Constructing Suitable Ordinary Pairing-friendly Curves

a case of elliptic curves and genus two hyperelliptic curves.

Ezekiel Justin Kachisa

BEd(Sc). M.Sc.

A Dissertation submitted in fulfilment of the

requirements for the award of

Doctor of Philosophy (Ph.D)

to the

Dublin City University

Faculty of Engineering and Computing

School of Computing

Supervisor: Professor Michael Scott

September, 2011

Declaration

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of Doctor of Philosophy is entirely my own work, that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed: Ezekiel Justin Kachisa

Student ID: 57107645

Date: September, 2011

Acknowledgements

First and foremost I owe this to Jesus Christ. Thank You Lord!.

My special thanks goes to my supervisor, Professor Micheal Scott for his dynamic guidance, encouragement and patience than was perhaps warranted by my seeming determination to finishing this work. He is a wonderful and hard-working mentor from whom I have learned a great deal.

I would like to give a special thank you to my dear wife Jean Kachisa for her love, support and great patience. This made me study in a sweet and peaceful environment. To Ezekiel Jr., Peace, Praise and Rachael this is your benchmark work hard, I love you!

My deepest gratitude go to my mom Florence Kamutu, my uncle Elywn Phiri and all my close relatives, and friends Edward Lubaini, Paul Kubwalo and Atipatsa Kaminga for their love and support and encouragement through out the course. To my lab-mates; it was worthy to be with you guys.

I also would like to send my special thanks to my parents-in-law, the Nkhonjera family.

I am indebted to Claude Shannon Institute for the financial support, the management of the Malawi Institute of Education for allowing me to pursue my dreams.

To Justin Kachisa Sr. this is for your ever wise encouragements and guidance you must be a very happy spirit to see this materialise. Gone too soon.

Ireland, Dublin, Ezekiel Justin Kachisa

Abstract

One of the challenges in the designing of pairing-based cryptographic protocols is to construct suitable pairing-friendly curves: Curves which would provide efficient implementation without compromising the security of the protocols. These curves have small embedding degree and large prime order subgroup. Random curves are likely to have large embedding degree and hence are not practical for implementation of pairing-based protocols.

In this thesis we review some mathematical background on elliptic and hyperelliptic curves in relation to the construction of pairing-friendly hyperelliptic curves. We also present the notion of pairing-friendly curves. Furthermore, we construct new pairing-friendly elliptic curves and Jacobians of genus two hyperelliptic curves which would facilitate an efficient implementation in pairing-based protocols. We aim for curves that have smaller ρ-values than ever before reported for different embedding degrees.

We also discuss optimisation of computing pairing in Tate pairing and its variants. Here we show how to efficiently multiply a point in a subgroup defined on a twist curve by a large cofactor. Our approach uses the theory of addition chains. We also show a new method for implementation of the computation of the hard part of the final exponentiation in the calculation of the Tate pairing and its variants.

Contents

List of Tables

List of Notations

Most symbols are well understood from context. Unless otherwise stated:

$\mathbb{G}$	a cyclic group	3
$\mathbb{Z}_r$	integers modulo r	4
$e(P,Q)$	pairing of P and Q	3
ζ_k	primitive kth root of unity	8
f(D)	a function evaluated at a divisor	5
$J_{\mathcal{C}}$	Jacobian variety of a curve $\mathcal{C}$	7
$\Phi_k(z)$	kth cyclotomic polynomial	8
$\mathbb{Z}, \mathbb{Q}$	a field of integers, rationals	9
$\mathbb{Q}(\zeta_k)$	kth cyclotomic field	9
$\mathbb{F}(\mu_r)$	a field generated by rth roots of unity	11
$\mathcal{A}$	an abelian variety of dimension g	10
μ_r	rth roots of unity	11
$\mathcal{O}$	a point at infinity	30
$\mathcal{E}/\mathbb{F}_p$	elliptic curve defined over a finite field	30
$\mathcal{E}(\mathbb{F}_p)$	$\mathbb{F}_p$-rational points in $\mathcal{E}$	31
$\mathcal{C}, \mathcal{E}$	curve equation	36
End$(\mathcal{E})$	endormorphism ring of $\mathcal{E}$	37
$\mathcal{E}[r]$	group of r-torsion points on the curve $\mathcal{E}$	41
$\gamma(\zeta_\ell)$	element of $\mathbb{Q}(\zeta_\ell)$	54

Chapter 1

Introduction

1.1 Background

Elliptic curves were independently introduced to cryptography in 1985 by Victor Miller [66] and Neal Koblitz [52] . While in 1989, to get a more general class of curves and possibly larger group orders, Neal Koblitz [53] proposed the use of divisor class groups on Jacobians of hyperelliptic curves.

The proposals of Elliptic Curve Cryptography (ECC) and Hyperelliptic Curve Cryptography (HECC) were as an alternative to public-key systems such as RSA algorithms [78]. The advantage of ECC and HECC is that for suitably chosen curves there is no known subexponential algorithm like the number field sieve algorithm [59] for integer factorization, to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP) or the Hyperelliptic Curve Discrete Logarithm Problem (HECDLP). Consequently, this leads to smaller key length in ECC and HECC to achieve the same level of security as in public-key systems based on factorisation and the Discrete Logarithm Problem (DLP) in finite fields. The shorter key length, in turn, leads to faster encryption and decryption, savings in bandwidth and efficient implementation.

1.2 Bilinear pairings

Initially, pairings were used for cryptanalysis purposes. In 1993, Menezes, Okamoto and Vanstone [63] showed how it is possible, using the Weil pairing, to convert a discrete logarithm problem on elliptic curves to a discrete logarithm problem in a finite field. This cryptanalysis is known as MOV-reduction. In particular, if the curve is supersingular and the Weil pairing is defined over any r-torsion subgroup then with MOV-reduction one can solve the DLP in a sub-exponential time. This is achieved by establishing an isomorphism between the subgroup of points on a curve $\mathcal{C}$, generated by a point P, and a subgroup of r-th roots of unity. Similar work was later done by Frey and Rück [35] by using the Tate pairing.

However some 'constructive' use of pairings were later proposed by different researchers. For instance, Joux [48], Sakai, Ohgishi and Kasahara [80] and Boneh and Franklin [13] proposed cryptosystems using elliptic curve pairings.

The cryptosystem proposed by Joux in 2000 for example, is analog to the Diffie-Hellman protocol [25] for key exchange. The Joux's key exchange protocol, allows three parties to share a private key in only one round which the Diffie-Hellman protocol does in two rounds. In 1984, Shamir [90] conceptualised a public-key encryption scheme where the public key of each person is directly linked to his or her identity. This idea removed the need for its certification by a trusted certification authority. Sakai, Ohgishi and Kasahara [80] and independently Boneh and Franklin [13] devised the first practical implementation of such an Identity-Based Encryption scheme using bilinear maps.

The following is the definition of a non-degenerate bilinear pairing [10]:

Definition 1.2.1. *Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be finite cyclic additive groups of prime order r and $\mathbb{G}_T$ be a finite cyclic multiplicative group of order r. A non-degenerate bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ that satisfies the following properties:*

i. bilinear

$$\begin{aligned} e(P + P', Q) &= e(P, Q).e(P', Q); \\ e(P, Q + Q') &= e(P, Q).e(P, Q'); \end{aligned}$$

for all P, $P' \in \mathbb{G}_1$ and Q, $Q' \in \mathbb{G}_2$ and $a, b, \in \mathbb{Z}_r$.

ii. non-degenerate*: For all $P \in \mathbb{G}_1$, $P \neq \mathcal{O}$ there is some $Q \in \mathbb{G}_2$ such that $e(P, Q) \neq 1$. For all $Q \in \mathbb{G}_2$, $Q \neq \mathcal{O}$ there is some $P \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.*

iii. computable*: e can be efficiently computed.*

That is the function e bilinearly maps two elements, $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$ to an element, rth root of unity, in $\mathbb{G}_T$. The bilinearity condition is the main property of the pairing. In fact, it is the one property that facilitates the efficient reduction of the DLP in $\mathbb{G}_1$ to the DLP in $\mathbb{G}_T$. Moreover, the non-degeneracy property ensures that the mapping is not trivial; that is, sending every pair of elements of $\mathbb{G}_1$ and $\mathbb{G}_2$ to the identity element of $\mathbb{G}_T$. This would not be interesting and practical.

The pairing can be delivered by either the Weil pairing or the Tate pairing and its variants (we introduce this in Section 5.1.1 later). In this thesis, we identify $\mathbb{G}_1$ as a group of points on a curve defined over a base field and $\mathbb{G}_2$ as a group of points on a curve defined over some extension of the base field. The computational complexity of the Tate pairing is less than that of the Weil pairing.

1.2.1 Security considerations

The security of pairing-based protocols relies on the hardness of the problems stated in Definitions 1.2.2, 1.2.3 and others. We say that a problem in a group $\mathbb{G}$ is hard if no polynomial algorithm solves the problem with non-negligible probability, see [97] for more details.

Definition 1.2.2 (Discrete Logarithm Problem (DLP))**.** *Let $\mathbb{G}$ be additive cyclic group of order r generated by P. For $P, Q \in \mathbb{G}$, find $a \in \mathbb{Z}_r$ such that $Q = aP$.*

In 1970, Diffie and Hellman showed that cryptographic protocols can be constructed if one assumes that the Computational Diffie-Hellman Problem (CDHP) is hard. The CDHP in a cyclic group $\mathbb{G}$, is to compute g^{ab} given a triple, (g, g^a, g^b), where g is uniform in $\mathbb{G}$ and a, b are uniform in $\mathbb{Z}_r$. A variant of the CDHP in pairings is known as Bilinear Diffie-Hellman Problem (BDHP). In its general terms it is defined as follows [97]:

Definition 1.2.3 (Bilinear Diffie-Hellman Problem (BDHP))**.** *Let $\mathbb{G}_1$ be a finite additive cyclic group generated by P_1, $\mathbb{G}_2$ be a finite additive cyclic group generated by P_2 and $\mathbb{G}_T$ be a finite multiplicative cyclic group, let e be a bilinear pairing on $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ and let $a, b, c \in \mathbb{Z}_r$. Given values x, y, z, $\in \{1, 2\}$ and P_1, P_2, aP_x, bP_y and cP_z compute the value of the bilinear pairing, $e(P_1, P_2)^{abc}$.*

Groups in which the BDHP is hard and for which the group law can be performed efficiently are possible candidates for pairing-based cryptographic applications.

We consider two types of groups here; the group of points on elliptic curves, and the group of points on the Jacobian of genus 2 hyperelliptic curves. In these groups under certain conditions, there is no method like index calculus known to solve the DLP. If the groups are chosen with care, then the most efficient way to solve the DLP is by means of parallelised Pollard-rho method [77] and it has a fully exponential running time of $\sqrt{\pi|\mathbb{G}|/2}$ group operations.

1.2.2 Divisors

Divisors are useful tools for tracking the zeros and poles of a rational function. We need these tools to construct a group law on hyperelliptic curves. We state the results only. The proofs can be found in [95], [10] or [103].

Let $\mathcal{C}$ be a non-singular projective curve defined over a field $\mathbb{F}$ and let $\bar{\mathbb{F}}$ be its algebraic closure. A divisor D is defined as follows:

Definition 1.2.4. *A divisor D is a formal sum of all symbols (P) given by*

$$D = \{ \sum_{P \in \mathcal{C}(\bar{\mathbb{F}})} n_P P : n_P \in \mathbb{Z}\} \tag{1.1}$$

where only a finite number of n_p are non-zero and P is an $\bar{\mathbb{F}}$-point on the curve $\mathcal{C}$.

Set of divisors of the curve forms a free abelian group generated by the points on $\mathcal{C}$, referred to as the divisor group of $\mathcal{C}$ which we represent by $Div(\mathcal{C})$. The degree of a divisor D is defined to be

$$\deg(D) = \sum_{P \in \mathcal{C}(\bar{\mathbb{F}})} n_P \in \mathbb{Z}$$

and the *order* of D at P, is defined by:

$$ord_P(D) = n_P \in \mathbb{Z}.$$

The divisors of degree *zero* form a subgroup of $Div(\mathcal{C})$, which is a set defined as:

$$Div^0(\mathcal{C}) = \{D \in Div(\mathcal{C})| \deg(D) = 0\}.$$

The support of D, denoted by $supp(D)$, is defined as the finite set of points P with $n_P \neq 0$.

Let $\bar{\mathbb{F}}(\mathcal{C})$ be the function field of rational functions on $\mathcal{C}$. Let $f \in \bar{\mathbb{F}}(\mathcal{C})$ be a non zero function. Then the rational function f on $\mathcal{C}$ has an associated divisor

$$div(f) = \sum_{P \in \mathcal{C}(\bar{\mathbb{F}})} ord_P(f)(P)$$

which keeps track of the number and location of its *zeros* and *poles*. A divisor which is the divisor of a function in this way is called a principal divisor. We denote this by $Princ(\mathcal{C})$ and is defined as:

$$Princ(\mathcal{C}) = \{D \in Div(\mathcal{C})|D = div(f), f \neq 0, \text{for} f \in \bar{\mathbb{F}}(\mathcal{C})\}.$$

In fact $Princ(\mathcal{C})$ is a subgroup of $Div^0(\mathcal{C})$. Moreover, for non-zero rational functions f, $g \in \bar{\mathbb{F}}(\mathcal{C})$, $div(fg) = div(f) + div(g)$ and $div(f/g) = div(f) - div(g)$.

Two divisors D and D' are said to be equivalent, $D \sim D'$, if $D' = D + div(f)$ for some non-zero $f \in \bar{\mathbb{F}}(\mathcal{C})$.

We refer to D as prime to D' if $supp(D) \cap supp(D') = \emptyset$. Furthermore, we say, D is effective or positive divisor when all $n_P \geq 0$.

For an element α in the Galois group of $\bar{\mathbb{F}}$ over $\mathbb{F}$ and for a divisor,

$D \in Div(\mathcal{C})$, Gal$(\bar{\mathbb{F}}/\mathbb{F})$ acts on the divisor as follows:

$$(\sum_{P \in \mathcal{C}(\bar{\mathbb{F}})} n_P(P))^{\alpha} = \sum_{P \in \mathcal{C}(\bar{\mathbb{F}})} n_P(P^{\alpha}).$$

A divisor D is said to be defined over $\mathbb{F}$ if $D^{\alpha} = D$ for all $\alpha \in$ Gal$(\bar{\mathbb{F}}/\mathbb{F})$.

The equivalence classes of divisors of degree zero, $Div^0(\mathcal{C})$, form a group known as the *Picard group* denoted by $Pic^0(\mathcal{C})$. The $Pic^0(\mathcal{C})$ is a quotient group of degree zero divisors modulo principal divisors, that is $Div^0(\mathcal{C})/Princ^0(\mathcal{C})$.

If $\mathcal{C}$ is an elliptic curve $\mathcal{E}/\mathbb{F}$ for example, then for every divisor $D \in Div^0(\mathcal{E})$ there is a unique point $P \in \mathcal{E}(\mathbb{F})$ such that $D \sim (P) - \mathcal{O}$. This gives a one-to-one correspondence between $Pic^0(\mathcal{E})$ and $\mathcal{E}(\mathbb{F})$.

In general, if a curve has a rational point then there is a natural isomorphism between the degree zero part of the $Pic^0(\mathcal{C})$ group of genus two hyperelliptic curve $\mathcal{C}$ and and its Jacobian $J_{\mathcal{C}}$ which is an abelian variety into which the curve embeds. In this thesis for genus 2 hyperelliptic curve, $\mathcal{C}$, we identify the Picard group $Pic^0(\mathcal{C})$ with $J_{\mathcal{C}}$.

1.3 Cyclotomic polynomials

1.3.1 Introduction

Cyclotomic polynomials play a very important role in the construction of pairing-friendly curves. For proofs and more on this area the reader is referred to [102] and [43].

Definition 1.3.1. *Let k be a positive integer. A complex number ζ is called a kth root of unity if $\zeta^k = 1$.*

From the polar form of complex numbers we know that there are k kth roots of unity which are exactly the numbers

$$e^{\frac{2\pi i}{k}}, e^{\frac{2\pi i}{k}2}, \ldots, e^{\frac{2\pi i}{k}k} = 1.$$

Definition 1.3.2. *Let ζ be a kth root of unity. If m is the smallest positive integer such that $\zeta^m = 1$, then m is called the order of ζ which we denote by Ord_ζ.*

Definition 1.3.3. *Let ζ be an kth root of unity. Then ζ is called a primitive kth root of unity, denoted ζ_k, if $Ord_\zeta = k$.*

Definition 1.3.4. *Let k be a positive integer. Denote ζ_k a primitive kth root of unity. Then the kth cyclotomic polynomial is the monic polynomial given by the following equation:*

$$\Phi_k(z) = \prod_{\substack{1 \leq s \leq k \\ gcd(s,k)=1}} (z - \zeta_k^s) \tag{1.2}$$

The polynomial $\Phi_k(z)$ is irreducible over $\mathbb{Q}$, has integer coefficients and of degree $\varphi(k)$, where $\varphi(.)$ is the Euler's totient function. Furthermore, by setting $\Phi_1(z) = z - 1$ one can recursively generate the other cyclotomic polynomials by using the following theorem:

Theorem 1.3.1. *Let m be a positive integer. Then*

$$z^m - 1 = \prod_{d|m} \Phi_d(z). \tag{1.3}$$

Here we state the first 10 cyclotomic polynomials:

$$\begin{aligned}
\Phi_1(z) &= z-1; \\
\Phi_2(z) &= z+1; \\
\Phi_3(z) &= z^2+z+1; \\
\Phi_4(z) &= z^2+1; \\
\Phi_5(z) &= z^4+z^3+z^2+z+1; \\
\Phi_6(z) &= z^2-z+1; \\
\Phi_7(z) &= z^6+z^5+z^4+z^3+z^2+z+1; \\
\Phi_8(z) &= z^4+1; \\
\Phi_9(z) &= z^6+z^3+1; \\
\Phi_{10}(z) &= z^4-z^3+z^2-z+1.
\end{aligned}$$

1.3.2 Cyclotomic fields

When a complex primitive root of unity is adjoined to the field of rational numbers $\mathbb{Q}$, a cyclotomic field or cyclotomic number field is constructed. For a positive integer $k > 2$ and ζ_k a primitive kth root of unity we denote the kth cyclotomic field by $\mathbb{Q}(\zeta_k)$. This field contains all kth roots of unity and is the splitting field of the kth cyclotomic polynomial $\Phi_k(z)$, over $\mathbb{Q}$.

The ring of integers of a cyclotomic field always has a power basis over $\mathbb{Z}$. Specifically, the ring of integers of $\mathbb{Q}(\zeta_k)$ is $\mathbb{Z}[\zeta_k]$.

1.4 Pairing-friendly abelian varieties

A general literature on abelian varieties can be sourced from [47],[79],[91],[104], or [54]. In this section, we introduce the notion of pairing-friendly abelian varieties.

An *abelian variety* $\mathcal{A}$ defined over a field $\mathbb{F}$, is a projective algebraic variety that is also an algebraic group with $\mathbb{F}$-rational point $\mathcal{O}$, the identity element, morphisms $\psi : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$, the addition law and $\Theta : \mathcal{A} \to \mathcal{A}$, the inverse. That is, it has a group law that can be defined by regular functions.

The group law on abelian variety is necessarily commutative and the variety is non-singular. An elliptic curve for example, is a one-dimensional abelian variety and an abelian surface is a two-dimensional abelian variety.See [104] and [47] for more details.

1.4.1 Embedding degree

We introduce the notion of the embedding degree. Let $\mathcal{A}$ be an abelian variety defined over a finite field $\mathbb{F}_p$, let $\mathbb{F}_p$-rational points of $\mathcal{A}$ be denoted by $\mathcal{A}(\mathbb{F}_p)$, assume $\mathcal{A}$ contains an additive cyclic group of prime order r. Let $\mu_r \subset \bar{\mathbb{F}}_p$ be the group of rth roots of unity in algebraic closure of $\mathbb{F}_p$. We define the Tate pairing as a non degenerate bilinear map

$$\mathcal{A}(\mathbb{F}_p)[r] \times \hat{\mathcal{A}}(\mathbb{F}_p)/r\hat{\mathcal{A}}(\mathbb{F}_p) \mapsto \mathbb{F}_p^{\times}/(\mathbb{F}_p\times)^r$$

where $\hat{\mathcal{A}}$ is the dual of $\mathcal{A}$. The quotient group $\mathbb{F}_p^{\times}/(\mathbb{F}_p\times)^r$ is isomorphic to μ_r. That means; in order to obtain pairing values of order r we must work over a field containing the rth roots of unity. If k is a positive integer then we say $\mathcal{A}$ has embedding degree k with respect to r if Definition 1.4.1 is satisfied.

Definition 1.4.1 ([31]). *Let $\mathcal{A}$ be an abelian variety defined over $\mathbb{F}_p$, let r be a prime distinct from the characteristic of $\mathbb{F}_p$. Then $\mathcal{A}$ has embedding degree k with respect to r if*

- *$\mathcal{A}$ has an $\mathbb{F}_p$-rational point of order r and*
- *$[\mathbb{F}_p(\mu_r) : \mathbb{F}_p] = k$.*

The name embedding degree, is derived from the fact that the k-extension field of $\mathbb{F}_p$ is the smallest field over which the pairing can be used to embed an additive cyclic group of order r, a subset of $\mathcal{A}(\mathbb{F}_p)$, into a multiplicative cyclic group $\mathbb{F}_p(\zeta_r)$.

We will say a curve $\mathcal{C}$ has embedding degree k with respect to a prime integer r if and only if a Jacobian does.

Lemma 1.4.1. *Let $\mathcal{A}$ be an abelian variety over a finite field $\mathbb{F}_p$ with $\mathbb{F}_p$-rational point of order r. If r is relatively prime to p then the following conditions are equivalent:*

1. *$\mathcal{A}$ has embedding degree with respect to r.*
2. *k is the smallest integer such that r divides $p^k - 1$.*
3. *k is the multiplicative order of p modulo r*

   Furthermore, if r is a prime not dividing k then these conditions are equivalent to:

4. *$\Phi_k(p) \equiv 0$ (mod r), where Φ_k is the kth cyclotomic polynomial.*

Proof. See [31] □

1.4.2 Frobenius endomorphism

Let p be an odd prime, $\mathbb{F}_p$ a finite field of order q with $char(\mathbb{F}_p) = p$. Let g be a positive integer and $\mathcal{A}$ be an abelian variety of dimension g defined over $\mathbb{F}_p$. Then the Frobenius endomorphism π, of $\mathcal{A}/\mathbb{F}_p$ has a characteristic polynomial $\chi_{\mathcal{A}}$. This is a degree $2g$ monic polynomial with integer coefficients of the form:

$$\chi_{\mathcal{A}} = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + p a_{g-1} t^{g-1} + p^g. \tag{1.4}$$

In fact this polynomial determines $\mathcal{A}$ up to $\mathbb{F}_p$-isogeny, thus two abelian varieties $\mathcal{A}$ and $\mathcal{A}'$ are $\mathbb{F}_p$-isogenous if and only if $\chi_{\mathcal{A}}$ is equal to $\chi_{\mathcal{A}'}$ [47].

If $\mathcal{A}$ is a g-dimensional simple abelian variety defined over a field $\mathbb{F}_p$ and $K = \mathbb{Q}(\pi) \subset \mathrm{End}(\mathcal{A}) \otimes \mathbb{Q}$, the number field generated by the Frobenius endomorphism π, then the $\mathbb{F}_p$-rational points of $\mathcal{A}$ form the kernel of the endomorphism $(\pi - 1)$. And hence in the case where $K = \mathbb{Q}(\pi)$ is the full endomorphism algebra, $\mathrm{End}(\mathcal{A}) \otimes \mathbb{Q}$, the number $\#\mathcal{A}(\mathbb{F}_p)$ is completely determined by $\chi_{\mathcal{A}}$ according to the formula:

$$\#\mathcal{A}(\mathbb{F}_p) = \chi(1) = Norm_{K/\mathbb{Q}}(\pi - 1). \tag{1.5}$$

Moreover, we say $\mathcal{A}$ is ordinary if the middle coefficient of $\chi_{\mathcal{A}}$ is prime to the field characteristic and $\mathcal{A}$ is supersingular if $\mathcal{A}$ is $\bar{\mathbb{F}}_p$-isogenous to a product of supersingular abelian varieties of lower dimensions.

If r is a prime integer then r-torsion points on $\mathcal{A}$ are denoted as $\mathcal{A}(\mathbb{F}_p)[r] \subseteq \mathcal{A}(\mathbb{F}_p)$. This is a group of points defined as:

$$\mathcal{A}(\mathbb{F}_p)[r] = \{P \ \in \mathcal{A}(\mathbb{F}_p) |\ rP = \mathcal{O}\} \tag{1.6}$$

where $\mathcal{O}$ is the identity of the group.

When developing a pairing-based protocol one chooses a large prime, say r, and the embedding degree k such that the DLP in both $\mathcal{A}(\mathbb{F}_p)[r] \subseteq \mathcal{A}(\mathbb{F}_p)$, and $\mathbb{F}_p(\zeta_r)^*$ are computationally of similar difficulty.

Typically, for practical purposes, abelian varieties must have small embedding degree k. Otherwise the computations will not be feasible in $\mathbb{F}_{p^k}$. With today's recommendations for security and applicability reasons the size of p^k should at least be 1024 bits in length. While a large prime order subgroup of size r should be at least 160 bits, see Table 1.1.

This leads to understanding *pairing-friendly* abelian varieties as the one that satisfies the following [32]:

- $\mathcal{A}(\mathbb{F}_p)$ has a large prime order subgroup, $\mathcal{A}(\mathbb{F}_p)[r]$, so that the DLP is suitably hard.
- the embedding degree k of $\mathcal{A}(\mathbb{F}_p)$ with respect to $\mathcal{A}(\mathbb{F}_p)[r]$ is sufficiently small so that the arithmetic in $\mathbb{F}_{p^k}$ can be efficiently implemented and large enough so that the DLP in $\mathbb{F}_{p^k}$ is hard.

Pairing-friendly abelian varieties satisfy conditions in the Proposition 1.4.1 below.

Proposition 1.4.1 ([33]). *Let $\mathcal{A}(\mathbb{F}_p)$ be a simple abelian variety, let $\mathbb{F}_p$ be a finite field and let π be the Frobenius endomorphism and assume $K = \mathbb{Q}(\pi)$ is a full algebra endomorphism, $End(\mathcal{A}) \otimes \mathbb{Q}$. Let k be a positive integer, Φ_k be the kth cyclotomic polynomial, and r a prime number such that $r \nmid pk$. If we have*

$$\begin{aligned} Norm_{K/\mathbb{Q}}(\pi - 1) &\equiv 0 \mod r; & (1.7) \\ \Phi_k(p) &\equiv 0 \mod r; & (1.8) \end{aligned}$$

then $\mathcal{A}$ has embedding degree k with respect to r.

In an ordinary one-dimensional abelian variety, the elliptic curves, the number field generated by the Frobenius endomorphism π, is a quadratic imaginary field, $K = \mathbb{Q}(\pi) = End(\mathcal{A}) \otimes \mathbb{Q}$. In this instance π corresponds to the imaginary quadratic integer such that $Norm_{K/\mathbb{Q}}(\pi) = \pi\bar{\pi} = p$ and its trace can be viewed as $t = \pi + \bar{\pi}$. The conditions in Proposition 1.4.1 are then equivalent to:

$$\begin{aligned} (p+1-t) &\equiv 0 \mod r; && (1.9) \\ \Phi_k(p) &\equiv 0 \mod r. && (1.10) \end{aligned}$$

The first relation, in both instances, ensures that the order of the abelian variety has a large prime factor while the second one ensures that the embedding degree of the abelian variety is k.

The efficiency of computations on $\mathcal{A}(\mathbb{F}_p)$ is determined by $\#\mathcal{A}(\mathbb{F}_p) \approx p^g$ in relation to the size of the prime order subgroup r. For efficient implementations one usually wishes to choose $\mathcal{A}$ with an r as close to $\#\mathcal{A}(\mathbb{F}_p)$ as possible.

A parameter, ρ, is used as a measure of this efficiency. It roughly approximates the ratio of the bit size of the entire group $\mathcal{A}(\mathbb{F}_p)$ to the bit size r of the cryptographic group. The ρ-value of a g-dimensional abelian variety $\mathcal{A}$, defined over a finite field $\mathbb{F}_p$, is defined as:

$$\rho = \frac{g \log p}{\log r} \tag{1.11}$$

where log is the natural logarithm. For a secure and efficient implementation of protocols, the ideal situation is to have $\rho \approx 1$.

Supersingular abelian varieties exhibit the above qualities. That is; having a small embedding degree and reaching the ideal case for ρ-values. Unfortunately there is skepticism over their use because the more interesting supersingular varieties are only defined with small characteristic field in which index calculus attack is particularly powerful [21] and have small embedding degree k. Hence Miyaji et al.[69], Barreto and Naehrig [8] and Freeman [29] proposed methods for constructing ideal one-dimensional ordinary pairing-friendly abelian varieties for embedding degrees k. Furthermore, with the growing deployment of pairing-based cryptographic protocols there is a need to have at our disposal abelian varieties of various embedding degrees k, to cater for different levels of security, see Table 1.1.

The question now is:

> *Given positive integers g and k construct a g-dimensional ordinary pairing-friendly abelian variety $\mathcal{A}$, defined over a finite field $\mathbb{F}_p$, such that:*
>
> - *$\#\mathcal{A}(\mathbb{F}_p)$ has a large prime factor r;*
> - *$\mathcal{A}$ has embedding degree k with respect to r;*
> - *the ρ-value of $\mathcal{A}$ is as close to one as possible.*

We address this problem by describing constructions of ordinary elliptic curves and Jacobians of genus two hyperelliptic curves, with a large prime-order subgroup and have prescribed embedding degree k.

Our methods are based on the Brezing-Weng method for constructing pairing-friendly elliptic curves [17] and the Kawazoe-Takahashi method of constructing genus two pairing-friendly hyperelliptic curves [51]. In our construction we look for abelian varieties with smaller ρ-values than any previously reported; as field arithmetic on such abelian varieties is faster compared to those varieties with larger ρ-values [32].

Table 1.1 outlines the recommended sizes of r and p^k at different levels of security for dimension one and two abelian varieties [32]. The listed bit sizes are those matching the security levels of the SKIPJACk, Triple-DES, AES small, AES-Medium and AES-Large symmetric key encryption schemes.

Table 1.1: *Bit sizes parameters r and p^k*

Security level (bits)	Subgroup size r (bits)	Extension field size p^k (bits)	$k.\rho$	
			genus 1	genus 2
80	160	960-1280	6 - 8	12 - 16
112	224	2200-3600	10 - 16	20 - 32
128	256	3000-5000	12 - 20	24 - 40
192	384	8000-10000	20 - 26	40 - 52
256	512	14000-18000	28 - 36	56 - 72

1.4.3 Families of curves

Our approach in constructing families of pairing-friendly curves is to use polynomials to define parameters. Polynomials were used in other constructions such as those due to Miyaji, Nakabayashi and Takano [69]; Barreto, Lynn and Scott [7]; Scott and Barreto [86] and Brezing and Weng [17]. This is good for implementors since it brings flexibility in choosing curves of specified bit size. Hence we have the notion of *a family* of pairing-friendly curves as presented in [32].

Here we need the polynomials we construct to take in infinite values of integers and primes. To that effect there is famous conjecture by Buniakowski [16] and reformulated by Schinzel and Sierpiński [81].

However, for our purpose we also consider polynomials with rational coefficients. Before we state the adapted conjectures we need the following definition [32]:

Definition 1.4.2. *Let $g(z)$ be a polynomial with rational coefficients. Then $g(z)$ represents integers if there exists $z_0 \in \mathbb{Z}$ such that $g(z_0)$ is an integer.*

In other words, there must be infinitely many integers z_0, such that $g(z)$ is an integer too. It turns out that it is enough using representatives of $\mathbb{Z}_n$

to test the condition in Definition 1.4.2; that is on $z_0 \in [0, 1, 2, \ldots n-1]$ for some n such that $n.g(z) \in \mathbb{Z}[z]$. If one of the values of z_0 evaluates the polynomial to an integer then we say it represents integers.

Conjectures 1.4.1 and 1.4.2 describe conditions that will likely make a polynomial with rational coefficients take infinite prime values [16], [32].

Conjecture 1.4.1. *Let $g(z)$ be a polynomial with rational coefficients. Suppose $g(z)$ is a non constant irreducible polynomial with a positive leading coefficient and represents integers. Moreover, suppose that there is no prime p which divides $g(z)$ for every integer value of z. Then $g(z)$ is prime for infinitely many positive integer values of z.*

This was later generalised to a family of polynomials by Schinzel and Sierpiński [81] who gave several applications to elementary number theory. It is extended here to include polynomials with rational coefficients.

Conjecture 1.4.2. *Let $g_1(z), \cdots g_j(z)$ be a polynomials with rational coefficients. Let $g_1(z), \cdots g_j(z)$ be non constant irreducible polynomials with a positive leading coefficient and represents integers. Moreover, suppose that there is no prime p for which*

$$\prod_{i=1}^{i=j} g_i(z) \equiv 0 \bmod\ p$$

for every value of z. Then there are infinitely many positive integers z for which $g_1(z), \cdots, g_j(z)$ are simultaneously prime.

Moreover, if $g(z_0) = \pm 1$ for some value z_0 then $g(z)$ will automatically represent integers and primes.

Example 1.4.1. *Consider $g(z) = (z^{10}+z^9+z^8-z^6+2z^5-z^4+z^2-2z+1)/3$*

$$\begin{aligned} g(0) &= 1/3; \\ g(1) &= 1; \\ g(2) &= 1777/3. \end{aligned}$$

Hence, only when $z \equiv 1 \bmod 3$ *will* $g(z)$ *represents integers and primes.*

1.5 Complex multiplication method

In this section we complete the picture of constructing pairing-friendly curves. A curious reader may consult [94], [9], [20] or [105] for more on theoretical background on complex multiplication. This idea originated in [2] in the circumstances of primality proving.

As we have seen the security of protocols developed from curves depend on the hardness of the DLP in the group of points on the curve. In particular, on the large prime order subgroup of the group of points on the curve. The tradition has been to pick a curve which is defined over a finite field, count the number of points on this curve and find out whether a group of points on this curve has a subgroup of prime order size. This is not efficient with the construction of pairing-friendly curves considering the divisibility conditions we require on the prime order subgroup and security needed for different protocols. Moreover, random curves are likely to have large embedding degrees.

However, with the complex multiplication method (CM) one can construct curves with known number of points on it.

1.5.1 CM in elliptic curves

The ultimate goal here is the following. Suppose we are given a prime p and a non-negative number n, in the so called Hesse-Weil interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ construct an elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_p$ with n $\mathbb{F}_p$-points:

$$\#\mathcal{E}(\mathbb{F}_p) = n = p + 1 - t \tag{1.12}$$

where t is the trace of the Frobenius endomorphism of $\mathcal{E}$ over $\mathbb{F}_p$.

Let D be a positive integer such that $-D$ is a fundamental discriminant of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. That is $-D$ is a number congruent to 1 or 0 modulo 4 and that no odd prime divides D to a power grater than one. We refer to $\mathfrak{d}$ as a square free positive integer such that $K = \mathbb{Q}(\sqrt{-\mathfrak{d}})$; in other words:

$$D = \begin{cases} \mathfrak{d} & \text{if} \quad \mathfrak{d} \equiv 3 \bmod 4 \\ 4\mathfrak{d} & \text{if} \quad \text{otherwise.} \end{cases}$$

We denote the imaginary quadratic order of discriminant $-D$ by $\mathfrak{O}_{-D}$. Furthermore, we write h_{-D} the class number of $\mathfrak{O}_{-D}$. If p is the prime number then p is said to be a norm in $\mathfrak{O}_{-D}$ if and only if we can solve the equation:

$$4p = t^2 + Dy^2 \tag{1.13}$$

in integers t, y.

In such a scenario elliptic curves with $n = p + 1 - t$ or $n' = p + 1 + t$ can be constructed by complex multiplication method. For an ordinary elliptic curve defined over a field L, endomorphism $End(\mathcal{E})$, is either $\mathbb{Z}$ or an order in an imaginary quadratic number field. The curve $\mathcal{E}$, is said to have complex multiplication if its endomorphism $End(\mathcal{E})$, is equal to an order in an imaginary quadratic number field.

Unless otherwise noted, in this thesis we henceforth write D to mean the absolute value of the discriminant and $\mathfrak{d}$ a positive square free integer.

Let τ be a complex algebraic number of degree two in Poincaré half plane $\mathfrak{H} = \{e = \mathfrak{a} + i\mathfrak{b} : \mathfrak{a}, \mathfrak{b} \in \mathbb{R}, \mathfrak{b} > 0\}$. Let $Q(x,y) = ax^2 + bxy + cy^2$ be a quadratic form and denote by $\tau = \frac{-b+\sqrt{-D}}{2a}$ the root of $Q(x,1)$. We denote $j([a,b,c])$ to mean $j(\tau)$.

Suppose $\mathcal{H}_K$ is a Hilbert class field of K, namely the maximal unramified Abelian extension of K. Its Galois group is isomorphic to the class group of K:

$$Gal(\mathcal{H}_K) \simeq Cl_K.$$

The degree of $\mathcal{H}_K$ over $\mathbb{Q}(\tau)$ is equal to h_{-D}, the class number.

The following proposition, the proof of which can be obtained from [2], relates the Hilbert class field to the values of the j-function at points in $\mathfrak{H}$.

Proposition 1.5.1. *Let $K = \sqrt{-D}$. The Hilbert class field of K can be obtained by adjoining a value of $j([a,b,c])$, where $[a,b,c] \in Cl_K$ is any one of the reduced quadratic forms of the discriminant $-D$. The minimal polynomial of the $j([a,b,c])$'s, denoted as $H_{-D}(z)$, has integer coefficients. The Galois group $Gal(\mathcal{H}_K)$ is isomorphic to the class group Cl_K and if $f \in Cl_K$ then we denote $\sigma(g)$ to mean the corresponding element in $Gal(\mathcal{H}_K)$. The action of $\sigma(g)$ on j is given by*

$$\sigma(g)(j(f)) = j(g^{-1} \cdot f).$$

The Hilbert class polynomial $H_{-D}(z) \in \mathbb{Z}$, generates the Hilbert class field $\mathcal{H}_K$. This monic polynomial of degree h_{-D} is defined by:

$$H_{-D}(z) = \prod_{\tau \in \mathcal{S}} (x - j(\tau)) \tag{1.14}$$

where $\mathcal{S} = \{\tau = \frac{-b+\sqrt{-D}}{2a} : b^2 - 4acy = -D,\ |b| \leq a \leq \sqrt{\frac{|D|}{3}},\ a \leq c,$ $gcd(a, b, c) = 1$ and if $|b| = a$ or $a = c$ then $b \geq 0\}$.

It follows that if τ is a quadratic number of discriminant $-D$ in $\mathcal{H}_K$ then $j(\tau)$ is an algebraic integer of degree h_{-D}.

The roots $j(\tau)$, of the Hilbert class polynomial $H_{-D}(z)$ are the j-invariants of the elliptic curve $\mathcal{E}_\tau$ with complex multiplication by an order in $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{-D})$.

Using sufficiently accurate complex approximations of the zeros in Equation 1.14, as suggested in [20], the quantity $j(\tau)$ can be computed as follows: Let $\mathcal{B} = e^{2i\pi\tau}$ and define the quantity $\triangle(\tau)$ as:

$$\triangle(\tau) = \mathcal{B}\left(1 + \sum_{n \geq 1} (-1)^n (\mathcal{B}^{n(3n-2)/2} + \mathcal{B}^{n(3n+1)/2})\right)^{24}, \tag{1.15}$$

then

$$j(\tau) = \frac{(256f(\tau) + 1)^3}{f(\tau)} \tag{1.16}$$

where

$$f(\tau) = \frac{\triangle(2\tau)}{\triangle(\tau)}.$$

The following theorem describes the behaviour of certain rational primes in the Hilbert class field [2].

Theorem 1.5.1. *Let $K = \mathbb{Q}(\sqrt{-D})$ and $\mathcal{H}$ be the Hilbert class field of K. Then if p is a rational prime the following statements are equivalent.*

- *p is a norm in K*

- *p splits completely in $\mathcal{H}$*
- *$H_{-D}(z)$ modulo p slits completely into linear factors with roots in $\mathbb{F}_p$*
- *$4p = t^2 + |D|y^2$ has a solution in rational integers.*

Since we wish to construct a curve over $\mathbb{F}_p$ with complex multiplication by an order of discriminant $-D$ the j-invariant of such a curve is an element of a finite field $\mathbb{F}_p$. So for a particular fundamental discriminant $-D$ which satisfies Equation 1.13 we compute $H_{-D}(z)$. Any zero of the irreducible polynomial $H_{-D}(z) \in \mathbb{Z}[z]$ generates $\mathcal{H}_K$ over K and the polynomial $H_{-D}(z) \in \mathbb{F}_p[z]$, splits into linear factors. The roots of $H_{-D}(z)$ in $\mathbb{F}_p$ are the j-invariants of the elliptic curves defined over $\mathbb{F}_p$ having endomorphism ring isomorphic to the ring of integers $\mathfrak{O}_{-D}$ of K. If one of roots to Equation 1.14 is j_0, then we write down the equation as outlined in Lemma 1.5.1. We proceed by checking the order of the curve if it is n. If not, we have constructed a curve with n' points.

However, the running time of CM method is exponential in $\log p$; as such for an efficient implementation D should be small. Due to results of Enge and Sutherland [28], given the current computation power, the method can construct curves over finite fields when $|D| \leq 10^{15}$.

The curves for various j_0 are defined in Lemma 1.5.1 below [9]:

Lemma 1.5.1. *The following hold for elliptic curves $\mathcal{E}/\mathbb{F}_p$.*

- *Every element in $\mathbb{F}_P$ is the j-invariant of an elliptic elliptic curve over $\mathbb{F}_p$.*
- *If $D > 4$ then all elliptic curves with given j-invariant, $j \neq 0$,1728 over $\mathbb{F}_p$ are given by*

$$y^2 = x^3 + 3\mathfrak{y}c^2x + 2\mathfrak{y}c$$

where $\mathfrak{y} = \frac{j_0}{1728 - j_0}$ *and* $c \in \mathbb{F}_p$.

- *Suppose* $\mathcal{E}$ *and* $\mathcal{E}'$ *have the same* j*-invariant but are not isomorphic over* $\mathbb{F}_p$*. If* $j \neq 0$ *or* $j \neq 1728$ *then* $\mathcal{E}'$ *is a quadratic twist of* $\mathcal{E}$ *and if* $\#\mathcal{E} = p + 1 - t$ *then* $\#\mathcal{E}' = p + 1 + t$*.*
- *If* $D \leq 4$ *and* $j = 0$ *or* $j = 1728$*, elliptic curves over* $\mathbb{F}_p$ *are given by:*

$$\begin{aligned} \mathcal{E} : y^2 =& x^3 + B \ \text{ when } \ j = 0 \\ \mathcal{E} : y^2 =& x^3 + Ax \ \text{ when } \ j = 1728 \end{aligned}$$

where A*,* $B \in \mathbb{F}_p^*$*. Furthermore, if* $\#\mathcal{E} \neq p + 1 - t$ *consider cubic, quartic or sextic twist of* $\mathcal{E}$*.*

The method is summerised in Algorithm 1.5.1 and give a toy example in Example 1.5.1 below.

Algorithm 1.5.1: Complex multiplication algorithm

```
For a prime integer $p$, integers $t$ and $D$ satisfying Equation 1.13
    1. Construct the Hilbert class polynomial $H_{-D}(z) \in \mathbb{Z}[z]$ for $-D$.
    2. Find a root $j_0 \in \mathbb{F}_p$ of $H_D(z) \in \mathbb{F}_p[z]$. This is the $j$-invariant of the
       curve to be constructed
    3. Construct the equation of an elliptic curve $\mathcal{E}$ as in Theorem 1.5.1
       with $j_0$.
    4. Check the order of $\mathcal{E}$. If it is not $p + 1 - t$, then consider the twist.
    5. Return $\mathcal{E}$.
```

Example 1.5.1. *For* $D = 19$ *take* $p = 10111019$ *a prime and suppose*

$t = -1760$. *Then the CM Equation 1.13 becomes*

$$\begin{aligned} -19y^2 &= 1760^2 - 4(10111019) \\ y^2 &= 2^2 701^2 \end{aligned}$$

which has the solution $y = 2 \cdot 701$. *It turns out that Hilbert class polynomial* $H_{-D}(z)$ *is as follows:*

$$H_{-D}(z) = z + 884736.$$

Clearly, $H_{-D}(z)$ *has a root* $j_0 = -884736 \equiv 9226283$ *modulo p. Using Theorem 1.5.1 we compute c*

easily. There are two elliptic curves. These are:

$$\begin{aligned} \mathcal{E}_1 &: y^2 = x^3 + 7331964x + 4887976 \\ \mathcal{E}_2 &: y^2 = x^3 + 6789932x + 7304986. \end{aligned}$$

It is easy then to verify that $\mathcal{E}_2$ *is the curve with the right order.*

In the remainder of this thesis we will consider values of D sufficiently small such that corresponding CM curves may be efficiently constructed.

1.6 Addition chains

Addition chains are used to ease computations on powering, by reducing the total number of computations needed to generate such an exponent. In an algorithm for example, in order to compute m^v we would compute intermediate exponents of m first before arriving at the value m^v. The list of these intermediate exponents is what we refer to as an *addition chain*.

We define an addition chain as follows [98]:

Definition 1.6.1. *Let v be a positive integer. An addition chain for v is an increasing sequence $C = c_0, c_1, ..., c_n$, such that c_i is a positive integer for $i \in \{0, 1, 2, \cdots, n\}$ with $c_0 = 1$ and $c_n = v$. Moreover, for each $i > 0$ there exist j and j', $0 < j \leq j' < i$, such that $c_i = c_j + c_{j'}$. The length of C is defined to be n.*

In general, an element c_i in the addition chain relates to computing m^{c_i} in the exponentiation algorithm. The elements c_i in an addition chain reflect the fact that m^{c_i} can only be computed by multiplying to known powers of m.

What does this say? Consider the following chain for example, $(1, 2, 4, 6, 12)$, of length 5. This chain shows that m^{12} can be computed using only 4 multiplications by successively computing

$$\begin{aligned} m^2 &= m.m \\ m^4 &= (m^2)^2 \\ m^6 &= m^4.m^2 \\ m^{12} &= (m^6)^2. \end{aligned}$$

In some instances, such as abelian groups on curves, inversion is relatively cheap [22]. Allowing inversions during the exponentiation routine is relating to taking the additive inverse of an element in the addition chain. Definition 1.6.1 can be adapted to allow subtractions by requiring that for each c_i there exists a pair $j', j < i$ such that either $c_j + c_{j'} = c_i$ or $c_j - c_{j'} = c_i$.

This approach gives rise to so-called *addition-subtraction chains.* The shortest addition- subtraction chain is evidently at most as long as the shortest addition chain.

Finding an addition or addition-subtraction chain of minimal length is a difficult task; the problem is in fact NP-complete [106]. However, there are several techniques to compute relatively short chains. See [44] for a comparison of different algorithms.

1.6.1 Vector addition chain

We finally introduce a vector addition chain. A vector addition chain of given vectors is the shortest list of vectors that minimizes the number of multiplications in multinomial powers $m_0^{c_0} \cdot m_1^{c_1} \cdots m_n^{c_n}$. The property that each intermediate results is a product of powers of the $m_i^{c_i}$ now translates to the property that each term in the corresponding sequence of vectors is the sum of previous terms. To achieve this we use the Olivos' algorithm introduced in [74].

Suppose $C = (c_0, c_1, \cdots, c_n)$ is a shortest addition sequence of length n which we can write as $[c_0, c_1, \cdots, c_n]$. Then in Olivos' algorithm we need to:

- set the initial vectors as unit vectors:
  $[1, 0, 0, \ldots, 0, 0]$, $[0, 1, 0, \ldots, 0, 0]$, $\cdots [0, 0, 0, \ldots, 0, 1]$. That is vectors with a 1 on the ith position for $i \in \{0, 1, \cdots, n\}$ and 0s elsewhere.
- find a subsequent vectors as a linear combination of two preceding vectors by working towards the final vector.
- find the last vector equal the given vector addition sequence, $C = [c_0, c_1, \cdots, c_n]$ as follows:

$$\begin{array}{l}
[1,\quad 0,\cdots,0,\quad 0] \\
[0,\quad 1,\cdots,0,\quad 0] \\
\quad\ddots \\
[0,\quad 0,\cdots,0,\quad 1] \\
\quad\ddots \\
[c_0,\quad c_2,\quad \cdots,\quad c_n]
\end{array}$$

The length of the vector addition chain is the number of vectors after the initial vectors.

We utilize the ideas in this section to develop our contribution in Chapter 5

1.7 Organisation

Our main contribution in this thesis is the construction of new ordinary pairing-friendly elliptic curves and genus two pairing-friendly hyperelliptic curves and their efficient implementation. We aim at constructing curves with a small ρ-value because such curves facilitate a secure and efficient implementation of pairing based cryptography.

In Chapter 2 we introduce elliptic curves and discuss a general framework for constructing pairing-friendly elliptic curves.

In Chapter 3, we construct pairing-friendly elliptic curves using a new approach which generalises the Brezing-Weng method [17]. In addition, we demonstrate our method by giving some interesting cryptographic examples. This work which also appears in [50] is a joint work with Edward Schaefer and Mike Scott.

We turn our attention to the question of constructing two-dimensional abelian varieties in Chapter 4. Here we discuss theoretical foundations on Jacobians of ordinary genus 2 hyperelliptic curves. Furthermore, we present a method of constructing such Jacobians. The method generalises the Kawazoe-Takahashi construction presented in [51]. Using the proposed algorithm we give new cryptographic examples with better ρ-values than previously reported. This work is also reported in [49].

In Chapter 5, we look at implementation issues in pairings. The contents of this chapter result from joint work with Michael Scott, Naomi Benger, Manuel Charlemagne and Luis J. Dominguez Perez which appears in [88] and [87]. Here we present a method for fast multiplication in $\mathbb{G}_2$ and an efficient way of computing the final exponentiation in a pairing. In both optimisations we make use of the polynomial structure of the parameters in the family.

Chapter 2

Pairing-friendly elliptic curves

2.1 Introduction

In this chapter we give a short introduction to elliptic curves defined over finite fields for cryptographic purposes only. In particular, to aid the understanding of the theory and concepts for constructing pairing-friendly elliptic curves. We also discuss some notable constructions of pairing-friendly elliptic curves. This is by no means a complete discussion. For a more systematic treatment of elliptic curves, see [94], [103], [9] [3] and [45] while [32] gives a good collection of strategies for constructing pairing-friendly elliptic curves. We start by looking at elliptic curves.

2.2 Elliptic curves

The following is a definition of an elliptic curve [45]:

Definition 2.2.1. *Let $\mathbb{F}$ be a field. An elliptic curve $\mathcal{E}$ over $\mathbb{F}$ is a smooth* *curve*

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

in so called "long Weierstrass form" where the coefficients a_i lie in $\mathbb{F}$ and the discriminant of $\mathcal{E}, \triangle \not\equiv 0$ in $\mathbb{F}$, where $\triangle$ is defined as:

$$\begin{aligned} \triangle &= -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9dd_2d_4d_6 \quad \text{with} \\ d_2 &= a_1^2 + 4a_2; \\ d_4 &= 2a_4 + a_1a_3; \\ d_6 &= a_3^2 + 4a_6; \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_1a_3^2 - a_4^2; \end{aligned}$$

together with a special point known as the point at infinity, $\mathcal{O}$.

By *smooth* curve, we mean a curve with no singular points, in other words no points where both partial derivatives in x and y vanish. We denote by $\mathcal{E}(\mathbb{F})$ the set of couples $(x, y) \in \mathbb{F}^2$ such that (x, y) are solutions of Equation 2.1 and $\mathcal{E}$ defined over $\mathbb{F}$ by $\mathcal{E}/\mathbb{F}$.

2.2.1 Short Weierstrass form

Consider the following change of variables in Equation 2.1 when the $char(\mathbb{F}) \neq 2, 3$:

$$\begin{aligned} x &= \frac{x - 3a_1^2 - 12a_2}{36}, \\ y &= \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24}. \end{aligned}$$

This transforms Equation 2.1 to the equation of an isomorphic curve of the form:

$$\mathcal{E} : y^2 = x^3 + Ax + B. \tag{2.2}$$

We refer to this simplier form as a *short Weierstrass form.* When using this equation, there is a simple criterion to ensure that the curve in Equation 2.2 has no singular points. That is ascertaining that the curve's discriminant $\Delta = 4A^3 + 27B^2 \neq 0$.

2.2.2 The Group law

We center our discussions on elliptic curves of the form in Equation 2.2, the short Weierstrass form. Elliptic curves are of great use in a number of cryptographic protocols, mainly because it is possible to take two points on such a curve and generate a third point on the same curve. In fact, we will show that by defining an addition operation and introducing an extra point, a point at infinity, the points on the elliptic curve $\mathcal{E}/\mathbb{F}$ generate an additive abelian group. This group can then be used to develop a similar instance of the discrete logarithm problem which is the basis for most public key cryptosystems.

The *chord-and-tangent* rule for adding two points in $\mathcal{E}(\mathbb{F})$ provides $\mathcal{E}(\mathbb{F})$ with the needed abelian structure where the point at infinity $\mathcal{O}$, is the identity element. See [94], [3] and [103]. Figure 2.1 illustrates the group law on an elliptic curve $\mathcal{E}$.

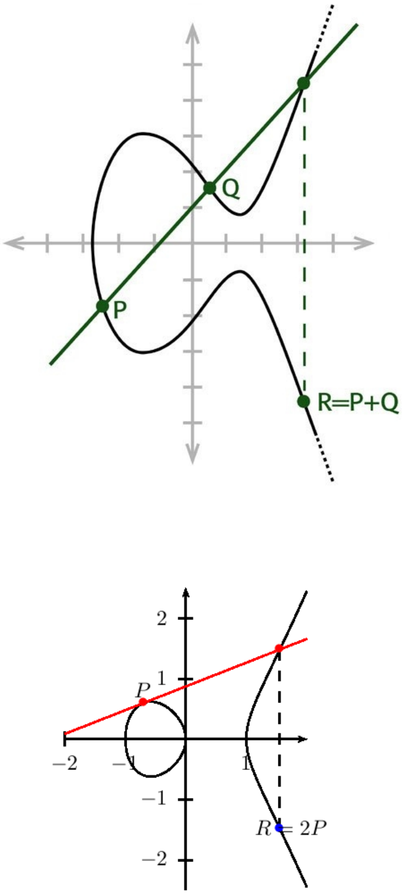

Figure 2.1: *Elliptic curves point additon and doubling.*

To add two points on the curve, say P and Q, one proceeds by drawing a straight line to connect the two points and extending the line so that it intersects the curve at a third point. If points P and Q are not distinct then the straight line is a tangent to the curve $\mathcal{E}$. This third point is $-(P+Q)$. Reflecting $-(P+Q)$ in the x-axis we obtain another rational point $(P+Q)$.

The process is generalised in Theorem 2.2.1 [94]:

Theorem 2.2.1. *Let $\mathcal{E}/\mathbb{F}$ be an elliptic curve given by $y^2 = x^3 + Ax + B$. The chord-tangent method defines an addition on the set $\mathcal{E}(\mathbb{F})$ of $\mathbb{F}$-rational* *points on $\mathcal{E}$; let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on $\mathcal{E}$ with $P, Q \neq \mathcal{O}$. We then define $P + Q = (x_3, y_3)$ as follows:*

a). If $x_1 \neq x_2$ then $x_3 = m^2 - x_1 - x_2$ and $y_3 = m(x_1 - x_3) - y_1$.

where $m = \frac{y_2 - y_1}{x_2 - x_1}$

b). If $x_1 = x_2$ but $y_1 \neq y_2$ then $P + Q = \mathcal{O}$.

c). If $P = Q$ and $y_1 \neq 0$ then $x_3 = m^2 - 2x_1$ and $y_3 = m(x_1 - x_3) - y_1$ where $m = \frac{3x_1^2 + A}{2y_1}$.

d). If $P = Q$ and $y_1 = 0$, then $P + Q = \mathcal{O}$ Also we define $P + \mathcal{O} = P$ for all points P on $\mathcal{E}$.

This addition law can be shown to be *commutative* and *associative*, effectively making $(\mathcal{E}(\mathbb{F}), +)$ an abelian group. Theorem 2.2.2 describes these properties.

Theorem 2.2.2 ([103], Theorem 2.1 page 15)**.** *The addition of points on an elliptic curve $\mathcal{E}$ defined over a field $\mathbb{F}$ satisfies the following properties:*

1. *commutativity: $P + Q = Q + P$ for all P, Q on $\mathcal{E}$*

2. *existence of identity: $P + \mathcal{O} = P$ for all points P on $\mathcal{E}$.*

3. *existence of inverse: Given P on $\mathcal{E}$, there exists P' on $\mathcal{E}$ such that $P + P' = \mathcal{O}$. This point P', is usually denoted by $-P$.*

4. *associativity: $(P + Q) + R = P + (Q + R)$ for all P, Q, R on $\mathcal{E}$*

In other words, the points on $\mathcal{E}$ form an abelian group with $\mathcal{O}$ as the identity element.

Proof. For proofs of these properties, we refer to [103] or [94]. □

2.2.3 The order of the curve

If $\mathbb{F}$ is a finite field say, $\mathbb{F}_p$, then the total number of points on $\mathcal{E}$, denoted by $\#\mathcal{E}(\mathbb{F}_p)$, is described by the bound known as *Hasse's theorem* stated below. The proof of the theorem can be found in [94] or [103].

Theorem 2.2.3. *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{F}_p$. Then $(\sqrt{p}-1)^2 \leq \#\mathcal{E}(\mathbb{F}_p) \leq (\sqrt{p}+1)^2$.*

In other words, since $2\sqrt{p}$ is small with regard to p then the theorem is stating that the number of points on the elliptic curve has roughly as many elements as $\mathbb{F}_p$ itself.

The following simple example is an illustration of an abelian group on elliptic curves using some of the basic built-in Magma commands for elliptic curves.

Example 2.2.1. *The following example shows the structure of a cyclic group on elliptic curves.*

```
>p:=373;
> F_p:=GF(p);              //finite field
> E:=EllipticCurve([F_p|0,6]);
> E;             // Gives the details on the elliptic curve
Elliptic Curve defined by y^2 = x^3 + 6 over GF(373)
>  #E;         // Number of points in E(F_373)
349
>  IsCyclic(AbelianGroup(E));
true
> Generators(E);      // Points that would generate all other
    points in E(F_p)
[ (90 : 263 : 1) ]
> E!0;   // Point at infinity
(0 : 1 : 0)
> P:=E![90,263,1];  // Sets P equal to the point [90:263:1] in
     E(F_373)
> P+P;
(263 : 60 : 1)
> 2*P;
```

```
(263 : 60 : 1)
> -P;             // Computes the inverse of P
(90 : 110 : 1)
> Order(P);        // Computes the order of P
349
> for i in [1..Order(P)] do // Generating all points in E(F_p)
for> print(i*P);
for> end for;
(90 : 263 : 1)
(263 : 60 : 1)
(307 : 52 : 1)
...
...
...
(263 : 313 : 1)
(90 : 110 : 1)
(0 : 1 : 0)
```

We also consider the same equation defined over some extension of $\mathbb{F}_p$, say $\mathbb{F}_{p^e}$, for some positive integer e. It is worth mentioning here that in this case we still require A, B to remain in $\mathbb{F}_p$. In fact, if $\mathcal{E}/\mathbb{F}_p$ then $\mathcal{E}$ is also defined over any extension $\mathbb{F}_{p^e}$ of $\mathbb{F}_p$ and the group $\mathcal{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points is a subgroup of the group $\mathcal{E}(\mathbb{F}_{p^e})$ of $\mathbb{F}_{p^e}$-rational points. Consequently, if $\#\mathcal{E}(\mathbb{F}_p)$ is known then $\#\mathcal{E}(\mathbb{F}_{p^e})$ is characterised as follows:

Theorem 2.2.4 ([45], Theorem 3.11 page 83)**.** *Let $\#\mathcal{E}(\mathbb{F}_p) = p + 1 - t$. Let β and $\bar{\beta}$ be the roots of the trinomial $z^2 - tz + p$, we can then write $z^2 - tz + p = (z - \beta)(z - \bar{\beta})$. Then, for all integers $e > 1$, we have $\#\mathcal{E}(\mathbb{F}_{p^e}) = p^e + 1 - (\beta^e + \bar{\beta}^e)$.*

Here $(\beta^e + \bar{\beta}^e)$ can be computed using the Lucas sequence $\{S_e\}$ [11] where we define

$$\begin{aligned} S_0 &= 2 \\ S_1 &= \beta + \bar{\beta} = t \end{aligned}$$

and then define recursively

$$S_e = S_1 S_{e-1} - p S_{e-2}$$

and have

$$\#\mathcal{E}(\mathbb{F}_{p^e}) = p^e + 1 \pm S_e.$$

We use Example 2.2.1 to demonstrate this in Magma:

Example 2.2.2. *Compute $\#\mathcal{E}(\mathbb{F}_{p^2})$ in Example 2.2.1*

```
> p:=373;
> F_p:=GF(p);
> E:=EllipticCurve([F_p|0,6]);
> E;
Elliptic Curve defined by y^2 = x^3 + 6 over GF(373)
> #E;
349
> t:=#E-(p+1);
> F_p2:=GF(p^2);
> E2:=EllipticCurve([F_p2|0,6]);
> E2;
Elliptic Curve defined by y^2 = x^3 + 6 over GF(373^2)
> S_0:=2;
> S_1:=t;
> S_2:=S_1*S_1-p*S_0;
> EF_p2:=p^2+1-S_2;
> EF_p2;
139251
> EF_p2 eq #E2;
true
```

2.2.4 Curve endomorphisms

Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{F}_q$. The set of all points on $\mathcal{E}$ whose coordinates are elements of any finite extension of $\mathbb{F}_q$ is also denoted by $\mathcal{E}$.

Endomorphism ϕ of $\mathcal{E}/\mathbb{F}_q$ is a rational map :

$$\phi : \mathcal{E} \to \mathcal{E}$$

such that $\phi(\mathcal{O}) = \mathcal{O}$ and $\phi(Q) = (g(Q), g'(Q))$ for some rational functions g and g' whose coefficients lie in $\mathbb{F}_q$ and for all $Q \in \mathcal{E}$. The set of all endomorphism of $\mathcal{E}/\mathbb{F}_q$, denoted by $End(\mathcal{E})$, forms a ring under addition and multiplication, which is referred to as the endomorphism ring of $\mathcal{E}/\mathbb{F}_q$.

An endomorphism is also a group homomorphism i.e

$$\phi(Q + Q') = \phi(Q) + \phi(Q') \tag{2.3}$$

for all $Q, Q' \in \mathcal{E}(\mathbb{F}_q)$.

The characteristic polynomial of an endomorphism ϕ is defined to be the monic polynomial $f(z) \in \mathbb{Z}[z]$ of least degree, such that $f(\phi)Q = \mathcal{O}$ for all $Q \in \mathcal{E}$. If $\mathcal{E}/\mathbb{F}_q$ is non-supersingular curve then the degree $f(z)$ is equal to 1 or 2 [45].

The qth-power Frobenius map, on an elliptic curve $\mathcal{E}/\mathbb{F}_q$ defined as:

$$\phi_q = \begin{cases} \mathcal{E}(\bar{\mathbb{F}_q}) & \to \mathcal{E}(\bar{\mathbb{F}_q}) \\ (x, y) & \mapsto (x^q, y^q) \\ \mathcal{O} & \mapsto \mathcal{O} \end{cases} \tag{2.4}$$

is a special endomorphism of an elliptic curve $\mathcal{E}/\mathbb{F}_q$ known as *Frobenius endomorphism.* The map ϕ_q, maps points on $\mathcal{E}$ to points on $\mathcal{E}$ and respects the group law.

It follows from Theorem 2.2.3 that the characteristic polynomial of ϕ_q is given by:

$$z^2 - tz + q \tag{2.5}$$

where $t = q + 1 - \#\mathcal{E}(\mathbb{F}_q)$ is the trace of the Frobenius, ϕ_q, see [45] and [94] for more details.

The Trace of Frobenius otherwise known as the *trace* reveals other structures of the curve related to the type and cryptographic relevance of the curve.

Definition 2.2.2. *Let p be a prime. An elliptic curve $\mathcal{E}/\mathbb{F}_p$ is supersingular curve if $p|t$, where t is the trace. If gcd $(p, t) = 1$, then $\mathcal{E}$ is an ordinary curve.*

Menezes, Okamoto and Vanstone [63] showed that for supersingular elliptic curves their embedding degree, k, is always less than or equal to 6. These are popular for the bilinear cryptographic protocols, as it is easy to implement $\mathbb{F}_{p^k}$ when k is small.

However, with the MOV-attack [63] and Frey-Rück attack [35] shows that supersingular elliptic curves are weak for cryptographic purposes because of their low embedding degree. The interest then is to construct ordinary pairing-friendly elliptic curves with higher embedding degree than the supersingular curves.

2.3 Twists of curves

One of the optimisations in implementing pairings on ordinary pairing-friendly curves, is to place one of the inputs to the pairing on the curve, $\mathcal{E}/\mathbb{F}_p$, and the other on a twisted curve, $\mathcal{E}'/\mathbb{F}_{p^e}$, where there exists a group of points of order r which is isomorphic to a group of points on the curve defined over the full k-th extension of the base field.

Definition 2.3.1 ([94]). *Let $\mathcal{E}/\mathbb{F}_p$ with be an elliptic curve that has embedding degree $k > 1$ with respect to prime r. Then $\mathcal{E}'$ is said to be a twist of $\mathcal{E}$ of degree d if there exists an isomorphism $\eta_d : \mathcal{E}' \to \mathcal{E}$ defined over $\mathbb{F}_{p^d}$ with d minimal.*

Let $\mathcal{E}'$ be a twist of $\mathcal{E}$ of degree d such that $r|\#\mathcal{E}'(\mathbb{F}_{p^e})$ for some $d|k$ and $e.d = k$. If d is less than k, we can define $\mathbb{G}_2$ to be the unique subgroup of order r on $\mathcal{E}'/\mathbb{F}_{p^e}$.

The degree d-twist of a curve can always be 2 if k is even. This is known as a *quadratic twist*. Moreover, k being even has other advantages as it enables the denominator elimination optimization in pairing computation [6].

If a pairing-friendly elliptic curve has CM discriminant $D = 4$ and $4|k$ quartic twists can then be applied. Thus we can choose $e = k/4$. While if the CM discriminant of the curve is 3 and $6|k$ then we can choose $e = k/6$ and in a such a case we say that the sextic twist exists.

Clearly, in these cases in a bilinear map e, see to Definition 1.2.1, we would define our points in $\mathbb{G}_2$ on a rather smaller finite field than originally expected and hence easier to manipulate the points. This choice of an input in pairing computation reduces the running time of the algorithms because we can avoid full $\mathbb{F}_{p^k}$ arithmetic to compute the line functions in Miller's algorithm (see later in Chapter 5).

Twisted curves of $\mathcal{E}$ for various choices of d are described in Table 2.1. Here δ is an element of $\mathbb{F}_q^*$, the choice of which result in a curve easily mapped to the original, while other choices lead to either a quadratic, or quartic or sextic twists. The details for the theoretical description of twists can be obtained from [94] and [46].

Since it is only when considered over a full extension $\mathbb{F}_{p^k}$ that a curve supports bilinearity, we need to map the points from the twisted curve back to the original curve. This mapping is shown in column 4 of Table 2.1 which is required for the line function evaluation in the computation of the pairing.

Table 2.1: *Structures and maps of twist curves*

d	Curve equation	Twist curve equation $\mathcal{E}'$	$\mathcal{E}' \mapsto \mathcal{E}$
2	$y^2 = x^3 + Ax + B$	$y^2 = x^3 + \frac{A}{\delta^2}x + \frac{B}{\delta^3}$	$(x, y) \mapsto (\delta x, \delta^{3/2}y)$
4	$y^2 = x^3 + Ax$	$y^2 = x^3 + \frac{A}{\delta}x$	$(x, y) \mapsto (\delta^{1/2}x, \delta^{3/4}y)$
6	$y^2 = x^3 + B$	$y^2 = x^3 + \frac{B}{\delta}$ or $y^2 = x^3 + \frac{B}{\delta^3}$	$(x, y) \mapsto (\delta^{1/3}x, \delta^{1/2}y)$

Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{F}_q$ with $q = p^e$. To compute the order of the twist curve, $\#\mathcal{E}'(\mathbb{F}_q)$, we may apply Theorem 2.2.4. Nevertheless, the next result, proved in [46], determines the possible values of $\#\mathcal{E}(\mathbb{F}_q)$ as $\mathcal{E}$ varies over all elliptic curves defined over $\mathbb{F}_q$ where $q = p^e$ [46].

Proposition 2.3.1. *Let $\mathcal{E}/\mathbb{F}_q$ be an elliptic curve with $\#\mathcal{E} = q + 1 - t$, admitting a twist $\mathcal{E}'$ of degree d. Then the possible group orders of $\mathcal{E}'(\mathbb{F}_q)$ are given by the following:*

$$\begin{aligned}
d = 2: \quad & \#\mathcal{E}'(\mathbb{F}_q) = q + 1 + t; \\
d = 3: \quad & \#\mathcal{E}'(\mathbb{F}_q) = q + 1 - (3T - t)/2 \quad \text{with } T = \pm\sqrt{\frac{t^2 - 4q}{-3}} \\
& \#\mathcal{E}'(\mathbb{F}_q) = q + 1 - (-3T - t)/2 \quad \text{with } T = \pm\sqrt{\frac{t^2 - 4q}{-3}}; \\
d = 4: \quad & \#\mathcal{E}'(\mathbb{F}_q) = q + 1 + T \quad \text{with } T = \pm\sqrt{t^2 - 4q} \\
& \#\mathcal{E}'(\mathbb{F}_q) = q + 1 - T \quad \text{with } T = \pm\sqrt{t^2 - 4q}; \\
d = 6: \quad & \#\mathcal{E}'(\mathbb{F}_q) = q + 1 - (-3T + t)/2 \quad \text{with } T = \pm\sqrt{\frac{t^2 - 4q}{-3}} \\
& \#\mathcal{E}'(\mathbb{F}_q) = q + 1 - (3T + t)/2 \quad \text{with } T = \pm\sqrt{\frac{t^2 - 4q}{-3}}.
\end{aligned}$$

2.4 Torsion points

Torsion points are points in $\mathcal{E}$ whose orders are finite. Let $\mathcal{E}/\mathbb{F}_p$ be an elliptic curve, let the algebraic closure of $\mathbb{F}_p$ be denoted by $\bar{\mathbb{F}_p}$ and let $r \in \mathbb{Z}_{>0}$ and $P \in \mathcal{E}(\mathbb{F}_p)$ and denote $\overbrace{P + P + ... + P}^{r}$ by $[r]P$. For a given r we define a subgroup of r-torsion points in $\mathcal{E}(\mathbb{F}_p)$ by:

$$\mathcal{E}[r] = \{P \in \mathcal{E}(\bar{\mathbb{F}}_p) | [r]P = \mathcal{O}\}.$$

This group acts as the kernel of the multiplication by r endomorphism. If p and r are co-prime, then $\mathcal{E}[r]$ is isomorphic to $\mathbb{Z}_r \times \mathbb{Z}_r$. This means that $\mathcal{E}[r]$ has r^2 elements but no element of order r^2. This case where p and r are relatively prime will be of particular interest to construct the pairings. In particular, the group $\mathbb{G}_1$ is an r-torsion subgroup of $\mathcal{E}(\mathbb{F}_p)$ of order r with $\mathcal{O}$ the identity element of the group. Furthermore, to avoid degeneracy in the Tate pairing and its variants, $\mathbb{G}_2$ must be different from $\mathbb{G}_1$, thus we chose $\mathbb{G}_2$ as a r-torsion subgroup of $\mathcal{E}(\mathbb{F}_{p^k})$ and $\mathbb{G}_T$ would correspond to μ_r, the group of rth-roots of the unity in $\mathbb{F}^*_{p^k}$, defined as follows

$$\mu_r = \{\tau \in \mathbb{F}^*_{p^k} | \, \tau^r = 1\}. \tag{2.6}$$

2.5 Constructing pairing-friendly elliptic curves

To construct suitable ordinary pairing-friendly elliptic curves with embedding degree k, discriminant D, and efficiently computable pairings we look for integer values that satisfy the following:

- p a prime, that defines the size of the finite field over which our hypothetical curve will be defined;
- r a prime, that defines the size of the cryptographic group and the

largest prime factor of $\#\mathcal{E} = p + 1 - t$ such that $r | p^k - 1$;

- t an integer such that $\gcd(p, t) = 1$, and $t \leq 2\sqrt{p}$, t is defined to be the trace of Frobenius endomorphism of the curve such that the curve has $p + 1 - t$ points and $\Phi_k(t - 1) \equiv 0$ modulo r;
- for some sufficiently small integer $D > 0$ and some integer y, we have $4p - t^2 = Dy^2$.

If the degree of the class polynomial $H_{-D}(z)$ is not too large, for such a triple (t, r, p), we can construct an elliptic curve $\mathcal{E}/\mathbb{F}_p$ with a prime order subgroup of size r, embedding degree k and CM discriminant D using the CM method.

Considering the above facts in polynomial context, we would like to parameterize t, r, p as polynomials $t(z)$, $r(z)$, $p(z)$. With Definition 1.4.2 and Conjectures 1.4.1 and 1.4.2 in mind, a family of pairing-friendly elliptic curves in this context are defined as [32]:

Definition 2.5.1. *Let $t(z)$, $r(z)$, and $p(z)$ be polynomials with rational coefficients. For a given positive integer k and a positive integer D, the triple $(t(z), r(z), p(z))$ represents a family of elliptic curves with embedding degree k and CM discriminant D if the following conditions are satisfied:*

a. $p(z)$ represents primes.

b. $r(z)$ represents primes.

c. $t(z)$ represents integers.

d. $r(z)$ divides $p(z) + 1 - t(z)$.

e. $r(z)$ divides $\Phi_k(t(z) - 1)$, where Φ_k is the kth cyclotomic polynomial.

f. $Dy^2 = 4p(z) - t(z)^2$ for some positive integer D and some integer y.

In Definition 2.5.1, part $d.$ says that the curve has a large prime order subgroup of size r while part $e.$, using Lemma 1.4.1, ensures that the curve has embedding degree k. Moreover, by Equation 1.13, the last condition ensures that there exists an ordinary elliptic curve defined over $\mathbb{F}_{p(z)}$ with trace $t(z)$ by the CM method. This is done by finding integer solutions to the CM Equation:

$$Dy^2 = 4p(z) - t(z)^2 = 4h(z)r(z) - (t(z) - 2)^2. \tag{2.7}$$

The ρ-value of such a family of curves is defined to be:

Definition 2.5.2 ([32]). *Let $t(z), r(z), p(z) \in \mathbb{Q}[z]$, and suppose $(t(z), r(z), p(z))$ represents a family of elliptic curves with embedding degree k. The ρ-value of the family $(t(z), r(z), p(z))$ is given by $\rho = lim_{z\to\infty} \frac{\log(p(z))}{\log(r(z))} = \frac{\deg(p(z))}{\deg(r(z))}$.*

2.6 Some constructions

The problem of constructing pairing-friendly elliptic curves has been studied by several researchers. The difference has been the construction of individual curves or a family of curves. Here we recall some notable constructions. For a thorough discussion of different constructions with many examples refer to [32].

2.6.1 The Cocks-Pinch method

One of the earliest methods of constructing ordinary pairing-friendly elliptic curves with arbitrary embedding degree k was proposed by Cocks and Pinch. This method, otherwise known as the CP method in this thesis, constructs individual curves. As observed in [32], the size of the field p is approximately equal to the square of the size of the prime order subgroup i.e

r^2. This characterises the Cocks-Pinch curves with the ρ-value of approximately 2 and hence results into slower implementation compared to curves with ρ-value closer to 1.

However, Cocks and Pinch curves are easy to generate and in constructing the curves one chooses the size of the prime subgroup of size r. Moreover, the method was later generalized to produce families of pairing-friendly elliptic curves with arbitrary embedding degree k with better ρ-values. Furthermore, Freeman [30] and Freeman, Stevenhagen and Streng [33] used the same approach to construct abelian varieties of higher dimensions.

The algorithm for constructing Cocks-Pinch curves is as follows [32]:

Algorithm 2.6.1: Cocks-Pinch pairing-friendly elliptic curves

```
Fix a positive integer $k$ and positive square-free integer $\mathfrak{d}$. Execute
the following steps:

    1. Let $r$ be a prime such that $k$ divides $r - 1$ and $(\frac{-\mathfrak{d}}{r}) = 1$.

    2. Let $z$ be a primitive $k$th root of unity in $(\mathbb{Z}/\mathbb{Z}_r)^\times$. (Such a $z$ exists
       since $k|r - 1$)
       Let $t' = z + 1$.

    3. Let $y' = (t' - 2)/\sqrt{-\mathfrak{d}} \bmod r$.

    4. Let $t \in \mathbb{Z}$ be congruent to $t'$ mod $r$ and let $y \in \mathbb{Z}$ be congruent to $y'$
       mod $r$.

    5. Let $p = (t^2 + \mathfrak{d}y^2)/4$ for some integer $y$.
```

If p is prime, then we construct an elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_p$ with a prime order subgroup of size r, and embedding degree k by CM method.

The approach in Algorithm 2.6.1 is to choose r for a particular embedding degree k, a discriminant $\mathfrak{d}$ and then try to find the trace of the

Frobenius t and the prime size of the field p such that CM norm Equation 1.13 is satisfied.

2.6.2 Dupont-Enge-Morain method

The Dupont-Enge-Morain method [26] is similar to the CP method. The only difference being the approach of constructing the prime subgroup of order r. In this method the authors use resultants to compute r and t simultaneously and then p such that the CM equation is satisfied.

The algorithm for constructing Dupont-Enge-Morain curves is as follows:

Algorithm 2.6.2: Dupont-Enge-Morain pairing-friendly elliptic curves

```
Fix a positive integer $k$. Execute the following steps:
    1. Compute the resultant $R(e) = Res_z(\Phi_k(z-1), e + (z-2)^2)$
    2. Choose $e$ such that $R(e)$ has a large prime factor $r$.
    3. Compute $g(z) = \gcd(\Phi_k(z-1), e + (z-2)^2) \in \mathbb{F}_r[z]$.
    4. Let $t'$ be a root of $g(z)$ modulo $r$.
    5. Let $t \in \mathbb{Z}$ be a unique lift of $t'$ to $(0, r]$.
    6. Let $p = \frac{(e+t^2)}{4}$.
```

If p is a prime integer, use the CM method to construct an elliptic curve defined over $\mathbb{F}_p$ with a prime order subgroup of size r. This method can be used to generate curves of arbitrary embedding degree k. However, the ρ-value of these curves is again around 2 as for the CP curves.

2.6.3 Miyaji-Nakamula-Takano method

The first polynomial families of parameters for ordinary pairing-friendly elliptic curves were proposed by Miyaji, Nakabayashi and Takano [69] for embedding degrees, $k = 3, 4$ and 6. In this Section we present a general idea of the construction.

The following conditions must be satisfied to construct MNT curves:

$$\begin{aligned} \Phi_k(t-1) &= e \cdot r; \\ h.r &= p + 1 - t; \\ Dy^2 &= 4p - t^2; \\ |t| &\leq 2\sqrt{p}; \end{aligned}$$

where $\Phi_k(\cdot)$ is the k-the cyclotomic polynomial, r and p are primes, and h is called the cofactor and D is the discriminant of the curve. Substituting the first and second equations in the third we get:

$$Dy^2 = 4h\frac{\Phi_k(t-1)}{e} - (t-2)^2. \tag{2.8}$$

The challenge has been to find integer solutions to Equation 2.8 for small D and arbitrary y.

Originally in [69] authors only considered cases for which $h = e = 1$. However, the method is extended by Scott and Barreto in [86] by considering the values of $h \in \{2, 3, 4, 5\}$ and $e > 1$. With such approach more suitable ordinary pairing-friendly curves of MNT-type are found for $k = 3, 4$ and 6.

Theorem 2.6.1 below describes the MNT curves.

Theorem 2.6.1 ([69]). *Let p be a prime and let $\mathcal{E}$ be an ordinary elliptic curve defined over a finite field $\mathbb{F}_p$ such that r is prime. Let $t = p + 1 - r$.*

1) Suppose $p > 64$. $\mathcal{E}$ has embedding degree $k = 3$ if and only if there exists $z \in \mathbb{Z}$ such that $t = -1 \pm 6z$ and $p = 12z^2 - 1$.

2) Suppose $p > 36$. $\mathcal{E}$ has embedding degree $k = 4$ if and only if there exists $z \in \mathbb{Z}$ such that $t = -z$ or $t = z + 1$ and $p = z^2 + z + 1$.

3) Suppose $p > 64$. $\mathcal{E}$ has embedding degree $k = 6$ if and only if there exists $z \in \mathbb{Z}$ such that $t = -1 \pm 2z$ or and $p = 4z^2 + 1$.

Proof. We show for the case of $k = 3$. For the other cases refer to [69].

First, consider the conditions for the embedding degree k, refer to Lemma 1.4.1. The condition $\Phi_k(p) \equiv 0 \pmod r$ becomes

$$\Phi_3(p) = p^2 + p + 1 = e \cdot r \text{ with } e \in \mathbb{Z} \tag{2.9}$$

$$\tag{2.10}$$

Setting the order of the cuve as:

$$n = p + 1 - t$$

we can factor Equation 2.9 as

$$(p + 1 - t)(p + 1 + t - e) = p - t^2. \tag{2.11}$$

Using the Hasse-Weil bound (i.e. $|t| \leq 2\sqrt{p}$) the problem reduce to the following cases:

$$-3 \leq (1 + \frac{1}{p} + \frac{t}{p})(p + 1 + t - e) \leq 1.$$

Assuming $p > 64$, $(1 + \frac{1}{p} + \frac{t}{p})$ turns to 1 and hence it is enough to solve for the following cases:

$$(p+1+t-e) = -3,\ -2,\ -1,\ 0,\ 1.$$

Substituting the values of $(p+1+t-e)$ into Equation 2.11 we can show that $\{-2, 0\}$ is the only possible set of values. Then $(t, p) = (-1 \pm 6z, 12z^2 - 1)$ or $(\pm\sqrt{z}, z)$ for $z \in \mathbb{Z}$.

Working backwards finishes the proof for 'and only if' part. □

To construct MNT curves, we need to solve the complex multiplication equation. To do this we need to transform the equations in Theorem 2.6.1 into generalized Pell equations.

By linear change of variables the CM equation $Dy^2 = 4p(z) - t(z)^2$ transforms into a generalised Pell equation of the form $z'^2 - SDy^2 = m$. The cases for each embedding degree in MNT curves are as follows:

- $k = 3$, setting $z' = 6z \pm 3$ we get $z'^2 - 3Dy^2 = 24$;
- $k = 4$, setting $z' = 3z + 2$ when $t = -z$ or $z' = 3z + 1$ if $t = z + 1$ we get $z'^2 - 3Dy^2 = -8$;
- $k = 6$, setting $z' = 6z \mp 1$ we get $z'^2 - 3Dy^2 = -8$.

2.6.4 Barreto-Naehrig construction

Galbraith, McKee and Valença [38] studied the factorisation of $\Phi_k(u(z))$ for $k \in \{5, 8, 10, 12\}$ with $u(z)$ as a quadratic polynomial. They noted that if $u(z) - \zeta_k = 0$ has a solution in $\mathbb{Q}(\zeta_k)$ then $\Phi_k(u(z))$ factors into two irreducible polynomials, where the degree of each of the irreducible factors is a multiple of $\varphi(k)$.

For $k = 12$, the goal in this construction is to choose $t(z)$ and define $r(z)$

as one of irreducible factors of $\Phi_{12}(t(z)-1)$ such that $f(z) = 4r(z) - (t(z) - 2)^2$ has multiple roots.

By constructing $K \cong \mathbb{Q}[z]/r(z)$ and mapping ζ_{12} to $6z^2$ in K, Barreto and Naehrig [8] found the following family of $k = 12$ curves:

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

For values $z_0 \in \mathbb{Z}$ for which $r(z)$ and $p(z)$ represents primes the triple $(t(z), r(z), p(z))$ parameterizes a family of curves of embedding degree 12. The ρ-value of this family is equal to 1 and has a complex multiplication discriminant equal to -3. BN curves are not rare; that is, it is easy to specify the bit size of r by selecting appropriate size of $z_0 \in \mathbb{Z}$ until both $r(z_0)$ and $p(z_0)$ are prime. The desired elliptic curve can then be generated using the CM method.

2.6.5 Freeman construction

Using the idea of Galbraith, McKee and Valença [38] for factorisation of $\Phi_k(u(z))$ for $k = 10$ and a technique from the MNT construction for solving the complex multiplication equation, Freeman [29] constructed a family of pairing friendly curves of embedding degree, $k = 10$. Even though it is highly unlikely that the right hand side of Equation 2.7 reduces to a quadratic for $\varphi(k) > 2$, Freeman discovered such a curve when $\varphi(k) = 4$. The parameters are as follows:

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

In this case $Dy^2 = 15z^2 + 10z + 3$ and by linear change of variables $z' = 15z + 5$, the generalised Pell equation reduces to $z'^2 - 15Dy^2 = -20$.

2.6.6 Brezing-Weng method

The Brezing-Weng method, first introduced in [17], is a construction that uses the Cocks and Pinch idea over polynomials to construct near ideal pairing-friendly elliptic curves for a general embedding degree, k. This means that in order to obtain the families they parametrize t, r, p as polynomials $t(z)$, $r(z)$, $p(z)$.

Brezing and Weng used the cyclotomic fields to generate examples of pairing-friendly elliptic curves. Algorithm 2.6.3 summarises the Brezeng-Weng construction.

Algorithm 2.6.3: [[32]]Brezing-Weng algorithm for finding pairing-friendly elliptic curves

For a fixed positive integer k and positive square-free integer $\mathfrak{d}$, execute the following steps:

1. *Choose a number field K containing $\sqrt{-\mathfrak{d}}$ and a primitive kth root of unity ζ_k.*

2. *Find an irreducible (but not necessarily monic) polynomial $r(z) \in \mathbb{Z}[z]$ such that $\mathbb{Q}[z]/r(z) \cong K$.*

3. *Let $t(z) \in \mathbb{Q}[z]$ be a polynomial mapping to $\zeta_k + 1 \in K$.*

4. *Let $y(z) \in \mathbb{Q}[z]$ be a polynomial mapping to $\frac{\zeta_k - 1}{\sqrt{-\mathfrak{d}}} \in K$.*

5. *Let $p(z) = (t(z)^2 + \mathfrak{d}y(z)^2)/4 \in \mathbb{Q}[z]$.*

If $p(z)$ and $r(z)$ represent primes and $t(z)$ represents integers then the triple $(t(z), r(z), p(z))$ represents a family of curves with embedding degree k and discriminant $-\mathfrak{d}$. The ρ-value of this family is defined by $\rho = \frac{\mathrm{deg(p(z))}}{\mathrm{deg(r(z))}}$.

When working modulo an irreducible polynomial, the power of a field element will be a polynomial of degree *at least one less* than that of the irreducible polynomial. In some instances it may even be much less than this. In Brezing and Weng curves this instance occurs and curves constructed with this method have a ρ-value much less than 2, and closer to 1, unlike the Cocks-Pinch method.

Furthermore, this method is favourable when the complex multiplication discriminant is -4 or -3. In [32], the authors extend the method to find more curves with complex multiplication discriminant equal to -8.

All in all, in the next chapter we utilize this construction by defining K

to be generated by other elements rather than ζ_k. With this approach we find that we construct more curves with interesting properties.

Chapter 3

New construction of pairing-friendly elliptic curves

3.1 Introduction

In this chapter we construct new pairing-friendly elliptic curves by the Brezing-Weng method presented in Chapter 2 Section 2.6.6. Our approach is to define a number field K, to be generated by elements of the cyclotomic field which are a linear combination of a power basis with integer coefficients.

The results reported here also appears in [50].

3.2 Outline of our Algorithm

In our construction, for a particular embedding degree k and a complex multiplication discriminant D, we look for a set of polynomials $(t(z), \tilde{r}(z)/e, p(z))$ with e some integer and $t(z)$ defines the trace, $\tilde{r}(z)/e$ defines the prime size of the cryptographic group and $p(z)$ defines the field in which the elliptic curve is defined. The idea here is to allow some small integer factor e when searching for a prime size of the cryptographic group. That is; if for some case $\tilde{r}(z)$ does not represent primes then we can divide by some integer e such that the quotient is a prime. This means we can represent the order of the curve as follows:

$$\tilde{r}(z)c'(z) = p(z) + 1 - t(z) \tag{3.1}$$

where $\tilde{r}(z) = e.r(z)$ with $e.c'(z) = c(z)$ referred to as the cofactor and $r(z)$ representing primes. Combining Equation 3.1 and complex multiplication Equation 1.13 in polynomial terms we get:

$$\begin{aligned} Dy(z)^2 &= 4p(z) - t(z)^2 && (3.2)\\ &= 4\tilde{r}(z)c'(z) - (t(z) - 2)^2 && (3.3)\\ &= 4r(z)c(z) - (t(z) - 2)^2. && (3.4) \end{aligned}$$

Instead of using a cyclotomic polynomial to define the number field we use minimal polynomials of the elements $\gamma(\zeta_\ell)$ of the cyclotomic field, $\mathbb{Q}(\zeta_\ell)$, with ℓ some multiple of the embedding degree k.

Elements of $\mathbb{Q}(\zeta_\ell)$ are easily represented as polynomials of degree less than $\varphi(\ell)$ with integer coefficients. Here we consider $\gamma(\zeta_\ell)$ to be of the form:

$$\gamma(\zeta_\ell) = \sum_{i=0}^{\varphi(\ell)-1} a_i \zeta_\ell^i \tag{3.5}$$

where $a_i \in \mathbb{Z}$ and ζ_ℓ is ℓ-th primitive root of unity.

For practical reasons we let a_i lie in some integer interval say, $[\mathcal{L}, -\mathcal{L}]$ and allow a maximum of $\mathcal{M}$ non-zero coefficients in $\gamma(\zeta_\ell)$.

If the element, $\gamma(\zeta_\ell)$, is in $\mathbb{Q}(\zeta_\ell)$ but not in any proper subfield then we find the minimal polynomial of $\gamma(\zeta_\ell)$ in $\mathbb{Q}(\zeta_\ell)$ which we set as $\tilde{r}(z)$. Otherwise, we know $\gamma(\zeta_\ell)$ gives a minimal polynomial whose degree is less than $\varphi(\ell)$. We proceed by using the Brezing-Weng construction to look for pairing-friendly elliptic curves, with predefined k and D.

3.2.1 Finding $\tilde{r}(z)$

Now suppose $\gamma(\zeta_\ell)$ is not in any proper subfield. Then we know that the degree of its minimal polynomial $\tilde{r}(z)$, is $\varphi(\ell)$. This is so because $[\mathbb{Q}(\zeta_\ell) : \mathbb{Q}] = \varphi(\ell)$ [102]. In addition, since $\tilde{r}(\gamma(\zeta_\ell)) = 0$, then we can compute $\tilde{r}(z)$ explicitly using the following equation:

$$\tilde{r}(z) = \prod_{i=1}^{\varphi(\ell)} (z - \gamma_i(\zeta_\ell)) \tag{3.6}$$

where $\gamma_i(\zeta_\ell)$ are the conjugates of $\gamma(\zeta_\ell)$.

In Example 3.2.1 we demonstrate the computation of a minimal polynomial for $\ell = 8$.

Example 3.2.1. *Let $\ell = 8$. Consider $\gamma(\zeta_8) = \zeta_8 - 2\zeta_8^3 \in \mathbb{Q}(\zeta_8)$. Since $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \varphi(8) = 4$ and $\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \in \mathbb{Q}(\zeta_8)$ then*

$$\zeta_8 - 2\zeta_8^3 = 3\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$$

and Equation 3.6 becomes:

$$\begin{aligned} \tilde{r}(z) &= (z - (3\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}))(z - (3\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})) \\ &\times (z - (-3\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}))(z - (-3\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})) \end{aligned}$$

$$\begin{aligned}
&= ((z-3\frac{\sqrt{2}}{2})^2+(\frac{\sqrt{2}}{2})^2)((z+3\frac{\sqrt{2}}{2})^2+(\frac{\sqrt{2}}{2})^2) \\
&= (z^2-3\sqrt{2}z+5)(z^2+3\sqrt{2}z+5) \\
&= (z^2+5)^2-(3\sqrt{2}z)^2 \\
&= z^4+10z^2+25-18z^2 \\
&= z^4-8z^2+25.
\end{aligned}$$

$\Rightarrow \zeta_8 - 2\zeta_8^3$ *has a minimal polynomial* $\tilde{r}(z) = z^4 - 8z^2 + 25.$

However, since we need to loop through many elements $\gamma(\zeta_\ell)$, `Magma` [15] and `PariGP` [75] have internal function for computing minimal polynomials of elements of a field. The function in `Magma` for example is as follows:

Example 3.2.2. *Computing a minimal polynomial in* `Magma`

```
Magma
> F:= NumberField(Rationals());
> P<z> := PolynomialRing(F);
> f:=CyclotomicPolynomial(8);
> K<z> := ext<F|f>;
> r := MinimalPolynomial(z-2*z^3);
> r;
z^4 - 8*z^2 + 25
```

Recall, we denote D to mean the absolute value of the discriminant and $\mathfrak{d}$ a positive square free integer. The full algorithm is as follows:

Algorithm 3.2.1: New Algorithm for finding pairing-friendly elliptic curves

For a fixed positive integers k and positive square-free integer $\mathfrak{d}$, execute the following steps:

1. Choose a number field $K \cong \mathbb{Q}[z]/\Phi_\ell(z)$ containing $\sqrt{-\mathfrak{d}}$ and a primitive kth root of unity, ζ_k, i.e set D be $\mathfrak{d}$ if $\mathfrak{d} \equiv 3 \bmod 4$, $4\mathfrak{d}$ otherwise and let $\ell = lcm(D, k)$
2. Compute a minimal polynomial of $\gamma(\zeta_\ell) \in \mathbb{Q}(\zeta_\ell)$ call it $\tilde{r}(z)$. Re-define $K \cong \mathbb{Q}[z]/\tilde{r}(z)$
3. Compute the polynomial $l(z)$ modulo $\tilde{r}(z)$ mapping to ζ_k.
4. Let $t(z) = l(z) + 1$, which maps to $\zeta_k + 1$ in $\mathbb{Q}[z]/\tilde{r}(z)$.
5. Using the algebraic relationship between ζ_k and $\sqrt{-\mathfrak{d}}$, find a polynomial $s(z)$ representing $\sqrt{-\mathfrak{d}}$ in $\mathbb{Q}[z]/\tilde{r}(z)$.
6. Compute the polynomial $y(z) = (t(z) - 2)s(z)/(-\mathfrak{d})$ in $\mathbb{Q}[z]/\tilde{r}(z)$.
7. Compute the polynomial $p(z) = (t(z)^2 + \mathfrak{d}y(z)^2)/4$, and compute ρ. If $p(z)$ represents primes and the ρ-value is better than the best known, then:
   (a) find the smallest positive number $n \in \mathbb{Z}$, such that $p(z) \in \mathbb{Z}[z]$;
   (b) find the residue classes b modulo n such that $p(z) \in \mathbb{Z}$ for $z \equiv b \bmod n$;
   (c) find the subset of those residue classes for which $t(z) \in \mathbb{Z}$ for $z \equiv b \bmod n$.
8. If $\tilde{r}(nz + b) = e \cdot r(z)$ where e is a constant in $\mathbb{N}$ and $r(z)$ represents primes, then output $t(z), \tilde{r}(z), p(z), n, b, e$.

Thus for a given value of k and $\mathfrak{d}$, $(t(nz + b), \tilde{r}(nz + b)/e, p(nz + b))$ represents a family of pairing-friendly elliptic curves. The ρ-value of this family of curves is defined as $\rho = \frac{\deg\ p(z)}{\deg\ r(z)}$.

3.2.2 Algorithm explained

This algorithm is potentially very time consuming as the number of possibilities for Equation 3.5 in any number field is huge. For example, using counting argument, the number of choices we have in a number field is

$$\sum_{i=1}^{\varphi(\ell)} \mathcal{S}^i \binom{\varphi(\ell)}{i} \tag{3.7}$$

for any absolute size of the range of search space for our coefficients $\mathcal{S}$.

So our approach is to restrict the search for a favourable element in some way. We take two approaches to achieve this.

Firstly, for each value of k we restrict our search to cases where k is even and $\mathfrak{d}$ is 1 or 3. These cases lead to curves which support higher order twists of degree 4 and 6 (see, Section 2.3) and supports denominator elimination optimisation in pairing computation [6]. We also consider odd values of k which are divisible by 3, as these cases support cubic twist and a type of denominator elimination, see [70] and [60].

Secondly, we search through a possible power basis. This is a polynomial of degree $\varphi(\ell)-1$ but with $\varphi(\ell)$ terms. We find that using a search restricted to a polynomial with up to $\mathcal{M} = 3$ (non-zero terms) and coefficients limited to the range -3 to $+3$ in Equation 3.5 usually lead to favourable elements. This means that Expression 3.7 reduces to

$$\sum_{i=1}^{3} 6^i \binom{\varphi(\ell)}{i} \tag{3.8}$$

choices.

The search is then conducted for all eligible k values from 8 to 40. In some cases, such as $k = 34$ and $k = 38$, we had to further restrict the search to power basis polynomials with up to $\mathcal{M} = 2$ and coefficients ranging from -1 to $+1$, as the value of $\varphi(\ell)$ is too large.

On Intel(R) Core(TM)2 Duo CPU 3.00GHz it takes a week to find all the families reported here.

The search programs are written in a mixture of `NTL` [93] and `PariGP` [75] and for comparison purposes we also use a simple `NTL` program that generates Brezing and Weng families of pairing friendly curves. This program can be found at Mike Scott's website [84].

Step 1 and 2: Set up

The first two steps in the algorithm involve the construction of a number field, K which is isomorphic to $\mathbb{Q}[z]/\Phi_\ell(z)$ and contains ζ_k and $\sqrt{-\mathfrak{d}}$. To achieve this case we set

$$D = \begin{cases} \mathfrak{d} & \text{if } D \equiv 3 \mod 4 \\ 4\mathfrak{d} & \text{if } D \ \textit{otherwise} \end{cases}$$

for any square free integer $\mathfrak{d}$ and define $\ell = lcm(D, k)$. Lemma 3.2.1 below gives the choice of the cyclotomic field containing both ζ_k and $\sqrt{-\mathfrak{d}}$.

Lemma 3.2.1. $\mathbb{Q}(\zeta_D)$ *is the minimal cyclotomic field containing* $\sqrt{-\mathfrak{d}}$*, where* $-D$ *is the discriminant of* $\mathbb{Q}(\sqrt{-\mathfrak{d}})$*.*

Proof. By Conductor-discriminant formulas [102], $-D$ is equal to its conductor. □

Hence this way ensures that $\mathbb{Q}(\zeta_\ell)$ is our minimal ℓ-th cyclotomic field containing both ζ_k and $\sqrt{-\mathfrak{d}}$. We then choose a favourable element $\gamma(\zeta_\ell)$, compute its minimal polynomial and call it $\tilde{r}(z)$.

Step 3, 4 and 5: representing ζ_k and $\sqrt{-\mathfrak{d}}$

Now suppose $K \simeq \mathbb{Q}[z]/\tilde{r}(z)$ where degree of $\tilde{r}(z)$ is $\varphi(\ell)$. We compute the polynomials $l(z)$ which maps to ζ_k. There are $\varphi(k)$ primitive kth roots of unity in $\mathbb{Q}(\zeta_\ell) \cong \mathbb{Q}[z]/\tilde{r}(z)$. We consider all the primitive roots. One such obvious root is $z^{\ell/k}$ for z the primitive ℓth root of unity. If $\gcd(\sigma, k) = 1$, then $(z^{\ell/k})^\sigma$ is another primitive kth root of unity.

Similarly, there are $\varphi(D)$ primitive D-th roots of unity, but there are only two possibilities for a square root of $-\mathfrak{d}$. That is $\pm\sqrt{-\mathfrak{d}}$. So say $z^{\ell/D}$ is corresponding to $\zeta_D \in K$, then since $\sqrt{-\mathfrak{d}} \in \mathbb{Q}(\zeta_D)$ we can find the solution of the polynomial $z^2 + \mathfrak{d}$ in K.

Step 6,7 and 8: computing the family

Computations in these steps are done modulo $\tilde{r}(z)$ except when computing $p(z)$. We ensure that the computed polynomials $t(nz+b), \tilde{r}(nz+b)/e, p(nz+b)$ satisfy Definition 2.5.1 by using Conjectures 1.4.2 and 1.4.2.

Finally, one can use the CM method to find the equation of the elliptic curve using the integers D, t, r and p.

3.3 New curves

The following examples demonstrate the construction of new families of pairing-friendly elliptic curves. Most of our examples also improve the existing ρ-values found in the literature. It is easy to verify that $(t(nz+b), \tilde{r}(nz+b)/e, p(nz+b))$ for a particular embedding degree, satisfy the conditions given in Definition 2.5.1.

However, we give a thorough proof for the first example. The proofs for the other examples basically follow the same line by taking the appropriate

ζ_k and $\sqrt{-\mathfrak{d}}$.

3.3.1 $k = 8$ family

We start however with the case $k = 8$, where we set no records in terms of ρ, but nevertheless find some interesting new families of pairing-friendly curves. For this embedding degree there is a known Brezing and Weng family of curves for $\mathfrak{d} = 3$ and $\ell = 24$ [17].

Example 3.3.1 ([17])**.** *Brezing-Weng family*

$$\begin{aligned} k &= 8,\ \mathfrak{d} = 3; \\ t(z) &= z^5 - z + 1; \\ p(z) &= (z^{10} + z^9 + z^8 - z^6 + 2z^5 - z^4 + z^2 - 2z + 1)/3; \\ r(z) &= z^8 - z^4 + 1; \\ \rho &= 5/4. \end{aligned}$$

Such a family suffers from the fact that we cannot use a possible higher order twist (quartic) for $\mathbb{G}_2$, which must therefore, in this case, be represented by points on $\mathcal{E}(\mathbb{F}_{p^4})$.

However for a family of curves with $k = 8$ and and complex multiplication equal to 4 the *quartic twist* for $\mathbb{G}_2$ would be possible. Using our proposed method for $K \cong \mathbb{Q}(\zeta_8)$ and searching through the range in which $a_i \in [-2, 2]$ and setting $\mathcal{M} = 2$, we find the following family.

Theorem 3.3.1. *Let $k = \ell = 8$ and $\mathfrak{d} = 1$. Let $\gamma(\zeta_8) = \zeta_8 - 2\zeta_8^3 \in \mathbb{Q}(\zeta_8)$*

and define polynomials $\tilde{r}(z), p(z), t(z)$ *as follows*

$$\begin{aligned}\tilde{r}(z) &= z^4 - 8z^2 + 25;\\ t(z) &= (2z^3 - 11z + 15)/15;\\ p(z) &= (z^6 + 2z^5 - 3z^4 + 8z^3 - 15z^2 - 82z + 125)/180.\end{aligned}$$

Then $(t(30z \pm 5), \tilde{r}(30z \pm 5)/450, p(30z \pm 5))$ *represent a family of ordinary pairing-friendly elliptic curves with embedding degree* 8*. The* ρ*-value of this family is* 3/2*.*

Proof. Consider $\gamma(\zeta_8) = \zeta_8 - 2\zeta_8^3 \in \mathbb{Q}(\zeta_8)$. The minimal polynomial of $\gamma(\zeta_8)$ in $\mathbb{Q}(\zeta_8)$ is computed as $\tilde{r}(z)$. Now working in $\mathbb{Q}[z]/\tilde{r}(z)$ choosing $\zeta_8 \mapsto (2z^3 - 11z)/15$ and $\sqrt{-\mathfrak{d}} \mapsto (z^2 - 4)/3$, we apply Algorithm 3.2.1 to get $t(z)$ and $p(z)$ as stated. By construction, $\tilde{r}(z), p(z), t(z)$ satisfy Proposition 1.4.1. Since the ultimate goal is to get integers, using `PariGP` we find that $(t(30z \pm 5), \tilde{r}(30z \pm 5)/450, p(30z \pm 5))$ represent a family of curves with embedding degree $k = 8$. □

Clearly, the ρ-value of this family is inferior to the ρ-value of Brezing-Weng family. However as already stated, curves with complex multiplication equal to 4 have automorphism of order 4 and hence $\mathbb{G}_2$ can now be represented by points on a curve defined over a smaller extension field, that is $\mathbb{F}_{p^2}$. See [1] for an efficient implementation of this type of a curve.

Furthermore, this family does not set any new record as similar family of curves with same ρ-value are also reported before this result in [32] and independently with [99].

Examples of $k = 8$ curves

In this section we generate some examples of pairing-friendly elliptic curves with various cryptographic subgroup sizes for embeeding degree $k = 8$. We use a `Magma` code in Listing 3.1 to generate the parameters p and r and then use a `C`$^{++}$`/NTL` program implemented by Mike Scott [84] to get the curve equation with complex multiplication discriminant $-D$.

The function `KSSCurves`, acting on a specified seed z, also outputs the trace of Frobenius t and the co-factor c of the curve.

Listing 3.1: `Magma` *code for finding p and r*

```
// Input  <- any random integer number;
// Output -> p,r,t,z Integers, p and r primes.
KSSCurves:= function(z)
while (z-b) mod n ne 0 do
  z:=z+1;
end while;
while true do
  r:=rtilde(nz+b) div e;
  if IsPrime(r) then
    p:=p(nz+b);
    if IsPrime(p) then
      break;
    end if;
  end if;
  z:=z+n;
end while;
t:=t(nz+b);
c:=(p+1-t) div r;
return p,r,t,c;
end function;
```

Refer to Table 1.1. A curve of embedding degree $k = 8$ and $\rho = 1.5$ would be suitable at both 112 and 128- bit security level. Here we give one such example in each case.

Example 3.3.2.

$$
\begin{aligned}
k =& 8,\ D = 4,\ p\ is\ 341\ bits\ r\ is\ 224\ bit\ prime\\
p =& 405000000000739249200000562231872099228054574284079453691844733893 73\backslash\\
& 81400850294762406470524090160653389;\\
r =& 1800000000002190360000000999516026840202712955911899417164927011 2553;\\
\mathcal{E}\ :& y^2 = x^3 - 3x.
\end{aligned}
$$

Example 3.3.3.

$$
\begin{aligned}
k =& 8,\ D = 4,\ p\ is\ 386\ bits\ r\ is\ 254\ bit\ prime\\
p =& 976433513559724882989400889832739443685211989918097185359821976670\backslash\\
& 669416871669971613406361756273929440029664625899 73;\\
r =& 446675898243241026070174240545626460972192127135451594400731354 8449\backslash\\
& 499747108088018152964210221280296105202633 8393;\\
\mathcal{E}\ :& y^2 = x^3 - 3x.
\end{aligned}
$$

3.3.2 $k = 12$ family, the BN curves

Interestingly, our method can also construct the Barreto-Naehrig family of pairing-friendly elliptic curves of $k = 12$. An efficient implementation of this family is discussed thoroughly in [24], where the authors show how one can avoid a full $\mathbb{F}_{p^{12}}$ arithmetic by providing explicit formulas for sextic twist implementation for evaluation of the line functions required by Miller's algorithm.

Searching through $a_i \in [-2, 2]$ and setting $\mathcal{M} = 4$ we find the element $\gamma(\zeta_{12}) = \zeta_{12}^3 - \zeta_{12}^2 + \zeta_{12} + 2 \in \mathbb{Q}(\zeta_{12})$ which we use to get a family of BN curves.

Theorem 3.3.2. *Let* $k = \ell = 12$ *and* $\mathfrak{d} = 3$. *Let* $\gamma(\zeta_{12}) = \zeta_{12}^3 - \zeta_{12}^2 + \zeta_{12} + 2 \in \mathbb{Q}(\zeta_{12})$ *and define polynomials* $\tilde{r}(z), t(z), p(z)$ *as follows:*

$$\begin{aligned}\tilde{r}(z) &= z^4 - 6z^3 + 18z^2 - 36z + 36;\\ t(z) &= (z^2 + 6)/6;\\ p(z) &= (z^4 - 6z^3 + 24z^2 - 36z + 36)/36.\end{aligned}$$

Then $(t(6z), \tilde{r}(6z)/36, p(6z))$ *represent a family of ordinary pairing-friendly elliptic curves with embedding degree* 12. *The* ρ*-value of this family is* 1.

Proof. See the arguments in Theorem 3.3.1. We work in $\mathbb{Q}[z]/\tilde{r}(z)$ choosing $\zeta_{12} \mapsto z^2/6$ and $\sqrt{-\mathfrak{d}} \mapsto (z^3 - 3z^2 + 6z - 9)/3$. □

3.3.3 $k = 16$ family

A family with CM discriminant equal to 4 for embedding degree $k = 16$, exhibits quartic twists. This means that for an efficient implementation it is possible to define $\mathbb{G}_2$ to be a group of points on the curve defined over $\mathbb{F}_{p^4}$. Here we search through $a_i \in [-2, 2]$ and set $M = 2$, we find $-2\zeta_{16}^5 + \zeta_{16} \in \mathbb{Q}(\zeta_{16})$ as one of the favourable elements. Theorem 3.3.3 describes this family in detail.

Theorem 3.3.3. *Let* $k = \ell = 16$ *and* $\mathfrak{d} = 1$. *Let* $\gamma(\zeta_{16}) = -2\zeta_{16}^5 + \zeta_{16} \in$

$\mathbb{Q}(\zeta_{16})$ *and define polynomials* $\tilde{r}(z)t(z), p(z)$ *as follows:*

$$\begin{aligned}
\tilde{r}(z) &= z^8 + 48z^4 + 625;\\
t(z) &= (2z^5 + 41z + 35)/35;\\
p(z) &= (z^{10} + 2z^9 + 5z^8 + 48z^6 + 152z^5 + 240z^4 + 625z^2 +\\
&\quad 2398z + 3125)/980.
\end{aligned}$$

Then $(t(70z \pm 25), \tilde{r}(70z \pm 25)/61250, p(70z \pm 25))$ *represent a family of ordinary pairing-friendly elliptic curves with embedding degree* 16*. The* ρ*-value of this family is* 5/4.

Proof. See the arguments in Theorem 3.3.1. We work in $\mathbb{Q}[z]/\tilde{r}(z)$ and choose $\zeta_{16} \mapsto (2z^5 + 41z)/35$ and $\sqrt{-\mathfrak{d}} \mapsto (z^4 + 24)/7$. □

This is an improvement over the old record value of $\rho = 11/8$.

Examples of $k = 16$ curves

A curve for $k = 16$ and $\rho = 1.25$ could be better implemented at 128 or 192 security levels (see Table 1.1) . Here we give both examples.

Example 3.3.4.

$k =$16, $D = 4$, *p is* 329 *bits r is* 256 *bit prime*

$p =$99828774206817717387981613632000871971220109626921497243235722208588\
   00720234411457746445641213203213;

$r =$638674178780437250345865800686827844954476848189702963315697579770\
   07320538113;

$\mathcal{E}: y^2 = x^3 + 5x.$

Example 3.3.5.

$$
\begin{aligned}
k =& 16,\ D = 4,\ p \textit{ is } 489 \textit{ bits } r \textit{ is } 383 \textit{ bit prime}\\
p =& 1021213698985459740731013033509745813259402472963300693113390012 4\backslash\\
& 171607242657723036473920423167581762492459896863655650041065014 43209\backslash\\
& 547345752401333;\\
r =& 163368406557549004208185462131426867918377679945709753444313572 88616\\
& 909671884311072269221657942686660371056900408673;\\
\mathcal{E} :& y^2 = x^3 + 2x
\end{aligned}
$$

3.3.4 $k = 18$ family

For $k = 18$ and CM discriminant $D = 3$ the curves exhibits sextic twists. Here we search through $a_i \in [-3, 3]$ and setting $\mathcal{M} = 2$ we find the following family.

Theorem 3.3.4. *Let $k = \ell = 18$ and $\mathfrak{d} = 3$ Let $\gamma(\zeta_{18}) = -3\zeta_{18}^5 + \zeta_{18}^2 \in \mathbb{Q}(\zeta_{18})$ and define polynomials $\tilde{r}(z), t(z), p(z)$ as follows:*

$$
\begin{aligned}
\tilde{r}(z) &= z^6 + 37z^3 + 343;\\
t(z) &= (z^4 + 16z + 7)/7;\\
p(z) &= (z^8 + 5z^7 + 7z^6 + 37z^5 + 188z^4 + 259z^3 + 343z^2 +\\
&\quad 1763z + 2401)/21.
\end{aligned}
$$

Then $(t(42z+14), \tilde{r}(42z+14)/343, p(42z+14))$ represent a family of ordinary pairing-friendly elliptic curves with embedding degree 18. The ρ-value of this family is $4/3$.

Proof. See the arguments in Theorem 3.3.1. We work in $\mathbb{Q}[z]/\tilde{r}(z)$ choosing

$\zeta_{18} \mapsto (2z^4 + 39z)/7$ and $\sqrt{-\mathfrak{d}} \mapsto 2z^3 + 37$. □

This is a significant improvement in ρ over the old record value of $19/12$.

Examples for $k = 18$ curves

This is a good choice for the 192-bits security level.

Example 3.3.6.

$$
\begin{aligned}
k =& 18,\ D = 3,\ p \textit{ is } 517 \textit{ bits } r \textit{ is } 383 \textit{ bit prime}\\
p =& 31280453921396494952006229544150614768045970820994712980980571515 7027\backslash\\
& 29379585055360801613143086470712542538756772665150987415840403133861643\backslash\\
& 9956764110764403;\\
r =& 11962587735482097731337863148189738422407465494101714367961138605717 99\backslash\\
& 3172156757776754729626355718035935460735 0114537;\\
\mathcal{E} :& y^2 = x^3 + 11.
\end{aligned}
$$

3.3.5 $k = 32$ family

Until now there has not been a good choice of pairing-friendly families of curves which are a good fit for the AES-256 level of security, for larger values of k. For the embedding degree $k = 32$, there is a Brezing and Weng family of curves with $\rho = 17/16$, but with $\mathfrak{d} = 3$, which is the "wrong" discriminant ($3 \nmid k$). The best one can do here is to represent $\mathbb{G}_2$ by a group of points on a curve $\mathcal{E}/\mathbb{F}_{p^{16}}$. Here we suggest an alternative curve which has an automorphism of order 4, where $\mathbb{G}_2$ can be a group of points on a curve $\mathcal{E}'/\mathbb{F}_{p^8}$.

Example 3.3.7 ([17]). *Brezing-Weng family*

$$\begin{aligned}
k &= 32,\ \mathfrak{d} = 3;\\
t(z) &= z^{17} - z + 1;\\
p(z) &= (z^{34} + z^{33} + z^{32} - z^{18} + 2z^{17} - z^{16} + z^2 - z + 1)/3;\\
r(z) &= z^{32} - z^{16} + 1;\\
\rho &= 17/16.
\end{aligned}$$

Theorem 3.3.5. *Let $k = \ell = 32$ and $\mathfrak{d} = 1$. Let $\gamma(\zeta_{32}) = -3\zeta_{32} + 2\zeta_{32}^9 \in \mathbb{Q}(\zeta_{32})$ and define polynomials $\tilde{r}(z), t(z), p(z)$ as follows:*

$$\begin{aligned}
\tilde{r}(z) &= z^{16} + 57120z^8 + 815730721;\\
t(z) &= (-2z^9 - 56403z + 3107)/3107;\\
p(z) &= (z^{18} - 6z^{17} + 13z^{16} + 57120z^{10} - 344632z^9 + 742560z^8 +\\
&\quad 815730721z^2 - 4948305594z + 10604499373)/2970292.
\end{aligned}$$

Then $(t(6214z \pm 325), \tilde{r}(6214z \pm 325)/93190709028482, p(6214z \pm 325))$ represent a family of ordinary pairing-friendly elliptic curves with embedding degree 32. The ρ-value of this family is 9/8.

Proof. We work in $\mathbb{Q}[z]/\tilde{r}(z)$ choosing $\zeta_{32} \mapsto (-2z^9 - 56403z)/3107$ and $\sqrt{-\mathfrak{d}} \mapsto (z^8 + 28560)/239$. □

Examples for $k = 32$ curves

Example 3.3.8.

$$k = 32,\ D = 4,\ p\ is\ 456\ bits\ r\ is\ 512\ bit\ prime$$

$$\begin{aligned}
p =& 42778375828599189082245059938205442096674398225466249447643217330\backslash \\
& 99178379611844717408097739327298086862636585618969819947736160196 0\backslash \\
& 776145426307133570925594101874170137007835082668201 69;
\end{aligned}$$

$$\begin{aligned}
r =& 13276777022727811310997148343578745596674841193277234710069303803\backslash \\
& 52616972230314111779675588875583254086677129873924804742836771972 68\backslash \\
& 2694689671142894870 7041;
\end{aligned}$$

$$\mathcal{E}\ : y^2 = x^3 - 3x.$$

3.3.6 $k = 36$ family

Theorem 3.3.6. *Let $k = \ell = 36$ and $\mathfrak{d} = 3$. Let $\gamma(\zeta_{36}) = 2\zeta_{36} + \zeta_{36}^7 \in \mathbb{Q}(\zeta_{36})$ and define polynomials $\tilde{r}(z), t(z), p(z)$ as follows:*

$$\begin{aligned}
\tilde{r}(z) &= z^{12} + 683z^6 + 117649; \\
t(z) &= (2z^7 + 757z + 259)/259; \\
p(z) &= (z^{14} - 4z^{13} + 7z^{12} + 683z^8 - 2510z^7 + \\
&\quad 4781z^6 + 117649z^2 - 386569z + 823543)/28749.
\end{aligned}$$

Then $(t(777z + 287), \tilde{r}(777z + 287)/161061481,\ p(777z + 287))$ represent a family of ordinary pairing-friendly elliptic curves with embedding degree 36. The ρ-value of this family is $7/6$.

Proof. Working in $\mathbb{Q}[z]/\tilde{r}(z)$ we choose $\zeta_{36} \mapsto (2z^7 + 757z)/259$ and $\sqrt{-\mathfrak{d}} \mapsto (2z^6 + 683)/37$. □

Again this is an improvement in ρ over the old record value of 17/12.

Examples of $k = 36$ curves

Example 3.3.9.

$$k = 36,\ D = 3,\ p \textit{ is } 614 \textit{ bits } r \textit{ is } 512 \textit{ bit prime}$$

$p =$410803687730142857447437508057751682669963481995389418153798321521\
284547298280212913734970341586816079838057503146027085569686141799873\
21998155548175320874191793446470216187748749394757;

$r =$7160493398860400714190770003245558326039580239536138979123491008825;
928581757313936188471893680834532456483932850896474895071365268434386
643812340063458729;

$\mathcal{E}\ : y^2 = x^3 + 5.$

3.3.7 $k = 40$ family

Theorem 3.3.7. *Let* $k = \ell = 40$ *and* $\mathfrak{d} = 1$. *Let* $\gamma(\zeta_{40}) = -2\zeta_{40} + \zeta_{40}^{11} \in \mathbb{Q}(\zeta_{40})$ *and define polynomials* $\tilde{r}(z), t(z), p(z)$ *as follows:*

$$\begin{aligned} \tilde{r}(z) &= z^{16} + 8z^{14} + 39z^{12} + 112z^{10} - 79z^{8} \\ &+ 2800z^{6} + 24375z^{4} + 125000z^{2} + 390625; \\ t(z) &= (2z^{11} + 6469z + 1185)/1185; \\ p(z) &= (z^{22} - 2z^{21} + 5z^{20} + 6232z^{12} - 10568z^{11} + 31160z^{10} \\ &+ 9765625z^{2} - 13398638z + 48828125)/1123380. \end{aligned}$$

Then the triple $(t(2370z \pm 1205), \tilde{r}(2370z \pm 1205)/2437890625, p(2370z \pm 1205))$ *represent a family of ordinary pairing-friendly elliptic curves with embedding degree* 40. *The* ρ*-value of this family is* $11/8$.

Proof. In $\mathbb{Q}[z]/\tilde{r}(z)$ consider $\zeta_{40} \mapsto (2z^{11} + 6469z)/1185$ and $\sqrt{-\mathfrak{d}} \mapsto (z^{10} + 3116)/237$. □

Again this is an improvement in ρ over the old record value of $23/16$.

Example 3.3.10.

$$
\begin{aligned}
&k = 40,\ D = 4,\ p\ is\ 528\ bits\ r\ is\ 368\ bit\ prime\\
p =&7883939200467563981697986896300269813703703520945594948989703334\backslash\\
&718625643261770704786968372789144557093419214412968893615837884828\backslash\\
&70490679844766113107084522058 9;\\
r =&375523118238511238071845237635722567112016821386203251898688303\backslash\\
&96483774320680934361865714109094415049668140 2721;\\
\mathcal{E}\ :&y^2 = x^3 + x.
\end{aligned}
$$

Example 3.3.11.

$$
\begin{aligned}
&k = 40,\ D = 4,\ p\ is\ 545\ bits\ r\ is\ 380\ bit\ prime\\
p =&90488807492525339745442379555880084296998048958065362949072594 55\backslash\\
&268180313928759168890711703696099057697965024161091977653921386403\backslash\\
&36297296020235881051488640314974 09;\\
r =&17969199975725503413627956629748719030400344098259670907431247 62\backslash\\
&62102601061961444806957255307198594771802689975920 1;\\
\mathcal{E}\ :&y^2 = x^3 - 3x.
\end{aligned}
$$

3.4 Conclusion

Our method presented in Algorithm 3.2.1 constructs new ordinary pairing-friendly elliptic curves with improved ρ-values. The main idea in the construction is to use minimal polynomials of the elements of the cyclotomic field other than the cyclotomic polynomial $\Phi_k(z)$ to define the cyclotomic field $\mathbb{Q}(\zeta_k)$.

Moreover, the curves constructed admit higher order twists. This means that $\mathbb{G}_2$ can be represented as a group of points on a curve defined over a smaller field than anticipated.

Chapter 4

Genus 2 pairing-friendly hyperelliptic curves

4.1 Introduction

Developing protocols, which are based on the DLP, using divisor class groups on hyperelliptic curves was first suggested by Neil Koblitz [53].

Even though there are many constructions accredited to construction of pairing-friendly abelian varieties of dimension one, as discussed in Chapter 2, there are very few explicit construction for higher dimensions. In this chapter we discuss the construction of ordinary pairing-friendly Jacobian of genus two hyperelliptic curves.

One may ask why hyperelliptic curves? Well, one of the advantage of genus two hyperelliptic curves over elliptic curves is that one can construct cryptographic protocols at the same security level as elliptic curves using a defining field of half the size. What does this mean? This means that if we need, for example, a 1024-bit field to implement a secure protocol based on Elliptic Curve Cryptography we only need a 512-bit field size for Hyperelliptic Curve Cryptography.

Our main result in this chapter is found in Algorithms 4.5.1 and 4.5.2 which produce new families of genus two pairing-friendly hyperelliptic curves by generalising the Kawazoe-Takahashi approach [51]. By using our approach we observe that we can construct curves that were not reported before and improve some ρ-values of genus two pairing-friendly hyperelliptic curves. This work is also reported in [49].

4.2 Pairing-friendly hyperelliptic curves

In this section, we review some facts on constructing pairing-friendly hyperelliptic curves. Firstly, as in other previous chapters, we let $p > 2$ be a prime and r a prime distinct from p and denote a hyperelliptic curve of genus g defined over a field $\mathbb{F}$ by $\mathcal{C}/\mathbb{F}$.

Definition 4.2.1 ([103]). *A hyperelliptic curve of genus g over a field $\mathbb{F}$ is the non-singular projective model of a smooth affine curve given by an equation of the form:*

$$\mathcal{C} : y^2 + h(x)y = f(x), \tag{4.1}$$

where $h, f \in \mathbb{F}[x], \deg(f) = 2g+1, \deg(h) \leq g$, and f is a monic polynomial.

To ensure that $\mathcal{C}$ is smooth, it suffices to verify that the partial derivatives $2y + h$ and $f' - h'y$ do not simultaneously vanish at any point of $\mathcal{C}(\bar{\mathbb{F}})$.

Suppose Ł is a field extension of $\mathbb{F}$ then the set

$$\mathcal{C}(\text{Ł}) = \{(x, y) \in \text{Ł} \times \text{Ł} | y^2 + h(x)y = f(x)\} \cup \{\mathcal{O}\}$$

is called the Ł-rational points on $\mathcal{C}$ and the point $\mathcal{O}$, is referred to as a point at infinity. If the characteristic of $\mathbb{F}$ is not equal to 2, we can transform the

Equation 4.1 to an equation of the form:

$$y^2 = f(x) \tag{4.2}$$

with f monic of degree $2g + 1$. Throughout this thesis we consider *hyperelliptic curves* of the form as in Equation 4.2 where $f(x)$ has no multiple roots.

Figure 4.1 below presents an example of the graph of a hyperelliptic curve of genus two over the reals.

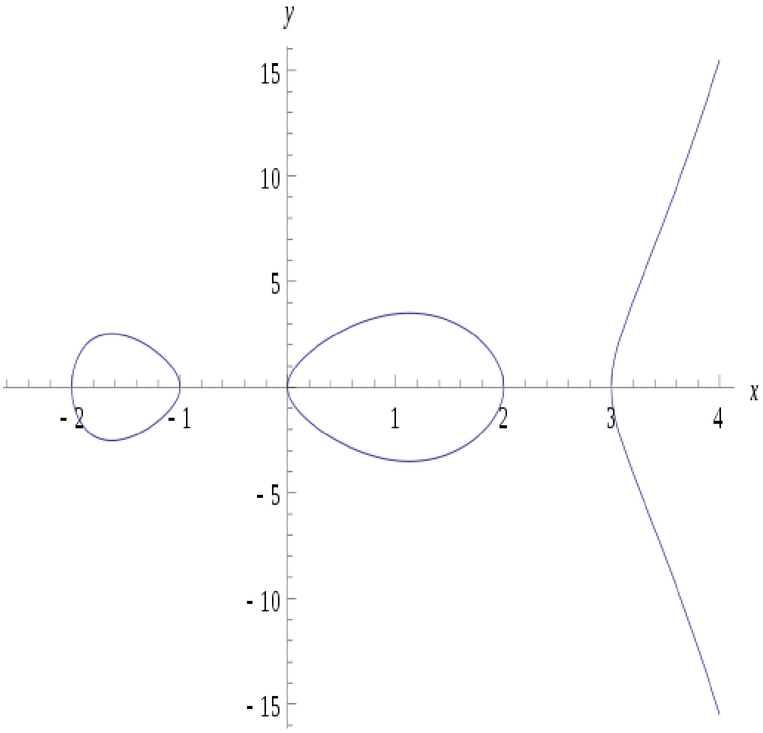

Figure 4.1: *An example of a hyperelliptic curve of genus* 2 *over the reals*

As opposed to the case of elliptic curves, there is no natural way to provide $\mathcal{C}(\mathbb{L})$ with a group structure. This is so because in general, a straight line intersects a curve, $\mathcal{C}$, in $2g+1$ points. Hence, the clever way to proceed is to consider a different object related to $\mathcal{C}$, which to each field extension $\mathbb{L}$

of $\mathbb{F}$ associates a group. This object is called the Jacobian of $\mathcal{C}$.

Recalling the discussion from Section 1.2.2, a Jacobian of $\mathcal{C}$ over a finite field $\mathbb{F}_p$ is an abelian group formed by a group of rational divisors of degree zero modulo principal divisors.

The group operation in the Jacobian of a hyperelliptic curve was first proposed by Cantor [18]. The $\mathbb{F}_p$-rational points of the Jacobian denoted as $J_{\mathcal{C}}(\mathbb{F}_p)$ are given in *Mumford representation.* The representation is through a unique pair of polynomials $[a(x), b(x)]$. When the degree of $a(x)$ is less or equal to g then the divisor is referred to as a *reduced divisor.* The *Mumford representation* is defined as follows:

Definition 4.2.2 ([3])**.** *A divisor D in Mumford representation is a pair $[a(x), b(x)]$ of polynomials in $\mathbb{F}[x]$ such that*

- *$a(x)$ is monic;*
- *deg $(b(x)) <$ deg $(a(x)) \leq g$;*
- *$b(x)^2 - f(x) \equiv 0$ mod $a(x)$.*

The identity element in the group structure of $J_{\mathcal{C}}(\mathbb{F})$ is $\mathcal{O} = (1, 0)$ and the inverse of $(a(x), b(x))$ is $(a(x), -b(x))$.

Now suppose $D_1 = (a_1(x), b_1(x))$ and $D_2 = (a_1(x), b_2(x))$ to be two divisor classes in $J_{\mathcal{C}}(\mathbb{F})$. Cantor's algorithm for adding $D_1 + D_2 = D_3 = [a_3(x), b_3(x)]$ is as follows [3]:

Algorithm 4.2.1: Cantor's algorithm

```
Input: Two divisors $D_1 = [a_1(x), b_1(x)] = [a_1, b_1]$
and $D_2 = [a_2(x), b_2(x)] = [a_2, b_2]$ on a curve $\mathcal{C} : y^2 = f(x)$

Output: $D_3 = [a_3(x), b_3(x)] = [a_3, b_3]$

1. Compute $e_1, e_2, d_1$ such that $d_1 = gcd(a_1, a_2)$
   and $d_1 = e_1a_1 + e_2a_2$
2. Take $c_1, c_2, d$ such that $d = \text{gcd }(d_1, b_1 + b_2)$ is monic
   and $c_1d_1 + c_2(b_1 + b_2) = d$.
3. Define $s_1 = c_1e_1$, $s_2 = c_2e_2$, $s_3 = c_2$,
   and find $d = s_1a_1 + s_2a_2 + s_3(b_1 + b_2)$.
4. Put $a = \frac{a_1a_2}{d^2}$, and $b = \frac{(s_1a_1b_2 + s_2a_2b_1 + s_3(b_1b2 + f))}{d} \bmod a$.
5. Put $a' = \frac{(f - b^2)}{a}$ and $b = b \bmod a'$
6. If deg $a' > g$ then $a \leftarrow$ monic $(a')$, $b \leftarrow b'$, go to 5
7. Put $a_3 \leftarrow$ monic $a'$, $b_3 \leftarrow b'$
```

Figure 4.2 represents a hyperelliptic curve of genus two over the reals. It illustrates the group law on the Jacobian. It shows $D_1 + D_2 = D_3$.

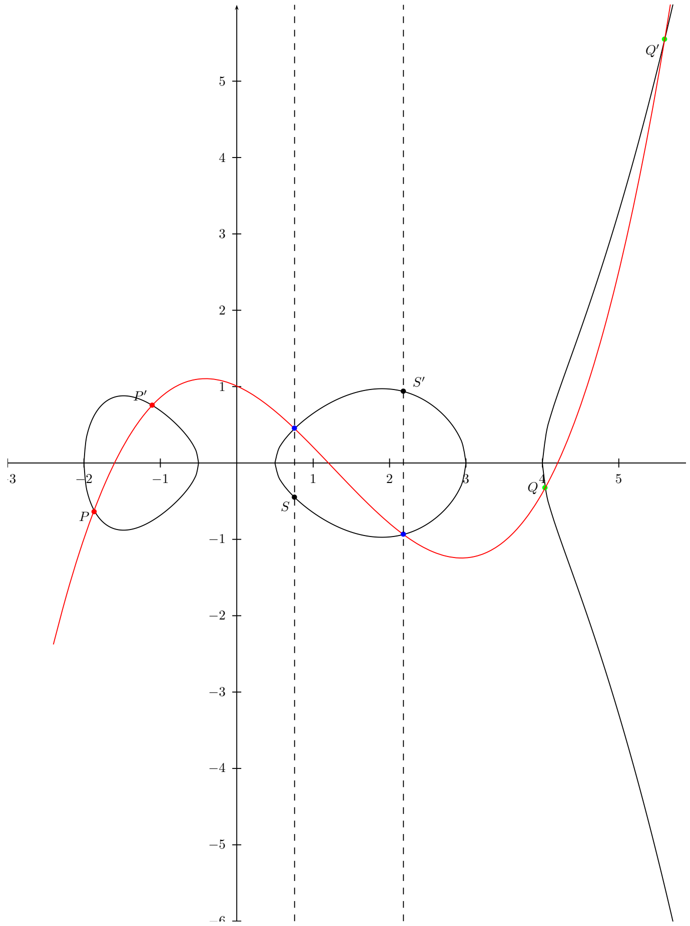

Figure 4.2: *Hyperelliptic curve: addition of divisor classes represented by* $D_1 = (P) + (P')$ *and* $D_2 = (Q) + (Q')$ *giving* $D_3 = (S) + (S')$

4.2.1 Order of the Jacobian

The number of points on a hyperelliptic curve $\mathcal{C}$, and the number of divisors in $J_{\mathcal{C}}$ over the base field and its extensions is dependent on the characteristic polynomial, $\chi(t)$. For genus 2 hyperelliptic curves Equation 1.4 becomes:

$$\chi(t) = t^4 - a_1 t^3 + a_2 t^2 - a_1 p t + p^2 \tag{4.3}$$

with $a_1, a_2 \in \mathbb{F}_p$ and furthermore $\mid a_1 \mid \leq 4p$ and $\mid a_2 \mid \leq 6p$. A challenge is to determine all values of a_1 and a_2 which occur in this way for genus two curves, $\mathcal{C}/\mathbb{F}_p$. If we know $\chi(t)$ it is easy to compute $\#\mathcal{C}/\mathbb{F}_p$ and $\#\mathcal{C}/\mathbb{F}_{p^i}$ for $1 \leq i \leq g$. In genus two this is given by the following relation [42]:

$$\#\mathcal{C}/\mathbb{F}_p = p - a_1 \quad \text{and} \quad \#\mathcal{C}/\mathbb{F}_{p^2} = p - a_1^2 + 2a_2 \tag{4.4}$$

However, our interest is in the order of the Jacobian of genus 2 hyperelliptic curve $\#J_{\mathcal{C}}$, which can be computed using Equation 4.3 as:

$$\#J_C = \chi(1) = 1 - a_1 + a_2 - a_1 p + p^2. \tag{4.5}$$

The Hasse-Weil bound puts the order of the Jacobian of the curve in a rather small interval. Theorem 4.2.1 describes the bounds on the cardinalities of $\#\mathcal{C}(\mathbb{F}_p)$ and $\#J_{\mathcal{C}}(\mathbb{F}_p)$.

Theorem 4.2.1. *Let $\mathcal{C}$ be a hyperelliptic curve of genus g defined over a finite field $\mathbb{F}_p$. Then we have*

$$\left\lceil (\sqrt{p} - 1)^{2g} \right\rceil \leq \#J_{\mathcal{C}}(\mathbb{F}_p) \leq \left\lfloor (\sqrt{p} + 1)^{2g} \right\rfloor. \tag{4.6}$$

$$|\#\mathcal{C}(\mathbb{F}_p) - (p + 1)| \leq 2g\sqrt{p}. \tag{4.7}$$

4.3 Freeman-Satoh genus 2 curves

The first explicit construction of ordinary pairing-friendly hyperelliptic curves was shown by David Freeman [31]. Freeman modeled the Cocks-Pinch method to construct ordinary hyperelliptic curves of genus 2. His algorithm produce curves over prime fields with prescribed embedding degree k with ρ-value ≈ 8. The ρ-value of the curves constructed made them unattractive for an efficient implementation.

However, Freeman and Satoh [34] proposed an algorithm for generating Jacobian of genus two pairing-friendly hyperelliptic curves. In this construction they showed that if an elliptic curve $\mathcal{E}$, is defined over a finite field $\mathbb{F}_p$, and $\mathcal{A}$ is an abelian variety isogenous over $\mathbb{F}_{p^d}$ to a product of two isomorphic elliptic curves then the abelian variety $\mathcal{A}$, is isogenous over $\mathbb{F}_p$ to a primitive subvariety of the Weil restriction of $\mathcal{E}$ from $\mathbb{F}_{p^d}$ to $\mathbb{F}_p$.

Notably, with this approach Freeman and Satoh constructed Jacobian of hyperelliptic curves with improved ρ-value compared to previously reported curves. The best for example, achieves a ρ-value of $20/9$ for an embedding degree $k = 27$, see [34] for examples.

4.4 Kawazoe-Takahashi pairing-friendly hyperelliptic curves

Kawazoe and Takahashi [51] presented an algorithm which constructed hyperelliptic curves of the form $y^2 = x^5 + ax$ with ordinary Jacobians. Their construction used two approaches; one was based on the Cocks-Pinch method of constructing ordinary pairing-friendly elliptic curves and the other was based on cyclotomic polynomials. Both approaches were based on the predefined sizes of the Jacobian as presented in [36].

Theorem 4.4.1 below outlines the characteristic polynomials which defines hyperelliptic curve, $\mathcal{C}$ of the form $y^2 = x^5 + ax$ defined over $\mathbb{F}_p$.

Theorem 4.4.1 ([36],[51])**.** *Let p be an odd prime, $\mathcal{C}$ a hyperelliptic curve defined over $\mathbb{F}_p$ by equation $y^2 = x^5 + ax$, $J_{\mathcal{C}}$ the Jacobian variety of $\mathcal{C}$ and $\chi(t)$ the characteristic polynomial of the pth power Frobenius map of $\mathcal{C}$. Then the following holds: (In the following c, d are integers such that $p = c^2 + 2d^2$ and $c \equiv 1$ (mod 4), $d \in \mathbb{Z}$ (such c and d exists if and only if $p \equiv 1, 3$ (mod 8)).*

1) If $p \equiv 1$ (mod 8) and $a^{(p-1)/2} \equiv -1$ (mod p), $2(-1)^{(p-1)/8}d \equiv (a^{(p-1)/8} + a^{3(p-1)/8})c$ (mod p), then $\chi(t) = t^4 - 4dt^3 + 8d^2t^2 - 4dpt + p^2$.

2) If $p \equiv 1$ (mod 8) and $a^{(p-1)/4} \equiv -1$ (mod p) or if $p \equiv 3$ (mod 8) and $a^{(p-1)/2} \equiv -1$ (mod p), then $\chi(t) = t^4 + (4c^2 - 2p)t^2 + p^2$.

3) If $p \equiv 1$ (mod 16) and $a^{(p-1)/8} \equiv 1$ (mod p), or $p \equiv 9$ mod 16 and $a^{(p-1)/8} \equiv -1$ (mod p), then $\chi(t) = (t^2 - 2ct + p)^2$.

4) If $p \equiv 1$ (mod 16) and $a^{(p-1)/8} \equiv -1$ (mod p), or $p \equiv 9$ mod 16 and $a^{(p-1)/8} \equiv 1$ (mod p), then $\chi(t) = (t^2 + 2ct + p)^2$.

5) If $p \equiv 3$ (mod 8) and $a^{(p-1)/2} \equiv 1$ (mod p), then $\chi(t) = (t^2 + 2ct + p)(t^2 - 2ct + p)$.

Using the formulae in Theorem 4.4.1 (1) and (2) Kawazoe and Takahashi developed a Cocks-Pinch-like method to construct genus 2 ordinary pairing-friendly hyperelliptic curves of the form $y^2 = x^5 + ax$. The $J_{\mathcal{C}}$ for these cases is a simple ordinary Jacobian over $\mathbb{F}_p$. As expected the curves generated by the Cocks-Pinch-like method had ρ-values close to 4.

In addition, Kawazoe and Takahashi also presented cyclotomic families. With this method the authors managed to construct a $k = 24$ curve with $\rho = 3.000$.

In both cases the ultimate goal is to find integers c and d such that there is a prime $p = c^2 + 2d^2$ with $c \equiv 1 \pmod 4$ and $\chi(1)$ having a large prime factor. Algorithms 4.4.1 and 4.4.2 developed from Theorem 4.4.1 construct individual genus 2 pairing-friendly hyperelliptic curves with $\rho \approx 4$. The proofs of these algorithms for their 'pairing-friendliness' involves ensuring that p constructed in this way is a root of unity mudulo r and that $\chi(1)$ has a large prime factor r.

Algorithm 4.4.1: Kawazoe-Takahashi type I pairing-friendly Hyperelliptic curves with $\#J_C = 1^4 - 4d + 8d^2 - 4dp + p^2$

Input: $k \in \mathbb{Z}$.
Output: a hyperelliptic curve defined by $y^2 = x^5 + ax$. with Jacobian group having a prime subgroup of order r.

1. Choose r, a prime such that $lcm(8, k)$ divides $r - 1$.
2. Choose ζ, a primitive kth root of unity in $(\mathbb{Z}/r\mathbb{Z})^\times$, ω, a positive integer such that $\omega^2 \equiv -1 \bmod r$ and σ, a positive integer such that $\sigma^2 \equiv 2 \bmod r$.
3. Compute integers, c, d such that:
   - $c \equiv (\zeta + \omega)(\sigma^2(\omega + 1))^{-1} \bmod r$ and $c \equiv 1 \bmod 4$
   - $d \equiv (\zeta\omega + 1)(2(\omega + 1))^{-1} \bmod r$.
4. Compute a prime $p = c^2 + 2d^2$ such that $p \equiv 1 \bmod 8$.
5. Find $a \in \mathbb{F}_p$ such that:
   - $a^{(p-1)/2} \equiv -1 \bmod p$ and
   - $2(-1)^{(p-1)/8} d \equiv (a^{(p-1)/8} + a^{3(p-1)/8}) c \bmod p$.
6. Define a hyperelliptic curve $\mathcal{C}$ by $y^2 = x^5 + ax$.

Algorithm 4.4.2: Kawazoe-Takahashi type II pairing-friendly Hyperelliptic curves with $\#J_C = 1 + (4c^2 - 2p) + p^2$

```
Input: $k \in \mathbb{Z}$
Output: a hyperelliptic curve defined by $y^2 = x^5 + ax$ with Jacobian
group having a prime subgroup of order $r$.

  1. Choose $r$, a prime such that $lcm(8, k)$ divides $r - 1$.
  2. Choose $\zeta$, a primitive $k$th root of unity in $(\mathbb{Z}/r\mathbb{Z})^\times$, $\omega$, a positive
     integer such that $\omega^2 \equiv -1 \bmod r$ and $\sigma$ a positive integer such that
     $\sigma^2 \equiv 2 \bmod r$.
  3. Compute integers, $c, d$ such that:
       • $c \equiv 2^{-1}(\zeta - 1)\omega \bmod r$ and $c \equiv 1 \bmod 4$
       • $d \equiv (\zeta + 1)(2\sigma)^{-1} \bmod r$.
  4. Compute a prime $p = c^2 + 2d^2$ such that :
       • $p \equiv 1, 3 \bmod 8$
       • $\delta^{(p-1)/2} \equiv -1 \bmod p$ for some integer $\delta \in \mathbb{Z}$
  5. Find $a \in \mathbb{F}_p$ such that:
       • $a \equiv \delta^2 \bmod p$ when $p \equiv 1 \bmod 8$ or
       • $a \equiv \delta \bmod p$ when $p \equiv 3 \bmod 8$.
  6. Define a hyperelliptic curve $\mathcal{C}$ by $y^2 = x^5 + ax$.
```

The key feature in both algorithms is that r is chosen such that $r - 1$ is divisible by 8 so that $\mathbb{Z}/r\mathbb{Z}$ contains both square roots of -1 and 2 for both c and d to satisfy the conditions in the algorithm.

4.5 Generalisation of Kawazoe-Takahashi construction

We observe that one can do better if the algorithms are parametrized by polynomials in order to construct curves with specified bit size. We represent *families* of pairing-friendly curves for which parameters c, d, r, p are parametrized as polynomials $c(z), d(z), r(z), p(z)$ in a variable z.

When working with the polynomials we consider polynomials with rational coefficients as in Chapter 3. Definition 4.5.1 below describes a family of Kawazoe-Takahashi-type of pairing-friendly hyperelliptic curves.

Definition 4.5.1. *Let $c(z), d(z), r(z)$ and $p(z)$ be non-zero polynomials with rational coefficients. For a given positive integer k the couple $(r(z), p(z))$ parameterizes a family of Kawazoe-Takahashi type of hyperelliptic curves with Jacobian $J_{\mathcal{C}}$ whose embedding degree is k if the following conditions are satisfied:*

(i) *$c(z)$ represents integers such that $c(z) \equiv 1$ mod 4;*

(ii) *$d(z)$ represents integers;*

(iii) *$p(z) = c(z)^2 + 2d(z)^2$ represents primes such that $p(z) \equiv 1$ or 3 mod 8;*

(iv) *$r(z)$ represents primes;*

(v) *$r(z)|1-4d(z)+8d(z)^2-4d(z)p(z)+p(z)^2$ or $r(z)|1+(4c(z)^2-2p(z))+p(z)^2$;*

(vi) *$\Phi_k(p(z)) \equiv 0$ mod $r(z)$, where Φ_k is the kth cyclotomic polynomial.*

And we define the ρ-value of this family of curves as

$$\rho = \tfrac{2\deg\, p(z)}{\deg\, r(z)}.$$

In Definition 4.5.1 part (i) and (ii) ensures that the polynomial representation of c and d conforms with the conditions. While condition (v) of Definition 4.5.1 ensures that for a given z for which $p(z)$ and $r(z)$ represents primes and $r(z)$ divides the order of the Jacobian $\#J_{\mathcal{C}}(z)$. In other words, the order of the Jacobian of the constructed curve has a prime order subgroup of size $r(z)$. Finally, condition (vi) of Definition 4.5.1 ensures that the Jacobian of the constructed curve has embedding degree k.

With these definitions we now adapt Algorithms 4.4.1 and 4.4.2 to the polynomial context. This can be seen in Algorithms 4.5.1 and 4.5.2 below generalizing Algorithms 4.4.1 and 4.4.2 respectively. In particular, we construct our curves by taking a similar approach as described in Chapter 3 for constructing pairing-friendly elliptic curves. Even though this method is time consuming as it involves searching for a right element, it mostly gives a favorable irreducible polynomial $r(z)$, which defines the size of the prime order subgroup.

Recall, we find a minimal polynomial of an element $\gamma(\zeta_\ell) \in \mathbb{Q}(\zeta_\ell)$ and call it $\tilde{r}(z)$, where $\gamma(\zeta_\ell)$ is not in any proper subfield of $\mathbb{Q}(\zeta_\ell)$. Since $\gamma(\zeta_\ell)$ is in no proper subfield, then we have $\mathbb{Q}(\zeta_\ell) = \mathbb{Q}(\gamma(\zeta_\ell))$, where the degree of $\mathbb{Q}(\gamma(\zeta_\ell))$ over $\mathbb{Q}$ is $\varphi(\ell)$, where $\varphi(.)$ is *Euler totient function.*

Proof. The proof of this construction is an application of the Kawazoe-Takahashi construction in a polynomial setting. It is enough to show that $p(z)$ constructed in this way is in fact $s(z)$ modulo $\tilde{r}(z)$ and that $\#J_{\mathcal{C}}(z)$ has an irreducible factor $\tilde{r}(z)$. The first part is achieved by substituting $c(z)$ and $d(z)$ into $p(z)$ and reducing it modulo $\tilde{r}(z)$ while the second part is realised by utilising the structure of $d(z)$ and substituting it into $\#J_{\mathcal{C}}(z)$. □

With this approach, apart from reconstructing the Kawazoe-Takahashi genus 2 curves, we discover new families of pairing-friendly hyperelliptic curves of embedding degrees $k = 2, 7, 8, 10, 11, 13, 22, 26, 28, 44$ and 52 with $2 < \rho \leq 3$.

The success depends on the choice of the number field K. Thus, in the

Algorithm 4.5.1: Our generalization for finding pairing-friendly hyperelliptic curves with $\#J_{\mathcal{C}}(z) = 1 - 4d(z) + 8d(z)^2 - 4d(z)p(z) + p(z)^2$

```
Input: $k \in \mathbb{Z}, \ell = lcm(8, k), K \cong \mathbb{Q}[z]/\Phi_\ell(z)$.
Output: Hyperelliptic curve of genus 2 defined by $y^2 = x^5 + ax$.

  1. Choose an irreducible polynomial $\tilde{r}(z) \in \mathbb{Z}[z]$.
  2. Choose polynomials $s(z), \omega(z)$ and $\sigma(z)$ in $\mathbb{Q}[z]$ such that $s(z)$ is a
     primitive $k$th root of unity, $\omega(z) = \sqrt{-1}$ and $\sigma(z) = \sqrt{2}$ in $K$.
  3. Compute polynomials, $c(z), d(z)$ such that:
       • $c(z) \equiv (s(z) + \omega(z))(\sigma(z)(\omega(z) + 1))^{-1}$ in $\mathbb{Q}[z]/\tilde{r}(z)$.
       • $d(z) \equiv (s(z)\omega(z) + 1)(2(\omega(z) + 1))^{-1}$ in $\mathbb{Q}[z]/\tilde{r}(z)$.
  4. Let $p(z)$ be an irreducible polynomial such that $p(z) = c(z)^2 + 2d(z)^2$.
  5. For $z_0 \in \mathbb{Z}$ such that $c(z_0), d(z_o), p(z_0)$, represent integers and that
     $c(z_0) \equiv 1 \bmod 4$
       • find the subset of those residue classes for which $p(z_0)$ and $\tilde{r}(z_0)$
         represents primes and $p(z_0) \equiv 1 \bmod 8$.
  6. Find $a \in \mathbb{F}_{p(z_0)}$ satisfying:
       • $a^{(p(z_0)-1)/2} \equiv -1 \bmod p(z_0)$. and
       • $2(-1)^{(p(z_0)-1)/8} d(z_0) \equiv (a^{(p(z_0)-1)/8} + a^{3(p(z_0)-1)/8}) c(z_0) \bmod$
         $p(z_0)$.
  7. Output $(\tilde{r}(z_0), p(z_0), a)$.
  8. Define a hyperelliptic curve $\mathcal{C}$ by $y^2 = x^5 + ax$.
```

Algorithm 4.5.2: Our generalization for finding pairing-friendly hyperelliptic curves with $\#J_{\mathcal{C}}(z) = 1 + (4c(z)^2 - 2p(z)) + p(z)^2$

Input: $k \in \mathbb{Z}, \ell = lcm(8, k), K \cong \mathbb{Q}[z]/\Phi_\ell(z)$
Output: Hyperelliptic curve of genus 2 defined by $y^2 = x^5 + ax$.

1. Choose an irreducible polynomial $\tilde{r}(z) \in \mathbb{Z}[z]$.
2. Choose polynomials $s(z), \omega(z)$ and $\sigma(z)$ in $\mathbb{Q}[z]$ such that $s(z)$ is a primitive kth root of unity, $\omega(z) = \sqrt{-1}$ and $\sigma(z) = \sqrt{2}$ in K.
3. Compute polynomials, $c(z), d(z)$ such that
    - $c(z) \equiv 2^{-1}(s(z) - 1)\omega(z) \bmod \tilde{r}(z)$
    - $d(z) \equiv (s(z) + 1)(2\sigma(z))^{-1} \bmod \tilde{r}(z)$.
4. Let $p(z)$ be an irreducible polynomial such that $p(z) = c(z)^2 + 2d(z)^2$
5. For $z_0 \in \mathbb{Z}$ such that $c(z_0), d(z_o), p(z_0)$, represent integers and that $c(z_0) \equiv 1 \bmod 4$
    - find the subset of those residue classes for which $p(z_0)$ and $\tilde{r}(z_0)$ represents primes and $p(z_0) \equiv 1$ or $3 \bmod 8$.
6. Find $a \in \mathbb{F}_p(z_0)$ such that:
    - $a = \delta^2$ when $p(z_0) \equiv 1 \bmod 8$ or
    - $a = \delta$ when $p(z_0) \equiv 3 \bmod 8$.
7. Output $(\tilde{r}(z_0), p(z_0), a)$.
8. Define a hyperelliptic curve $\mathcal{C}$ by $y^2 = x^5 + ax$.

initial step we set K to be isomorphic to a cyclotomic field $\mathbb{Q}(\zeta_\ell)$ for some $\ell = lcm(8, k)$. The condition on ℓ ensures $\mathbb{Q}[z]/\tilde{r}(z)$ contains square roots of -1 and 2.

However, with most values of $k > 10$ which are not multiples of 8, the degree of $\tilde{r}(z)$ tends to be large. As observed in [32], for such a family of curves this limits the number of curves one can find (see Table 1.1 for appropriate sizes of r).

4.5.1 The algorithm explained

Step 1: Set up

This involves initializing the algorithm by setting $\mathbb{Q}(\zeta_\ell)$ defined as $\mathbb{Q}[z]/\Phi_\ell(z)$. The choice of this field should ensure that it contains ζ_k, $\sqrt{-1}$ and $\sqrt{2}$. The ideal choice, in such a case, is $\mathbb{Q}(\zeta_8, \zeta_k) = \mathbb{Q}(\zeta_\ell)$, where $\ell = lcm(k, 8)$. This follows from Lemma 4.5.1 below.

Lemma 4.5.1. *Let ℓ be a positive integer and ζ_ℓ be a primitive ℓth root of unity. If $8|\ell$ then the ℓth cyclotomic field, $\mathbb{Q}(\zeta_\ell)$, contains ζ_k and $\sqrt{-1}$ and $\sqrt{2}$.*

Proof. Since $8|\ell$ then $\mathbb{Q}(\zeta_\ell)$ contains primitive eighth, ζ_8, and fourth, ζ_4, roots of unity.

$$\begin{aligned}
\text{Consider} \quad (1+i)^2 &= 1 + 2i + i^2 \\
&= 2i. \\
\text{Hence} \quad 2 &= -i(1+i)^2. \\
\text{Therefore} \quad \sqrt{2} &= \sqrt{-i}(1+i) \\
&= \zeta_4\zeta_8(1+\zeta_4).
\end{aligned}$$

□

Step 2: Representing $\zeta_k, \sqrt{-1}$ and $\sqrt{2}$

We search for a favorable element, $\gamma(\zeta_\ell) \in \mathbb{Q}(\zeta_\ell)$ such that the minimal polynomial of $\gamma(\zeta_\ell)$ has degree $\varphi(\ell)$ and we call this $\tilde{r}(z)$. We redefine our field to $\mathbb{Q}[z]/\tilde{r}(z)$. In this field we find polynomials that represent $\zeta_k, \sqrt{-1}$ and $\sqrt{2}$.

For ζ_k there are $\varphi(k)$ numbers of primitive kth roots of unity. In fact if $\gcd(\alpha, k) = 1$ then ζ_k^α is also a primitive kth root of unity. To find the polynomial representation of $\sqrt{-1}$ and $\sqrt{2}$ in $\mathbb{Q}[z]/\tilde{r}(z)$ is simple. Consider for example $\sqrt{2}$. Let z be a primitive ℓth root of unity in $K = \mathbb{Q}[z]/(\Phi_\ell(z))$ then $z^{\ell/4}$ and $z^{\ell/8}$ are the primitive 4th and 8th roots of unity respectively. By using Lemma 4.5.1 we can therefore, represent $\sqrt{2}$ in K as:

$$\begin{aligned} \sqrt{2} &= \zeta_4\zeta_8(1+\zeta_4) \\ &= z^{\ell/4}.z^{\ell/8}(1+z^{\ell/4}) \\ &= z^{3\ell/8} + z^{5\ell/8} \in \mathbb{Q}[z]/\tilde{r}(z). \end{aligned}$$

Steps 3,4,5: Finding the family

All computations in the algorithm are done modulo $\tilde{r}(z)$ except when computing $p(z)$. It is likely that polynomials $p(z), c(z)$ and $d(z)$ have rational coefficients. At this point polynomials are tested to determine whether they represent integers or primes as per Definition 4.5.1.

4.5.2 New curves

We now present a series of new curves constructed using the approach described above. Proving the theorems is simple considering $\gamma(\zeta_\ell)$ has minimal polynomial $\tilde{r}(z)$. We give a proof of Theorem 4.5.1. For the other curves the proofs are similar.

We start by constructing a curve of embedding degree, $k = 7$. It is interesting to note that here we get a family with $\rho = 8/3$.

Theorem 4.5.1. *Let $k = 7, \ell = 56$. Let $\gamma(\zeta_\ell) = \zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $\tilde{r}(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
\tilde{r}(z) &= z^{24} - 24z^{23} + 276z^{22} - 2024z^{21} + 10625z^{20} - 42484z^{19} + 134406z^{18} \\
&\quad -344964z^{17} + 730627z^{16} - 1292016z^{15} + 1922616z^{14} - 2419184z^{13} + \\
&\quad 2580005z^{12} - 2332540z^{11} + 1784442z^{10} - 1150764z^{9} + 621877z^{8} - \\
&\quad 279240z^{7} + 102948z^{6} - 30632z^{5} + 7175z^{4} - 1276z^{3} + 162z^{2} - 12z + 1; \\
p(z) &= (z^{32} - 32z^{31} + 494z^{30} - 4900z^{29} + 35091z^{28} - 193284z^{27} + 851760z^{26} - \\
&\quad 3084120z^{25} + 9351225z^{24} - 24075480z^{23} + 53183130z^{22} - \\
&\quad 101594220z^{21} + 168810915z^{20} - 245025900z^{19} + 311572260z^{18} - \\
&\quad 347677200z^{17} + 340656803z^{16} - 292929968z^{15} + 220707810z^{14} - \\
&\quad 145300540z^{13} + 83242705z^{12} - 41279004z^{11} + 17609384z^{10} - 6432920z^{9} + \\
&\quad 2023515z^{8} - 569816z^{7} + 159446z^{6} - 49588z^{5} + 16186z^{4} - 4600z^{3} + \\
&\quad 968z^{2} - 128z + 8)/8; \\
c(z) &= (-z^{9} + 9z^{8} - 37z^{7} + 91z^{6} - 147z^{5} + 161z^{4} - 119z^{3} + 57z^{2} - \\
&\quad 16z + 2)/2; \\
d(z) &= (z^{16} - 16z^{15} + 119z^{14} - 546z^{13} + 1729z^{12} - 4004z^{11} + \\
&\quad 7007z^{10} - 9438z^{9} + 9867z^{8} - 8008z^{7} + 5005z^{6} - 2366z^{5} + \\
&\quad 819z^{4} - 196z^{3} + 28z^{2})/4.
\end{aligned}$$

Then $(\tilde{r}(2z), p(2z))$ represents a family of genus 2 hyperelliptic curves. The ρ-value of this family is $8/3$.

Proof. Since $\zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ has minimal polynomial $\tilde{r}(z)$, we apply Algorithm 4.5.1 by working in $\mathbb{Q}(\zeta_{56})$ defined as $\mathbb{Q}[z]/\tilde{r}(z)$. We choose $\zeta_7 \mapsto (z-1)^{16}$,

$\sqrt{-1} \mapsto (z-1)^{14}$ and $\sqrt{2} \mapsto z(z-1)^7(z-2)(z^6-7z^5+21z^4-35z^3+35z^2-21z+7)(z^6-5z^5+11z^4-13z^3+9z^2-3z+1)$. Applying Algorithm 4.5.1 we find $p(z)$ as stated. Computations with `PariGP` [75], show that both $\tilde{r}(2z)$ and $p(2z)$ represents primes and $c(2z)$ represents integers equivalent to 1 modulo 4. Furthermore, by Algorithm 4.5.1 the Jacobian of our hypothetical curve has a large prime order subgroup of order $\tilde{r}(2z)$ and embedding degree, $k = 7$. □

Considering $z_0 = 758$ we give an example of a 254- bit prime subgroup that is constructed using the parameters in Theorem 4.5.1.

Example 4.5.1.

$$\begin{aligned}
r &= 2137485553256666528907136658652514287617426818411415448 4\backslash \\
&\quad 92440542523013009 0001; \quad \text{(254 bits)} \\
p &= 741504661189142770769829861344257948821797401549707353 15\backslash \\
&\quad 4351080954816427650424459756660957817976 66897; \\
c &= -2102247714969368735010398 4375; \\
d &= 1925493003348938127179315304456050968604370111 44944; \\
a &= 3; \\
\rho &= 2.646; \\
\mathcal{C} : y^2 &= x^5 + 3x.
\end{aligned}$$

The next curve is of embedding degree, $k = 8$. According to [107] this family of curves admits higher order twists. This means that it is possible to have both inputs to a pairing defined over base field. The previous record was $\rho = 4$. In Theorem 4.5.2 below we outline the parameters that defines a family of hyperelliptic curves with $\rho = 3$.

Theorem 4.5.2. *Let $k = \ell = 8$. Let $\gamma(\zeta_\ell) = \zeta_\ell^3 + \zeta_\ell^2 + \zeta_\ell + 3 \in \mathbb{Q}(\zeta_8)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
\tilde{r}(z) &= z^4 - 12z^3 + 60z^2 - 144z + 136; \\
p(z) &= (11z^6 - 188z^5 + 1460z^4 - 6464z^3 + 17080z^2 - 25408z + 16448)/64; \\
c(z) &= (3z^3 - 26z^2 + 92z - 120)/8; \\
d(z) &= (-z^3 + 8z^2 - 26z + 32)/8.
\end{aligned}$$

Then $(\tilde{r}(32z)/8, p(32z))$ represents a family of genus 2 hyperelliptic curves with embedding degree 8. The ρ-value of this family is 3.

We can do the same here as in Theorem 4.5.1 to show that the set of polynomials above define a family of hyperelliptic curves for embedding degree 8. Specifically, in $\mathbb{Q}[z]/\tilde{r}(z)$ we choose:

$$\begin{aligned}
\zeta_8 &\mapsto (z^3 - 8z^2 + 28z - 36)^7; \\
\sqrt{-1} &\mapsto (z - 3)(z^2 - 6z + 14); \\
\sqrt{2} &\mapsto (z^2 - 6z + 12)/2.
\end{aligned}$$

This type of a curve is recommended at the 128 bit security level, see Table 1.1. Below we give an example obtained using the above parameters.

Example 4.5.2.

$$\begin{aligned}
r &= 131072000000000989850828800028032436273920352833179209074 2\backslash \\
&\quad 4776433635287258931 37; \text{ (257 bits)} \\
p &= 18454937600002090565474713698674225176676787947450456041 8\backslash \\
&\quad 25253266950693364290488511618376615764127711271298317288 4737;
\end{aligned}$$

$$\begin{aligned}
c &= 1228800000000695988992000013140209336688082695322003440625;\\
d &= -4096000000000231996416000004380073001064027565137751569916;\\
a &= 3;\\
\rho &= 3.012.\\
\mathcal{C} : y^2 &= x^5 + 3x.
\end{aligned}$$

Theorem 4.5.3. *Let $k = 10, \ell = 40$. Let $\gamma(\zeta_\ell) = \zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $\tilde{r}(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
\tilde{r}(z) &= z^{16} - 16z^{15} + 120z^{14} - 560z^{13} + 1819z^{12} - 4356z^{11} + 7942z^{10} -\\
&\quad 11220z^9 + 12376z^8 - 10656z^7 + 7112z^6 - 3632z^5 + 1394z^4 -\\
&\quad 392z^3 + 76z^2 - 8z + 1;\\
p(z) &= (z^{24} - 24z^{23} + 274z^{22} - 1980z^{21} + 10165z^{20} - 39444z^{19}\\
&\quad +120156z^{18} - 294576z^{17} + 591090z^{16} - 981920z^{15} + 1360476z^{14} -\\
&\quad 1578824z^{13} + 1536842z^{12} - 1253336z^{11} + 853248z^{10} - 482384z^9 +\\
&\quad 225861z^8 - 88872z^7 + 31522z^6 - 11676z^5 + 4802z^4 - 1848z^3 +\\
&\quad 536z^2 - 96z + 8)/8;\\
c(z) &= (-z^7 + 7z^6 - 22z^5 + 40z^4 - 45z^3 + 31z^2 - 12z + 2)/2;\\
d(z) &= (z^{12} - 12z^{11} + 65z^{10} - 210z^9 + 450z^8 - 672z^7 + 714z^6 -\\
&\quad 540z^5 + 285z^4 - 100z^3 + 20z^2)/4.
\end{aligned}$$

Then $(\tilde{r}(4z), p(4z))$ represents a family of genus 2 hyperelliptic curve. The

ρ-value of this family is 3. Here we choose

$$\begin{aligned}
\zeta_{10} &\mapsto (z-1)^{12};\\
\sqrt{-1} &\mapsto (z-1)^{10};\\
\sqrt{2} &\mapsto z(z-2)(z-1)^5(z^4-5z^3+10z^2-10z+5)(z^4-3z^3+4z^2-2z+1).
\end{aligned}$$

Below is a curve of embedding degree 10 with a prime order subgroup of size 249 bits. The ρ-value of its J_C is 3.036.

Example 4.5.3.

$$\begin{aligned}
r &= 47457491054103014068159312355967539444301108619814810948\backslash\\
&\quad 2797931132143318041; \quad (249 \text{ bits})\\
p &= 339268047683548227442734898907507152190802484314819125499\backslash\\
&\quad 393410802175044822928270159666053912399467210953623356417;\\
c &= -1189724159035338550797061406711295;\\
d &= 411866512163557810321097788276510052727469786602189684736;\\
a &= 3;\\
\rho &= 3.036;\\
\mathcal{C}: y^2 &= x^5+3x.
\end{aligned}$$

The next curve is of embedding degree, $k = 28$.

Theorem 4.5.4. *Let $k = 28, \ell = 56$. Let $\gamma = \zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $\tilde{r}(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
\tilde{r}(z) &= z^{24} - 24z^{23} + 276z^{22} - 2024z^{21} + 10625z^{20} - 42484z^{19} + \\
&\quad 134406z^{18} - 344964z^{17} + 730627z^{16} - 1292016z^{15} + 1922616z^{14} - \\
&\quad 2419184z^{13} + 2580005z^{12} - 2332540z^{11} + 1784442z^{10} - 1150764z^{9} + \\
&\quad 621877z^{8} - 279240z^{7} + 102948z^{6} - 30632z^{5} + 7175z^{4} - 1276z^{3} + \\
&\quad 162z^{2} - 12z + 1; \\
p(z) &= (z^{36} - 36z^{35} + 630z^{34} - 7140z^{33} + 58903z^{32} - 376928z^{31} + \\
&\quad 1946800z^{30} - 8337760z^{29} + 30188421z^{28} - 93740556z^{27} + 252374850z^{26} - \\
&\quad 594076860z^{25} + 1230661575z^{24} - 2254790280z^{23} + 3667649460z^{22} - \\
&\quad 5311037640z^{21} + 6859394535z^{20} - 7909656300z^{19} + 8145387218z^{18} - \\
&\quad 7487525484z^{17} + 613613430z^{16} - 4473905808z^{15} + 2893567080z^{14} - \\
&\quad 1653553104z^{13} + 830662287z^{12} - 364485108z^{11} + 138635550z^{10} - \\
&\quad 45341540z^{9} + 12681910z^{8} - 3054608z^{7} + 660688z^{6} - 141120z^{5} + 32008z^{4} - \\
&\quad 7072z^{3} + 1256z^{2} - 144z + 8)/8; \\
c(z) &= (-z^{11} + 11z^{10} - 55z^{9} + 165z^{8} - 331z^{7} + 469z^{6} - 483z^{5} + \\
&\quad 365z^{4} - 200z^{3} + 76z^{2} - 18z + 2)/2; \\
d(z) &= (z^{18} - 18z^{17} + 153z^{16} - 816z^{15} + 3059z^{14} - 8554z^{13} + 18473z^{12} - \\
&\quad 31460z^{11} + 42757z^{10} - 46618z^{9} + 40755z^{8} - 28392z^{7} + 15561z^{6} - \\
&\quad 6566z^{5} + 2058z^{4} - 448z^{3} + 56z^{2})/4.
\end{aligned}$$

Then $(\tilde{r}(2z), p(2z))$ represents a family of genus 2 hyperelliptic curve.

The ρ-value of this family is $\rho \approx 3$. Here we choose

$$\begin{aligned}
\zeta_{28} &\mapsto (z-1)^{18};\\
\sqrt{-1} &\mapsto (z-1)^{14};\\
\sqrt{2} &\mapsto z(z-2)(z-1)^7(z^6-7z^5+21z^4-35z^3+35z^2-21z+7)\\
&\quad (z^6-5z^5+11z^4-13z^3+9z^2-3x+1).
\end{aligned}$$

Here is a curve with a 255 bit prime order subgroup constructed from the above parameters:

Example 4.5.4.

$$\begin{aligned}
r &= 424919600539385944351122192376667674313110063571221116\backslash\\
&\quad 690362883228500208481;\\
p &= 10948891695013050372882471239448013664796533168415352392\backslash\\
&\quad 56833619302663216719518472851456451963664706050519126312 1;\\
c &= -661115396488771699930556119523 37239;\\
d &= 73989498224454294419334385377521846525339047033183899840 0;\\
a &= 23;\\
\rho &= 2.972.\\
\mathcal{C}: y^2 &= x^5+23x.
\end{aligned}$$

The following family for $k=24$ has a same ρ-value as a family of $k=24$ curves reported in [51]. One can use the following parameters to construct a *Kawazoe-Takahashi Type II* pairing-friendly hyperelliptic curve of embedding degree $k=24$ with $\rho=3$ using Algorithm 4.5.2.

Theorem 4.5.5. *Let $k=\ell=24$. Let $\gamma=\zeta_{24}+1 \in \mathbb{Q}(\zeta_{24})$ and define* *polynomials* $\tilde{r}(z), p(z), c(z), d(z)$ *by the following:*

$$\begin{aligned}
\tilde{r}(z) &= z^8 - 8z^7 + 28z^6 - 56z^5 + 69z^4 - 52z^3 + 22z^2 - 4z + 1;\\
p(z) &= (2z^{12} - 28z^{11} + 179z^{10} - 688z^9 + 1766z^8 - 3188z^7 +\\
&\quad 4155z^6 - 3948z^5 + 2724z^4 - 1336z^3 + 443z^2 - 88z + 8)/8;\\
c(z) &= (-z^6 + 7z^5 - 20z^4 + 30z^3 - 25z^2 + 11z - 2)/2;\\
d(z) &= (z^5 - 4z^4 + 5z^3 - 2z^2 - z)/4.
\end{aligned}$$

Then $(\tilde{r}(8z+4)/8, p(8z+4))$ represents a family of genus 2 hyperelliptic curves with embedding degree 24. The ρ-value of this family is 3. Here we choose

$$\begin{aligned}
\zeta_{24} &\mapsto (z-1)^{23};\\
\sqrt{-1} &\mapsto (z-1)^6;\\
\sqrt{2} &\mapsto (z-1)(z^4 - 4z^3 + 5z^2 - 2z - 1).
\end{aligned}$$

The following family is of embedding degree $k = 2$ with $\rho = 3$. In this case the parameters correspond to a quadratic twist $\mathcal{C}'$ of the curve $\mathcal{C}$ whose order of $J_{\mathcal{C}}$ has a large prime of size r.

Theorem 4.5.6. *Let* $k = 2\,, \ell = 8$. *Let* $\gamma = \zeta_8^2 + \zeta_8 + 1 \in \mathbb{Q}(\zeta_8)$ *and define polynomials* $\tilde{r}(z), p(z), c(z), d(z)$ *by the following:*

$$\begin{aligned}
\tilde{r}(z) &= z^4 - 4z^3 + 8z^2 - 4z + 1; \\
p(z) &= (17z^6 - 128z^5 + 480z^4 - 964z^3 + 1089z^2 - 476z + 68)/36; \\
c(z) &= (z^3 - 4z^2 + 7z - 2)/2; \\
d(z) &= (-2z^3 + 7z^2 - 14z + 4)/6.
\end{aligned}$$

Then $(\tilde{r}(36z + 8)/9, p(36z + 8))$ represents a family of genus 2 hyperelliptic curve. The ρ-value of this family is 3. In $\mathbb{Q}[z]/r(z)$ we choose

$$\begin{aligned}
\zeta_2 &\mapsto ((2z^3 - 7z^2 + 14z - 4)/3)^2; \\
\sqrt{-1} &\mapsto (2z^3 - 7z^2 + 14z - 4)/3; \\
\sqrt{2} &\mapsto (z + 1)(z^2 - 3z + 4).
\end{aligned}$$

Here is a curve with a 164 bit prime subgroup generated from the above parameters:

Example 4.5.5.

$$\begin{aligned}
r &= 1866240767113923045167388159201163779990313800469 7; \\
p &= 10279256257891516489822674213746873409099825032526 5\backslash \\
&\quad 6165164129909459559679217; \\
c &= 233280071916861790309390681284245 60723; \\
d &= -155520047944596126877366449084261 34338; \\
a &= 10; \\
\rho &= 3.049.
\end{aligned}$$

Here our genus 2 hyperelliptic equation is $\mathcal{C}' : y^2 = x^5 + 10x$ and hence

$\mathcal{C} : y^2 = 20(x^5 + 10x)$ is the curve whose $\#J_{\mathcal{C}}$ has a large prime r and its embedding degree is 2 with respect to r.

We now present pairing-friendly hyperelliptic curves of embedding degree k, whose polynomial that defines the prime order subgroup $r(z)$, has degree greater or equal to 40. Currently these curves, as already pointed out, are only of theoretical interest. Since we would wish to specify the group sizes, the degree of $r(z)$ cannot be too large [32].

Theorem 4.5.7. *Let $k = 11, \ell = 88$. Let $\gamma = \zeta_\ell \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
r(z) &= z^{40} - z^{36} + z^{32} - z^{28} + z^{24} - z^{20} + z^{16} - z^{12} + z^8 - z^4 + 1;\\
p(z) &= (z^{48} - 2z^{46} + z^{44} + 8z^{24} + z^4 - 2z^2 + 1)/8;\\
c(z) &= -(z^{13} + z^{11})/2;\\
d(z) &= 1/4(z^{24} - z^{22} - z^2 + 1);\\
\rho &= 12/5;
\end{aligned}$$

Family $(r(4z+3)/89, p(4z+3))$.

Theorem 4.5.8. *Let $k = 13, \ell = 104$. Let $\gamma = \zeta_\ell + 1 \in \mathbb{Q}(\zeta_\ell)$ and define polynomials $r(z), p(z), c(z), d(z)$ by the following:*

$$\begin{aligned}
r(z) &= z^{48} - 48z^{47} + 1128z^{46} + ... + 2z^2 - 24z + 1;\\
p(z) &= (z^{64} - 64z^{63} + 2016z^{62} - ... + 4040z^2 - 256z + 8)/8;\\
c(z) &= -(z^{19} - 19z^{18} + 171z^{17} + ... + 249z^2 - 32z + 2)/2;\\
d(z) &= (z^{32} - 32z^{31} + 496z^{30} - ... + 20995z^4 - 2340z^3 + 156z^2)/4;\\
\rho &= 8/3;
\end{aligned}$$

Family $(r(8z+4), p(8z+4)$.

Theorem 4.5.9. *Let* $k = 22, \ell = 88$. *Let* $\gamma = \zeta_\ell \in \mathbb{Q}(\zeta_\ell)$ *and define polynomials* $r(z), p(z), c(z), d(z)$ *by the following:*

$$\begin{aligned}
r(z) &= z^{40} - z^{36} + z^{32} - z^{28} + z^{24} - z^{20} + z^{16} - z^{12} + z^{8} - z^{4} + 1;\\
p(z) &= (z^{56} - 2z^{50} + z^{44} + z^{28} + z^{12} - 2z^{6} + 1)/8;\\
c(z) &= -(z^{17} + z^{11})/2;\\
d(z) &= (z^{34} - z^{22} + z^{12} + 1)/4;\\
\rho &= 14/5;
\end{aligned}$$

Family $(r(4z+3)/89, p(4z+3))$.

Theorem 4.5.10. *Let* $k = 26, \ell = 104$. *Let* $\gamma = \zeta_\ell \in \mathbb{Q}(\zeta_\ell)$ *and define polynomials* $r(z), p(z), c(z), d(z)$ *by the following:*

$$\begin{aligned}
r(z) &= z^{48} - z^{44} + z^{40} - z^{36} + z^{32} - z^{28} + z^{24} - z^{20} + z^{16} - z^{12} + z^{8} - z^{4} + 1;\\
p(z) &= (z^{56} - 2z^{54} + z^{52} + 8z^{28} + z^{4} - 2z^{2} + 1)/8;\\
c(z) &= -(z^{15} + z^{13})/2;\\
d(z) &= (z^{28} - z^{26} - z^{2} + 1)/4;\\
\rho &= 7/3;
\end{aligned}$$

Family $(r(4z+3), p(4z+3))$.

4.6 Conclusion

In this Chapter we have presented an algorithm that finds genus 2 pairing-friendly hyperelliptic curves of type $y^2 = x^5 + ax$. In addition we have presented new curves and improved ρ-values for some previously reported families of curves. The curves are summerised in Table 4.1.

Table 4.1: *Families of curves, $k < 60$, with $2.000 < \rho \leq 3.000$*

k	Degree($\tilde{r}(z)$)	Degree($p(z)$)	ρ-value
2	4	6	3.000
7	24	32	2.667
8	4	6	3.000
10	16	24	3.000
11	40	48	2.400
13	48	64	2.667
22	40	56	2.800
24	8	12	3.000
26	48	56	2.333
28	24	36	3.000
44	48	64	2.600
52	48	60	2.500

Chapter 5

Implementation issues

5.1 Introduction

Efficient pairing computation is as significant as finding good curves as discussed in Chapters 3 and 4. There is a considerable amount of work done by various researchers in trying to optimise the efficiency of computing the pairings. Mainly, the effort has been to optimise the *Miller loop* and the *final exponentiation* parts of the algorithm see [6], [85] [1] and [24].

In this Chapter, we describe some efficient implementations of bilinear pairings. We pay particular attention to efficient computations in $\mathbb{G}_2$ and the *final exponentiation* optimisation. This work also appears in [88] and [87].

5.1.1 Computing the pairing

The most efficient way to compute a pairing is by using the Tate pairing or its variants. Here we introduce the Tate and the Ate pairings for elliptic curves.

The Tate pairing

Let $\mathcal{E}$ be an elliptic curve defined over a finite field $\mathbb{F}_p$, with an embedding degree k. Let r be a prime distinct from p such that r is a large prime factor of $\#\mathcal{E}(\mathbb{F}_p)$. Assume r^2 does not divide $p^k - 1$. For every integer s, let $f_{s,P}$ be the function with a divisor:

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

then the Tate pairing [35] is a well-defined non-degenerate, bilinear pairing defined by the following map:

$$\begin{aligned} \mathcal{E}(\mathbb{F}_p)[r] \quad &\times \quad \mathcal{E}(\mathbb{F}_{p^k})/r\mathcal{E}(\mathbb{F}_{p^k}) \longrightarrow \mathbb{F}_{p^k}^{\times}/(\mathbb{F}_{p^k}^{\times})^r \\ e_r(P,Q) \quad &\mapsto \quad \langle P,Q\rangle_r = f_{r,P}(Q). \end{aligned}$$

The value of this pairing is only defined up to a coset of $(\mathbb{F}_{p^k}^{\times})^r$. However, for practical purposes, we exponentiate the value of the pairing say, f, by a quantity $\frac{p^k-1}{r}$ to obtain a unique representative of this class. This process eliminates all rth powers leaving an exact rth root of unity in $\mathbb{F}_{p^k}$ and is referred to as the reduced Tate pairing.

The best known method to date for computing bilinear pairings is *Miller's algorithm* see [67], [10], [6] or [3]. Miller's algorithm is basically the 'double and add' algorithm for elliptic curve point multiplication combined with an evaluation of certain intermediate functions which are the straight lines used in the addition process (see Section 2.2.2).

In the algorithm, to compute the pairing we use the line functions l and v to evaluate the point addition between any two points. For example, let $R = (x_R, y_R)$ and $T = (x_T, y_T)$ be points on the curve $\mathcal{E}/\mathbb{F}_{p^k}$. The values of line function $l_{R,T}(Q)$ and vertical function $v_{R+T}(Q)$ are distances calculated between the lines that arise when adding point R to point T and the fixed point Q. The values of these functions are given by the following formulas:

$$l_{R,T}(Q) = (y_Q - y_R) - \lambda(x_Q - x_R) \tag{5.1}$$

$$v_{R+T}(Q) = (x_Q - y_{R+T}) \tag{5.2}$$

where λ is the slope of the straight line through R and T given as follows:

$$\lambda = \begin{cases} \dfrac{y_T - y_R}{x_T - x_R} & \text{if } T \neq R \\ \dfrac{3x_R^2}{2y_R^2} & \text{if } T = R. \end{cases}$$

Below is a basic Algorithm to compute Tate pairing [10].

Algorithm 5.1.1: Basic Miller's Algorithm

```
Require: $r \in \mathbb{Z}$ $P$, $Q \in \mathcal{E}$
Ensure : $f_{r,P}(Q)^{\frac{p^k-1}{r}}$
$T \leftarrow P$;
$f \leftarrow 1$;
for $i \leftarrow \lfloor \log(r) \rfloor - 1$ down to 0 do
    $f \leftarrow f^2 \cdot l_{T,T}(Q)/v_{2T}(Q)$;
    $T \leftarrow 2T$;
    if $r_i = 1$ then
        $f \leftarrow f \cdot l_{T,P}(Q)/v_{T+P}(Q)$;
        $T \leftarrow T + P$
    end
end
$f \leftarrow f^{\frac{p^k-1}{r}}$;
return $f$.
```

The Miller's algorithm can be simplified further for even embedding degrees. Suppose $k = 2k'$ and the extension field $\mathbb{F}_{p^k}$ built as a quadratic extension over $\mathbb{F}_{p^{k'}}$. Then one can use the denominator elimination method to ease the computation of the pairing. The simplification is stated in Theorem 5.1.1[6].

Theorem 5.1.1. *Let* $P \in \mathcal{E}(\mathbb{F}_p)[r]$*. Suppose* $Q = (x, y) \in \mathcal{E}(\mathbb{F}_{p^k})$ *and* $x \in \mathbb{F}_{p^{k'}}$*. Then* v_{2T} *and* v_{T+P} *denominators in the Miller's algorithm can be discarded without changing the value of the pairing* $e(P, Q)$*.*

The Ate pairing

The Ate pairing [46] is a well-defined non-degenerate pairing that generalises the Eta pairing [5] to ordinary elliptic curves and is defined on $\mathbb{G}_2 \times \mathbb{G}_1$. That is the arguments are swapped with respect to the Eta pairing.

The Ate pairing bilinear map is defined by the following:

$$\begin{array}{rcl} \mathcal{E}(\mathbb{F}_{p^k})[r] \cap Ker(\pi_p - [p]) & \times & \mathcal{E}(\mathbb{F}_p)[r] \cap Ker(\pi_p - [1]) \longrightarrow \mathbb{F}_{p^k}^{\times}/(\mathbb{F}_{p^k}^{\times})^r \\ e_t(Q, P) & \mapsto & \langle Q, P \rangle_t = f_{t-1,Q}(P)^{\frac{p^k-1}{r}}. \end{array}$$

In the ate pairing the number of iterations in the Miller loop depends on the size of the trace of the Frobenius t rather than on the size of the subgroup r. Thus, as noted in [85] if $\omega = \log r / \log |t|$ is greater than one for a particular family then it may be possible to compute the ate pairing faster than the Tate pairing.

5.2 Cofactor multiplication in $\mathbb{G}_2$

Some pairing-based protocols, such the Identity Based Encryption scheme by Boneh and Franklin [13], require hashing of identities to $\mathbb{G}_1$ or $\mathbb{G}_2$. The process involves hashing an input to some x in the finite field, and then solve for a corresponding y on the curve. The process is repeated as many times as necessary until it yields a point (x, y) on the curve and multiply this point by a cofactor.

However, Tate pairing and its variants require $\mathbb{G}_2$ to be a group of points of prime order r on a curve defined over some extension of $\mathbb{F}_p$. In this case, to hash to an identity requires a multiplication by large cofactor because the group $\mathbb{G}_2$, is defined over a larger field. This is considered to be inefficient.

Galbraith and Scott [39] presented an efficiently computable homomorphism of the groups $\mathbb{G}_2$ and $\mathbb{G}_T$ in a pairing. This is based on a technique of Gallant, Lambert and Vanstone [40] of fast point multiplication on curves. In their method the authors used the homomorphism:

$$\psi = \phi^{-1}\pi_p\phi$$

where $\phi : \mathcal{E}' \to \mathcal{E}$ is the isomorphism which maps points on the twisted curve $\mathcal{E}'(\mathbb{F}_{p^e})$, to points on the isomorphic group on $\mathcal{E}(\mathbb{F}_{p^k})$, and π_p is the pth power Frobenius map on $\mathcal{E}$, see Section 2.3. The general points in $\mathcal{E}'(\mathbb{F}_{p^e})$ satisfy the following identity [39]

$$\psi^2(P) - [t]\psi(P) + [p]P = 0 \tag{5.3}$$

with $P \in \mathcal{E}'(\mathbb{F}_{p^e})$.

With Equation 5.3 in mind we work with polynomials to handle the problem of multiplication by a large cofactor. We observe that since we can represent the order of the elliptic curve $\mathcal{E}'(\mathbb{F}_{p^e})$, as $\#\mathcal{E}'(\mathbb{F}_{p(z)^e})$ then we can defined the cofactor in polynomial terms as follows, (see Section 2.2.3):

$$c(z) = \#\mathcal{E}'(\mathbb{F}_{p(z)^e})/r(z) \tag{5.4}$$

with $p(z)$ a polynomial defining the field and $r(z)$ a polynomial defining the prime order subgroup on the curve $\mathcal{E}/(\mathbb{F}_{p(z)})$.

We now express $c(z)$ to the base $p(z)$ as follows:

$$c(z) = \sum_i c_i p(z)^i \qquad c_i \in \mathbb{Q} \tag{5.5}$$

and then use the relation

$$[p]P = [t]\psi(P) - \psi^2(P) \tag{5.6}$$

recursively if necessary to reduce the co-factor multiplication to a form:

$$[c_0 + p(c_1 + p(c_2 + ...))]P = \sum_i [g_i]\psi^i(P) \tag{5.7}$$

where all of the g_i are less than p. Note for example that

$$[c_1.p]P = [c_1.t]\psi(P) - [c_1]\psi^2(P). \tag{5.8}$$

A further applications of the homomorphism may be necessary to effect a complete reduction. In some circumstances we will also find the following identity to be useful:

$$\Phi_k(\psi(P)) = 0 \tag{5.9}$$

where Φ_k is the k-th cyclotomic polynomial. Equation 5.9 allows terms of degree greater or equal to $\varphi(k)$ to be replaced with terms of lower degree.

In the case that $k = de$ with $gcd(d, e) = 1$, we observe that the twisting isomorphism ϕ defining the twist of degree e can be chosen so that the twisted curve $\mathcal{E}'$ is actually defined over $\mathbb{F}_p$ (in this case ϕ is defined over $\mathbb{F}_{p^d}$). In this case the cofactor $c(z)$ can be factored as $h(z).c'(z)$ where

$h(z) = \#\mathcal{E}'(\mathbb{F}_{p(z)})$.

The endomorphism $\pi' - 1$, where π' is the pth-power Frobenius map on $\mathcal{E}'$, projects into the subgroup of $\#\mathcal{E}'(\mathbb{F}_{p^d})$ of order $c'(z) \cdot r(z)$. Thus we only need to perform a multiplication by $c'(z)$ to obtain a point of order $r(z)$. In this case our algorithm only needs to be applied to a smaller cofactor $c'(z)$.

This approach of reducing the cofactor multiplication to the evaluation of polynomial of powers $\psi^i(P)$ with coefficients less than p is done using Algorithm 5.2.1.

This algorithm takes in as inputs an integers k which is the embedding degree; a polynomial $p(z)$ which defines the size of the finite field; a polynomial $t(z)$ which parameterises the trace of the Frobenius of the pairing-friendly curve and a polynomial $c(z)$ parameterising the hard part of the multiplication to be performed to obtain a point of order r.

The first part of the algorithm (lines $3 - 6$) expresses $c(z)$ to the base $p(z)$ while the second part of the algorithm (lines $8 - 13$) expresses $c(z)$ to the base $\psi(.)$ The coefficients of the base $\psi(.)$ representation are computed using the coefficients of the base $p(z)$ representation and the appropriate coefficients of the equation:

$$[p^j]P = \sum_{i=0}^{j} \tbinom{j}{i} t(z)^{j-i}(-1)^i \psi^{j+i}(P), \tag{5.10}$$

obtained by applying induction on Equation 5.6. After $c(z)$ has been expressed to the base $\psi(.)$, the coefficients $g_i(z)$ are checked. If the degree of $g_i(z)$ is greater than the degree of $p(z)$ the identity in Equation 5.3 is applied again (see lines $15 - 20$ and examples Section 5.2.1). Finally, the relation in Equation 5.9 is exploited to obtain a base $\psi(.)$ representation of $c(z)$ of degree less than $\varphi(k)$.

5.2.1 Application of the algorithm

Let us demonstrate this approach by first working through the algorithm using the MNT $k = 6$ curves. Recall the parameters for MNT $k = 6$ curves from Section 2.6.3 in Theorem 2.6.1 .

Step 1: Lines 3-6 of Algorithm 5.2.1

Since k is even and the CM discriminant of these curves is not equal to -3 the best we could do is to use the quadratic twist for an efficient implementation.

This means that $\mathbb{G}_2$ is a group of points of order r in $\mathcal{E}'(\mathbb{F}_{p^3})$. From Section 2.2.3 using Theorem 2.2.4 the order $\#\mathcal{E}'(\mathbb{F}_{p^3})$, is computed explicitly as follows in polynomial terms:

$$\begin{aligned}
s_0 &= 2 \\
p(z) &= z^2+1 \\
t(z) &= z+1 \\
s_1 &= t(z) \\
s_2 &= s_1 \cdot s_1 - (p(z) \cdot s_0) \\
&= -z^2+2z-1 \\
s_3 &= s_1 \cdot s_2 - p(z) \cdot s_1 \\
&= -2z^3-2 \\
\#\mathcal{E}'(\mathbb{F}_{p^3}) &= p^3+1+s_3 \\
&= z^6+3z^4-2z^3+3z^2.
\end{aligned}$$

from which we can compute the cofactor $c(z)$, easily as:

$$c(z) = \frac{\#\mathcal{E}'(\mathbb{F}_{p^3})}{r(z)} = \frac{z^6+3z^4-2z^3+3z^2}{z^2-z+1} = z^4+z^3+3z^2. \tag{5.11}$$

Algorithm 5.2.1: Reduction of cofactor to base $\psi(.)$

```
Require: $k$, $t(z)$, $c(z)$
Ensure : Coefficients of a base $\psi(.)$ : $g_0(z), g_1(z), ...g_{\varphi(k)-1}$ with deg
         $g_i(z) <$ deg $p(z)$
$f \leftarrow \lfloor \deg(c(z))/\deg(p(z)) \rfloor$;
◇ Express $c(z)$ to the base $p$;
for $i \leftarrow 0$ to $f$ do
    $c_i(z) \leftarrow c(z)$ mod $p(z)$;
    $c(z) \leftarrow c(z)$ div $p(z)$;
end
◇ Using Equation 5.6 make first pass to determine $g_i$ of $c(z)$ to the
base $\psi(.)$ ;
for $j \leftarrow 0$ to $f$ do
    $g_{2j} \leftarrow 0,\ g_{2j+1} \leftarrow 0$;
    for $i \leftarrow 0$ to 1 do
        $g_{j+i} \leftarrow g_{j+i} + \binom{j}{i} t(z)^{j-1}(-1)^i c_j(z)$;
    end
end
◇ Make a second pass to force all the coefficients to have degree <
degree $p$;
$g_{2f+1} \leftarrow 0,\ g_{2f+2} \leftarrow 0$;
for $j \leftarrow 1$ to $2f$ do
    $w(z) \leftarrow g_j(z)$ div $p(z)$;
    $g_j(z) \leftarrow g_j(z)$ mod $p(z)$;
    $g_{j+1}(z) \leftarrow g_{j+1}(z) + t(z)w(z)$;
    $g_{j+2}(z) \leftarrow g_{j+2}(z) - w(z)$;
end
◇ Finally exploit Equation 5.9; $a_i$ is the coefficient of $z^i$ in $\Phi_k(z)$;
for $j \leftarrow 2f + 2$ down to $\varphi(k)$ do
    for $i \leftarrow 1$ to $\varphi(k)$ do
        $g_{j-i}(z) \leftarrow g_{j-i}(z) - a_{\varphi(k)-i} \cdot g_j(z)$;
    end
    $g_j(z) \leftarrow 0$;
end
```

Running through lines $3-6$ in the algorithm we express the cofactor in Equation 5.11, to the base $p(z)$ which becomes:

$$c(z) = p(z)^2 + (z+1)p(z) + (-z-2). \tag{5.12}$$

Step 2: Lines 8-20 of Algorithm 5.2.1

Using the identity in Equation 5.3, applying it to each term in Equation 5.12 involving the power of $p(z)$, we express $[c(z)]P$ to the base $\psi(.)$. This can be seen in lines $8-13$ in Algorithm 5.2.1. Here we get

$$[-z-2]P + [z^2+2z+1]\psi(P) + [z^2+z]\psi^2(P) + [-2z-2]\psi^3(P) + \psi^4(P).$$

Since the degrees of some of the coefficients in the expression above are equal to the degree of $p(z)$, we apply Equation 5.3 again to finally get:

$$[-z-2]P + [2z]\psi(P) + [z^2]\psi^2(P) + [-2z-2]\psi^3(P). \tag{5.13}$$

This action can be seen in lines $15-20$ in Algorithm 5.2.1.

Step 3: Lines 22-27 of Algorithm 5.2.1

Now consider Equation 5.9, since $\psi^2(P) = \psi(P) - P$ we can substitute this in the expression above for $\psi^2(P)$. With lines 22-27 in Algorithm 5.2.1 Expression 5.13 reduces to

$$\psi(4zP) - 2zP. \tag{5.14}$$

Compared to explicit point multiplication by $z^4 + z^3 + 3z^2$, the expression above is equivalent to multiplication only by z, two doublings, one application of homomorphism and a point addition.

5.2.2 The Freeman Curves

Recall the parameters for the family of pairing-friendly elliptic curves of embedding degree 10 discovered by David Freeman from Section 2.6.5.

The best that can be done for $\mathbb{G}_2$ is to represent it as a group of points in $\mathcal{E}'(\mathbb{F}_{p^5})$ (quadratic twist).

Here we can compute $\#\mathcal{E}'(\mathbb{F}_{p^5})$ as in MNT $k = 6$ curves. This is a particularly large and rather awkward extension, and the cofactor multiplication threatens to be huge. In fact $c(z)$ in this particular case works out as the rather intimidating degree 16 polynomial of the following form:

$$\begin{aligned} c(z) \quad = \quad & 390625z^{16} + 1562500z^{15} + 4062500z^{14} + 7421875z^{13} \\ & +10750000z^{12} + 12593750z^{11} + 12356250z^{10} + 10203125z^{9} \\ & +7178125z^{8} + 4284375z^{7} + 2171000z^{6} + 920250z^{5} + 322400z^{4} \\ & +89875z^{3} + 19120z^{2} + 2740z + 217. \end{aligned}$$

This has $p(z) + 1 + t(z)$ as a factor; and choosing the quadratic twist $\mathcal{E}'$ to be defined over $\mathbb{F}_p$ then the multiplication by $p(z) + 1 + t(z)$ can be handled by the transformation $P \leftarrow \pi'(P) - P$, and so the hard-part of the cofactor multiplication can be reduced to:

$$\begin{aligned} c'(z) \quad = \quad & 15625z^{12} + 46875z^{11} + 93750z^{10} + 128125z^{9} \\ & +138125z^{8} + 116875z^{7} + 80875z^{6} + 44875z^{5} + 20225z^{4} \\ & +7075z^{3} + 1880z^{2} + 325z + 31. \end{aligned}$$

Applying our algorithm we find that multiplying P by $c'(z)$ can be expressed as:

$$\sum_{i=0}^{3}[g_i(z)]\psi^i(P) \tag{5.15}$$

where

$$\begin{aligned} g_0(z) &= -5z^2 - 10z - 2; \\ g_1(z) &= -25z^3 - 20z^2 - 10z - 4; \\ g_2(z) &= 3; \\ g_3(z) &= -25z^3 - 10z^2 - 5z. \end{aligned}$$

We proceed by computing $zP,\ z^2P = z.zP,\ z^3P = z.z^2P$, and then

$$\psi^i(P), \psi^i(zP), \psi^i(z^2P) \text{ and } \ \psi^i(z^3P) \text{ for } 1 \le i \le 3.$$

and this becomes:

$$\begin{aligned} &[25](-\psi^3(z^3P) - \psi(z^3P)) + [20](\psi(z^2P)) + [10](-\psi^3(z^2P) - \psi(zP) - zP) \\ &+ [5](-\psi^3(zP) - z^2P) + [4](-\psi(P)) + [3]\psi^2(P) + [2](-P), \end{aligned}$$

which we can represent as:

$$25A + 20B + 10C + 5D + 4E + 3F + 2G,$$

when A, B, C, D, E, F and G are calculated using just 4 extra point additions.

We proceed to form the smallest addition sequence which includes all of the small multipliers in the above expression as follows:

$$\{\underline{1}, 2, 3, 4, 5, 10, 20, 25\}.$$

Then find a vector addition chain for [2, 3, 4 5 10 20 25] as follows (see Section 1.6.1):

A	B	C	D	E	F	G
[1	0	0	0	0	0	0]
[0	1	0	0	0	0	0]
[0	0	1	0	0	0	0]
[0	0	0	1	0	0	0]
[0	0	0	0	1	0	0]
[0	0	0	0	0	1	0]
[0	0	0	0	0	0	1]
[1	1	0	0	0	0	0]
[1	0	0	1	0	0	0]
[2	2	0	0	0	0	0]
[2	2	1	0	0	0	0]
[4	4	2	0	0	0	0]
[5	4	2	1	0	0	0]
[5	4	2	1	1	0	0]
[10	8	4	2	2	0	0]
[10	8	4	2	2	0	1]
[10	8	4	2	2	1	1]
[5	4	2	1	0	1	0]
[20	16	8	4	4	2	2]
[25	20	10	5	4	3	2]

This shows that using the Olivos algorithm we get 9 extra point additions and 4 point doublings as shown below:

$$\begin{aligned}
&\Gamma_0 \leftarrow A + B\\
&\Gamma_1 \leftarrow A + D\\
&\Gamma_0 \leftarrow 2\ \cdot \Gamma_0\\
&\Gamma_0 \leftarrow \Gamma_0 + C\\
&\Gamma_0 \leftarrow 2\ \cdot \Gamma_0\\
&\Gamma_1 \leftarrow \Gamma_0 + \Gamma_1\\
&\Gamma_0 \leftarrow \Gamma_1 + E\\
&\Gamma_0 \leftarrow 2\ \cdot \Gamma_0\\
&\Gamma_0 \leftarrow \Gamma_0 + G\\
&\Gamma_0 \leftarrow \Gamma_0 + F\\
&\Gamma_1 \leftarrow \Gamma_1 + F\\
&\Gamma_0 \leftarrow 2\ \cdot \Gamma_0\\
&\Gamma_0 \leftarrow \Gamma_0 + \Gamma_1.
\end{aligned}$$

where the final result is in Γ_0.

5.2.3 The $k = 8$ family of curves

Recall the parameters of $k = 8$ curves reported from Chapter 3 in Theorem 3.3.1. Since the CM discriminant of this family is -4 and the embedding degree is 8, the best that can be done for $\mathbb{G}_2$ is to represent it as a group of points in $\mathcal{E}'(\mathbb{F}_{p^2})$. We can proceed by first computing the order of the twist

$\#\mathcal{E}'(\mathbb{F}_{p^2})$, using Theorem 2.2.4 and secondly, the cofactor

$$c(z) = \#\mathcal{E}'(\mathbb{F}_{p(z)^2})/r(z). \tag{5.16}$$

Proceeding as before we work through Algorithm 5.2.1 to get:

$$\begin{aligned} g_0(z) &= (2z^5 + 4z^4 - z^3 + 50z^2 + 65z - 36)/6; \\ g_1(z) &= (2z^5 + 4z^4 - z^3 - 7z^2 - 25z + 75)/6; \\ g_2(z) &= (-15z^2 - 30z - 75)/6. \end{aligned}$$

The common denominator of 6 which appears in each $g_i(z)$ above can be dealt with by completing the hashing to $\mathbb{G}_2$ with the point multiplication $[6.c(z)]P$; this still results in a point of order r as 6 and r are co-prime. To complete the calculation we need an addition sequence which includes all of the integer coefficients that arise:

$$\{1, 2, 4, \underline{5}, \underline{6}, 7, \underline{10}, 15, 25, 30, 36, 50, 65, 75\}, \tag{5.17}$$

where the underlined numbers are the extra numbers included to complete the sequence (see Section 1.6). Proceeding as for the Freeman curves case, the computation using this addition sequence can compute the vectorial addition chain which can be completed with 18 point additions and 5 point doublings.

5.2.4 The $k = 18$ family of curves

Recall the parameters for the family of $k = 18$ curves from Chapter 3 in Theorem 3.3.4. For this family of curves, as for the BN curves, z can be chosen with a low Hamming weight. Since the CM discriminant of this family is -3 and the embedding degree is 18, the best that can be done for $\mathbb{G}_2$ is to represent it as a group of points in $\mathcal{E}'(\mathbb{F}_{p^3})$. Proceeding as before we compute $\#\mathcal{E}'(\mathbb{F}_{p^3})$ and the cofactor works out to be:

$$\begin{aligned} c(z) &= z^{18} + 15z^{17} + 96z^{16} + 409z^{15} + 1791 + z^{14} + 7929z^{13} + 27539z^{12} \\ &\quad +81660z^{11} + 256908z^{10} + 757927z^{9} + 1803684z^{8} + 4055484z^{7} \\ &\quad +9658007z^{6} + 19465362z^{5} + 30860595z^{4} + 50075833z^{3} + 82554234z^{2} \\ &\quad +88845918z + 40301641 \end{aligned}$$

In this case using Algorithm 5.2.1 we get:

$$\begin{aligned} g_0(z) &= (-5z^7 - 26z^6 - 98z^5 - 381z^4 - 867z^3 - 1911z^2 - 5145z - 5774)/3; \\ g_1(z) &= (-5z^7 - 18z^6 - 38z^4 - 323z^3 - 28z^2 + 784z)/3; \\ g_2(z) &= (5z^7 - 18z^6 - 38z^4 - 323z^3 + 1029z + 343)/3; \\ g_3(z) &= (-11z^6 - 70z^5 - 98z^4 - 176z^3 - 1218z^2 - 2058z - 686)/3; \\ g_4(z) &= (28z^2 + 245z + 343)/3. \end{aligned}$$

Using the same reasoning as in the $k = 8$ case, the denominator is removed by performing the evaluation $[3c(z)]P$. The best addition sequence we could find that includes all of the coefficients of $g_i(z)$ is as follows:

$$\{\underline{1}, \underline{2}, \underline{3}, 5, \underline{7}, \underline{8}, 11, 18, 26, 28, \underline{31}, 38, \underline{45}, \underline{69}, 70, \underline{78}, 98, 176, 245, \\ \underline{253}, 323, 343, 381, \underline{389}, 686, 784, \underline{829}, 867, 1029, 1218, \underline{1658}, 1911, 2058, \underline{4116}, \\ 5145, 5774\}.$$

This can be used to complete the calculation in 51 point additions and 5 point doublings using the vectorial addition chain.

5.3 The final exponentiation

The final exponentiation by $\frac{p^k-1}{r}$ can be expressed as :

$$\frac{p^k-1}{r} = \prod_{d/k,d<k} \Phi_d(p) \quad \frac{\Phi_k(p)}{r} \tag{5.18}$$

where the first factor, $\prod_{d/k,d<k} \Phi_d(p)$, can be computed easily by using the pth power Frobenius operations and $\Phi_k(.)$ is the kth cyclotomic polynomial. Computing the last part poses a challenge and is referred to as the *hard exponentiation.*

Let us consider for example the BN curves (see Section 2.6.4 for parameters). In this case Equation 5.18 is expressed as:

$$\frac{p^{12}-1}{r} = (p^6-1)\cdot(p^2+1)\frac{(p^4-p^2+1)}{r}.$$

Recall that p and r have a special form. Both are polynomials in z. Therefore this hard part of the final exponentiation $\dfrac{(p^4-p^2+1)}{r}$, can be computed explicitly as a large polynomial in z. This can in turn be expressed to the base p as:

$$p^3+(6z^2+1)p^2+(36z^3-18z^2+12z+1)p+(36z^3-30z^2+18z-1).$$

The naive way is to use the method of multi-exponentiation coupled with the Frobenius [64], so that the final exponentiation is the computation of:

$$(f^{p^3})\cdot(f^{p^2})^{(6z+1)}\cdot(f^p)^{(36z^3-18z^2+12z+1)}\cdot f^{(36z^3-30z^2+18z-1)}$$

Nevertheless, in [24] they proceed by express the exponent to the base

p. This means that the power of the expression will be less than $\varphi(k)$ where $\varphi(.)$ is *Euler totient* function. That is:

$$\frac{\Phi(p)}{r} = \sum_{i=0}^{\varphi(k)-1} \lambda_i \, p^i.$$

That is if the value of the base is m then we need to compute

$$\prod_{i=0}^{\varphi(k)-1} m^{\lambda_i \, p^i}$$

which can be re-arranged to become

$$\prod_{i=0}^{\varphi(k)-1} (m^{p^i})^{\lambda_i}.$$

The idea here is to use the Frobenius to compute the m^{p^i} in the the Expression 5.3 while the hard part can be computed using the multi-exponentiation algorithm [64].

5.4 Our way of computing the hard part

We utilize the structure of the polynomial that defines the field size p, and the size of the cryptographic group r, to optimise the computation of the hard-part of the final exponentiation. We demonstrate our optimisation by working through the families of $k = 8$ and $k = 18$ curves which are reported in Chapter 3.

5.4.1 The k = 8 family of curves

Recall the parameters of the $k = 8$ curves from Chapter 3 in Theorem 3.3.1. In this case the hard part of final exponentiation is to the power

$\Phi_8(p(z))/r(z)$ which becomes $(p^4+1)/r(z)$ and proceed as follows.

Firstly, we express the hard part to the base p and get:

$$\sum_{i=0}^{3} \lambda_i \, p(z)^i$$

where

$$\begin{aligned}
\lambda_3 &= (15z^2 + 30z + 75)/6;\\
\lambda_2 &= (2z^5 + 4z^4 - z^3 + 26z^2 - 55z - 144)/6;\\
\lambda_1 &= (-5z^4 - 10z^3 - 5z^2 - 80z + 100)/6;\\
\lambda_0 &= (z^5 + 2z^4 + 7z^3 + 28z^2 + 10z + 108)/6.
\end{aligned}$$

To make the computations easier we eliminate the denominator in the above set of equations. This means we are evaluating the pairing to the sixth power. Fortunately, this does not affect the bilinearity property of the pairing when r is of cryptographic size.

Secondly, we construct almost optimal addition chain sequence which contains all the exponents of the above equations. Fortunately, in our case we are dealing with small values and the number sets already contains some subsets of an addition sequence.

It is easy, both manually or through computer search, to find an almost optimal addition sequence for that given set of numbers.

$$\{1, 2, 4, 5, 7, 10, 15, \underline{25}, 26, 28, 30, \underline{36}, \underline{50}, 55, 75, 80, 100, 108, 144.\}$$

The extra numbers to complete the addition sequence are underlined. The vectorial addition chain (see Section 1.6.1) derived from the addition sequence just requires 27 multiplication and 6 squarings in order to complete the hard part of the final exponentiation.

5.4.2 The k = 18 family of curves

Recall the parameters of the $k = 18$ curves from Chapter 3 in Theorem 3.3.4. The hard part of final exponentiation is to the power $\Phi_{18}(p(z))/r(z)$. Proceeding again as above, we compute:

$$
\begin{aligned}
\lambda_5(z) &= (49z^2 + 245z + 343)/3; \\
\lambda_4(z) &= (7z^6 + 35z^5 + 49z^4 + 112z^3 + 581z^2 + 784z)/3; \\
\lambda_3(z) &= (5z^7 - 25z^6 - 35z^5 - 87z^4 - 450z^3 - 609z^2 + 54)/3; \\
\lambda_2(z) &= (-49z^5 - 245z^4 - 343z^3 - 931z^2 - 4802z - 6517)/3; \\
\lambda_1(z) &= (14z^6 + 70z^5 + 98z^4 + 273z^3 + 1407z^2 + 1911z)/3; \\
\lambda_0(z) &= (-3z^7 - 15z^6 - 21z^5 - 62z^4 - 319z^3 - 434z^2 + 3)/3.
\end{aligned}
$$

Using the same argument as in the $k = 8$ curves case, we evaluate the cube of the pairing to remove the awkward denominator of 3. In this case the coefficients again nearly form a natural addition chain. Our best attempt to find an addition sequence containing all of the exponents in the above, is as follows:

$$
\begin{gathered}
\underline{1}, \underline{2}, 3, \underline{4}, 5, 7, \underline{8}, 14, 15, \underline{16}, 21, 25, \underline{28}, 35, \underline{42}, 49, 54, 62, 70, \\
87, 98, 112, \underline{147}, 245, 273, \underline{294}, 319, 343, \underline{392}, 434, 450, 581, \\
609, 784, 931, \underline{1162}, 1407, \underline{1862}, 1911, \underline{3724}, \underline{4655}, 4802, 6517.
\end{gathered}
$$

The vectorial chain derived from this addition sequence requires just 56 multiplications and 14 squarings to complete the calculation of the hard part of the final exponentiation. We use the solution above as the computations are performed over an extension field and squaring are therefore notably cheaper than multiplications.

5.5 Conclusion

The Tate pairing and its variants, ate and R-ate, are the most efficient pairings to date. These pairings require an element from $\mathbb{G}_2$ to be also of prime order. Hashing to a point in $\mathbb{G}_2$ requires additional multiplication by a large cofactor. In this chapter, we have shown how to efficiently multiply a point in $\mathbb{G}_2$ defined on a twist curve by a large cofactor.

Finally, we have also described a new approach for implementation of the hard part of the final exponentiation in the calculation of the Tate pairing or its variants, which is generally applicable, faster and requires less memory than the previously described methods.

Chapter 6

Summary of contributions

6.1 Introduction

An efficient and secure implementation of pairing-based protocols depends on what are known as *pairing-friendly* curves. These are curves with a large prime order subgroup and a small embedding degree. However, the embedding degree of most randomly generated curves is too large for an efficient implementation. Hence there are two main problems to be addressed when aiming at a practical implementation of the pairing-based protocols. The first is the construction of pairing-friendly curves. The second is to make pairing computations more efficient and suitable for different pairing-based protocols. In this thesis we addressed both areas to some extent.

6.2 Pairing-friendly elliptic curves

The construction of pairing-friendly elliptic curves is addressed in Chapter 3. Inspired by the work of Brezing and Weng [17] we construct new curves. The main idea in the construction is to use minimal polynomials of the elements of the cyclotomic field other than the cyclotomic polynomial $\Phi_\ell(z)$

to define the cyclotomic field $\mathbb{Q}(\zeta_\ell)$. The potential of the method has been illustrated by constructing families of pairing-friendly elliptic curves of degrees $8, 12, 16, 18, 32, 36$ and 40.

However, since we require $\ell = lcm(k, D)$, with a large D the search space for an element $\gamma(\zeta_\ell)$ becomes huge making this method not favourable in such a case. Furthermore, the limits imposed on $\mathcal{M}$ and $\mathcal{L}$ might, in one way or the other, lead to missing some good curves.

Maybe by extending the search space, further families of ideal or near ideal pairing-friendly curves might be found.

We also have seen that the proposed curves have nice properties favouring an efficient implementation. For instance, these curves have a small ρ-value interpreted as the ratio of a cryptographic group's required bandwidth to its security level. In fact, curves with smaller ρ-values provide the best performance in implementations. Furthermore, these curves admit higher order twists of either degree 6 or 4. Use of twisted curves facilitate an efficient implementation of $\mathbb{G}_2$ in the pairing computation by defining the group on a curve defined on a much smaller field than anticipated.

However, elliptic curves with small class number are very special and therefore might be considered weak from a cryptographic viewpoint. Even though there is no known attack taking advantage of this yet, we might want to generate curves with slightly larger class number to avoid the potential attacks. This becomes a challenge if we need to keep the ρ-values as attractive as they are.

As such the question of constructing ordinary pairing-friendly elliptic curves of prime or near prime order is still open for most embedding degrees.

6.3 Genus two pairing-friendly hyperelliptic curves

Based on the work of Kawazoe and Takahashi [51], in Chapter 4 we have presented a generalisation of a construction of genus 2 pairing-friendly hyperelliptic curves of type $y^2 = x^5 + ax$. With our approach we find new curves and improve ρ-values for some previously reported curves.

A problem with some of the reported curves is that the degree of the polynomial $r(z)$, which defines the prime order subgroup, is greater than 40. As pointed out in [32] if we would like to generate pairing-friendly curves and wish to specify the field and prime subgroup sizes the degree of the polynomials $p(z)$ and $r(z)$ should not be too large. For example, if one wants to construct curves at 256-bit security level with a degree 32 polynomial that defines the prime subgroup, we could expect to find only about four curves (see [32]).

Furthermore, the ρ-value of most of these curves are still large when compared to the pairing-friendly elliptic curve case. Referring to Table 1.1 we see that for most of our reported curves their value $k \cdot \rho$ falls outside the range of the table. We would like the ρ-value of the families to be closer to 1.

6.4 Implementation optimisation

The two variants of Tate pairing; the ate[46] and the R-ate [58] pairings are the most efficient pairings to date. Both pairings require an element from $\mathbb{G}_2$ to be of prime order. Hashing to a point in $\mathbb{G}_2$ therefore, would require a multiplication by a large cofactor. In Chapter 5 we have shown how to efficiently multiply a point in $\mathbb{G}_2$ defined over on a twisted curve by a large cofactor. Our approach uses the theory of additional chains which includes a problem of finding the shortest possible addition sequence. We observe that sometimes it is preferable to use slightly longer addition sequence which trades addition for doublings since in most cases point doublings are significantly faster than point additions. This scenario is complex and requires a further investigation.

Finally, we have also shown a new method for implementing the hard part of the final exponentiation in the calculation of the Tate pairing and its variants, which is generally applicable, faster and requires less memory than the previously described methods.

Bibliography

[1] C. A. Antonio, S. Tanaka, and K. Nakamula. Implementing Cryptographic Pairings Over Curves of Embedding Degrees 8 and 10. Cryptology ePrint Archive, Report 2007/426, 2007. `http://eprint.iacr.org/2007/426.pdf`.

[2] A. O. L. Atkin and F. Morain. Elliptic Curves and Primality Proving. *Mathematics of Computation*, 61(203):29–68, 1993.

[3] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* CRC Press, 2005.

[4] J. Balakrishnan, J. Belding, S. Chisholm, K. Eisentraeger, K. E. Stange, and E. Teske. Pairings on Hyperelliptic Curves. *Computing Research Repository*, abs/0908.3731, 2009. `http://www.math.psu.edu/eisentra/pairings.pdf`.

[5] P. S. L. M. Barreto, S. D. Galbraith, C. O'Eigeartaigh, and M. Scott. Efficient Pairing Computation on Supersingular Abelian Varieties. *Designs, Codes and Cryptography*, 42(3):239–271, 2007.

[6] P. S. L. M. Barreto, H. Yong Kim, B. Lynn, and M. Scott. Efficient Algorithms for Pairing-Based Cryptosystems. In M. Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 354–368. Springer, 2002.

[7] P. S. L. M. Barreto, B. Lynn, and M. Scott. Constructing Elliptic Curves with Prescribed Embedding Degrees. In S. Cimato and C. Galdi and G. Persiano, editor, *Security in Communication Networks*, volume 2576 of *Lecture Notes in Computer Science*, pages 257–267. Springer, 2002.

[8] P. S. L. M. Barreto and M. Naehrig. Pairing-Friendly Elliptic Curves of Prime Order. In B. Preneel and S. E. Tavares, editor, *Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer, 2005.

[9] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Note series.* Cambridge University Press, 1999.

[10] I. F. Blake, G. Seroussi, and N. P. Smart. *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, 2005.

[11] D. Bleichenbacher, W. Bosma, and A. K. Lenstra. Some Remarks on Lucas-Based Cryptosystems. In D. Coppersmith, editor, *Advances in Cryptology—CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 386–396. Springer-Verlag, 1995.

[12] D. Boneh and X. Boyen. Short Signatures Without Random Oracles. In C. Cachin and J. Camenisch, editor, *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73. Springer, 2004.

[13] D. Boneh and M. K. Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.

[14] D. Boneh, B. Lynn, and H. Shacham. Short Signatures from the Weil Pairing. *Journal of Cryptology*, 17(4):297–319, 2004.

[15] W. Bosma, J. J. Cannon, and C. Playoust. The Magma Algebra System I: The User language. *Journal of Symbolic Computation*, 24(3/4):235–265, 1997.

[16] V. Bouniakowsky. Nouveaux théorémes relatifs á la distinction des nombres premiers et é la décomposition des entiers en facteurs. *Mém. Acad. Sci. Saint-Pétersbourg*, 6(3):305–329, 1857.

[17] F. Brezing and A. Weng. Elliptic Curves Suitable for Pairing Based Cryptography. *Designs, Codes and Cryptography*, 37(1):133–141, 2005.

[18] D. G. Cantor. Computing in the Jacobian of a Hyperelliptic Curve. *Mathematics of Computation*, 48(177):95–95, 1987.

[19] C. Cocks and R. G. E. Pinch. ID-based Cryptosystems Based on Weil Pairing. Unpublished manuscript, 2001.

[20] H. Cohen. *A Course in Computational Algabraic Number Theory*, volume 138. Springer-Verlag Berlin, 1993.

[21] D. Coppersmith. Fast Evaluation of Discrete Logarithms in Fields of Characteristic Two. *IEEE Transactions on Information Theory*, 30(4):587–594, 1984.

[22] P. de Rooij. Efficient Exponentiation Using Precomputation and Vector Addition Chains. In A. de Santis, editor, *EUROCRYPT: Advances in Cryptology: Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 389–399, 1994.

[23] S. Van der Kruijssen. Addition Chains - Efficient Computing Powers. Bachelor's thesis, VU University Amsterdam, 2007.

[24] A. Jun Devegili, M. Scott, and R. Dahab. Implementing Cryptographic Pairings over Barreto-Naehrig Curves. In T. Takagi and T. Okamoto and E. Okamoto and T. Okamoto, editor, *Pairing-Based Cryptography - Pairing 2007, Tokyo, Japan, Proceedings*, volume 4575 of *Lecture Notes in Computer Science*, pages 197–207. Springer, 2007.

[25] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(5):644–654, 1976.

[26] R. Dupont, A. Enge, and F. Morain. Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields. *J. Cryptology*, 18(2):79–89, 2005.

[27] K. Eisentraeger and K. Lauter. A CRT Algorithm for Constructing Genus 2 Curves over Finite Fields. In F. Rodier and S. Vladut, editors, *Arithmetic, Geometry and Coding Theory (AGCT-10), Séminaires et Congrés, Proceedings*, volume 21, pages 161–176. Société Mathématique de France, 2011.

[28] A. Enge and A. V. Sutherland. Class Invariants by the CRT Method. In G. Hanrot, F. Morain, and E. Thomé, editors, *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France. Proceedings*, volume 6197 of *Lecture Notes in Computer Science*, pages 142–156. Springer, 2010.

[29] D. Freeman. Constructing Pairing-friendly Elliptic Curves with Embedding Degree 10. In F. Hess, S. Pauli, and M. E. Pohst, editors, *Algorithmic Number Theory, ANTS-VII, Berlin, Germany, Proceedings*, volume 4076 of *Lecture Notes in Computer Science*, pages 452–465. Springer, 2006.

[30] D. Freeman. Constructing Pairing-Friendly Genus 2 Curves with Ordinary Jacobians. In T. Takagi and T. Okamoto and E. Okamoto and T. Okamoto, editor, *Pairing-Based Cryptography - Pairing 2007, Tokyo, Japan, Proceedings*. Springer, 2007.

[31] D. Freeman. A Generalized Brezing-Weng Algorithm for Constructing Pairing-friendly Ordinary Abelian Varieties. In S. D. Galbraith and K. G. Paterson, editors, *Pairing-Based Cryptography - Pairing 2008, Egham, UK, Proceedings*, volume 5209 of *Lecture Notes in Computer Science*, pages 146–163. Springer, 2008.

[32] D. Freeman, M. Scott, and E. Teske. A Taxonomy of Pairing-Friendly Elliptic Curves. *J. Cryptology*, 23(2):224–280, 2010.

[33] D. Freeman, P. Stevenhagen, and M. Streng. Abelian Varieties with Prescribed Embedding Degree. In A. J. van der Poorten and A. Stein, editor, *Algorithmic Number Theory Symposium, Proceedings*, volume

5011 of *Lecture Notes in Computer Science*, pages 60–73. Springer, 2008.

[34] D. M. Freeman and T. Satoh. Constructing Pairing-friendly Hyperelliptic Curves Using Weil Restriction. *Journal of Number Theory*, 131(5):959 – 983, 2011.

[35] G. Frey and H. Rück. A Remark Concerning m-divisibility and the Discrete Logarithm in the Divisor Class Group of Curves. *J. Mathematics of Computation*, 62(206):865–874, 1994.

[36] E. Furukawa, M. Kawazoe, and T. Takahashi. Counting Points for Hyperelliptic Curves of Type $y^2 = x^5 + ax$ over Finite Prime Fields. In M. Matsui and R. J. G. Zuccherato, editors, *Selected Areas in Cryptography,Ottawa, Canada, Proceedings*, volume 3006 of *Lecture Notes in Computer Science*, pages 26–41. Springer, 2003.

[37] S. D. Galbraith, K. Harrison, and D. Soldera. Implementing the Tate Pairing. In C. Fieker and D. R. Kohel, editors, *Algorithmic Number Theory, ANTS-V, Sydney, Australia, Proceedings*, volume 2369 of *Lecture Notes in Computer Science*, pages 324–337. Springer, 2002.

[38] S. D. Galbraith, J. F. McKee, and P. C. Valença. Ordinary Abelian Varieties Having Small Embedding Degree. *Finite Fields and Their Applications*, 13(4):800–814, 2007.

[39] S. D. Galbraith and M. Scott. Exponentiation in Pairing-friendly Groups Using Homomorphisms. In S. D. Galbraith and K. G. Paterson, editors, *Pairing-Based Cryptography - Pairing 2008, Egham, UK, Proceedings*, volume 5209 of *Lecture Notes in Computer Science*, pages 211–224. Springer, 2008.

[40] R. P. Gallant, R. J. Lambert, and S. A. Vanstone. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. In J. Kilian, editor, *Advances in Cryptology - CRYPTO 2001, Santa Barbara, California, USA, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 190–200. Springer, 2001.

[41] P. Gaudry. An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves. In B. Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, Bruges, Belgium, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 19–34. Springer, 2000.

[42] P. Gaudry and R. Harley. Counting Points on Hyperelliptic Curves over Finite Fields. In W. Bosma, editor, *Algorithmic Number Theory, ANTS-IV, Leiden, The Netherlands, Proceedings*, volume 1838 of *Lecture Notes in Computer Science*, pages 313–332. Springer, 2000.

[43] Y. Ge. Elementary Properties of Cyclotomic Polynomials. *Mathematical Reflections*, 76(2):1–8, 2008.

[44] D. M. Gordon. A Survey of Fast Exponentiation Methods. *Journal of Algorithms*, 27(1):129–146, 1998.

[45] D. Hankerson, A. J. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography.* Springer-Verlag, 2004.

[46] F. Hess, N. P. Smart, and F. Vercauteren. The Eta Pairing Revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006.

[47] J. S. Milne. Abelian Variety. http:/www.jmilne.org/, 2008. `http://www.jmilne.org/math/`.

[48] A. Joux. A One Round Protocol for Tripartite Diffie-Hellman. *J. Cryptology*, 17(4):263–276, 2004.

[49] E. J. Kachisa. Generating More Kawazoe-Takahashi Genus 2 Pairing-Friendly Hyperelliptic Curves. In M. Joye and A. Miyaji and A. Otsuka, editor, *Pairing-Based Cryptography - Pairing 2010, Yamanaka Hot Spring, Japan, Proceedings*, volume 6487 of *Lecture Notes in Computer Science*, pages 312–326. Springer, 2010.

[50] E. J. Kachisa, E. F. Schaefer, and M. Scott. Constructing Brezing-Weng Pairing-friendly Elliptic Curves Using Elements in the Cyclotomic Field. In S. D. Galbraith and K. G. Paterson, editors, *Pairing-Based Cryptography - Pairing 2008, Egham, UK, Proceedings*, volume 5209 of *Lecture Notes in Computer Science*, pages 126–135. Springer, 2008.

[51] M. Kawazoe and T. Takahashi. Pairing-friendly Hyperelliptic Curves with Ordinary Jacobians of Type $y^2 = x^5 + ax$. In S. D. Galbraith and K. G. Paterson, editors, *Pairing-Based Cryptography - Pairing 2008, Egham, UK. Proceedings*, volume 5209 of *Lecture Notes in Computer Science*, pages 164–177. Springer, 2008.

[52] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.

[53] N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, 1(3):139–150, 1989.

[54] S. Lang. *Abelian Varieties.* Springer, 1983.

[55] S. Lang. *Elliptic Functions*, volume 112. Springer-Verlag Berlin, 1987.

[56] S. Lang. *Algebra.* Graduate Texts in Mathematics. Springer, 2002.

[57] G. J. Lay and H. G. Zimmer. Constructing Elliptic Curves with Given Group Order over Large Finite Fields. In L. M. Adleman and M. A.

Huang, editors, *Algorithmic Number Theory, First International Symposium, ANTS-I, Ithaca, NY, USA, Proceedings*, volume 877 of *Lecture Notes in Computer Science*, pages 250–263. Springer, 1994.

[58] E. Lee, H. S. Lee, and C. M. Park. Efficient and Generalized Pairing Computation on Abelian Varieties. *IEEE Transactions on Information Theory*, 55(4):1793–1803, 2009.

[59] A. K. Lenstra, H. W. Lenstra, M. S. Manasse, and J. M. Pollard. The Number Field Sieve. In B. Awerbuch, editor, *22nd Annual Symposium on Theory of Computing, Proceedings*, pages 564–572, Baltimore, MD, USA, 1990. ACM Press.

[60] X. Lin, C. Zhao, F. Zhang, and Y. Wang. Computing the Ate Pairing on Elliptic Curves with Embedding Degree $k = 9$. *IEICE Transactions*, 91-A(9):2387–2393, 2008.

[61] D. Marcus. *Number Fields.* Springer-Verlag, New York, 1977.

[62] K. Matthews. Thue's Theorem and the Diophantine Equation $x^2 - Dy^2 = \pm N$. *Mathematics of Computation*, 71(239):1281–1286, 2002.

[63] A. Menezes, S. Vanstone, and T. Okamoto. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. In B. Awerbuch, editor, *The 23rd Annual Symposium on the Theory of Computing, Proceedings*, pages 80–89, New Orleans, LS, 1991. ACM Press.

[64] A. J. Menezes, P. C. van Oorschot, and S. A. Vanston. *Handbook of Applied Cryptography.* CRC Press, 1996.

[65] M. Mignotte and A. Tall. A Note on Addition Chains. *International Journal of Algebra*, 5(6):269 – 274, 2011.

[66] V. S. Miller. Uses of Elliptic Curves in Cryptography. In H. C. Williams, editor, *Advances in cryptology — CRYPTO '85: Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer-Verlag, 1985.

[67] V. S. Miller. The Weil Pairing, and its Efficient Calculation. *Journal of Cryptology*, 17(4):235–261, 2004.

[68] A. Miyaji. On Ordinary Elliptic Curve Cryptosystems. In H. Imai, R. L. Rivest, and T. Matsumoto, editors, *Advances in Cryptology—ASIACRYPT '91*, volume 739 of *Lecture Notes in Computer Science*, pages 460–469, Fujiyoshida, Japan, 1991. Springer-Verlag.

[69] A. Miyaji, M. Nakabayashi, and S. Takano. New Explicit Conditions of Elliptic Curve Traces for FR-Reduction. *TIEICE: IEICE Transactions on Communications/Electronics/Information and Systems*, E84(5):1234 –1243, 2001.

[70] N. El Mrabet, N. Guillermin, and S. Ionica. A Study of Pairing Computation for Elliptic Curves with Embedding Degree 15. Cryptology ePrint Archive, Report 2009/370, 2009. `http://eprint.iacr.org/2009/370`.

[71] M. Naehrig, P. S. L. M. Barreto, and P. Schwabe. On Compressible Pairings and their Computation. In S. Vaudenay, editor, *Progress in Cryptology - AFRICACRYPT 2008, Casablanca, Morocco. Proceedings*, volume 5023 of *Lecture Notes in Computer Science*, pages 371–388. Springer-Verlag, 2008.

[72] K. Nagao. Improvement of Thériault Algorithm of Index Calculus of Jacobian of Hyperelliptic Curves of Small Genus. Technical report, 2004. http://eprint.iacr.org/2004/161.

[73] National Institute of Standards and Technology. Digital Signature Standard. http://csrc.nist.gov, 2011. http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.

[74] J. Olivos. On Vectorial Addition Chains. *Journal of Algorithms*, 2(1):13–21, 1981.

[75] PARI-GP. PARI-GP, Version 2.3.2. http://pari.math.u-bordeaux.fr/, 2006. http://pari.math.u-bordeaux.fr/.

[76] L. J. D. Perez, E. J. Kachisa, and M. Scott. Implementing Cryptographic Pairings:a magma tutorial. Cryptology ePrint Archive, Report 2009/072, 2009. http://eprint.iacr.org/2009/072.pdf.

[77] J. M. Pollard. Monte Carlo Methods for Index Computation mod p. *Mathematics of Computation*, 32(143):918–924, 1978.

[78] R. L. Rivest, A. Shamir, and L. Adelman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[79] H. Rück. Abelian Surfaces and Jacobian Varieties Over Finite Fields. *Compos. Math.*, 76(3):351–366, 1990.

[80] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems Based on Pairing. In *2000 Symposium on Cryptography and Information Security (SCIS2000), Okinawa, Japan*, 2000.

[81] A. Schinzel and W. Sierpinski. Sur certaines hypothéses concernant les nombres premiers. *Acta Arith.*, 4:185–208, 1958.

[82] R. Schoof. Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p. *Mathematics of Computation*, 44:483–494, 1985.

[83] M. Scott. A C^{++} Implementation of the Schoof's Algorithms for Counting Points on an Arbitrary Elliptic Curve. htt://www.dcu.ie, 2002. `ftp://ftp.computing.dcu.ie/pub/crypto/cm.cpp`.

[84] M. Scott. An NTL Program to Find Brezing and Weng Curves. http://www.computing.dcu.ie, 2007. `ftp://ftp.computing.dcu.ie/pub/crypto/bandw.cpp`.

[85] M. Scott. Implementing Cryptographic Pairings. In T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, editors, *Pairing-Based Cryptography - Pairing 2007, Tokyo, Japan, Proceedings*, volume 4575 of *Lecture Notes in Computer Science*. Springer, 2007.

[86] M. Scott and P. S. L. M. Barreto. Generating more MNT Elliptic Curves. *Designs, Codes and Cryptography*, 38(2):209–217, 2006.

[87] M. Scott, N. Benger, M. Charlemagne, L. J. Dominguez Perez, and E. J. Kachisa. Fast Hashing to G_2 on Pairing-friendly Curves. In H. Shacham and B. Waters, editor, *Pairing-Based Cryptography - Pairing 2009, Palo Alto, CA, USA, Proceedings*, volume 5671 of *Lecture Notes in Computer Science*, pages 102–113. Springer, 2009.

[88] M. Scott, N. Benger, M. Charlemagne, L. J. Dominguez Perez, and E. J. Kachisa. On the Final Exponentiation for Calculating Pairings on Ordinary Elliptic Curves. In H. Shacham and B. Waters, editor, *Pairing-Based Cryptography - Pairing 2009, Palo Alto, CA, USA,*

Proceedings, volume 5671 of *Lecture Notes in Computer Science*, pages 78–88. Springer, 2009.

[89] I. R. Shafarevich. *Basic Algebraic Geometry*, volume 213 of *Grundlehren der math. Wissenschaften.* Springer, 1977.

[90] A. Shamir. Identity-based Cryptosystem and Signature Scheme. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology – CRYPTO ' 84*, volume 196 of *Lecture Notes in Computer Science*, pages 120–126. Springer-Verlag, Berlin Germany, 1985.

[91] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions.* Princeton University Press, Revised edition, 1998.

[92] V. Shoup. Efficient Computation of Minimal Polynomials in Algebraic Extensions of Finite Fields. In S. Dooley, editor, *International Symposium on Symbolic and Algebraic Computation, Simon Fraser University, Vancouver, BC, Canada*, pages 53–58. ACM Press, 1999.

[93] V. Shoup. A Library for Doing Number Theory. http://www.shoup.net, 2006. `http://www.shoup.net/ntl/`.

[94] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate texts in Mathematics.* Springer, 1986.

[95] J. H. Silverman. *Advanced Topics in the Arithmetics of Elliptic Curves*, volume 151 of *Graduate texts in Mathematics.* Springer, 1994.

[96] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Springer-Verlag, Berlin-Heidelberg-New York, 1992.

[97] N. P. Smart and F. Vercauteren. On Computable Isomorphisms in Efficient Asymmetric Pairing-based Systems. *Discrete Applied Mathematics*, 155(4):538–547, 2007.

[98] M. Stam. *Speeding up Subgroup Cryptosystems.* PhD thesis, Technische Universiteit Eindhoven, 2003.

[99] S. Tanaka and K. Nakamula. Constructing Pairing-Friendly Elliptic Curves Using Factorization of Cyclotomic Polynomials. In S. D. Galbraith and K. G. Paterson, editors, *Pairing-Based Cryptography - Pairing 2008, Egham, UK. Proceedings*, volume 5209 of *Lecture Notes in Computer Science*, pages 136–145. Springer, 2008.

[100] J. Tate. Endomorphisms of abelian Varieties over Finite Fields. *Invent Math.*, 2(1):134–144, 1966.

[101] N. Thériault. Index Calculus Attack for Hyperelliptic Curves of Small Genus. In Chi-Sung Laih, editor, *Advances in Cryptology - ASIACRYPT 2003, Taipei, Taiwan, Proceedings*, volume 2894 of *Lecture Notes in Computer Science*, pages 75–92. Springer, 2003.

[102] L. C. Washington. *Introduction to Cyclotomic Fields.* Springer, Springer, Verlag, 1982.

[103] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography.* Chapman & Hall/CRC, New York, 2nd edition, 2008.

[104] W. Waterhouse. Abelian Varities over Finite Fields. *Annales scientifiques del l'E.N.S. Ecole Norm.Sup*, 2(4):521–560, 1969.

[105] A. Weng. Constructing Hyperelliptic Curves of Genus 2 Suitable for Cryptography. *Mathematics of Computation*, 72(241):435–458, 2003.

[106] Y. Yacobi. Exponentiating Faster with Addition Chains. In I. B. Damgård, editor, *Advances in Cryptology—EUROCRYPT 1990, Proceedings*, volume 473 of *Lecture Notes in Computer Science*, pages 222–229. Springer-Verlag, 1990.

[107] F. Zhang. Twisted Ate Pairing on Hyperelliptic Curves and Applications. *Science China Information Sciences*, 53(8):1528–1538, 2010.