P, Q) = f_{T^c \bmod r,P}(Q)^{(q^k-1)/r}, \ o < c < k.$

In these definitions, the loop length may be shortened as the original pairings for certain choice of $c$.

**Example 3.10.1 ([77])** *We consider Barreto-Naehrig curves [7] for* $k = 12$ *that we shall discuss more precisely in the following chapter. These curves are parameterized by the polynomial* $t(x) = 6x^2+1$, $r(x) = 36x^4+36x^3+18x^2+6x+1$ *and* $q(x) = 36x^4+36x^3+24x^2+6x+1$. *Barreto and Naehrig have shown that these curves parameterized by* $(t, r, q)$ *have a twist of degree* $6$. *Therefore, we can consider*

$$\lambda = (t-1)^{k/d} = (6x^2)^2 \equiv 36x^4 \pmod r$$

*For positive values of x, the length of* $\lambda$ *is about the same as the length of r. Therefore, using the Eta pairing does not give any advantage. However, if we use generalized Eta pairing for* $c = 4$, *we obtain* $\lambda^4 = -\lambda$ *since* $\lambda$ *is a primitive sixth root of unity. In this case, we have* $-\lambda \equiv -36x^4 \equiv 36x^3 + 18x^2 + 6x + 1 \pmod r$ *and thus the length of* $-\lambda$ *is about* $3/4$ *of the length of r. This yields a faster pairing than the Tate pairing.*

*For negative values of x, we obtain* $\lambda \equiv -36x^3 - 18x^2 - 6x - 1 \pmod r$ *that the length is about 3/4 of the length of r. Therefore, the Eta pairing works faster than the Tate pairing.*

**Example 3.10.2 ([96])** *We consider the family of elliptic curves with embedding degree* $k = 22$ *introduced by Murphy and Fitzpatrick [76]. These curves are parameterized by the polynomial* $t(x) = -x^{16} + 1$ *and* $r(x) = x^{20} - x^{18} + x^{16} - x^{14} + x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$. *We have* $T = t - 1 \equiv -x^{16} \pmod r$ *such that the length of T is about the same as the length of r. Therefore, using the Ate pairing does not give any advantage. However, if we use generalized Ate pairing for* $c = 7$, *we obtain* $T^7 \equiv x^2 \pmod r$. *Therefore, the length of* $T^7$ *is about* $1/10$ *of the length of r. This yields a faster pairing than the Tate pairing.*

# CHAPTER 4

# PAIRING-FRIENDLY ELLIPTIC CURVES

One of the most important method to find suitable elliptic curves for pairing-based cryptographic protocol is the complex multiplication (CM) method. In this chapter, we discuss this method and show how to use it to construct pairing friendly elliptic curves of varying embedding degrees. We also classify these curves according to their construction methods and study them in details. Furthermore, we focus our attention to the elliptic curves of the form $y^2 = x^3 - c$ over $\mathbb{F}_q$ and compute explicitly their number of points $\#E(\mathbb{F}_q)$. In particular, we show that the elliptic curve $y^2 = x^3 - 1$ over $\mathbb{F}_q$ for the primes $q$ of the form $27A^2 + 1$ has an embedding degree $k = 1$ and belongs to Scott-Barreto families in our classification.

## 4.1 Complex Multiplication

We will briefly explain the *complex multiplication (CM) method* to construct elliptic curves with a specified number of points. This method was first introduced by Atkin and Morain in [1]. For a detailed discussion, one can look at [11, 47]. The CM method, which was originally devised for use in primality testing, constructs a curve with endomorphism ring $\mathrm{End}(E)$ isomorphic to the ring of integers in a quadratic imaginary field $\mathbb{Q}(\sqrt{-D})$. This is done as follows: Let $q$ be a prime. According to the Theorem 2.5.1 (Hasse Theorem), $Z = 4q - t^2$ has to be positive. Therefore, there is a unique factorization of $Z$ of the form $Dy^2$, where $D, y \in \mathbb{Z}$ and $D$ is square free (i.e. contains no square factors). Consequently, we get so-called the CM equation

$$Dy^2 = 4q - t^2.$$

The number $D$ is called a CM discriminant for the prime $q$. For every such $D$, there exists a Hilbert class field polynomial $H_D(x) \in \mathbb{Z}[x]$ for which the computation of $H_D(x)$ will be discussed in Section 4.3. One can consider the Hilbert polynomial $H_D(x)$ as a polynomial in $\mathbb{F}_q[x]$, and finds a root $j_0 \in \mathbb{F}_q$. This $j_0$ is the $j$-invariant of the curve to be constructed.

- If $j_0 \neq 0, 1728$, the elliptic curve constructed by CM method will have the form

  $$y^2 = x^3 + 3mc^2x + 2mc^3,$$

  where $m = j_0/(1728 - j_0)$ and $c \in \mathbb{F}_q^*$. In this case, suppose $E$ and $E^{'}$ have the same $j$-invariant but are not isomorphic over $\mathbb{F}_q$, then $E^{'}$ is the quadratic twist of $E$. If $\#E(\mathbb{F}_q) = q + 1 - t$, then $\#E^{'}(\mathbb{F}_q) = q + 1 + t$. In particular, if $E$ is given by

  $$E\ :\ y^2 = x^3 + ax + b,$$

  then $E^{'}$ can be given by

  $$E^{'}\ :\ y^2 = x^3 + ac^2x + bc^3,$$

  where $c$ is a quadratic nonresidue in $\mathbb{F}_q$. In order to decide the order of $E$, one can generate a random point $P$ of $E$ and check if $(q + 1 - t)P = \infty$. If not, the order must be $q + 1 + t$.

- If $j_0 = 0$, the curve has the form $y^2 = x^3 + b$ for some $b$. In this case, one can try different values of $b$ until a curve with the correct order is found. Lynn [67, Section 6.17] enumerate all possible orders which are coming from the quadratic, cubic and sextic degree twist.

- If $j_0 = 1728$, the curve has the form $y^2 = x^3 + ax$ for some $a$. In this case, one can try different values of $a$ until a curve with the correct order is found. Lynn [67, Section 6.17] enumerate all possible orders which are coming from the quadratic and quartic degree twist.

The most time consuming part of the CM method is the construction of the Hilbert polynomial, as it requires high precision floating point complex arithmetic. The library packages providing arbitrary precision floating point numbers may not include routines for complex arithmetic. Therefore, one should consider a few basic facts which are given in [67, Section 5.12] to implement complex numbers using such a library.

**Remark 4.1.1** *Savas et al. [80] proposed a variant of the CM method to overcome the high computational requirements of the construction of the Hilbert polynomial. As opposed to the*

*CM method described above, this variant does not start with a specific q but start with a CM discriminant $D \equiv 3 \pmod 8$. In this variant, Hilbert polynomials can be constructed by using the precomputation phase and stored for later use.*

**Remark 4.1.2** *Konstantinou et al. [60] considered a variant of the CM method for constructing elliptic curves of prime order using Weber polynomials. They have shown that Weber polynomials in this case do not have roots in $\mathbb{F}_q$ but do have in the extension field $\mathbb{F}_{q^3}$. They have also presented a set of transformations for mapping the roots of Weber polynomials in $\mathbb{F}_{q^3}$ to the roots of their corresponding Hilbert polynomials in $\mathbb{F}_q$. Moreover, they have shown how a new class of polynomials, with degree equal to their corresponding Hilbert counterparts, can be used instead of Weber polynomials in the CM method, efficiently.*

## 4.2 Generalized Pell Equation

We now describe how to solve Pell-type equations that will be used in some construction of pairing-friendly curves. A *generalized Pell equation* is an equation of the form

$$x^2 - Dy^2 = N, \tag{4.1}$$

where $D$ is not a square. In order to find integer solutions of (4.1), we first find the minimal positive integer solution $(U, V)$ of the *Pell equation* given by

$$x^2 - Dy^2 = 1.$$

This is done by computing the continued fraction expansion of $\sqrt{D}$ (see [67, Section 4.17]). Then we find a so-called fundamental solution $(x_0, y_0)$ of (4.1) using one of the technique described by Matthews [69] or Robertson [79]. If a solution exists, then we have a family of solutions $(x_i, y_i)$ for $i \in \mathbb{Z}$ to (4.1) given by

$$x_i + y_i\sqrt{D} = (x_0 + y_0\sqrt{D})(U + V\sqrt{D})^i$$

## 4.3 Hilbert Polynomials

The simplest way to compute the $j$-invariant of the resulting curve is to construct the Hilbert polynomial $H_D(x)$ using the complex floating point arithmetic. In order to this, we adopt the method proposed in [1].

The only input for the construction of the Hilbert polynomial $H_D(x)$ is the CM discriminant $D$. The Hilbert class polynomial $H_D(x)$ for a given negative value of discriminant $D$ is defined by

$$H_D(x) = \prod (x - j(\tau)) \tag{4.2}$$

for a set of values of $\tau$ lying in the upper half (positive imaginary part) of the complex plane in the form

$$\tau = \frac{-b + \sqrt{D}}{2a},$$

where $a, b, c \in \mathbb{Z}$ satisfying the following conditions: $(i)$ $b^2 - 4ac = D$, $(ii)$ $|b| \leq a \leq \sqrt{|D|/3}$, $(iii)$ $a \leq c$, $(iv)$ $\gcd(a, b, c) = 1$ and $(v)$ if $|b| = a$ or $a = c$ then $b \geq 0$. The quadratic form $f(x, y) = ax^2 + bxy + cy^2$ denoted by the 3-tuple of integers $[a, b, c]$ that satisfy the above conditions is a primitive (no common factor coefficients) reduced positive definite binary quadratic form of discriminant $D$. Here, $\tau$ is the root of $f(x, 1) = 0$. The quantity $j(\tau)$ in (4.2) is called class invariant and is defined as follows: Let $z = e^{2i\pi\tau}$ and $h(\tau) = \Delta(2\tau)/\Delta(\tau)$, where

$$\Delta(\tau) = z\left(1 + \sum_{n\geq 1}(-1)^n(z^{n(3n-1)/2} + z^{n(3n+1)/2})\right)^{24}.$$

Then

$$j(\tau) = \frac{(256h(\tau) + 1)^3}{h(\tau)}.$$

Let $h_D$ be the degree or class number of $H_D(x)$. Then following [1], one can set the high precision for floating point arithmetic as follows:

$$10 + \binom{h_D}{\lfloor h_D/2 \rfloor} \pi\sqrt{D} \sum_{\tau} \frac{1}{a},$$

where the sum running over all the same set of the values of $\tau$ as the product in (4.2).

Cohen gives the algorithms to compute the Hilbert class polynomial [23, Algorithm 7.6.1] and reduced form of discriminant $D$ [23, Algorithm 5.3.1]. In particular, one will need a single root of the Hilbert polynomial over a finite field so as to generate elliptic curves using the CM method. The following states that the Hilbert polynomial have roots modulo prime $q$ under certain conditions

**Theorem 4.3.1 ([60])** *A Hilbert polynomial $H_D(x)$ with degree $h_D$ has exactly $h_D$ roots modulo $q$ if and only if the equation $4q = t^2 + Dy^2$ has integer solutions and $q$ does not divide the discriminant of the polynomial $H_D(x)$.*

In this respect, a procedure to find a root of the Hilbert polynomial modulo prime $q$ is described by Lynn in [67, Section 5.8].

## 4.4 Generating Pairing-Friendly Elliptic Curves

**Definition 4.4.1 ([33])** *Let $E$ be an elliptic curve over $\mathbb{F}_q$ with characteristic $p$ and let $k$ be the embedding degree. Then, $E$ is called* ***pairing-friendly*** *if the following conditions hold:*

*(1) For a prime $r$ dividing $\#E(\mathbb{F}_q)$, $r \geq \sqrt{q}$*

*(2) $k < \log_2(r)/8$*

This definition is analogous to the elliptic curves having small embedding degree and a subgroup of large prime-order $r$. The bound on the subgroup of order $r$ is deduced from the work by Luca and Shparlinski [66] that the curves having small embedding degree are abundant if $r < \sqrt{q}$ and quite rare if $r > \sqrt{q}$.

The classification of supersingular elliptic curves have been proposed in [70]. These curves have embedding degree at most 6 over any finite field. Therefore, a supersingular curve is always pairing-friendly if it has a large prime-order subgroup.

In order to achieve higher security levels and different embedding degrees, one must construct pairing-friendly ordinary elliptic curves. There are number of methods in the literature for constructing such curves, all of which do the following:

(1) Fix the embedding degree $k$, and then compute integers $t, r, q$ such that there is an elliptic curve $E(\mathbb{F}_q)$ having trace of the Frobenius $t$ and a subgroup of prime order $r$.

(2) Use the CM method to find the equation of the elliptic curve $E(\mathbb{F}_q)$.

The difficult part of such methods is finding $t, r$ and $q$ in Step (1). In this respect, an ordinary elliptic curve with these properties can be constructed if and only if the following conditions hold:

(1) $q$ is prime or a prime power with $\gcd(q, t) = 1$.

(2) $Dy^2 = 4q - t^2$ for some sufficiently small positive $D$ and some integer $y$.

(3) $r$ is prime such that $r \mid q + 1 - t$.

(4) $r \mid q^k - 1$, and $r \nmid q^i - 1$ for $1 \leq i < k$.

We will generally take $q$ to be a prime number. If we find the integers $q$, $t$, and $r$ satisfying above conditions, it is guaranteed that there exists an ordinary elliptic curve $E$ over $\mathbb{F}_q$ with embedding degree $k$ and a subgroup of order $r$. In condition (2), having sufficiently small $D$ is necessary for us to be able to find the equation of such a curve by using the CM method. If we use the condition (3) to write $q + 1 - t = hr$ for some $h$, then the CM equation can be rewritten by

$$Dy^2 = 4hr - (t - 2)^2,$$

where $h$ is the cofactor of the pairing-friendly curve. Condition (4) is equivalent to $E$ having embedding degree $k$ and then gives us the following fact which is crucial for the construction of prime order curves with embedding degree k. The proof can be found in [5, 33].

**Lemma 4.4.2** *Let $E$ be an elliptic curve over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t = hr$, where $r$ is prime and $t$ is the trace of $E$. Then, $E$ has embedding degree $k$ with respect to $r$ if and only if $r \mid \Phi_k(t - 1)$, where $\Phi_k$ is the kth cyclotomic polynomial .*

### 4.4.1 Families of Pairing-Friendly Elliptic Curves

In Section 4.4, we have shown that how to construct pairing-friendly elliptic curves by finding $t, r, q$ satisfying some conditions. From the implementation point of view, it is very important to construct curves of specified bit size. Therefore, Freeman, Scott and Teske [33] describe the families of pairing-friendly elliptic curves for which the curve parameters $t, r, q$ are given as polynomials $t(x), r(x), q(x)$ with respect to parameter $x$. This parametrization have been used by several different authors in the literature. Some of them are Miyaji, Nakabayashi and Takano [74], Barreto, Lynn and Scott [5], Scott and Barreto [82], Brezing and Weng [17] and Cocks and Pinch [22]. Their definition of a family of pairing-friendly curves forms the implicit ideas in these works.

The constructed polynomials will need to have some property that $q(x)$, the sizes of a field, is a prime power (in general prime) and $r(x)$, order of a subgroup, is a prime or a small cofactor times a prime. However, it is so difficult to show the polynomials $q$ and $r$ take an infinite number of primes. We note that not even known $x^2 + 1$ takes an infinite number of primes.

Freeman, Scott and Teske [33] give the following definition which is motivated by the fact: if $f(x) \in \mathbb{Z}[x]$, then a famous conjecture of Bouniakowski and Schinzel (see [62, page 323]) says that a nonconstant $f(x)$ takes an infinite number of prime values if and only if $f$ has positive leading coefficient, $f$ is irreducible and $\gcd(\{f(x) \mid x \in \mathbb{Z}\}) = 1$. We note that Bateman and Horn conjecture [8] gives the expected density of such prime values as we discussed in Section 2.2.

**Definition 4.4.3 ([33])** *Let $f(x)$ be a polynomial with rational coefficients. then we say that $f$ represents primes if the following conditions are satisfied:*

*(1)* *$f(x)$ is nonconstant.*

*(2)* *$f(x)$ has positive leading coefficient.*

*(3)* *$f(x)$ is irreducible.*

*(4)* *$f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$.*

*(5)* $\gcd(\{f(x) \mid x, f(x) \in \mathbb{Z}\}) = 1$.

**Definition 4.4.4 ([33])** *A polynomial $f(x) \in \mathbb{Q}[x]$ is integer-valued if $f(x) \in \mathbb{Z}$ for every $x \in \mathbb{Z}$.*

**Definition 4.4.5 ([33])** *Let $t(x)$, $r(x)$, and $q(x)$ be nonzero polynomials with rational coefficients.*

*(1)* *For a given integer $k > 0$ and square-free integer $D \in \mathbb{Z}^+$, the triple $(t, r, q)$ parameterizes a family of elliptic curves with embedding degree $k$ and discriminant $D$ if the following conditions are satisfied:*

*(i)* *$q(x) = p(x)^d$ for some $d \geq 1$ and primes $p(x)$.*

*(ii)* *$r(x)$ is nonconstant, irreducible, integer-valued and it has positive leading coefficient.*

*(iii)* $r(x)$ *divides* $q(x) + 1 - t(x)$.

*(iv)* $r(x)$ *divides* $\Phi_k(t(x) - 1)$.

*(v) The equation* $Dy^2 = 4q(x) - t(x)^2$ *has infinitely many integer solutions* $(x, y)$.

*(2) For* $(t, r, q)$ *as in* (1), *if* $x_0$ *is an integer and E is an elliptic curve over* $F_{q(x_0)}$ *with trace* $t(x_0)$, *then we say E is a curve in the family* $(t, r, q)$.

*(3) A family* $(t, r, q)$ *is ordinary if* $\gcd(t(x), q(x)) = 1$.

*(4) A family* $(t, r, q)$ *is complete if there is some* $y(x) \in \mathbb{Q}[x]$ *such that* $Dy(x)^2 = 4q(x) - t(x)^2$*; otherwise we say that the family is sparse.*

**Definition 4.4.6 ([33])** *Let* $t(x)$, $r(x)$, *and* $q(x)$ *be nonzero polynomials with rational coefficients. The triple* $(t, r, q)$ *parameterizes a potential family of curves with embedding degree k and discriminant D if conditions* $(ii) - (v)$ *of (1) in Definition 4.4.5 are satisfied.*

By using condition (2) in Definition 4.4.5, we can write the number of points of $E(\mathbb{F}_{q(x)})$ by

$$h(x)r(x) = q(x) + 1 - t(x),$$

where $h(x)$ is the cofactor of the family of the pairing-friendly curves. In practice, $h(x) = 1$ is the ideal case, eventhough it is so hard to achieve. Therefore, Freeman, Scott and Teske [33] define a parameter $\rho$ that represents the closeness of the constructed curves to the ideal case.

**Definition 4.4.7 ([33])** *(i) Let E be an elliptic curve over* $\mathbb{F}_q$, *and suppose that E has a subgroup of order r. The* $\rho$*-value of E (with respect to r) is*

$$\rho(E) = \frac{\log q}{\log r}.$$

*(ii) Let* $t(x), r(x), q(x) \in \mathbb{Q}[x]$, *and suppose that* $(t, r, q)$ *represents a family of elliptic curves with embedding degree k. The* $\rho$*-value of* $(t, r, q)$ *is*

$$\rho(t, r, q) = \lim_{x\to\infty} \frac{\log q(x)}{\log r(x)} = \frac{\deg q(x)}{\deg r(x)}.$$

## 4.5 Supersingular Elliptic Curves

The elliptic curve $E$ defined over $\mathbb{F}_q$ is said to be supersingular if the characteristic $p$ of $\mathbb{F}_q$ divides $t$, where $t = q+1-\#E(\mathbb{F}_q)$. Waterhouse [93, Theorem 4.1] showed that the number of points of supersingular elliptic curves are of the form $q+1-t$, where $t^2 \in \{0, q, 2q, 3q, 4q\}$. By using the factorizations of $q^k - 1$, it is easy to see that supersingular curves have embedding degrees $k \in \{1, 2, 3, 4, 6\}$. These curves are defined on prime fields $p \geq 5$ only for $k = 2$ [70] and constructed by making use of [61, Theorem 13.12]. The representatives of the isomorphism classes for supersingular curves over $\mathbb{F}_q$ of characteristic 2 and 3 have been determined by Menezes and Vanstone [71] and Morain [75], respectively.

The only known general method to construct supersingular elliptic curves is reduction of CM curves in characteristic zero that an explicit procedure will be discussed in Section 4.5.2.

Since supersingular elliptic curves with $k = 2$ is the only possible embedding degree over prime fields, we also consider non-prime fields $\mathbb{F}_q$ that $q$ will be of the form $2^n$, $3^n$ and $p^2$ for large primes $p$. These choices are because of the efficiency reasons. However, the fields $\mathbb{F}_q$ must be larger when $q = 2^n$ or $3^n$ than when $q = p$ or $p^2$ as a result of the index calculus method for discrete logarithm computation in finite fields of small characteristic given by Coppersmith [25].

We also discuss the minimal embedding field for non-prime fields following the work of Hitt [45] and Benger et al. [9]. It means that the fields of which the pairings take their values.

For pairing-based cryptographic applications, it is widely believed that supersingular curves are ”weak” curves depending on the Menezes-Okamoto-Vanstone (MOV) attack [70] and Frey-Rück (FR) attack [35]. However, Koblitz and Menezes argue about saying no known reasonable security advantage between nonsupersingular curve and supersingular curve having the same embedding degree. On the other hand, supersingular curves have also the distortion maps which gives an advantage for cryptographic applications [91].

In this section, we give the classification of supersingular elliptic curves relative to their embedding degrees.

### 4.5.1 Embedding Degree $k = 1$ Curves

Let $E$ be a supersingular elliptic curve over $\mathbb{F}_q$ with embedding degree $k = 1$. Then it is shown by Menezes, Okamoto and Vanstone in [70] that $q = p^n$ with even $n$. In this case, $t = \mp 2\sqrt{q}$, and therefore $\#E(\mathbb{F}_q) = q + 1 \mp 2\sqrt{q}$. By using Lemma 4.4.2, the subgroup of order $r$ must divide both $\#E(\mathbb{F}_q)$ and $\Phi_1(q) = q - 1$. It follows from this fact that $r$ is a factor of $\gcd(\#E(\mathbb{F}_q), q - 1) = \sqrt{q} \mp 1$. Therefore, such curves must have $\rho \geq 2$ by Definition 4.4.7.

If $q = 2^n$ with even $n$, supersingular elliptic curves having embedding degree $k = 1$ are listed in Table 4.1, where $\omega \in \mathbb{F}_q$ and $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\omega) = 1$ [71].

Table 4.1: Supersingular elliptic curves with $k = 1$ over $F_{2^n}$ for even $n$

| Curve | n | $\#E(\mathbb{F}_q)$ | Group Type |
|---|---|---|---|
| $y^2 + y = x^3$ | $n \equiv 0 \pmod 4$ | $q + 1 - 2\sqrt{q}$ | $\mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$ |
| | $n \equiv 2 \pmod 4$ | $q + 1 + 2\sqrt{q}$ | $\mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$ |
| $y^2 + y = x^3 + \omega$ | $n \equiv 0 \pmod 4$ | $q + 1 + 2\sqrt{q}$ | $\mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$ |
| | $n \equiv 2 \pmod 4$ | $q + 1 - 2\sqrt{q}$ | $\mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$ |

If $q = 3^n$ with even $n$, supersingular elliptic curves having embedding degree $k = 1$ are listed in Table 4.2, where $\gamma \in \mathbb{F}_q$ and $\sqrt{\gamma} \notin \mathbb{F}_q$ [75].

Table 4.2: Supersingular elliptic curves with $k = 1$ over $F_{3^n}$ for even $n$

| Curve | n | $\#E(\mathbb{F}_q)$ | Group Type |
|---|---|---|---|
| $y^2 = x^3 - x$ | $n \equiv 0 \pmod 4$ | $q + 1 - 2\sqrt{q}$ | $\mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$ |
| | $n \equiv 2 \pmod 4$ | $q + 1 + 2\sqrt{q}$ | $\mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$ |
| $y^2 = x^3 - \gamma^2 x$ | $n \equiv 0 \pmod 4$ | $q + 1 + 2\sqrt{q}$ | $\mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$ |
| | $n \equiv 2 \pmod 4$ | $q + 1 - 2\sqrt{q}$ | $\mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$ |

If $q = p^n$, with $p \geq 5$ and even $n$, in order to construct supersingular elliptic curves with embedding degree $k = 1$, we consider the following: we first set $q^{'} = \sqrt{q}$ and $t = q^{'} + 1 - \#E(\mathbb{F}_{q^{'}}) = 0$. Therefore $\#E(\mathbb{F}_{q^{'}}) = q^{'} + 1$. This means that the elliptic curves $E(\mathbb{F}_{q^{'}})$ has embedding degree $k = 2$. The characteristic polynomial of $q^{'}$-th power Frobenius map is $x^2 + q^{'} = (x + i\sqrt{q^{'}})(x - i\sqrt{q^{'}})$, where $i = \sqrt{-1}$. By Theorem 2.5.2, we can easily get the characteristic polynomial of the $q$-th power Frobenius map as $(x + q^{'})^2$, and so $\#E(\mathbb{F}_q) = (q^{'} + 1)^2 = q + 2\sqrt{q} + 1$. It follows from this fact that $E(\mathbb{F}_q)$ has embedding degree $k = 1$. We note that if $q^{'}$ is prime, then $\mathbb{F}_q$ is also the minimal embedding field for $E$.

For a supersingular elliptic curve $E$ over $\mathbb{F}_q$, where $q = p^n$ with even $n$ that has embedding degree $k = 1$, $E$ has minimal embedding field $\mathbb{F}_q$ if $\#E(\mathbb{F}_q) = q + 1 + 2\sqrt{q}$ and $\rho < 6(1 - \frac{1}{\log_2 r})$, $E$ has minimal embedding field $\mathbb{F}_{q^{1/2}}$ if $\#E(\mathbb{F}_q) = q + 1 - 2\sqrt{q}$ and $\rho < 4$ [9, Proposition 3.6].

### 4.5.2 Embedding Degree $k = 2$ Curves

Supersingular elliptic curves with embedding degree $k = 2$ offers the most flexibility. In other words, one can construct curves over prime fields with arbitrary subgroup of order $r$ and arbitrary $\rho$-value. In this case, $r$ should divide $\Phi_2(q) = q + 1$ and therefore $r$, being a divisor of $\#E(\mathbb{F}_q) = q + 1 - t$, divides t. This certainly holds if $t = 0$, and such supersingular curves can be defined over both prime and non-prime fields..

The only supersingular elliptic curve in characteristic 2 and 3 is the curve with $j$-invariant zero (see [21],[86, Section 5.4]). Explicitly, we will now give the trace-zero supersingular curves for fields $\mathbb{F}_q$ of characteristic 2 and 3, respectively.

If $q = 2^n$, there are 2 isomorphism classes of supersingular elliptic curves with embedding degree $k = 2$ which are obtained by Menezes and Vanstone [71]. These curves are listed in Table 4.3, where $\delta \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_4}(\delta) \neq 0$.

Table 4.3: Supersingular elliptic curves with $k = 2$ over $F_{2^n}$

| Curve | n | $\#E(\mathbb{F}_q)$ | Group Type |
|---|---|---|---|
| $y^2 + y = x^3$ | odd | $q + 1$ | Cyclic |
| $y^2 + y = x^3 + \delta x$ | even | $q + 1$ | Cyclic |

If $q = 3^n$, there are 4 isomorphism classes of supersingular elliptic curves with embedding degree $k = 2$ which are obtained by Morain [71]. These curves are listed in Table 4.4, where $\sqrt{\gamma} \notin \mathbb{F}_q^*$ with $q = 3^s$.

Table 4.4: Supersingular elliptic curves with $k = 2$ over $F_{3^n}$

| Curve | n | $\#E(\mathbb{F}_q)$ | Group Type |
|---|---|---|---|
| $y^2 = x^3 + x$ | odd | $q + 1$ | Cyclic |
| $y^2 = x^3 - x$ | odd | $q + 1$ | $\mathbb{Z}_{((q+1)/2)} \oplus \mathbb{Z}_2$ |
| $y^2 = x^3 - \gamma x$ | even | $q + 1$ | Cyclic |
| $y^2 = x^3 - \gamma^3 x$ | even | $q + 1$ | Cyclic |

For a supersingular curve $E$ over $\mathbb{F}_q$, where $q = p^n$, with $k = 2$, $E$ has minimal embedding field $\mathbb{F}_{q^2}$ if either $\rho < 3(1 - \frac{1}{\log_2 r})$ or $n$ is prime and $r > p + 1$ [9, Proposition 3.5].

In order to construct supersingular elliptic curves over prime fields $\mathbb{F}_q$ with $q \geq 5$, we combine the work of Koblitz and Menezes [59, Section 7] and the work of Bröker [19, Section 3.4]. In this respect, for a given subgroup of order $r$, if we choose any $h$ such that $q + 1 = hr$ is prime, then we have the following curves over $\mathbb{F}_q$ with embedding degree $k = 2$:

(i) If $q \equiv 3 \pmod 4$, $y^2 = x^3 + ax$ for any $a \in \mathbb{F}_q^*$.

(ii) If $q \equiv 5 \pmod 6$, $y^2 = x^3 + b$ for any $b \in \mathbb{F}_q^*$.

(iii) If $q \equiv 1 \pmod{12}$, $y^2 = x^3 + 3mc^2x + 2mc^3$ for any $c \in \mathbb{F}_q^*$ and $m = j/(1728 - j)$. Here, $j \in \mathbb{F}_q$ is a root of the Hilbert class polynomial $H_D$ of $\mathbb{Q}(\sqrt{-D})$, where $D$ is the smallest prime such that $D \equiv 3 \pmod 4$ and $\chi_2(-D) = -1$ in $\mathbb{F}_q$.

The most popular supersingular elliptic curves are given by the equations $y^2 = x^3 + ax$ and $y^2 = x^3 + b$. Their endomorphism rings are isomorphic to the ring of integers $\mathbb{Z}[i]$ and $\mathbb{Z}[\delta]$, respectively. These two curves have also the distortion maps, which are easy to compute. In the sense of [91], the map $(x, y) \mapsto i(x, y) = (-x, iy)$ is a distortion map of the curve $y^2 = x^3 + ax$, where $i = \sqrt{-1} \in \mathbb{F}_{q^2}$ and the map $(x, y) \mapsto \delta(x, y) = (\beta x, y)$ is a distortion map of the curve $y^2 = x^3 + b$, where $\beta \neq 1 \in \mathbb{F}_{q^2}$ such that $\beta^3 = 1$.

### 4.5.3 Embedding Degree $k = 3$ Curves

In [74, Theorem 4], Miyaji, Nakabayashi, and Takano showed that supersingular elliptic curves having embedding degree $k = 3$ with respect to a subgroup of prime order $r > 3$

only exist over $\mathbb{F}_q$, where $q = p^n$ with even $n$, and $t = \pm\sqrt{q}$. When the characteristic $p > 3$, these curves are given by the following form [75]:

$$E(\mathbb{F}_q) \ : \ y^2 = x^3 + \gamma,$$

where $\gamma \in \mathbb{F}_q^*$ such that $\chi_3(\gamma) \neq 1$ in $\mathbb{F}_q^*$.

According to [74, Theorem 4], when we choose $q = p^2$ where $p \equiv 2 \pmod 3$, we obtain a family of supersingular elliptic curves with $k = 3$, which are parameterized by the triple $(t, r, q)$. In this case, $\#E(\mathbb{F}_{p^2}) = p^2 \pm p + 1$. If $t = -p$, then for some $p = 3x - 1$, we are able to find curves of prime order since $r(x) = (3x - 1)^2 + (3x - 1) + 1$ represents primes in the sense of Definition 4.4.3. If $t = p$, we may find curves that the number of points of those can be equal to 3 times a prime. Therefore, depending on the sign of t, we can summarize the families of supersingular elliptic curves with embedding degree $k = 3$ in Table 4.5.

Table 4.5: Family of supersingular curves with embedding degree $k = 3$

| t(x) | r(x) | q(x) |
|---|---|---|
| $-3x + 1$ | $9x^2 - 3x + 1$ | $(3x - 1)^2$ |
| $3x - 1$ | $3 \cdot (3x^2 - 3x + 1)$ | $(3x - 1)^2$ |

If $q = 2^n$ with even $n$, supersingular elliptic curves having embedding degree $k = 3$ are given in Table 4.6, where $\alpha, \beta \in \mathbb{F}_q$, $\sqrt[3]{\delta} \notin \mathbb{F}_q$ such that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\delta^{-2}\alpha) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\delta^{-4}\beta) = 1$ [71].

Table 4.6: Supersingular elliptic curves with $k = 3$ over $F_{2^n}$ for even $n$

| Curve | n | $\#E(\mathbb{F}_q)$ | Group Type |
|---|---|---|---|
| $y^2 + \delta y = x^3$ | $n \equiv 0 \pmod 4$ | $q + 1 + \sqrt{q}$ | Cyclic |
| | $n \equiv 2 \pmod 4$ | $q + 1 - \sqrt{q}$ | Cyclic |
| $y^2 + \delta y = x^3 + \alpha$ | $n \equiv 0 \pmod 4$ | $q + 1 - \sqrt{q}$ | Cyclic |
| | $n \equiv 2 \pmod 4$ | $q + 1 + \sqrt{q}$ | Cyclic |
| $y^2 + \delta^2 y = x^3$ | $n \equiv 0 \pmod 4$ | $q + 1 + \sqrt{q}$ | Cyclic |
| | $n \equiv 2 \pmod 4$ | $q + 1 - \sqrt{q}$ | Cyclic |
| $y^2 + \delta^2 y = x^3 + \beta$ | $n \equiv 0 \pmod 4$ | $q + 1 - \sqrt{q}$ | Cyclic |
| | $n \equiv 2 \pmod 4$ | $q + 1 + \sqrt{q}$ | Cyclic |

If $q = 3^n$ with even $n$, supersingular elliptic curves having embedding degree $k = 3$ are given in Table 4.7, where $\sqrt{\gamma} \notin \mathbb{F}_q$ and $\omega \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\omega) = 1$ [75].

Table 4.7: Supersingular elliptic curves with $k = 3$ over $F_{3^n}$ for even $n$

| Curve | n | $\#E(\mathbb{F}_q)$ | Group Type |
|---|---|---|---|
| $y^2 = x^3 - x + \omega$ | $n \equiv 0 \pmod 4$ | $q + 1 + \sqrt{q}$ | Cyclic |
| | $n \equiv 2 \pmod 4$ | $q + 1 - \sqrt{q}$ | Cyclic |
| $y^2 = x^3 - \gamma^2 x + \gamma^3\omega$ | $n \equiv 0 \pmod 4$ | $q + 1 - \sqrt{q}$ | Cyclic |
| | $n \equiv 2 \pmod 4$ | $q + 1 + \sqrt{q}$ | Cyclic |

For a supersingular elliptic curve $E$ over $\mathbb{F}_q$, where $q = p^n$ with even $n$ that has embedding degree $k = 3$, $E$ has minimal embedding field $\mathbb{F}_{q^3}$ if $\#E(\mathbb{F}_q) = q+1-\sqrt{q}$ and $\rho < \frac{10}{3}(1-\frac{1}{\log_2 r})$, $E$ has minimal embedding field $\mathbb{F}_{q^{3/2}}$ if $\#E(\mathbb{F}_q) = q + 1 + \sqrt{q}$ and $\rho < 4/3$ [9, Proposition 3.8].

### 4.5.4 Embedding Degree $k = 4$ Curves

In [74, Theorem 3], Miyaji, Nakabayashi, and Takano showed that supersingular elliptic curves having embedding degree $k = 4$ with respect to a subgroup of prime order $r > 2$ exists over $\mathbb{F}_q$, only if $q = 2^n$ with odd $n$, and $t = \pm\sqrt{2q}$. All possible such curves are listed in Table 4.8 (see [71]).

Table 4.8: Supersingular elliptic curves with $k = 4$ over $F_{2^n}$ for odd $n$

| Curve | n | $\#E(\mathbb{F}_q)$ | Group Type |
|---|---|---|---|
| $y^2 + y = x^3 + x$ | $n \equiv \pm1 \pmod 8$ | $q + 1 + \sqrt{2q}$ | Cyclic |
| | $n \equiv \pm3 \pmod 8$ | $q + 1 - \sqrt{2q}$ | Cyclic |
| $y^2 + y = x^3 + x + 1$ | $n \equiv \pm1 \pmod 8$ | $q + 1 - \sqrt{2q}$ | Cyclic |
| | $n \equiv \pm3 \pmod 8$ | $q + 1 + \sqrt{2q}$ | Cyclic |

For a supersingular elliptic curve $E$ over $\mathbb{F}_q$, where $q = 2^n$ with odd $n$ that has embedding degree $k = 4$, $E$ has minimal embedding field $\mathbb{F}_{q^4}$ if either $\rho < \frac{3}{2}(1 - \frac{1}{\log_2 r})$ or $n$ is prime and $r > 5$ [9, Proposition 3.2].

### 4.5.5 Embedding Degree $k = 6$ Curves

In [74, Theorem 4], Miyaji, Nakabayashi, and Takano showed that supersingular elliptic curves having embedding degree $k = 6$ with respect to a subgroup of prime order $r > 3$ exists over $\mathbb{F}_q$, only if $q = 3^n$ with odd $n > 1$, and $t = \pm\sqrt{3q}$. All possible such curves are listed in Table 4.9 depending on $\delta \in \mathbb{F}_q$ such that $\mathrm{Tr}(\delta) = 1$ (see [71]).

Table 4.9: Supersingular elliptic curves with $k = 6$ over $F_{3^n}$ for odd $n > 1$

| Curve | n | $\#E(\mathbb{F}_q)$ | Group Type |
|---|---|---|---|
| $y^2 = x^3 - x + \delta$ | $n \equiv 1 \pmod 4$ | $q + 1 + \sqrt{3q}$ | Cyclic |
| | $n \equiv 3 \pmod 4$ | $q + 1 - \sqrt{3q}$ | Cyclic |
| $y^2 = x^3 - x - \delta$ | $n \equiv 1 \pmod 4$ | $q + 1 - \sqrt{3q}$ | Cyclic |
| | $n \equiv 3 \pmod 4$ | $q + 1 + \sqrt{3q}$ | Cyclic |

For a supersingular elliptic curve $E$ over $\mathbb{F}_q$, where $q = 3^n$ with odd $n$ that has embedding degree $k = 6$, $E$ has minimal embedding field $\mathbb{F}_{q^6}$ if either $\rho < \frac{5}{3}(1 - \frac{1}{\log_2 r})$ or $n$ is prime and $r > 7$ [9, Proposition 3.3].

## 4.6 Ordinary Elliptic Curves

In the literature, there are three most general methods for constructing pairing-friendly ordinary elliptic curves that the name of those are MNT method, Cocks-Pinch method and Dupont-Enge-Morain method. All these algorithms are based on the CM method. If we recall that to construct families of pairing-friendly elliptic curves, we look for polynomials $t(x)$, $r(x)$ and $q(x)$ satisfying conditions given in Definition 4.4.5 and for which the CM equation

$$Dy^2 = 4q(x) - t(x)^2 = 4h(x)r(x) - (t(x) - 2)^2 \tag{4.3}$$

has infinitely many solutions $(x, y)$. Here, $h(x)$ is a cofactor satisfying $\#E(\mathbb{F}_{q(x)}) = h(x)r(x)$.

In this section, we classify pairing-friendly ordinary elliptic curves with respect to the their constructing methods. We first explain the Algorithms how these methods work and give corresponding family of curves examples. We also discuss the extension of these methods.

### 4.6.1 The MNT Method

Miyaji, Nakabayashi and Takano (MNT) [74] were the first authors to propose ordinary elliptic curves of prime order with prescribed embedding degree. In order to construct curves of prime order, we set the cofactor $h(x) = 1$. We now describe MNT method which is also used by Freeman [31].

We first fix the parameters $D$ and $k$, then choose polynomials $t(x)$ and $r(x)$ to get a quadratic polynomial in the right side of Eq. (4.3) so that we can make a substitution to transform the equation into a generalized Pell equation $X^2 - DY^2 = N$. Such equations have only a finite number of integral points by Siegel's theorem [86, Theorem IX.4.3]. Therefore, pairing-friendly ordinary elliptic curves constructed by using this method are so-called "*sparse families*".

**Algorithm 3:** The MNT Method

```
Input: $k \in \mathbb{Z}^+$, square-free poitive integer $D$.
Output: primes $q(x)$ and $r(x)$, an elliptic curve $E$ over $\mathbb{F}_{q(x)}$ with $h(x)r(x)$ points of
        embedding degree $k$.
Step 1 : Choose polynomials $t(x)$ and $h(x)$.
Step 2 : Choose $r(x)$ an irreducible factor of $\Phi_k(t(x) - 1)$.
Step 3 : Compute $q(x) = h(x)r(x) + t(x) - 1$.
Step 4 : Find integer solutions $(x, y)$ to CM equation $Dy^2 = 4h(x)r(x) - (t(x) - 2)^2$.
Step 5 : If $q(x)$ and $r(x)$ are both prime, use CM method to obtain an elliptic curve $E$
over $\mathbb{F}_{q(x)}$ of $h(x)r(x)$ points with embedding degree $k$.
```

#### 4.6.1.1 MNT Curves for $k = 3, 4, 6$

Miyaji, Nakabayashi and Takano (MNT) [74] were the first authors to describe an explicit construction of ordinary pairing-friendly elliptic curves. They showed how to obtain ordinary elliptic curves with the embedding degrees $k = 3, 4, 6$.

**Theorem 4.6.1 ([74])** *Let $E$ be an ordinary elliptic curve over $\mathbb{F}_q$ such that $r = \#E(\mathbb{F}_q) = q + 1 - t$ is prime. Then all possible polynomial representations for embedding degree $k = 3, 4, 6$ are listed in Table 4.10.*

Table 4.10: Representation of MNT curves

| k | q(x) | t(x) |
|---|---|---|
| 3 | $12x^2 - 1$ | $-1 \pm 6x$ |
| 4 | $x^2 + x + 1$ | $-x$ or $x + 1$ |
| 6 | $4x^2 + 1$ | $1 \pm 2x$ |

Miyaji et al. prove the theorem for $q > 64$, the remaininig cases can be demonstrated via a brute-force search. In all three cases, the right-hand side of the CM equation $Dy^2 = 4q(x) - t(x)^2$ becomes quadratic with respect to $x$. Using linear change of variables, the CM equation can be transformed into a generalized Pell equation which we give for all three cases as follows:

(1) For $k = 3$, the CM equation transforms into the generalized Pell equation $X^2 - 3DY^2 = 24$ using the change of variables $X = 6x \pm 3$.

(2) For $k = 4$, the CM equation transforms into the generalized Pell equation $X^2 - 3DY^2 = -8$ using the change of variables $X = 3x + 2$ if $t(x) = -x$ and $X = 3x + 1$ if $t(x) = x + 1$.

(3) For $k = 6$, the CM equation transforms into the generalized Pell equation $X^2 - 3DY^2 = -8$ using the change of variables $X = 6x \pm 1$.

Karabina and Teske [53, 55] show that for primes $r, q > 64$ there is an elliptic curve $E$ over $\mathbb{F}_q$ with embedding degree $k = 6$ and $\#E(\mathbb{F}_q) = r$ if and only if there is an elliptic curve $E$ over $\mathbb{F}_r$ with embedding degree $k = 4$ and $\#E(\mathbb{F}_r) = q$. Luca and Shparlinski [66] give a heuristic result which says MNT curves of prime order are sparse. On the other hand, specific examples of cryptographic applications for MNT curves of 160-bit, 192-bit and 256-bit prime order have been found by Page et al. [78].

#### 4.6.1.2 Freeman Curves for $k = 10$

Freeman [31] discovered one example for a family of curves with $k = 10$. He uses the following factorization obtained by Galbraith et al. [37]:

$$\Phi_{10}(u(x)) = (25x^4 + 25x^3 + 15x^2 + 5x + 1)(400x^4 + 400x^3 + 240x^2 + 60x + 11),$$

where $u(x) = 10x^2 + 5x + 2$. When taking $r(x)$ to be the first factor, he obtains $t(x) = u(x) + 1$ and $q(x) = r(x) + t(x) - 1$. In other words,

$$\begin{aligned} t(x) &= 10x^2 + 5x + 3 \\ r(x) &= 25x^4 + 25x^3 + 15x^2 + 5x + 1 \\ q(x) &= 25x^4 + 25x^3 + 25x^2 + 10x + 3. \end{aligned}$$

It follows from the polynomials that the CM equation becomes $Dy^2 = 15x^2 + 10x + 3$. Using the substitution $X = 15x + 5$, one can transform the CM equation into the generalized Pell equation $X^2 - 15Dy^2 = -20$. For any $D$, the latter equation has an integer solution. This gives a sparse family of curves with embedding degree $k = 10$ which is parameterized by $(t, r, q)$.

### 4.6.2 Extensions of the MNT Method

Scott-Barreto [82] and Galbraith-McKee-Valença [37] extended the MNT method by choosing a small constant cofactor $h$. Scott and Barreto [82] start with the equation (4.3), fix small integers $h$ and $d$. Then they substitute $r$ and $t$ by $\Phi_k(t-1)/d$ and $x + 1$, respectively, to obtain the equation in the form

$$Dy^2 = 4h\frac{\Phi_k(x)}{d} - (x-1)^2. \tag{4.4}$$

It is easy to see that the right-hand side of (4.4) is quadratic with respect to $x$ for $k = 3, 4$ or 6. Therefore, we can transform (4.4) into a generalized Pell equation by an appropriate linear transformation of $x$. As a result, The MNT method can be extended to obtain pairing-friendly ordinary curves of almost prime order with embedding degrees $k = 3, 4$ or 6.

Galbraith, McKee and Valença [37] give a complete characterization of curves with $k = 3, 4$ or 6 for cofactors $2 \leq h \leq 5$. As in the prime-order case, the CM equations $Dy^2 = 4q(x) - t(x)^2$ are quadratic with respect to $x$, and it can be transformed into the generalized Pell equations. Therefore, these family of curves are also *sparse*.

### 4.6.3 The Cocks-Pinch Method

Cocks and Pinch [22] propose a method to construct pairing-friendly ordinary elliptic curves with arbitrary embedding degree. The Cocks-Pinch method is important due to the efficiency of the algorithm. This method can be fully generalized to consruct families of curves with

$\rho < 2$ by Brezing and Weng in [17] that we discuss in Section 4.6.4. Furthermore, Freeman [32] and Freeman et al. [34] both generalized this method to construct pairing-friendly abelian varieties of arbitrary dimension $g \geq 2$.

```
Algorithm 4: The Cocks-Pinch Method to construct a curve for arbitrary $k$
    Input: $k \in \mathbb{Z}^+$, a prime $r$ such that $k \mid r - 1$, square-free poitive integer $D$ and
        $\chi_2(-D) = 1$ in $\mathbb{F}_r$.
    Output: a prime $q$, an elliptic curve $E$ over $\mathbb{F}_q$ of embedding degree $k$ with respect to $r$.
    Step 1 : Choose a $k$-th rooth of unity $z$ in $\mathbb{F}_r$.
    Step 2 : Let $t^{'} \in \mathbb{F}_r$ such that $t^{'} = z + 1$.
    Step 3 : Let $y \in \mathbb{Z}$ such that $y \equiv y^{'} \pmod{r}$ and $y^{'} = (t^{'} - 2)/\sqrt{-D}$.
    Step 4 : Let $t \in \mathbb{Z}$ such that $t \equiv t^{'} \pmod{r}$ and $q = (t^2 + Dy^2)/4$.
    Step 5 : If $q$ is a prime integer and $D < 10^{12}$, use the CM method to obtain an elliptic
    curve $E$ over $\mathbb{F}_q$ with trace $t$ and embedding degree $k$.
```

The main idea in this method (Algorithm 4) is to force $r$ to divide $Dy^2 + (t-2)^2$ when $y$ is constructed. The CM equation $4q - t^2 = Dy^2$ is satisfied with chosen $q$. When we write the CM equation in the form $Dy^2 = 4(q + 1 - t) - (t-2)^2$, we get $4(q + 1 - t) \equiv 0 \pmod{r}$. Furthermore, the choice of $t$ ensures that $\Phi_k(t - 1) \equiv 0 \pmod{r}$. In this method, in general $q \approx r^2$. Therefore, pairing-friendly ordinary elliptic curves consructed by using this method have $\rho \approx 2$ which is less preferred in cryptographic applications. In fact, Vercauteren [90] showed that for certain embedding degrees and certain discriminant $D$, there are no ordinary elliptic curves with smaller $\rho$ value.

Boneh et al. [14] showed that this method can be used to construct pairing-friendly curves of composite order $r$ with embedding degree $k$. However, Koblitz [58] proposed that it is not convenient to use composite order curves in pairing-based protocols due to the security weaknesses.

### 4.6.4 Extensions of the Cocks-Pinch Method

The Cocks-Pinch Method is extended by using two principal methods for constructing complete families, one due to Scott and Barreto [82] and the other due to Brezing and Weng [17] which is due originally the work of Barreto, Lynn and Scott [5]. Both methods start to fix an embedding degree $k$, choose an irreducible polynomial $r(x) \in \mathbb{Z}[x]$ such that $K \cong \mathbb{Q}[x]/(r(x))$ is a number field containing the $k$-th roots of unity, and then choose the polynomial $t(x)$ mapping to $1 + \zeta_k$, where $\zeta_k$ is the primitive $k$-th root of unity in $K$. At this point, the two methods differ from each other:

Brezing-Weng method: if $K$ contains $\sqrt{-D}$, then since $r(x) = 0$ in $K$, we can factor the CM equation (4.3) in $K$ as follows:

$$\left(t(x) - 2 + y\sqrt{-D}\right)\left(t(x) - 2 - y\sqrt{-D}\right) \equiv 0 \mod r(x)$$

Since $t(x) \mapsto 1 + \zeta_k$, it is now easy to see that if we choose $y(x)$ to be a polynomial mapping to $(\zeta_k - 1)/\sqrt{-D}$ in $K$, then the CM equation is automatically satisfied for any $x$, i.e., $q(x) = \left(t(x)^2 + Dy(x)^2\right)/4$. If $q(x)$ represents primes and $r(x)$ has positive leading coefficient, then $(t, r, q)$ parameterizes a complete family of pairing-friendly elliptic curves.

**Algorithm 5:** Brezing and Weng Method

```
Input: $D, k \in \mathbb{Z}^+$, an irreducible polynomial $r(x)$.
Output: a prime $q(x)$, an elliptic curve $E$ over $\mathbb{F}_{q(x)}$ of embedding degree $k$ with
        respect to $r(x)$.
Step 1 : Let $K$ be the number field $\mathbb{Q}[x]/(r(x))$.
Step 2 : Let $\sqrt{-D}, \zeta_k \in K$ where $\zeta_k$ is the primitive $k$-th root of unity.
Step 3 : Choose $t(x)$ to be a polynomial such that $t(x) \mapsto 1 + \zeta_k$.
Step 4 : Choose $y(x)$ to be a polynomial such that $y(x) \mapsto (\zeta_k - 1)/\sqrt{-D}$.
Step 5 : Compute $q(x) = (t(x)^2 + Dy(x)^2)/4$ in $\mathbb{Q}[x]$.
Step 6 : If $q(x)$ is a prime integer and $r(x)$ is prime, use CM method to obtain an elliptic
curve $E$ over $\mathbb{F}_{q(x)}$ with trace $t(x)$, subgroup of order $r(x)$ and embedding degree $k$.
```

Scott-Barreto Method: if we do not know $K$ contains an element of the form $\sqrt{-D}$ for some small $D$, then we may apply this method. They choose $t(x)$ and $r(x)$ from above and search the cofactors $h(x)$ by computer so that the right-hand side of the CM equation (4.3) becomes

$$Dy^2 = (ax + b)g(x)^2.$$

In this equation, if $a = 0$, then we take $D = b$ and $y = g(x)$. If $a > 0$, we make the substitution $x \mapsto \frac{Dz^2-b}{a}$ for any $D$. If we set $y = zg(x)$, the CM equation is automatically satisfied for any $z$. If $q(x)$ represents primes and $r(x)$ has positive leading coefficient, $(t, r, q)$ parameterizes a complete family of pairing-friendly elliptic curves.

The success of both methods extremely depends on the choice of the number field $K$. The simple choice of $K$ is to be a cyclotomic field $\mathbb{Q}(\zeta_l)$ for some $l$ which is a multiple of $k$. Here, we also define $r(x)$ to be the $l$-th cyclotomic polynomial $\Phi_l(x)$. In the light of above, $K$ contains $k$-th roots of unity. It is easy to see that from the theory of cyclotomic fields that $K$ contains $\sqrt{-D}$ with $D \in \mathbb{Z}^+$ under the following conditions $\Big($see [76] for more details$\Big)$:

$$\begin{cases} \sqrt{-1} \in K, & \text{if } l \equiv 0 \pmod 4, \\ \sqrt{-2} \in K, & \text{if } l \equiv 0 \pmod 8, \\ \sqrt{(\frac{-1}{p})p} \in K, & \text{if } p \text{ is odd prime and } l \equiv 0 \pmod p. \end{cases}$$

Therefore, we can choose cyclotomic fields to construct pairing-friendly ordinary elliptic curves by using both methods. Freeman et al. [33] call these families *"cyclotomic families"*.

It is also possible to construct those curves by defining $K$ to be an extension of a cyclotomic field using a non-cyclotomic polynomial. The first technique is done by evaluating the cyclotomic polynomial $\Phi_l(x)$ at some polynomial $u(x)$. $\Phi_l(u(x))$, being irreducible, does not give any advantage since we just evaluate $t, r$ and $q$ at $u(x)$. However, if $\Phi_l(u(x))$ can be factorized as $r_1(x)r_2(x)$ with irreducible $r_1$, we may choose the number field $K = \mathbb{Q}[x]/(r_1(x))$ which contains the $l$-th roots of unity. Here, $u(x)$ maps to an $l$-th root of unity $\zeta_l$ in $K$. If $\sqrt{-D} \in \mathbb{Q}(\zeta_l)$, then $\sqrt{-D} \in K$ that enables us to use Brezing-Weng method, otherwise we apply Scott-Barreto method. The second technique, due to Kachisa, Schaefer and Scott [52], is done by finding a non-cyclotomic polynomial $r(x)$ such that $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_l)$. One can find such a polynomial $r(x)$ by computing the minimal polynomial of a randomly chosen element in $\mathbb{Q}(\zeta_l)$. For such $r(x)$, the polynomial $t(x)$ which maps to $1 + \zeta_l$ in $K$ can be found, and then we can proceed as in the Brezing-Weng method.

Due to the rareness of nontrivial factorization of $\Phi_l(u(x))$ for the first technique and the polynomial $q(x)$ usually not representing primes for the second technique, Freeman et al. [33] call these families *"sporadic families"*. Eventhough such families are rare, one may have better $\rho$-values than elliptic curves constructed using a cyclotomic families. The most important example was obtained by Barreto and Naehrig [7], who used the first technique to construct curves of prime order with embedding degree $k = 12$.

#### 4.6.4.1 Cyclotomic Families

Barreto, Lynn and Scott [5] gave the first construction of these families by applying Algorithm 5. They construct families by taking the polynomial $r(x)$ to be the $k$-th cyclotomic polynomial $\Phi_k(x)$ in order to define the number field $K$. They also choose $\zeta_k \mapsto x$ in $K$, where $\zeta_k$ is a primitive $k$-th root of unity, so $t(x) = 1 + \zeta_k = 1 + x$ and using the fact that if $3 \mid k$, then $\sqrt{-3} \in K$. Brezing and Weng [17] give a more general construction by taking the polynomial $r(x)$ to be the $l$-th cyclotomic polynomial $\Phi_l(x)$ for some $l$ which is a multiple of desired embedding degree $k$ and choosing various representations of $\zeta_k \in K$.

Freeman, Scott and Teske [33, Theorem 6.1] state that the $\rho$-value of this family is

$$\rho(t, r, q) = \frac{2 \max\{\deg t(x), \deg y(x)\}}{\deg r(x)}.$$

We now give an example of a curve construction for $k = 10$ that are proposed by Brezing and Weng [17]. They choose the number field $K = \mathbb{Q}[x]/(r(x))$ by taking the polynomial $r(x)$ to be 20-th cyclotomic polynomial $\Phi_{20}(x)$. Thus, the field $K$ contains $\zeta_{10}$ and $\sqrt{-1}$. They also choose $\sqrt{-1} \mapsto x^5$ and $\zeta_{10} \mapsto -x^6 + x^4 - x^2 + 1$ and using Algorithm 5, $t(x) = \zeta_{10} + 1$ and $y(x) = x^5 - x^3$ that give $q(x)$ as required. In other words,

$$\begin{aligned} r(x) &= \Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1 \\ t(x) &= -x^6 + x^4 - x^2 + 2 \\ q(x) &= \frac{1}{4}(x^{12} - x^{10} + x^8 - 5x^6 + 5x^4 - 4x^2 + 4). \end{aligned}$$

Since $q(x)$ is irreducible and $q(0) = 1$, it represents primes in the sense of Definition 4.4.3. Therefore, $(t, r, q)$ represents a complete family of pairing-friendly elliptic curves with embeddind degree $k = 10$ and discriminant $D = 1$. The $\rho$-value of this family is $3/2$ which is better than the second family given in Table 4.11.

In Table 4.11, Freeman, Scott and Teske [33] extended the construction given by Brezing and Weng for prime embedding degrees $k > 2$. They choose number field $K$ to be a cyclotomic field $\mathbb{Q}(\zeta_{4k})$ defining $r(x) = \Phi_{4k}(x)$, so it contains a fourth root of unity $\sqrt{-1}$ that provides to choose $D = 1$. For these families, by using Magma [15], they also show that $q(x)$ is irreducible for all odd $k < 1000$.

Table 4.11: Families with odd $k < 1000$ and $D = 1$

| $k$ | $t(x), r(x), q(x)$ | $\rho$ |
|---|---|---|
| $k$ | $t(x) = -x^2 + 1$<br>$r(x) = \Phi_{4k}(x)$<br>$q(x) = \frac{1}{4}\left(x^{2k+4} + 2x^{2k+2} + x^{2k} + x^4 - 2x^2 + 1\right)$ | $(k + 2)/\varphi(k)$ |
| $2k$ | $t(x) = x^2 + 1$<br>$r(x) = \Phi_{4k}(x)$<br>$q(x) = \frac{1}{4}\left(x^{2k+4} - 2x^{2k+2} + x^{2k} + x^4 + 2x^2 + 1\right)$ | $(k + 2)/\varphi(k)$ |
| $4k$ | $t(x) = x + 1$<br>$r(x) = \Phi_{4k}(x)$<br>$q(x) = \frac{1}{4}\left(x^{2k+2} - 2x^{2k+1} + x^{2k} + x^2 + 2x + 1\right)$ | $(k + 1)/\varphi(k)$ |

In Table 4.12, Freeman, Scott and Teske [33] extended the construction given by Murphy and Fitzpatrick [76] for the embedding degree $k = 24$ to all $k \in \mathbb{Z}^+$ such that $3 \mid k$. They choose $K$ to be a cyclotomic field containing an eight root of unity. Such fields contain $\sqrt{-2}$ that provides to choose $D = 2$. For these families, by using Magma [15], they also show that $q(x)$ represents primes for all odd $k < 1000$ and $3 \mid k$.

Table 4.12: Families with $k < 1000$, $3 \mid k$, $l = \mathrm{lcm}(8, k)$ and $D = 2$

| $k$ | $t(x), r(x), q(x)$ | $\rho$ |
|---|---|---|
| odd | $t(x) = x^{l/k} + 1$<br>$r(x) = \Phi_l(x)$<br>$q(x) = \frac{1}{8}\left(2(x^{l/k}+1)^2+(1-x^{l/k})^2(x^{5l/24}+x^{l/8}-x^{l/24})^2\right)$ | $(5k/6 + 4)/\varphi(k)$ |
| even | | $(5k/12 + 2)/\varphi(k)$ |

In Table 4.13, Freeman, Scott and Teske [33] extended the construction given by Brezing and Weng [17] and Barreto, Lynn and Scott [5] for certain values of $k$ to all $k \in \mathbb{Z}^+$ such that $18 \nmid k$. They choose $K$ to be a cyclotomic field containing a cube root of unity. Such fields contain $\sqrt{-3}$ that provides to choose $D = 3$. For these families, by using Magma [15], they also show that $q(x)$ is irreducible for all odd $k \leq 1000$, except $18 \nmid k$. In particular, we have $\rho \leq 2$ for all $k \leq 1000$ except for $k = 4$ and $\rho < 2$ for all $5 \leq k \leq 1000$ except for $k = 6$ and $k = 10$.

Table 4.13: Families with $k \leq 1000$, $18 \nmid k$, $l = \text{lcm}(6, k)$ and $D = 3$

| $k$ | $t(x), r(x), q(x)$ | $\rho$ |
|---|---|---|
| $k \equiv 1 \pmod 6$ | $t(x) = -x^{k+1} + x + 1$<br>$r(x) = \Phi_{6k}(x)$<br>$q(x) = \frac{1}{3}(x+1)^2(x^{2k} - x^k + 1) - x^{2k+1}$ | $(l/3 + 2)/\varphi(l)$ |
| $k \equiv 2 \pmod 6$ | $t(x) = x^{k/2+1} - x + 1$<br>$r(x) = \Phi_{3k}(x)$<br>$q(x) = \frac{1}{3}(x-1)^2(x^k - x^{k/2} + 1) + x^{k+1}$ | $(l/3 + 2)/\varphi(l)$ |
| $k \equiv 3 \pmod 6$ | $t(x) = -x^{k/3+1} + x + 1$<br>$r(x) = \Phi_{2k}(x)$<br>$q(x) = \frac{1}{3}(x+1)^2(x^{2k/3} - x^{k/3} + 1) - x^{2k/3+1}$ | $(l/3 + 2)/\varphi(l)$ |
| $k \equiv 4 \pmod 6$ | $t(x) = x^3 + 1$<br>$r(x) = \Phi_{3k}(x)$<br>$q(x) = \frac{1}{3}(x^3-1)^2(x^k - x^{k/2} + 1) + x^3$ | $(l/3 + 6)/\varphi(l)$ |
| $k \equiv 5 \pmod 6$ | $t(x) = x^{k+1} + 1$<br>$r(x) = \Phi_{6k}(x)$<br>$q(x) = \frac{1}{3}(x^2 - x + 1)(x^{2k} - x^k + 1) + x^{k+1}$ | $(l/3 + 2)/\varphi(l)$ |
| $k \equiv 0 \pmod 6$ | $t(x) = x + 1$<br>$r(x) = \Phi_k(x)$<br>$q(x) = \frac{1}{3}(x-1)^2(x^{k/3} - x^{k/6} + 1) + x$ | $(l/3 + 2)/\varphi(l)$ |

#### 4.6.4.2 Sporadic Families of Brezing-Weng Curves

In the construction of number field $K$, Brezing and Weng consider only the cyclotomic polynomials $r(x)$. However, in some cases, non-cyclotomic polynomials on top of cyclotomic extensions are more efficient.

The first technique is done by evaluating the cyclotomic polynomial $\Phi_l(x)$ at some polynomial $u(x)$. If $\Phi_l(u(x))$ is irreducible, this does not give any advantage since we will just evaluate $t, r$ and $q$ at $u(x)$. However, if $\Phi_l(u(x))$ can be factorized as $r_1(x)r_2(x)$ with irreducible $r_1$, we may choose the number field $K = \mathbb{Q}[x]/(r_1(x))$ containing the $l$-th roots of unity. Here, $u(x)$ maps to an $l$-th root of unity in $K$. If $\sqrt{-D} \in \mathbb{Q}(\zeta_l)$, then $\sqrt{-D} \in K$ that enables us to use Brezing-Weng method.

Galbraith, McKee and Valença [37] have analyzed the factorizations of $\Phi_l(u(x))$ for $l = 5, 8, 10$ and 12 whenever $u(x)$ is quadratic and $\Phi_l$ has degree 4. For $l = 12$, there are two such $u(x)$ that Barreto and Naehrig used one such factorization of $\Phi_{12}(u(x))$ for $u(x) = 6x^2$ to consruct pairing-friendly elliptic curves of prime order which we give below:

**Example 4.6.2 (Barreto-Naehrig Curves for $k = 12$)** *Barreto and Naehrig [7] constructed pairing-friendly elliptic curves of prime order for* $k = 12$. *They use the following factorization discovered by Galbraith et al. [37]*

$$\begin{aligned}\Phi_{12}(u(x)) &= r(x)r(-x)\\ &= (36x^4 + 36x^3 + 18x^2 + 6x + 1)(36x^4 - 36x^3 + 18x^2 - 6x + 1),\end{aligned}$$

*where* $u(x) = 6x^2$. *By taking* $r(x)$ *to be the first factor, they obtain* $t(x) = u(x) + 1$ *and* $q(x) = r(x) + t(x) - 1$. *If* $K = \mathbb{Q}[x]/(r(x))$, *then* $\zeta_{12} \mapsto 6x^2$, *and using* $\sqrt{-3} = 2\zeta_{12}^2 - 1$, *they compute* $y(x) = 6x^2 + 4x + 1$. *In other words, they obtain*

$$\begin{aligned}t(x) &= 6x^2 + 1\\ r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1\\ q(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1.\end{aligned}$$

*It follows from the polynomials that the CM equation becomes* $Dy^2 = 3(6x^2 + 4x + 1)^2$. *A suitable curve can be found by choosing a value* $x_0$ *such that* $q(x_0)$ *and* $r(x_0)$ *are both prime. Then* $(t, r, q)$ *parameterizes a complete family of curves with embedding degree* $k = 12$, *discriminant* $D = 3$, *and* $\rho$*-value* 1.

If we use the other quadratic $u(x) = 2x^2$ for factorizing $\Phi_{12}(u(x)) = r(x)r(-x)$, we obtain $r(x) = 4x^4 + 4x^3 + 2x^2 + 2x + 1$. We also have $\zeta_{12} \mapsto 2x^2$ and $\sqrt{-3} = 2\zeta_{12}^2 - 1$. Taking these into consideration, we construct a degree four polynomial $q(x)$ for embedding degree 12 which never takes integer values. Instead of this, one can consider $\zeta_4 \mapsto (2x^2)^3 \pmod{r(x)}$ to get a pairing-friendly curves of embedding degree $k = 4$ as following example shows:

**Example 4.6.3 ([33])** *Let*

$$\begin{aligned} t(x) &= -4x^3 \\ r(x) &= 4x^4 + 4x^3 + 2x^2 + 2x + 1 \\ q(x) &= \frac{1}{3}(16x^6 + 8x^4 + 4x^3 + 4x^2 + 4x + 1). \end{aligned}$$

*Then $(t, r, q)$ parameterizes a complete family of curves with embedding degree $k = 4$, discriminant $D = 3$, and $\rho$-value* $3/2$.

Another example to construct curves of embedding degree $k = 8$ is given by Tanaka and Nakamula [89] using the same idea.

**Example 4.6.4 ([89])** *Let*

$$\begin{aligned} t(x) &= -9x^3 - 3x^2 - 2x \\ r(x) &= 9x^4 + 12x^3 + 8x^2 + 4x + 1 \\ q(x) &= \frac{1}{4}(81x^6 + 54x^5 + 45x^4 + 12x^3 + 13x^2 + 6x + 1). \end{aligned}$$

*Then $(t, r, q)$ parameterizes a complete family of curves with embedding degree $k = 8$, discriminant $D = 1$, and $\rho$-value* $3/2$.

The second technique for constructing non-cyclotomic polynomials that define a cyclotomic field is given by Kachisa, Schaefer and Scott [52], following the work of Kachisa [51]. They first choose an element $\alpha \in \mathbb{Q}(\zeta_l)$, and then set $r(x)$ to be the minimal polynomial of $\alpha$. If $\alpha$ does not lie in a proper subfield of $\mathbb{Q}(\zeta_l)$, which occurs in most cases, we have $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_l)$. In this case, we proceed as in the Brezing-Weng method.

**Example 4.6.5 ([52])** *Let $k = l = 16$. Then by setting $\alpha = -2\zeta_{16}^5 + \zeta_{16} \in \mathbb{Q}(\zeta_{16})$, which has minimal polynomial $r(x)$, they get $K = \mathbb{Q}[x]/(r(x)) \cong \mathbb{Q}(\zeta_{16})$. When taking $\zeta_{16} \mapsto \frac{1}{35}(2x^5 +$*

$41x)$ *in* $K$ *and* $\sqrt{-1} \mapsto -\frac{1}{7}(x^4 + 24)$, *they obtain* $t(x)$ *and* $y(x) = -\frac{1}{35}(x^5 + 5x^4 + 38x + 120)$, *respectively. In other words, they obtain*

$$\begin{aligned} t(x) &= \frac{1}{35}(2x^5 + 41x + 35) \\ r(x) &= x^8 + 48x^4 + 625 \\ q(x) &= \frac{1}{980}(x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125). \end{aligned}$$

*The polynomial* $q(x)$ *is irreducible. When* $x \equiv \pm 25 \pmod{70}$, $t(x)$ *and* $q(x)$ *represent integers and* $q(x)$ *represents primes. Then* $(t, r, q)$ *parameterizes a complete family of curves with embedding degree* $k = 16$, *discriminant* $D = 1$, *and* $\rho$*-value* $5/4$.

Kachisa, Schaefer and Scott [52] also give a complete families of curves with embedding degrees $k = 18, 32, 36$ and $40$ corresponding to the $\rho$-values $4/3, 9/8, 7/6$ and $11/8$, respectively.

#### 4.6.4.3 Scott-Barreto Families

In the method of Scott and Barreto [82], we again take the number field $K$ as a cyclotomic field such that $\sqrt{-D} \notin K$ which is different from the previous one. If we choose any polynomial $t(x)$ and an irreducible polynomial $r(x)$ such that $r(x) \mid \Phi_k(t(x) - 1)$, then $\mathbb{Q}[x]/(r(x))$ defines a cyclotomic field. We then search the cofactor $h(x)$ by computer so that the right-hand side of the CM Eq. (4.3) either a perfect square or a linear factor times a perfect square, i.e.,

$$Dy^2 = (ax + b)g(x)^2.$$

When we find such an $h(x)$, we can set $x$ to be the linear function of $Dz^2$ that makes the right-hand side of the CM Eq. (4.3) $D$ times a square polynomial with respect to $z$.

We now give an example of the complete family of pairing-friendly curves that the proof can be found in [33].

**Example 4.6.6 ([33])** *Let* $k = 6$. *Let*

$$\begin{aligned} t(x) &= -4x^2 + 4x + 2 \\ r(x) &= 16x^4 - 32x^3 + 12x^2 + 4x + 1 \\ q(x) &= 4x^5 - 8x^4 + 3x^3 - 3x^2 + \frac{17}{4}x + 1. \end{aligned}$$

*Let D be a positive square-free integer and $D \nmid 2 \cdot 3 \cdot 5 \cdot 911$. Then $(t(Dz^2), r(Dz^2), q(Dz^2))$ parameterizes a complete family of curves with embedding degree $k = 6$, discriminant D, and $\rho$-value $5/4$.*

The following example is constructed by Koblitz and Menezes [59] that can be viewed as an example of Scott-Barreto families.

**Example 4.6.7 ([59])** *Let $l \in 2\mathbb{Z}$, and let D be a positive square-free integer. Let*

$$\begin{aligned} t(x) &= 2 \\ r(x) &= x \\ q(x) &= Dl^2x^2 + 1. \end{aligned}$$

*Then $(t, r, q)$ parameterizes a complete family of curves with embedding degree $k = 1$, discriminant D, and $\rho$-value 2.*

Koblitz and Menezes [59] discuss the family of curves of the form $y^2 = x^3 - dx$ with $D = 1$. They give two explicit elliptic curves; one of them is $y^2 = x^3 - x$ if $lx \equiv 0 \pmod 4$, the other one is $y^2 = x^3 - 4x$ if $lx \equiv 2 \pmod 4$. Both curves have the special property that $E(\mathbb{F}_q) \cong \mathbb{Z}/(lx)\mathbb{Z} \times \mathbb{Z}/(lx)\mathbb{Z}$. In addition to this, these curve have distortion maps. The advantage of this construction is to have a lot of choice for $x$ and $l$, which allows us to choose $r$ and $q$ to be a special primes such as Solinas.

In [56], we discuss the family of elliptic curves of the form $y^2 = x^3 - c$ with $D = 3$. In this work, we give an explicit curve $y^2 = x^3 - 1$ over $\mathbb{F}_q$ with $q = 27A^2 + 1$. We showed that this curve has embedding degree $k = 1$, This was done by computing the number of points $\#E(F_q)$ of the curve $y^2 = x^3 - c$, which we discuss now.

**Theorem 4.6.8** *Let $q \equiv 1 \ (mod\ 3)$ be a prime, $c \in \mathbb{F}_q^*$ and let $\chi_2$, $\chi_3$ and $\chi_6$ be quadratic, cubic and sextic characters on $\mathbb{F}_q^*$, respectively. Let E be the elliptic curve given by the equation*

$$y^2 = x^3 - c.$$

*over $\mathbb{F}_q$. Write $q = a^2 + b^2 - ab$, where $a, b$ are integers and $a + b \equiv 1 \ (mod\ 3)$, where $a \equiv 1 \ (mod\ 3)$, $b \equiv 0 \ (mod\ 3)$. Then,* *(i) If $q \equiv 1 \ (mod\ 4)$ and $\chi_3(2) = 1$, then*

$$\#E(\mathbb{F}_q) = \begin{cases} q+1-(2a-b), & if\ \chi_6(c) = 1 \\ q+1+(2a-b), & if\ \chi_3(c) = 1\ and\ \chi_6(c) \neq 1 \\ q+1+(a+b)\ or \\ q+1+(a-2b), & if\ \chi_2(c) = 1\ and\ \chi_6(c) \neq 1 \\ q+1-(a+b)\ or \\ q+1-(a-2b), & if\ \chi_2(c) \neq 1\ and\ \chi_3(c) \neq 1 \end{cases}$$

*(ii) If $q \equiv 1 \ (mod\ 4)$ and $\chi_3(2) \neq 1$, then*

$$\#E(\mathbb{F}_q) = \begin{cases} q+1+(a-2b)\ or \\ q+1+(a+b), & if\ \chi_6(c) = 1 \\ q+1-(a-2b)\ or \\ q+1-(a+b), & if\ \chi_3(c) = 1\ and\ \chi_6(c) \neq 1 \\ q+1-(2a-b)\ or \\ q+1+(a+b)\ or \\ q+1+(a-2b), & if\ \chi_2(c) = 1\ and\ \chi_6(c) \neq 1 \\ q+1+(2a-b)\ or \\ q+1-(a+b)\ or \\ q+1-(a-2b), & if\ \chi_2(c) \neq 1\ and\ \chi_3(c) \neq 1 \end{cases}$$

*(iii) If $q \not\equiv 1 \ (mod\ 4)$ and $\chi_3(2) = 1$, then*

$$\#E(\mathbb{F}_q) = \begin{cases} q+1+(2a-b), & if\ \chi_6(c) = 1 \\ q+1-(2a-b), & if\ \chi_3(c) = 1\ and\ \chi_6(c) \neq 1 \\ q+1-(a+b)\ or \\ q+1-(a-2b), & if\ \chi_2(c) = 1\ and\ \chi_6(c) \neq 1 \\ q+1+(a+b)\ or \\ q+1+(a-2b), & if\ \chi_2(c) \neq 1\ and\ \chi_3(c) \neq 1 \end{cases}$$

*(iv) If $q \not\equiv 1 \ (mod\ 4)$ and $\chi_3(2) \neq 1$, then*

$$\#E(\mathbb{F}_q) = \begin{cases} q+1-(a-2b)\ or \\ q+1-(a+b), & if\ \chi_6(c) = 1 \\ q+1+(a-2b)\ or \\ q+1+(a+b), & if\ \chi_3(c) = 1\ and\ \chi_6(c) \neq 1 \\ q+1+(2a-b)\ or \\ q+1-(a+b)\ or \\ q+1-(a-2b), & if\ \chi_2(c) = 1\ and\ \chi_6(c) \neq 1 \\ q+1-(2a-b)\ or \\ q+1+(a+b)\ or \\ q+1+(a-2b), & if\ \chi_2(c) \neq 1\ and\ \chi_3(c) \neq 1 \end{cases}$$

**Proof of Theorem 4.6.8.** Using the facts given in [92, Section 4.4], the number of points of the elliptic curve $y^2 = x^3 - c$ over $\mathbb{F}_q$ can be expressed in terms of the characters and Jacobi sums as follows:

$$\begin{aligned}
\#E(\mathbb{F}_q) &= \#\{x, y \in \mathbb{F}_q \mid y^2 = x^3 - c\} + \#\{\infty\} \\
&= \sum_{\substack{m,n \in \mathbb{F}_q \\ m = n - c}} \#\{y^2 = m\}.\#\{x^3 = n\} + 1 \\
&= \sum_{m \in F_q} \sum_{j=0}^{1} \chi_2(m)^j \sum_{l=0}^{2} \chi_3(m + c)^l + 1 \\
&= \sum_{j=0}^{1} \sum_{l=0}^{2} \sum_{m \in F_q} \chi_2(c)^j \chi_2(c^{-1}m)^j \chi_3(c)^l \chi_3(c^{-1}m + 1)^l + 1.
\end{aligned}$$

Using the change of variables $c^{-1}m = -t$ in the first summation on the right and by Proposition 2.4.3 and Proposition 2.4.8 in Section 2.4, we get

$$\begin{aligned}
\#E(\mathbb{F}_q) &= \sum_{j=0}^{1} \chi_2(-c)^j \sum_{l=0}^{2} \chi_3(c)^l \sum_{t \in F_q} \chi_2(t)^j \chi_3(1 - t)^l + 1 \\
&= \sum_{j=0}^{1} \chi_2(-c)^j \sum_{l=0}^{2} \chi_3(c)^l J(\chi_2^j, \chi_3^l) + 1 \\
&= \sum_{j=0}^{1} \chi_2(-c)^j [J(\chi_2^j, \chi_{triv}) + \chi_3(c) J(\chi_2^j, \chi_3) + \chi_3(c)^2 J(\chi_2^j, \chi_3^2)] + 1 \\
&= J(\chi_{triv}, \chi_{triv}) + \chi_3(c) J(\chi_{triv}, \chi_3) + \chi_3(c)^2 J(\chi_{triv}, \chi_3^2) \\
&+ \chi_2(-c)[J(\chi_2, \chi_{triv}) + \chi_3(c) J(\chi_2, \chi_3) + \chi_3(c)^2 J(\chi_2, \chi_3^2)] + 1 \\
&= q + 1 + \chi_2(-c)[\chi_3(c) J(\chi_2, \chi_3) + \chi_3(c)^2 J(\chi_2, \chi_3^2)] \\
&= q + 1 + \chi_2(-c)[\chi_3(4c) J(\chi_3, \chi_3) + \overline{\chi_3}(4c) J(\overline{\chi_3}, \overline{\chi_3})] \\
&= q + 1 - \alpha - \overline{\alpha}
\end{aligned}$$

where

$$\alpha = -\chi_2(-c)\chi_3(4c) J(\chi_3, \chi_3) \in \mathbb{Z}[\delta].$$

If we choose $\alpha = a + b\delta$, then $\overline{\alpha} = a + b\delta^2 = (a - b) - b\delta$. Therefore, $\mathrm{Tr}(\alpha) = 2a - b$. It follows from Proposition 2.4.7 that we obtain

$$\begin{aligned}
\mathrm{N}(\alpha) = a^2 + b^2 - ab &= \chi_2(-c)\overline{\chi_2(-c)}\chi_3(4c)\overline{\chi_3(4c)} J(\chi_3, \chi_3)\overline{J(\chi_3, \chi_3)} \\
&= \chi_2(-c)\chi_2(-c)^{-1}\chi_3(4c)\chi_3(4c)^{-1}|J(\chi_3, \chi_3)|^2 \\
&= q
\end{aligned}$$

By using Proposition 2.4.10, we can write

$$\begin{aligned}\alpha &= -\chi_2(-c)\chi_3(4c)J(\chi_3,\chi_3) \equiv \chi_2(-c)\chi_3(4c) \quad (mod\ 3)\\ &\equiv \chi_2(-1)\chi_3(2)^2\chi_2(c)\chi_3(c) \quad (mod\ 3).\end{aligned}$$

**Lemma 4.6.9** *Let $\alpha = x + y\delta \in \mathbb{Z}[\delta]$.*

*(1) If $\alpha \equiv 1\ (mod\ 3)$, then $x \equiv 1, y \equiv 0\ (mod\ 3)$ and $x + y \equiv 1\ (mod\ 3)$.*

*(2) If $\alpha \equiv -1\ (mod\ 3)$, then $x \equiv 2, y \equiv 0\ (mod\ 3)$ and $x + y \equiv 2\ (mod\ 3)$.*

*(3) If $\alpha \equiv \delta\ (mod\ 3)$, then $x \equiv 0, y \equiv 1\ (mod\ 3)$ and $x + y \equiv 1\ (mod\ 3)$.*

*(4) If $\alpha \equiv -\delta\ (mod\ 3)$, then $x \equiv 0, y \equiv 2\ (mod\ 3)$ and $x + y \equiv 2\ (mod\ 3)$.*

*(5) If $\alpha \equiv \delta^2\ (mod\ 3)$, then $x \equiv 2, y \equiv 2\ (mod\ 3)$ and $x + y \equiv 1\ (mod\ 3)$.*

*(6) If $\alpha \equiv -\delta^2\ (mod\ 3)$, then $x \equiv 1, y \equiv 1\ (mod\ 3)$ and $x + y \equiv 2\ (mod\ 3)$.*

**Proof.** Suppose $\alpha \equiv 1\ (mod\ 3)$, so $\alpha - 1 = 3(u + v\delta)$ for some $u$ and $v$ in $\mathbb{Z}$. We have

$$(x - 1) + y\delta = 3u + 3v\delta.$$

Therefore, $x \equiv 1\ (mod\ 3)$, $y \equiv 0\ (mod\ 3)$ and $x + y \equiv 1\ (mod\ 3)$. This proves (1). The proofs of (2) − (6) are similar. ■

If $q \equiv 1\ (mod\ 4)$ and $\chi_3(2) = 1$, then $\chi_2(-1)\chi_3(2)^2\chi_2(c)\chi_3(c) = 1\ (mod\ 3)$ when $\chi_6(c) = 1$. Hence, $\alpha \equiv 1\ (mod\ 3)$. Lemma 4.6.9 yields $\alpha = a + b\delta$ with $a \equiv 1, b \equiv 0\ (mod\ 3)$ and $a + b \equiv 1\ (mod\ 3)$. This proves part of part ($i$) of Theorem 4.6.8. The other parts are proved similarly. This completes the proof of Theorem 4.6.8. ■

Let $E$ be the elliptic curve given by the equation

$$y^2 = x^3 - 1 \tag{4.5}$$

over $\mathbb{F}_q$ with $q = 27A^2 + 1$ and $D = 3$. It follows from Proposition 2.4.9 and Theorem 4.6.8 (i) that $E$ has an embedding degree 1. For the efficient and secure implementation, prime $q$ should be choosen specifically so that the arithmetic on $\mathbb{F}_q$ is fast and the discrete logarithm problem (DLP) on $\mathbb{F}_q^*$ is secure. Taking these into accounts and following [59], we must choose $A = rh$ such that $r$ and $q = 27A^2 + 1$ are prime. In order to maximize efficiency, we look for the following:

- $r$ and $q$ should have the approximate bit lengths in Table 4.14 that corresponds to the desired security level.
- $r$ should be a Solinas prime, i.e, a sum or difference of a small number of powers of 2.
- $q$ should be a special prime that is proposed in [43].

Table 4.14: Minimum bit lengths of $r$ and $q$

| security level in bits | 80 | 128 | 192 | 256 |
|---|---|---|---|---|
| minimum bits of prime subgroup of order $n$ | 160 | 256 | 384 | 512 |
| minimum bits of the field $\mathbb{F}_p$ | 1024 | 3072 | 8192 | 15360 |

We now give examples considering [59, Section 4]. In our examples, the bit lengths of $r$ and $q$ are equal to or just a little bit more than the minimum values given in Table 4.14 for the corresponding security level. We produce these examples using Maple 12.

**Example 4.6.10** *For 128-bits of security, let r be the prime* $2^{258} - 2^{60} + 1$ *and let* $h = 2^{1424}$. *Then,* $q = 27 \cdot (r \cdot h)^2 + 1 = 27 \cdot (2^{3364} - 2^{3167} + 2^{3107} + 2^{2968} - 2^{2909} + 2^{2848}) + 1$ *is prime.*

**Example 4.6.11** *For 192-bits of security, let r be the prime* $2^{384} - 2^{218} + 1$ *and let* $h = 2^{3985}$. *Then,* $q = 27 \cdot (r \cdot h)^2 + 1 = 27 \cdot (2^{8738} - 2^{8573} + 2^{8406} + 2^{8355} - 2^{8189} + 2^{7970}) + 1$ *is prime.*

**Example 4.6.12** *For 256-bits of security, let r be the prime* $2^{514} - 2^{114} + 1$ *and let* $h = 2^{7482}$. *Then,* $q = 27 \cdot (r \cdot h)^2 + 1 = 27 \cdot (2^{15992} - 2^{15593} + 2^{15479} + 2^{15192} - 2^{15079} + 2^{14964}) + 1$ *is prime.*

#### 4.6.4.4 Variable Discriminants $D$ in Cyclotomic Families

Freeman, Scott and Teske [33] introduced a new method to construct a family of curves with variable CM discriminant $D$. The examples given by Brezing and Weng method and some other methods assumed that the CM discriminant D is fixed. Most examples given by Brezing and Weng [17] and all of those given by Barreto, Lynn and Scott [5] require that $D = 3$. Although, elliptic curves with $D = 3$ are convenient for cryptographic applications, they have the unusual property of having an automorphism group of order 6 that is believed to help a future discrete logarithm attack [57]. From this point of view, cryptographers would like to have families of elliptic curves with variable $D$.

**Theorem 4.6.13 ([33])** *Suppose that $(t, r, q)$ parameterizes a complete potential family of elliptic curves with embedding degree $k$ and discriminant $D$. Let $y(x) \in \mathbb{Q}[x]$ such that $Dy(x)^2 = 4q(x) - t(x)^2$. Let $t$, $r$ and $q$ be even polynomials and $y$ be an odd polynomial. Define $t^{'}, r^{'}, q^{'}$ and $y^{'}$ to be polynomials such that*

$$t(x) = t^{'}(x^2), \quad r(x) = r^{'}(x^2), \quad q(x) = q^{'}(x^2), \quad y(x) = x \cdot y^{'}(x^2),$$

*Let $a$ be a positive integer satisfying the followings:*

*(1) $aD$ is square-free,*

*(2) $r^{'}(ax^2)$ is irreducible,*

*(3) $y^{'}(ax^2)$ is an integer for some integer $x$.*

*Then the triple $\left(t^{'}(ax^2), r^{'}(ax^2), q^{'}(ax^2)\right)$ parameterizes a complete potential family of elliptic curves with embedding degree $k$, discriminant $aD$ and $\rho$-value equal to $\rho(t, r, q)$.*

The difficult part in obtaining a family of curves is in this method to show that $q^{'}(ax^2)$ represents primes. In particular, Freeman, Scott and Teske [33] claim that they have often found that $\gcd(\{q(x) \mid x, q(x) \in \mathbb{Z}\}) > 1$. Their first application of Theorem 4.6.13 is to construct the following two examples which improve the first two examples in Table 4.11, respectively.

**Example 4.6.14** *Let $k$ be odd. Let*

$$\begin{aligned} t(x) &= 1 + (-1)^{(k+1)/2} x^{k+1} \\ r(x) &= \Phi_{4k}(x) \\ q(x) &= \frac{1}{4}\left(x^{2k+2} + x^{2k} + 4(-1)^{(k+1)/2} x^{k+1} + x^2 + 1\right). \end{aligned}$$

*Then $(t, r, q)$ parameterizes a complete potential family of pairing-friendly curves with embedding degree $k$, discriminant $D = 1$, and $\rho$-value $(k + 1)/\varphi(k)$.*

**Example 4.6.15** *Let $k$ be odd. Let*

$$\begin{aligned} t(x) &= 1 - (-1)^{(k+1)/2} x^{k+1} \\ r(x) &= \Phi_{4k}(x) \\ q(x) &= \frac{1}{4}\left(x^{2k+2} + x^{2k} - 4(-1)^{(k+1)/2} x^{k+1} + x^2 + 1\right). \end{aligned}$$

*Then $(t, r, q)$ parameterizes a complete potential family of pairing-friendly curves with embedding degree $2k$, discriminant $D = 1$, and $\rho$-value $(k+1)/\varphi(k)$.*

They apply Theorem 4.6.13 to both examples to obtain a complete family of curves with variable $D$. In Example 4.6.14, the polynomial $r(x)$ is equal to $\Phi_{4k}(x) = \Phi_k(-x^2)$ for odd $k$. Using the fact given in [33] that

(i) $\Phi_k(ax^2)$ is irreducible when $k \in \mathbb{Z}^+$ and $a$ is a square-free integer with $a \nmid k$,

(ii) $r(x) = r^{'}(ax^2) = \Phi_k(-ax^2)$ is irreducible for any square-free $a$ such that $a \nmid k$,

(iii) $y(x) = y^{'}(ax^2)$ is an integer for some $x$,

(iv) Using the substitution $x^2 \mapsto ax^2$, the new $q(x)$ is obtained by

$$q_a(x) = \frac{1}{4}\Big(a^{k+1}x^{2k+2} + a^k x^{2k} + 4(-a)^{(k+1)/2}x^{k+1} + ax^2 + 1\Big).$$

It follows from above that one obtains a potential family of elliptic curves with discriminant $D = a$ for any positive square-free integer $a$ such that $a \nmid k$. In order to obtain a family of such curves, it remains only to check that $q_a(x)$ represents primes or not. This was done in [33] by using the following facts:

(i) $f(ax^2)$ is irreducible when $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ is irreducible and $a$ is a square-free integer such that $a \nmid a_0 a_d \text{disc } f(x)$,

(ii) $\text{disc } f(x^2) = (\text{disc } f(x))^2$.

They conclude that if $k \equiv 3 \pmod 4$ and $k < 1000$, then for any square-free integer $a$ with $a \nmid \text{disc } q(x)$, the polynomial $q_a(x)$ is irreducible. According to the authors, $q^{'}(ax^2)$ represent primes for $k \equiv 3 \pmod 4$, $a \equiv 3 \pmod 4$ for square-free $a$. This certainly would give us a family of pairing-friendly elliptic curves with discriminant $a$.

Freeman, Scott and Teske [33] applied Theorem 4.6.13 to produce more examples incuding Example 4.6.15.

### 4.6.5 The Dupont-Enge-Morain Method

Dupont, Enge and Morain [26] propose a new method to construct pairing-friendly ordinary elliptic curves with arbitrary embedding degree as in the Cocks and Pinch method. In this new method, their approach is to compute $t$ and $r$ simultaneously using resultants, but the Cocks and Pinch method first fixes an $r$ and then computes the parameters $t$ and $q$ which satisfy CM equation.

**Algorithm 6:** The Dupont-Enge-Morain Method to construct a curve for arbitrary $k$

```
**Input**: $k \in \mathbb{Z}^+$, square-free positive integer $D$
**Output**: a prime $q$, an elliptic curve $E$ over $\mathbb{F}_q$ of embedding degree $k$ with respect to $r$.
Step 1 : Compute the resultant $R_k(a)$ =$\mathrm{Res}_x(\Phi_k(x-1), (x-2)^2 + a) \in \mathbb{Z}[a]$.
Step 2 : Choose $a \in \mathbb{Z}$ such that $R_k(a)$ is prime and set $r = R_k(a)$.
Step 3 : Choose $y \in \mathbb{Z}$ such that $a = Dy^2$ and test $R_k(Dy^2)$ is prime.
Step 4 : Compute $g(x) = \gcd(\Phi_k(x-1), (x-2)^2 + Dy^2) \in \mathbb{F}_r[x]$.
Step 5 : Let $t^{'}$ be a root of $g(x) \in \mathbb{F}_r[x]$.
Step 6 : Let $t \in \mathbb{Z}$ such that $t \equiv t^{'} \pmod{r}$ and $q = (t^2 + Dy^2)/4$.
Step 7 : If $q$ is a prime integer and $a = Dy^2$ with $D < 10^{12}$, use CM method to obtain
an elliptic curve $E$ over $\mathbb{F}_q$ with trace $t$ and embedding degree $k$.
```

The main idea behind on the Dupont-Enge-Morain method is to use the following well-known property of resultants: if $f$ and $g$ be polynomials over a field $K$, then $\mathrm{Res}(f, g) = 0$ if and ony if $f$ and $g$ have a common root in $\overline{K}$. For a more detailed background of resultants, one can refer to [62, 65].

When computing $\mathrm{Res}(\Phi_k(x-1), (x-2)^2 + a)$, we obtain a single variable polynomial $R_k$with respect to $a$ of degree $\varphi(k)$. If we choose $a = Dy^2$ with $y \in \mathbb{Z}$ such that $r = R_k(Dy^2)$ is an odd prime, then $r \equiv 1 \pmod{k}$ (see [33, Lemma 4.5]). This property implies that $\Phi_k(x)$ splits into distinct linear factors in $\mathbb{F}_r[x]$. Since $g(x) \mid \Phi_k(x-1)$, the polynomial $g(x)$ has a root $t^{'} \in \mathbb{F}_r$. Let $t \in \mathbb{Z}$ be the lift of $t^{'} \in \mathbb{F}_r$. Then the computed values of $t$ and $r$ satisfies $r \mid \Phi_k(t-1)$ and $r \mid Dy^2 + (t-2)^2$. If $q = (t^2 + Dy^2)/4$ is prime integer, CM equation holds. By using the CM method, we obtain an elliptic curve $E$ with $q + 1 - t \equiv 0 \pmod{r}$. As in the Cocks-Pinch method, in general $q \approx r^2$. Therefore, pairing-friendly ordinary elliptic curves consructed using by this method have $\rho \approx 2$.

The Cocks-Pinch method and the Dupont-Enge-Morain method are both efficient for constructing curves with arbitrary embedding degree. The only significant difference between these two methods is that while one can choose the subgroup size $r$ arbitrarily in the Cocks-Pinch method, $r$ is a value of the polynomial $R_k(a)$ of degree $\phi(k)$ in the Dupont-Enge-Morain method. Thus, the possible subgroup more restricted for the Dupont-Enge-Morain method. In the light of above, Freeman et al. [33] recommend using the Cocks-Pinch method for cryptographic applications.

### 4.6.6 Extension of the Dupont-Enge-Morain Method

In [29], Drylo extended the Dupont-Enge-Morain Method by choosing $Dy^2 = f(x)$ with $f(x) = g(x)h(x)^2$, where $g(x), h(x) \in \mathbb{Q}[x]$ and $\deg g(x) \leq 2$. Let $r(x) \in \mathbb{Q}[x]$ be an irreducible factor of $R_k(f(x))$, which can be efficiently found using Berlekamp's algorithm. Let $K = \mathbb{Q}[x]/(r(x))$. Then we assume that $t^{'}(x) = \gcd(\Phi_k(x-1), (x-2)^2 + f(x))$, which is an element of $K$. Let $t(x)$ be the lift of $t^{'}(x)$ in $\mathbb{Q}[x]$ with $\deg(t(x)) < \deg(r(x))$. Let $q(x) = (t(x)^2 + f(x))/4$. Then the triple $(t, r, q)$ parameterizes a potential family of curves with embedding degree $k$.

# CHAPTER 5

# EFFICIENT EXPONENTIATION IN PAIRING-BASED CRYPTOGRAPHY

One of the important components in pairing computations is the final exponentiation. In this chapter, we show how this computation can be done by using the linear recurrence relations. Moreover, we list all those work studied in the literature so far.

## 5.1 The Final Exponentiation

The final exponentiation $(q^k - 1)/r$ needed by the Tate pairing (and its derivatives) has been efficiently computed for supersingular elliptic curves with embedding degree $k = 2, 4, 6$ in [4]. Later, this is carried out in [67] as we explain now : Assume that the Tate pairing (and its derivatives) value obtained by the Miller's algorithm is $a$. We will now exponentiate $a$ by $\frac{q^k-1}{r}$. To do this, we first write

$$q^k - 1 = \prod_{d|k} \Phi_d(q).$$

Since $k$ is the embedding degree, $r$ has to divide cyclotomic polynomial $\Phi_k(q)$ (not to smaller degree of it). We compute $b = a^c$, where

$$c = \prod_{d|k, d<k} \Phi_d(q).$$

Since $\frac{\Phi_k(q)}{r}$ is an integer, we obtain the output $b^{\Phi_k(q)/r}$ using a standard exponentiation algorithm [24, Chapter 9]. We note that this method is faster than the previous approach given for supersingular elliptic curves in [4].

**Example 5.1.1** *Let $\mathbb{F}_{q^2} = \mathbb{F}(\alpha) \cong \mathbb{F}_q[x]/ < x^2 - \delta >$. Then we can write an element $a \in \mathbb{F}_{q^2}$ in the form $a = u + \alpha v$, where $u, v \in \mathbb{F}_q$ and $\alpha^2 = \delta$. It is clear that $q^2 - 1 = \Phi_2(q)\Phi_1(q)$ and*

$r \mid \Phi_2(q) = q + 1$. *We have*

$$b^{(q+1)/r} = (a^{q-1})^{(q+1)/r} = \Big(\frac{u - \alpha v}{u + \alpha v}\Big)^{(q+1)/r}.$$

*Since*

$$b = \frac{u - \alpha v}{u + \alpha v} = \frac{u^2 - v^2}{u^2 + v^2} - \alpha \frac{2uv}{u^2 + v^2},$$

*the field element b becomes "unitary" (see [46, 81]). In other words, $b\overline{b} = 1$, where $\overline{b}$ is the conjugate of b in $\mathbb{F}_{q^2}$. Then, we compute $b^{(q+1)/r}$ using a standard exponentiation algorithm to obtain $a^{(q^2-1)/r}$. As a result, we have effectively halved the size of the final powering using this approach.*

**Remark 5.1.2** *For $k = 2d$, the final exponent can be written by*

$$\frac{q^k - 1}{r} = (q^d - 1)\frac{(q^d + 1)}{\Phi_d(q)}\frac{\Phi_d(q)}{r}.$$

*After raising to the power of $q^d - 1$, the field element becomes unitary. This property gives us two important implications:*

*(i) squaring of unitary elements is significantly cheaper than squaring of non-unitary elements.*

*(ii) for unitary elements, any future inversions can be implemented by simple conjugation.*

## 5.2 Compression in Finite Fields

We first describe a method to represent elements of cyclotomic subgroups in $\mathbb{F}_{q^k}$ with fewer bits. This is so called compressed form of those elements in $\mathbb{F}_{q^k}$. A cyclotomic subgroup $G_{r,q,k}$ in $\mathbb{F}_{q^k}$ is defined to be a subgroup of prime order $r$ with $r \mid \Phi_k(q)$ and $r \nmid k$. We now show that the relatioships between coefficients of minimal polynomials for the elements of a cyclotomic subgroup $G_{r,q,k}$ and the corresponding linear recurrence relation. For more details, we refer the reader to look at [16].

Let $\alpha$ be an element of a cyclotomic subgroup $G_{r,q,k}$, where $k \geq 2$. Let

$$f_\alpha(x) = x^n - a_1 x^{n-1} + \cdots + (-1)^{n-1} a_{n-1} x + (-1)^n a_n$$

be the minimal polynomial of $\alpha$ over $\mathbb{F}_{q^d}$ for some $d$ dividing $k$ with $n = k/d > 1$. Then $a_n = 1$. It is clear that for $1 \le i \le n$, $a_i$'s are the elementary symmetric functions in variables $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$, namely

$$a_1 = \sum_{i=0}^{n-1} \alpha^{q^i},\ a_2 = \sum_{i<j} \alpha^{q^i+q^j},\ \ldots, a_n = \prod_{i=0}^{n-1} \alpha^{q^i}.$$

The polynomial $f_\alpha(x)$ allows us to introduce the $n$-th order linear recurrence relation $\{s_i\}$ which is defined by

$$s_t = a_1 s_{t-1} - a_2 s_{t-2} + \cdots - (-1)^n s_{t-n}, \qquad t \ge n.$$

The sequence $\{s_i\}$ of elements in $\mathbb{F}_{q^d}$ with fixed initial conditions

$$s_i = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha^i) = \alpha^i + \alpha^{iq} + \ldots + \alpha^{iq^{n-1}}$$

for $i = 0, \cdots, n-1$ is called the $n$-th order characteristic sequence over $\mathbb{F}_{q^d}$ generated by $\alpha$. For any integer $m$, the minimal polynomial of $\alpha^m$ is

$$f_{\alpha^m}(x) = x^n - a_{1,m}x^{n-1} + \cdots + (-1)^{n-1}a_{n-1,m}x + (-1)^n,$$

whose roots are $\alpha^{mq^i}$ for $i = 0, \cdots, n-1$. Hence, we may represent $\alpha^m$ (and its conjugates) by the set $\{a_{1,m}, a_{2,m}, \cdots, a_{n-1,m}\}$, where the elements are written by

$$a_{i,m} = \sum_{0 \le j_1 \le \cdots \le j_i \le n-1} \alpha^{m(q^{j_1}+q^{j_2}+\cdots+q^{j_i})}.$$

It follows from the equation above $a_{i,m} = a_{n-i,-m}$. The Newton's Formula [65] tells us that for any $i \in \{1, \cdots, n-1\}$, we can efficiently obtain $\{a_{1,m}, a_{2,m}, \cdots, a_{i,m}\}$ from the set $\{s_m, s_{2m}, \cdots, s_{im}\}$ and vice-versa using the following equalities:

$$\begin{aligned} s_{im} &= a_{1,m}s_{(i-1)m} - a_{2,m}s_{(i-2)m} + \cdots - (-1)^i i a_{i,m} \\ a_{i,m} &= i^{-1}\big((-1)^{i+1}s_{im} + \cdots + a_{i-1,m}s_m\big) \end{aligned}$$

In this section, our goal is to obtain shorter representation of $\alpha^m$. Thus, we now descibe two significant cases:

(1) If $k = 2l$ is even, then $\alpha \in \mathbb{F}_{q^{2l}}$ has order dividing $q^l + 1$. This implies that $\alpha^{mq^l} = \alpha^{-m}$.

Therefore, for $i = 1, \cdots, n-1$, we have

$$\begin{aligned} a_{n-i,m} &= a_{i,-m} \\ &= \sum_{0 \le j_1 \le \cdots \le j_i \le n-1} \alpha^{-m(q^{j_1}+q^{j_2}+\cdots+q^{j_i})} \\ &= \sum_{0 \le j_1 \le \cdots \le j_i \le n-1} \alpha^{mq^l(q^{j_1}+q^{j_2}+\cdots+q^{j_i})} \\ &= a_{i,m}^{q^l} \end{aligned}$$

Hence, we may represent $\alpha^m$ (and its conjugates) by the set $\{a_{1,m}, \cdots, a_{(n-1)/2,m}\}$.

(2) If $k = 2l$ with $d \mid l$, then we have $a_{n-i,m} = a_{i,m}^{q^l}$ for $i = 1, \cdots, n-1$ from the previous result. Since $d \mid l$, i.e., $n = k/d$ is even, we obtain $a_{i,m}^{q^l} = a_{i,m}$ and the result follows. Hence, we may represent $\alpha^m$ (and its conjugates) by the set $\{a_{1,m}, \cdots, a_{n/2,m}\}$.

**Lemma 5.2.1** *[16] Let $k = de$, with $e > 1$. Then for any element $\alpha$ of a cyclotomic subgroup $G_{r,q,k}$ and for any integer $m$, $\alpha^m$ can be represented using the following number of elements in $\mathbb{F}_{q^d}$:*

$$\begin{cases} e-1, & \text{if } de \text{ is odd} \\ \frac{e-1}{2}, & \text{if } d \text{ is even and } e \text{ is odd} \\ \frac{e}{2}, & \text{if } e \text{ is even} \end{cases}$$

### 5.2.1 Compression Factor 2

Let $\alpha$ be any element of $G_{r,q,2}$ in $\mathbb{F}_{q^2}^*$ and let

$$f_\alpha(x) = x^2 - a_1 x + 1$$

be the minimal polynomial of $\alpha$ over $\mathbb{F}_q$. The polynomial $f_\alpha(x)$ allows us to introduce the 2nd order linear recurrence relation $\{s_i\}$ which is defined by

$$s_t = a_1 s_{t-1} - s_{t-2}, \quad t \ge 2.$$

For any integer $m$, the minimal polynomial of $\alpha^m$ over $\mathbb{F}_q$ is

$$f_{\alpha^m}(x) = x^2 - a_{1,m} x + 1,$$

where $a_{1,m} = s_m = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha^m) = \alpha^m + \alpha^{mq}$. The sequence $\{a_{1,m}\}$ which is so called Lucas sequence is defined by the following recurrence relations:

$$a_{1,0} = 2, \; a_{1,1} = a_1, \; a_{1,u+1} = a_1 a_{1,u} - a_{1,u-1}.$$

In [88], Smith and Skinner showed that the elements of $G_{r,q,2}$ in $\mathbb{F}_{q^2}^*$ could be identified by $\{a_{1,m}\}$ only $1/2$ as many as in the ordinary case. More precisely, the elements of $G_{r,q,2}$ can be uniquely determined by their traces over $\mathbb{F}_q$. This construction yields a compression factor 2.

The Lucas sequence $\{a_{1,m}\}$ can be efficiently computed in Algorithm 1 depending on the relations

$$\begin{aligned} a_{1,u+v} &= a_{1,u}a_{1,v} - a_{1,u-v} \\ a_{1,2u} &= a_{1,u}^2 - 2 \end{aligned}$$

for $u, v \in \mathbb{Z}$.

**Algorithm 7:** Compute Lucas Sequence

```
Input: $a_1 \in \mathbb{F}_q$ and $m = \sum_{j=0}^{t} m_j 2^j \in \mathbb{Z}^+$ with $m_t = 1$
Output: $(a_{1,m}, a_{1,m+1})$
Step 1 : $(a_{1,y}, a_{1,y+1}) \leftarrow (2, a_1)$
Step 2 : for $j \leftarrow t$ to 0 do
Step 3 :     if $m_j = 1$ then
Step 4 :         $a_{1,y} \leftarrow a_{1,y}a_{1,y+1} - a_1, \quad a_{1,y+1} \leftarrow a_{1,y+1}^2 - 2$
Step 5 :     else
Step 6 :         $a_{1,y} \leftarrow a_{1,y}^2 - 2, \quad a_{1,y+1} \leftarrow a_{1,y}a_{1,y+1} - a_1$
Step 7 :     end if
Step 8 : end for
Step 9 : return $(a_{1,y}, a_{1,y+1})$
```

Algorithm 7 is left-to-right scanning one. It was developed right-to-left scanning algorithm in [95], which requires more temporary memories.

### 5.2.2 Compression Factor 3/2

Let $\alpha$ be any element of $G_{r,q,3}$ in $\mathbb{F}_{q^3}^*$ and let

$$f_\alpha(x) = x^3 - a_1x^2 + a_2x - 1$$

be the minimal polynomial of $\alpha$ over $\mathbb{F}_q$. For any integer $m$, the minimal polynomial of $\alpha^m$ over $\mathbb{F}_q$ is

$$f_{\alpha^m}(x) = x^3 - a_{1,m}x^2 + a_{1,-m}x - 1$$

where $a_{1,m} = s_m = \mathrm{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha^m) = \alpha^m + \alpha^{mq} + \alpha^{mq^2}$.

In [40], Gong and Harn showed that the elements of $G_{r,q,3}$ in $\mathbb{F}^*_{q^3}$ could be identified by $\{a_{1,m}, a_{1,-m}\}$ with a compression factor 3/2. They also obtained an efficient exponentiation algoritm for the compressed form of those elements depending on the relations

$$\begin{aligned} a_{1,u+v} &= a_{1,u}a_{1,v} - a_{1,u-v}a_{1,-v} + a_{1,u-2v} \\ a_{1,2u} &= a^2_{1,u} - 2a_{1,-u}. \end{aligned}$$

for $u, v \in \mathbb{Z}$.

### 5.2.3 Compression Factor 3

Let $\alpha$ be any element of $G_{r,q,6}$ in $\mathbb{F}^*_{q^6}$ and let

$$f_\alpha(x) = x^3 - a_1x^2 + a_2x - 1$$

be the minimal polynomial of $\alpha$ over $\mathbb{F}_{q^2}$. It follows from the fact that the conjugates over $\mathbb{F}_{q^2}$ of $\alpha \in \mathbb{F}_{q^6}$ are $\alpha$, $\alpha^{q^2}$ and $\alpha^{q^4}$. Therefore, we obtain $a_1 = \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\alpha) = \alpha^m + \alpha^{mq^2} + \alpha^{mq^4}$. The conjugates of $\alpha \in G_{r,q,6}$ are also $\alpha$, $\alpha^{q-1}$ and $\alpha^{-q}$ since $q^2 \equiv q - 1 \pmod{(q^2 - q + 1)}$ and $q^4 \equiv -q \pmod{(q^2 - q + 1)}$. This implies that $a_2 = \alpha\alpha^{q^2} + \alpha\alpha^{q^4} + \alpha^{q^2}\alpha^{q^4} = a_1^q$. Therefore, the minimal polynomial of $\alpha$ over $\mathbb{F}_{q^2}$ can be rewritten by

$$f_\alpha(x) = x^3 - a_1x^2 + a_1^qx - 1.$$

For any integer $m$, the conjugates of $\alpha^m$ are the roots of the polynomial

$$f_{\alpha^m}(x) = x^3 - a_{1,m}x^2 + a^q_{1,m}x - 1$$

over $\mathbb{F}_{q^2}$. The latter polynomial is fully determined by $\{a_{1,m}\}$.

Lenstra and Verheul introduced XTR [64] cryptosystem. Using the above procedure, they showed that the elements of $G_{r,q,6}$ in $\mathbb{F}^*_{q^6}$ could be identified by $\{a_{1,m}\}$ over $\mathbb{F}_{q^2}$ with a compression factor 3.

The XTR exponentiation $\{a_{1,m}\}$ can be efficiently computed in Algorithm 8 (see [64, Algorithm 2.3.7]) using the following relations

$$\begin{aligned} a_{1,u+v} &= a_{1,u}a_{1,v} - a^q_{1,v}a_{1,u-v} + a_{1,u-2v} \\ a_{1,2u} &= a^2_{1,u} - 2a^q_{1,u}. \end{aligned}$$

for $u, v \in \mathbb{Z}$.

**Algorithm 8:** Compute XTR exponentiation

```
Input: $a_1 \in \mathbb{F}_{q^2}$ and $m = \sum_{j=0}^{t} m_j 2^j \in \mathbb{Z}^+$ with $m_t = 1$
Output: $(a_{1,2m}, a_{1,2m+1}, a_{1,2m+2})$
 Step 1 : $(a_{1,y-1}, a_{1,y}, a_{1,y+1}) \leftarrow (3, a_1, a_1^2 - 2a_1^q)$
 Step 2 : for $j \leftarrow t$ to 0 do
 Step 3 :     if $m_j = 1$ then
 Step 4 :         $a_{1,y-1} \leftarrow a_{1,y}^2 - 2a_{1,y}^q$,
 Step 5 :         $a_{1,y} \leftarrow a_{1,y+1}a_{1,y} - a_{1,y}^q a_1 + a_{1,y-1}^q$
 Step 6 :         $a_{1,y+1} \leftarrow a_{1,y+1}^2 - 2a_{1,y+1}^q$
 Step 7 :     else
 Step 8 :         $a_{1,y-1} \leftarrow a_{1,y-1}^2 - 2a_{1,y-1}^q$
 Step 9 :         $a_{1,y} \leftarrow a_{1,y-1}a_{1,y} - a_{1,y}^q a_1^q + a_{1,y+1}^q$
Step 10 :         $a_{1,y+1} \leftarrow a_{1,y}^2 - 2a_{1,y}^q$
Step 11 :     end if
Step 12 : end for
Step 13 : return $(a_{1,y-1}, a_{1,y}, a_{1,y+1})$
```

### 5.2.4 Compression Factor 5/2

Giuliani and Gong [38] considered that the elements of $G_{r,q,10}$ in $\mathbb{F}_{q^{10}}^*$ and showed that those elements could be identified by $\{a_{1,m}, a_{2,m}\}$ over $\mathbb{F}_{q^2}$ with a compression factor 5/2. They obtained an algoritm to exponentiate the compressed form of those elements in [38] and also proposed more efficient algorithm in [39].

### 5.2.5 Compression Factor 4 and 6

Let $q = 3^t$ for any odd integer $t$, i.e., $t = 2l + 1$. Then $\sqrt{3q} = 3^{l+1}$ is an integer and

$$q^2 - q + 1 = (q + \sqrt{3q} + 1)(q - \sqrt{3q} + 1).$$

Shirase et al. introduced improved version of XTR [85]. They considered that the elements of $G_{r,q,6}$ with $r \mid q - \sqrt{3q} + 1$ in $\mathbb{F}_{q^6}^*$ and showed that those elements can be uniquely represented $\{a_{1,m}\}$ (up to conjugation over $\mathbb{F}_q$) with a compression factor 6. They also obtained an exponentiation algorithm of those elements by using an analogue of XTR algorithm and the following equalities

$$\begin{aligned} a_{1,m} &= \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_q}(\alpha^m) = \alpha^m + \alpha^{mq} + \cdots + \alpha^{mq^5} \\ b_{1,m} &= \mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(\alpha^m) = \alpha^m + \alpha^{mq^2} + \alpha^{mq^4} \end{aligned}$$

where $a_{1,m} = b_{1,m} + b_{1,m}^q$. If $a_{1,m}$ is given, then $b_{1,m}$ can be obtained efficiently using the following polynomial

$$x^2 - a_{1,m}x + a_{1,m}^{\sqrt{3q}}.$$

In fact, $b_{1,m}$ and $b_{1,m}^q$ are the roots of the above polynomial.

Later, using the same trick in [85], Karabina [53] showed that the elements of $G_{r,q,6}$ with $r \mid q \mp \sqrt{3q} + 1$ in $\mathbb{F}_{q^6}^*$, where $q = 3^{2l+1}$ can be uniquely represented by their traces over $\mathbb{F}_q$ with a compression factor 6. He presented six exponentiation algorithms and compared them. The first works directly using the following polynomial

$$\begin{aligned} f(x) &= x^6 - a_{1,m}x^5 + (a_{1,m}^t + a_{1,m})x^4 \\ &- (a_{1,m}^2 + a_{1,m}^t + 2)x^3 + (a_{1,m}^t + a_{1,m})x^2 \\ &- a_{1,m}x + 1, \end{aligned}$$

where $t = \mp 3^{l+1}$ is the trace of the Frobenius. This algorithm is 59% faster than the algorithm proposed by Shirase et al. in [85].

He also achieved compression factor 4 for the subgroups $G_{r,q,6}$ with $r \mid q \mp \sqrt{2q} + 1$ in $\mathbb{F}_{q^4}^*$, where $q = 2^t$ for some odd $t$, i.e. $t = 2l + 1$. He presented five exponentiation algorithms for compression factor 4 and compared them. His first algoritm works directly with the polynomial

$$f(x) = x^4 + a_{1,m}x^3 + a_{1,m}^t x^2 + a_{1,m}x + 1,$$

where $t = \mp 2^{l+1}$.

### 5.2.6 Compression Factor 7/3

We consider the elements of $G_{r,q,14}$ in $\mathbb{F}_{q^{14}}^*$ and showed that any positive power $m$ of those elements could be identified by $\{a_{1,m}, a_{2,m}, a_{3,m}\}$ over $\mathbb{F}_{q^2}$ with a compression factor 7/3. Namely, let $\alpha$ be any element of $G_{r,q,14}$ in $\mathbb{F}^*_{q^{14}}$ and let

$$f_\alpha(x) = x^7 - a_1x^6 + a_2x^5 - a_3x^4 + a_3^p x^3 - a_2^p x^2 + a_1^p x - 1$$

be the minimal polynomial of $\alpha$ over $\mathbb{F}_{q^2}$. For any integer $m$, the minimal polynomial of $\alpha^m$ over $\mathbb{F}_{q^2}$ is

$$f_{\alpha^m}(x) = x^7 - a_{1,m}x^6 + a_{2,m}x^5 - a_{3,m}x^4 + a^p_{3,m}x^3 - a^p_{2,m}x^2 + a^p_{1,m}x - 1,$$

where

$$a_{1,m} = s_m = \mathrm{Tr}_{\mathbb{F}_{q^{14}}/\mathbb{F}_{q^2}}(\alpha^m) = \sum_{i=0}^{6} \alpha^{mq^{2i}},$$

$$a_{2,m} = \mathrm{Tr}_{\mathbb{F}_{q^{14}}/\mathbb{F}_{q^2}}\left(\alpha^{m(q^2+1)} + \alpha^{m(q^4+1)} + \alpha^{m(q^6+1)}\right) = \sum_{0 \le i < j \le 6} \alpha^{mq^{2i}+mq^{2j}},$$

and

$$\begin{aligned} a_{3,m} &= \mathrm{Tr}_{\mathbb{F}_{q^{14}}/\mathbb{F}_{q^2}}\left(\alpha^{m(q^4+q^2+1)} + \alpha^{m(q^6+q^2+1)} + \alpha^{m(q^8+q^2+1)} + \alpha^{m(q^8+q^4+1)} + \alpha^{m(q^{10}+q^2+1)}\right) \\ &= \sum_{0 \le i < j < k \le 6} \alpha^{mq^{2i}+mq^{2j}+mq^{2k}}. \end{aligned}$$

We have the following recurrence relations related to the sequences $\{a_{1,m}\}$, $\{a_{2,m}\}$ and $\{a_{3,m}\}$, but we could not find yet any efficient polynomial time algorithm to compute the m-th term of these sequences.

**Lemma 5.2.2** *For all integers u and v, we have the following:*

*(1)* $a_{1,2u} = a^2_{1,u} - 2a_{2,u}$

*(2)* $a_{2,2u} = a^2_{2,u} + 2a^p_{3,u} - 2a_{1,u}a_{3,u}$

*(3)* $a_{3,2u} = a^2_{3,u} - 2a^p_{1,u} + 2a_{1,u}a^p_{2,u} - 2a_{2,u}a^p_{3,u}$

*(4)* $a_{1,3u} = a^3_{1,u} - 3a_{1,u}a_{2,u} + 3a_{3,u}$

*(5)* $a_{1,u+v} = a_{1,u}a_{1,v} - a_{1,u-v}a_{2,v} + a_{1,u-2v}a_{3,v} - a_{1,u-3v}a^p_{3,v} + a_{1,u-4v}a^p_{2,v} - a_{1,u-5v}a^p_{1,v} + a_{1,u-6v}$

*(6)* $a_{2,u+v} = a_{2,u}a_{2,v} - a^p_{3,v}a_{2,u-v} - a^p_{1,v}a_{2,u-2v} + (a_{1,u-2v}a_{1,u-v} - a_{1,2u-3v})a^p_{2,v} + a_{1,u-v}a_{1,u-4v} + a_{1,u-2v}a_{1,u-3v} - 2a_{1,2u-5v} + (a_{1,2u-4v} - a_{1,u-v}a_{1,u-3v})a^p_{1,u} - a_{1,u}a_{1,v}a_{1,u+v} + a_{1,v}a_{1,2u+v} + a_{1,u}a_{1,u+2v} - 2a_{1,2u+2v} + a^2_{1,u+v}$

*(7)* $a_{3,u+v} = a_{3,u}a_{3,v} - a_{1,v}^{p}a_{3,u-v} + a_{1,u-2v}a_{2,u-v} + (2a_{1,u+v} - a_{1,u}a_{1,v})a_{2,u+v} - a_{1,u+v}a_{2,u}a_{2,v} + (a_{1,v}a_{1,u+2v} - a_{1,u+3v})a_{2,u} + (a_{1,u}a_{1,2u+v} - a_{1,3u+v})a_{2,v} - a_{1,u-v}a_{1,2u-3v} + a_{1,3u-4v} + 2a_{1,u} \cdot a_{1,2u+3v} + 2a_{1,v}a_{1,3u+2v} + 2(a_{1,u+v} - a_{1,u}a_{1,v})a_{1,2u+2v} + a_{1,u}a_{1,v}a_{1,u+v}^{2} - a_{1,u}a_{1,u+v}a_{1,u+2v} - a_{1,v}a_{1,u+v}a_{1,2u+v} + a_{1,u+2v}a_{1,2u+v} - 3a_{1,3u+3v} - a_{1,u+v}^{3}$

**Proof.**

$$\begin{aligned}
a_{1,u}^2 &= (\sum_{i=0}^{6} \alpha^{uq^i})^2 = (\sum_{i=0}^{6} \alpha^{2uq^i}) + 2(\sum_{0\le i<j\le 6} \alpha^{u(q^i+q^j)}) = a_{1,2u} + 2a_{2,u} \\
a_{2,u}^2 &= (\sum_{0\le i<j\le 6} \alpha^{u(q^i+q^j)})^2 \\
&= a_{2,2u} + 2\Big(\sum_{0\le i<j<k\le 6} (\alpha^{u(2q^i+q^j+q^k)} + \alpha^{u(q^i+2q^j+q^k)} + \alpha^{u(q^i+q^j+2q^k)}) \\
&+ 3\sum_{0\le i<j<k<l\le 6} (\alpha^{u(q^i+q^j+q^k+q^l)})\Big) \\
&= a_{2,2u} + 2\Big(\sum_{i=0}^{6} \alpha^{uq^i} \sum_{0\le i<j<k\le 6} \alpha^{u(q^i+q^j+q^k)} - \sum_{0\le i<j<k<l\le 6} \alpha^{u(q^i+q^j+q^k+q^l)}\Big) \\
&= a_{2,2u} + 2a_{1,u}a_{3,u} - 2a_{3,u}^{p},
\end{aligned}$$

which prove (1) and (2). The rest can be similarly proven. ■

## 5.3 Compressed Pairings

The compressed reduced Tate pairing (and its derivatives) $\epsilon(P, Q)$ is defined by $\mathrm{Tr}(\tau(P, Q)) = \mathrm{Tr}(f_{r,P}(D)^{(q^k-1)/r})$ in [82]. This corresponds to the first elementary symmetric function of the minimal polynomial for any elements of the cyclotomic subgroup $G_{r,q,k}$ in $\mathbb{F}_{q^k}^{*}$. It is convenient to extend the definition $\epsilon(P, Q)$ to $\mathrm{Tr}(f_{r,P}(D)^{i(q^k-1)/r})$ for $i = 1, \cdots k-1$ by considering Lemma 5.2.1, which provides an advantage to compute pairing values represented more than one element. This is done by using the Newton's Identity.

Some pairing-based cryptographic protocols have been used to take a profit from compressed pairings. The classical example is the BLS short signature scheme that was given in Section 3.3.2. We will now give the modified signature scheme for compressed pairings as follows [82]: Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order $n$. Let $P \in E(\mathbb{F}_{q^k})$ such that $G_1 =< P >$ and let $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map. Let $H : \{0, 1\}^* \rightarrow G_1^*$ be a cryptographic hash function.

- **Key Generation :** Pick a random $c \in \mathbb{Z}_n^*$ and compute $cP$. The secret key is $c$ and the public key $\xi$ is the $x$ coordinate of the point $cP$.

- **Sign :** Given a secret key $c$ and a message $m \in \{0,1\}^*$, compute $S = cH(m) \in E(\mathbb{F}_{q^k})$. The signature $\sigma$ is the $x$ coordinate of the point $S = cH(m)$, which is an element of $\mathbb{F}_{q^k}$.

- **Verify :** Given a public key $\xi$, a message $m$ and a signature $\sigma$, verify $\tau(P, \pm S) = \tau(\pm cP, H(m))$ or $\tau(P, \pm S) = \tau(\pm cP, H(m))^{-1}$.

In order to verify BLS signature scheme, one can simply check whether $\mathrm{Tr}(\tau(P, \pm S)) = \mathrm{Tr}(\tau(\pm cP, H(m)))$ using the property that any pairing value is unitary.

# CHAPTER 6

# CONCLUSION

It is well-known that there are bilinear, non-degenerate maps such as Weil, Tate, Eta and Ate. One of the most important thing is to use these pairings in cryptography. For this, we have to choose those elliptic curves so called pairing-friendly, where the cryptographic protocols are secure.

In this thesis, we studied these curves from the theoritical and implementation point of view. In particular, we focused our attention to the elliptic curves of the form $y^2 = x^3 - c$ over $\mathbb{F}_q$ and computed the number of points of these elliptic curves. Furthermore, we showed that the elliptic curve $y^2 = x^3 - 1$ over $\mathbb{F}_q$ for the primes $q$ of the form $27A^2 + 1$ has an embedding degree $k = 1$ and we gave examples of those primes $q$ providing the security equivalent to 128-, 192-, or 256-bit AES keys.

From the implementation point of view, the final exponentiation is the most important part for pairing computation. In this respect, we showed explicitly how the final exponentiation is related to the linear recurrence relations, and studied the work done in the literature. Moreover, for the embedding degree $k = 7d$ with even $d$, we developed several recurrence relations; however, we could not get any polynomial time algoritm to compute the $m$-th term of them. This is left as an open problem for which we hope to study in the future.

# REFERENCES

[1] A.O.L. Atkin, F. Morain, Elliptic curves and primality proving. Mathematics of Computation **61**, 29-68 (1993)

[2] R. Balasubramanian, N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. J. Cryptol. **11**(2), 141-145, (1998)

[3] P.S.L.M. Barreto, S. Galbraith, C. O hEigeartaigh, M. Scott, Efficient pairing computation on supersingular abelian varieties. Des. Codes Cryptogr. **42**(3), 239-271 (2007)

[4] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, M. Scott, Efficient algorithms for pairing-based cryptosystems, Advances in Cryptology - Crypto 2002. Lecture Notes in Computer Science, vol. 2442 (Springer-Verlag, 2002), pp. 354-368

[5] P.S.L.M. Barreto, B. Lynn, M. Scott, Constructing elliptic curves with prescribed embedding degrees, Security in Communication Networks - SCN 2002. Lecture Notes in Computer Science, vol. 2576 (Springer, Berlin, 2002), pp. 263-273

[6] P.S.L.M. Barreto, B. Lynn, M. Scott, On the selection of pairing-friendly groups, Selected Areas in Cryptography - SAC 2003. Lecture Notes in Computer Science, vol. 3006 (Springer-Verlag, 2004), pp. 17-25

[7] P.S.L.M. Barreto, M. Naehrig, Pairing-friendly elliptic curves of prime order, Selected Areas in Cryptography - SAC 2005. Lecture Notes in Computer Science, vol. 3897 (Springer, Berlin, 2006), pp. 319-331

[8] P.T. Bateman, R.A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers. Math. of Comp. **16**, 363-367 (1962)

[9] N. Benger, M. Charlemagne, D. Freeman, On the security of pairing-friendly abelian varieties over non-prime fields, Pairing-Based Cryptography - Pairing 2009. Lecture Notes in Computer Science, vol. 5671 (Springer, Berlin, 2009), pp. 52-65

[10] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, (Wiley-Intersci-ence, New York, 1998)

[11] I.F. Blake, G. Seroussi, N.P. Smart, Elliptic curves in cryptography (London Mathematical Society Lecture Note Series 265, Cambridge Univ. Press, 1999)

[12] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing. SIAM J. of Computing, **32**(3), 586-615 (2003). An extended abstract of this paper appears in Advances in Cryptology - Crypto 2001. Lecture Notes in Computer Science, vol. 2139 (Springer-Verlag, 2001), pp. 213-229

[13] D. Boneh, B. Lynn, H. Shacham, Short Signature from the Weil Pairing, Advances in Cryptology - Asiacrypt 2001. Lecture Notes in Computer Science, vol. 2248 (Springer-Verlag, 2001), pp. 514-532

[14] D. Boneh, K. Rubin, A. Silverberg, Finding composite order ordinary elliptic curves using the Cocks-Pinch method. J. Number Theory, 2010, to appear.

[15] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: The user language. J. Symb. Comput. **24**(3-4), 235-265 (1997)

[16] W. Bosma, J. Hutton, E. Verheul, Looking beyond XTR, Advances in Cryptology - Asiacrypt 2002. Lecture Notes in Computer Science, vol. 2501 (Springer-Verlag, 2002), pp. 46-63

[17] F. Brezing, A. Weng, Elliptic curves suitable for pairing based cryptography. Des. Codes Cryptogr. **37**, 133-141 (2005)

[18] A. Brouwer, R. Pellikaan, E. Verheul, Doing more with fewer bits, Advances in Cryptology - Asiacrypt 1999. Lecture Notes in Computer Science, vol. 1716 (Springer-Verlag, 1999), pp. 321-332

[19] R. Bröker, Constructing elliptic curves of prescribed order. Ph.D. thesis, Dept. of Mathematics, Leiden University, 2006.

[20] L. Charlap, R. Coley, An Elementary Introduction to Elliptic Curves II. CCR Expository Report 34, 1990. Available at: http://www.idaccr.org/reports/er34.ps

[21] Y. Choie, E. Jeong, Isomorphism classes of elliptic and hyperelliptic curves over finite fields of $\mathbb{F}_{(2g+1)^n}$. Finite Fields Appl. **10**(4), 583-614 (2004)

[22] C. Cocks, R.G.E. Pinch, Identity-based cryptosystems based on the Weil pairing. Unpublished manuscript, 2001

[23] H. Cohen, A course in computational algebraic number theory (volume 138 of Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1993)

[24] H. Cohen, G. Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, (Discrete Math. Appl., Chapman & Hall/CRC, 2006)

[25] D. Coppersmith, Fast evaluation of logarithms in fields of characteristic two. IEEE Trans. Inf. Theory **30**, 587-594 (1984)

[26] R. Dupont, A. Enge, F. Morain, Building curves with arbitrary small MOV degree over finite prime fields. J. Cryptol. **18**, 79-89 (2005)

[27] R. Dutta, R. Barua, P. Sarkar, Pairing-Based Cryptographic Protocols : A Survey. Preprint available at: http://eprint.iacr.org/2004/064.pdf

[28] I.M. Duursma, H.-S. Lee, Tate Pairing Implementation for Hyperelliptic Curves $y^2 = x^p - x + d$, Advances in Cryptology - Asiacrypt 2003. Lecture Notes in Computer Science, vol. 2894 (Springer-Verlag, 2003), pp. 111-123

[29] R. Drylo, On constructing optimal families of pairing-friendly elliptic curves. Institute of Mathematics of Polish Academy of Sciences Preprint 2010/715

[30] A. Enge, Elliptic Curves and Their Applications to Cryptography: An Introduction, (Kluwer Academic Publishers, Dordrecht, 1999)

[31] D. Freeman, Constructing pairing-friendly elliptic curves with embedding degree 10, Algorithmic Number Theory Symposium - ANTS VII. Lecture Notes in Computer Science, vol. 4076 (Springer, Berlin, 2006), pp. 452-465

[32] D. Freeman, Constructing pairing-friendly genus 2 curves with ordinary Jacobians, Pairing-Based Cryptography - Pairing 2007. Lecture Notes in Computer Science, vol. 4575 (Springer, Berlin, 2007), pp. 152-176

[33] D. Freeman, M. Scott, E. Teske, A Taxonomy of Pairing-Friendly Elliptic Curves. J. Cryptol. **23**, 224-280 (2010)

[34] D. Freeman, P. Stevenhagen, M. Streng, Abelian varieties with prescribed embedding degree, Algorithmic Number Theory Symposium - ANTS VIII. Lecture Notes in Computer Science, vol. 5011 (Springer, Berlin, 2008), pp. 60-73

[35] G. Frey, H. Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comput. **62**, 865-874 (1994)

[36] S. Galbraith, K. Harrison, D. Soldera, Implementing the Tate pairing, Algorithmic Number Theory Symposium - ANTS V. Lecture Notes in Computer Science, vol. 2369 (Springer, Berlin, 2002), pp. 324-337

[37] S. Galbraith, J. McKee, P. Valença, Ordinary abelian varieties having small embedding degree. Finite Fields Appl. **13**, 800-814 (2007)

[38] K. Giuliani, G. Gong, Efficient Key Agreement and Signature Schemes Using Compact Representations in $GF(p^{10})$. Proceedings of IEEE International Symposium on Information Theory - ISIT 2004 (Chicago, IL, 2004), pp. 13-13

[39] K. Giuliani, G. Gong, A New Algorithm to Compute Remote Terms in Special Types of Characteristic Sequences, Sequences and Their Applications - SETA 2006. Lecture Notes in Computer Science, vol. 4086 (Springer, Berlin, 2006), pp. 237-247

[40] G. Gong, L. Harn, Public-key cryptosystems based on cubic finite field extensions. IEEE Trans. Inf. Theory **45**(7), 2601-2605 (1999)

[41] R. Granger, F. Hess, R. Oyono, N. Theriault, F. Vercauteren. Ate Pairing on Hyperelliptic Curves, Advances in Cryptology - Eurocrypt 2007. Lecture Notes in Computer Science, vol. 4515 (Springer-Verlag, 2007), pp. 430-447

[42] G.H. Hardy, J.E. Littlewood, Some problems of partitio numerorum; III: On the expression of a number as a sum of primes. Acta Math. vol **44**, 1-70 (1923)

[43] T. Hasegawa, J. Nakajima, M. Matsui, A Small and Software Implemantation of Elliptic Curve Cryptosystems over GF($p$) on a 16-Bit Microcomputer. IEICE Trans. Fundamentals, vol. **E82-A**(1), 98-106 (1999)

[44] F. Hess, N. Smart, F. Vercauteren, The eta pairing revisited. IEEE Trans. Inf. Theory, **52**(10), 4595-4602 (2006)

[45] L. Hitt, On the minimal embedding field, Pairing-Based Cryptography - Pairing 2007. Lecture Notes in Computer Science, vol. 4575 (Springer, Berlin, 2007), pp. 294-301

[46] K. Hoffman, R. Kunze, Linear Algebra, 3rd ed. (Prentice Hall, New Jersey, USA, 1971)

[47] IEEE P1363/D13, Standard Specifications for Public-Key Cryptography, 1999

[48] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory (2nd ed., Springer-Verlag, New York, 1990)

[49] A. Joux, A One Round Protocol for Tripartite Diffie-Hellman, Algorithmic Number Theory Symposium - ANTS IV. Lecture Notes in Computer Science, vol. 1838 (Springer-Verlag, 2000), pp. 385-394

[50] M. Joye, J.-J. Quisquater, Efficient computation of full Lucas sequences. Electronics Letters **32**(6), 537-538 (1996)

[51] E.J. Kachisa, Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. M.Sc. Thesis, Mzuzu University, 2007

[52] E.J. Kachisa, E.F. Schaefer, M. Scott, Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field, Pairing-Based Cryptography - Pairing 2008. Lecture Notes in Computer Science, vol. 5209 (Springer, Berlin, 2008), pp. 126-135

[53] K. Karabina, On prime-order elliptic curves with embedding degrees 3, 4 and 6. M.Sc. Thesis, Univ. of Waterloo, Dept. of Combinatorics and Optimization, 2006

[54] K. Karabina, Factor-4 and 6 compression of cyclotomic subgroups of $\mathbb{F}^*_{2^{4m}}$ and $\mathbb{F}^*_{3^{6m}}$. J. Math Cryptol. **4**, 1-42 (2010)

[55] K. Karabina, E. Teske, On prime-order elliptic curves with embedding degrees 3, 4 and 6, Algorithmic Number Theory Symposium - ANTS VIII. Lecture Notes in Computer Science, vol. 5011 (Springer, Berlin, 2008), pp. 102-117

[56] B.B. Kırlar, On the elliptic curves $y^2 = x^3 - c$ with embedding degree one, J. Comput. Appl. Math., 2010 (In press)

[57] N. Koblitz, Good and bad uses of elliptic curves in cryptography. Mosc. Math. J. **2**(4), 693-715 (2002)

[58] N. Koblitz, A security weakness in composite-order pairing-based protocols with imbedding degree $k > 2$. Cryptology ePrint Archive Report 2010/227. Preprint available at http://eprint.iacr.org/2010/227

[59] N. Koblitz, A. Menezes, Pairing-based cryptography at high security levels, Cryptography and Coding - 10th IMA International Conference. Lecture Notes in Computer Science, vol. 3796 (Springer, Berlin, 2005), pp. 13-36

[60] E. Konstantinou, A. Kontogeorgis, Y.C. Stamatiou, C. Zaroliagis, On the Efficient Generation of Prime-Order Elliptic Curves. J. Cryptol. **23**(3), 477-503 (2010)

[61] S. Lang, Elliptic Functions (Springer, Berlin, 1987)

[62] S. Lang, Algebra, revised 3rd ed. (Springer, Berlin, 2002)

[63] E. Lee, H.-S. Lee, C.-M. Park, Efficient and generalized pairing computation on abelian varieties. IEEE Trans. Inf. Theory, **55**(4), 1793-1803 (2009)

[64] A. Lenstra, E. Verheul, The XTR public key system, Advances in Cryptology - Crypto 2000. Lecture Notes in Computer Science, vol. 1880 (Springer-Verlag, 2000), pp. 1-19

[65] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed. (Cambridge University Press, UK, 1997)

[66] F. Luca, I. Shparlinski, Elliptic curves with low embedding degree. J. Cryptol. **19**, 553-562 (2006)

[67] B. Lynn, On the Implementation of Pairing-Based Cryptography. Ph.D. Thesis, Dept. of Computer Science, Stanford University, 2007

[68] S. Matsuda, N. Kanayama, F. Hess, E. Okamoto, Optimised versions of the Ate and twisted Ate pairings. Cryptography and Coding - 11th IMA International Conference. Lecture Notes in Computer Science, vol. 4887 (Springer-Verlag, 2007), pp. 302-312

[69] K. Matthews, The Diophantine equation $x^2 - Dy^2 = N, D > 0$. Expo. Math. **18**, 323-331 (2000)

[70] A. Menezes, T. Okamoto, S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory **39**, 1639-1646 (1993)

[71] A. Menezes, S. Vanstone, Isomorphism classes of elliptic curves over finite fields of characteristic 2. Util. Math. **38**, 135-153 (1990)

[72] V. Miller, Short programs for functions on curves, IBM, Thomas J. Watson Research Center 1986. Available at http://crypto.stanford.edu/miller/

[73] V. Miller, The Weil pairing, and its efficient calculation. J. Cryptol. **17**(4), 235-262 (2004)

[74] A. Miyaji, M. Nakabayashi, S. Takano, New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fundam. **E84-A**(5), 1234-1243 (2001)

[75] F. Morain, Classes d'isomorphismes des courbes elliptiques supersingulières en caractéristique $\geq 3$. Utilitas Math. **52**, 241-253 (1997)

[76] A. Murphy, N. Fitzpatrick, Elliptic curves for pairing applications. Preprint available at: http://eprint.iacr.org/2005/302

[77] M. Naehrig, P.S.L.M. Barreto, P. Schwabe, On compressible pairings and their computation, Progress in Cryptology - Africacrypt 2008. Lecture Notes in Computer Science, vol. 5023 (Springer, Berlin, 2008), pp. 371-388

[78] D. Page, N. Smart, F. Vercauteren, A comparison of MNT curves and supersingular curves. Applicable Algebra in Engineering, Communication and Computing **17**, 379-392 (2006)

[79] J. Robertson, Solving the generalized Pell equation $x^2 - Dy^2 = N$. Unpublished manuscript, 2004

[80] E. Savas, T.A. Schmidt, C.K. Koc, Generating Elliptic Curves of Prime Order, Cryptographic Hardware and Embedded Systems - CHES 2001. Lecture Notes in Computer Science, vol. 2162 (Springer-Verlag, 2001), pp. 145-161

[81] M. Scott, P.S.L.M. Barreto, Compressed pairings, Advances in Cryptology - Crypto 2004. Lecture Notes in Computer Science, vol. 3152 (Springer-Verlag, 2004), pp. 140-156

[82] M. Scott, P.S.L.M. Barreto, Generating more MNT elliptic curves. Des. Codes Cryptogr. **38**, 209-217 (2006)

[83] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology - Crypto 1984. Lecture Notes in Computer Science, vol. 196 (Springer-Verlag, 1985), pp. 47-53

[84] D. Shanks, On the conjecture of Hardy and Littlewood concerning the number of primes of the form $n^2 + a$. Math. of Comp. **14**, 321-332 (1960)

[85] M. Shirase, D. Han, Y. Hibin, H. Kim, T. Takagi, A more compact representation of XTR cryptosystem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E91-A**(10), 2843-2850 (2008)

[86] J. Silverman, The Arithmetic of Elliptic Curves (Springer, Berlin, 1986)

[87] P.J. Smith, M.J.J. Lennon, LUC: A new public key system. In E.G. Douglas, editor, Proceedings of the Ninth IFIP International Symposium on Computer Security (Elsevier Science Publications, 1993), pp. 97-111

[88] P. Smith, C. Skinner, A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms, Advances in Cryptology - Asiacrypt 1994. Lecture Notes in Computer Science, vol. 917 (Springer-Verlag, 1994), pp. 357-364

[89] S. Tanaka, K. Nakamula, Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials, Pairing-Based Cryptography - Pairing 2008. Lecture Notes in Computer Science, vol. 5209 (Springer, Berlin, 2008), pp. 136-145

[90] F. Vercauteren, Optimal pairings. IEEE Trans. Inf. Theory , 2009, to appear.

[91] E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. J. Cryptol. **17**, 277-296 (2004)

[92] L.C. Washington, Elliptic Curves: Number Theory and Cryptography, (Chapman-Hall, New York, 2003)

[93] W. Waterhouse, Abelian varieties over finite fields. Ann. Sci. Ecole Norm. Sup. (IV) **2**, 521-560 (1969)

[94] H. C. Williams, An $m^3$ public-key encryption scheme, Advances in Cryptology - Crypto 1985. Lecture Notes in Computer Science, vol. 218 (Springer-Verlag, New York, 1986), pp. 358-368.

[95] S.-M. Yen, C.-S. Laih, Fast algorithms for LUC digital signature computation. IEE Proc. Comput. Tech. **142**(2), 165-169 (1995)

[96] C. Zhao, F. Zhang, J. Huang, A note on the ate pairing. Int. J. Inf. Security **7**(6), 379-382 (2008)

# VITA

## PERSONAL INFORMATION

**Surname, Name:** Kırlar, Barış Bülent

**Date and Place of Birth:** May 19, 1978 - Konya

**Marital Status:** Married with one daughter

**email:** kirlar@metu.edu.tr

## EDUCATION

| Degree | Institution | Year of Graduation |
|---|---|---|
| MS | METU, Department of Mathematics | 2005 |
| BS | Ankara University, Department of Mathematics | 2001 |

## WORK EXPERIENCE

| Year | Place | Enrollment |
|---|---|---|
| 2004 - Present | METU, Institute of Applied Mathematics | Research Assistant |
| 2002 - 2004 | METU, Department of Mathematics | Research Assistant |

## PUBLICATIONS

### A. Papers published in International Journals:

**A1.** B. B. Kırlar, On the elliptic curves $y^2 = x^3 - c$ with embedding degree one, Journal of Computational and Applied Mathematics, 2010 (In press)

**A2.** S. Akleylek, B. B. Kırlar, Ö. Sever, Z. Yüce, A New Short Signature Scheme with Random Oracle from Bilinear Pairings, Journal of Telecommunications and Information Technology, 2010 (In press)

### B. Papers published in International Conference Proceedings:

**B1.** S. Akleylek, B. B. Kırlar, Ö. Sever, Z. Yüce, Short Signature Scheme from Bilinear Pairings, Information Assurance and Cyber Defense (IST-091), Antalya, Turkey, 2010.

**B2.** B. B. Kırlar, Efficient Exponentiation in Pairing-Based Cryptography, Proceedings of 4th International Information Security and Cryptology Confence (ISCTURKEY 2010), Ankara, 2010, pp. 145-149

**C. Presentations in International Conferences:**

**C1.** S. Akleylek, B. B. Kırlar, Ö. Sever, Z. Yüce, Short Signature Scheme from Bilinear Pairings, Western European Workshop on Research in Cryptology (WEWoRC 2009), Austria, 2009

**C2.** B. B. Kırlar, On the elliptic curves $y^2 = x^3 - c$ with embedding degree one, 14th International Congress on Computational and Applied Mathematics (ICCAM 2009), Antalya, 2009

**D. Papers published in National Conference Proceedings:**

**D1.** S. Akleylek, B. B. Kırlar, Ö. Sever, Z. Yüce, Arithmetic on Pairing-Friendly Fields, Proceedings of Information Security and Cryptography Conference (ISCTURKEY 2008), Ankara, 2008, pp. 115-120

**D2.** S. Akleylek, B. B. Kırlar, Ö. Sever, Z. Yüce, Pairing-Based Cryptography: A Survey, Proceedings of Information Security and Cryptography Conference, (ISCTURKEY 2008), Ankara, 2008, pp. 121-125.