university of groningen

faculty of science and engineering

A Cryptosystem Based on the Weil Pairing on an Elliptic Curve

Author:
Laura Gioanna Paxton
(s4420454)

Supervisor:
prof. dr. Jaap Top
Second supervisor:
prof. dr. Cecília Salgado Guimarães da Silva

Bachelor's Thesis
in Mathematics
at the University of Groningen

August 8, 2024

Contents

1 Introduction

We are looking to build a cryptosystem using a Weil pairing following the example provided by Lawrence C. Washington [Was08, Chapter 6.9].

The study of elliptic curves has become a cornerstone of modern cryptography, providing robust frameworks for secure communication protocols. Elliptic Curve Cryptography (ECC) is particularly valued for its efficiency and security, making it a key component in both classical and emerging cryptosystems.

Previous research by Boneh and Franklin (2001) introduced Identity-Based Encryption (IBE) schemes that leveraged the algebraic structure of elliptic curves, offering significant advancements in cryptographic practices.

Motivated by the intrigue of dissecting the cryptosystem to analyse and present all its components, this thesis aims to extend Washington's IBE cryptosystem by incorporating novel parameters, specifically focusing on the elliptic curve described below in (4) with an endomorphism δ given in (3). The primary objective is to analyze the requirements and establish conditions under which these new parameters can be effectively integrated, therefore giving a detailed description of the system.

The main contributions of this thesis include:

1. A thorough examination of the elliptic curve's structure and endomorphism, compared against the Weil pairing requirements, leading to a non-trivial construction of a modified Weil pairing.
2. Determination of prime conditions p and ℓ to ensure compatibility with the modified Weil pairing and other algebraic structures
3. A detailed blueprint for future adaptations, enabling further exploration and optimization of cryptographic parameters.

This thesis is organized as follows: Chapter 2 introduces the concepts of elliptic curve cryptography, providing essential background knowledge, and describes Identity-Based Encryption (IBE) schemes, with a detailed overview of Boneh and Franklin's IBE system. Chapter 3 outlines the cryptosystem we aim to build, along with its specific requirements. Chapter 4 presents an analysis of the newly selected parameters, identifying the necessary conditions for their compatibility with the cryptosystem. Finally, Chapter 5 details the implementation of the cryptosystem using the Computational Algebra System, Magma. The thesis concludes with a brief summary and discussion of the results.

2 Elliptic Curve Cryptography and Identity Based Encryption

2.1 Elliptic Curve Cryptography

Elliptic Curve Cryptography, or ECC, was proposed independently by Neal Koblitz and Victor S. Miller in 1985 as an alternative to traditional public-key cryptosystems like RSA and DSA, as cited in [KMV00]. The reason for it being an attractive alternative and the reason why many present day crypto schemes use ECC is that it offers the same level of security with smaller key sizes compared to other public-key cryptosystems like RSA and DSA. This is due to the computational complexity of the simpler problems it is based on.
The base problem is the Elliptic Curve Discrete Logarithm Problem, or ECDLP. The ECDLP involves finding or computing an integer k having been given two points $P, Q \in E(K)$, where $Q = kP$. Solving this problem is significantly harder than the integer factorization problem or the discrete logarithm problem over finite fields, which RSA and DSA rely on, respectively. For RSA, the best-known attack is based on integer factorization, which can be solved using sub-exponential algorithms like the General Number Field Sieve. In contrast, the best-known attacks on ECC require solving the ECDLP, which currently only has exponential-time algorithms. This means that, as the key size increases, the difficulty of breaking ECC grows much faster than for RSA.
An example for the difference in key size is 3072-bits for an RSA scheme and 256-bits for an ECC scheme for the same level of security[RSA21].

To understand the ECDLP, one must understand the algebraic group structure of elliptic curves over finite fields and the definition of integer multiplication on a point of an elliptic curve. The following definitions have been taken from Silverman's book "The Arithmetic of Elliptic Curves", [Sil86].

First and foremost, the general form of the elliptic curve must be introduced: every elliptic curve can be given in the form

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

where a_1, a_3, a_2, a_4 and a_6 are all in some finite field K. In this case E is said to be defined over K, which one can denote as E/K. The points over the elliptic curve are defined as

$$E(K') = \{(x, y) \in K'^2 \text{ satisfying } y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

Note, K' is not necessarily the same finite field K of which the elliptic curve's coefficients are elements yet K is contained in K'. In the rest of the thesis the notation $E(K)$ will be used out of convention. Also, the inclusion of the point at infinity O is crucial for the algebraic structure to be well-defined. The reason for the existence of the point is the fact that every such curve can be written as the locus in $\mathbb{P}^2$ of a cubic equation with only one point on the line at infinity.

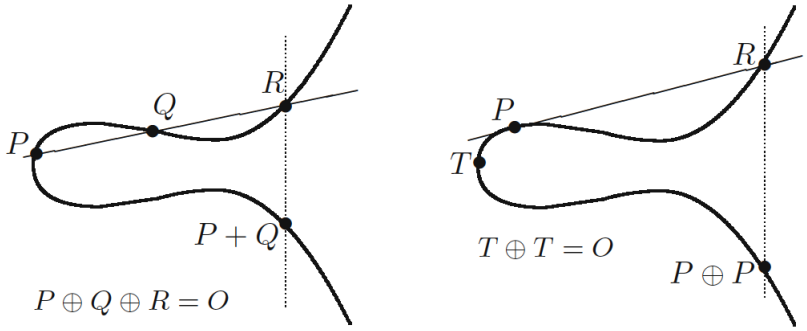
$E(K')$ forms an abelian group with elliptic point addition as the group operation. The point at infinity O acts as the identity element. It is clear by definition of addition how the point at infinity can act as an identity element.

The group operation of elliptic point addition has a unique definition:

Definition 1. *Let $P, Q \in E(K)$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to E at P), and let R be the third point of intersection of L with L. Let L' be the line through R and O. Then L' intersects E at R, O and a third point. We denote that third point by $P + Q$. In the figure, the group law is denoted by $\oplus$, instead of $+$.*

Being an abelian group, elliptic point addition satisfies the following properties:

- (associativity) $\forall P, Q, R \in E(K)$ we have $P + (Q + R) = (P + Q) + R$
- (unit element) $\forall P \in E(K)$ we have $O + P = P = P + O$
- (inverses) $\forall P \in E(K) \exists P' \in E(K)$ such that $P + P' = O = P' + P$



Addition of distinct points Adding a point to itself

- (commutativity)$\forall P, Q \in E(K)$ we have $P + Q = Q + P$

Often, the multiplication map, denoted $[m]P$ with $m \in \mathbb{Z}_{\geq 0}$, will be used to signify $[m]P = P + P + ... + P$, so adding P m times to itself. $[-m]P$ is defined as $[m](-P) = -P - P... - P$. An algorithmic definition of the group operation will follow after the introduction of the elliptic curve that will be discussed in this thesis. This is because the algorithm is coefficient dependent and therefore unique to each elliptic curve. The reader may skip forward to the section 4.1.1 in case of intrigue to see how the algorithm exists now.

Like any algebraic group, $E(K)$ has subgroups. One certain subgroup plays a major role in this thesis and will theretofore be introduced. Our interest lies in the n- torsion group. This subgroup contains points that are all of order that divides n. The definition is as follows:

Definition 2. *Let E be an elliptic curve over a finite field K , and let $n \geq 2$ be an integer. An n-torsion point of $E(K)$ is a point P of $E(K)$ such that $[n]P = O$. The set of n-torsion points is denoted $E(K)[n]$.*

2.2 Identity Based Encryption

2.2.1 A general Identity Based Encryption

The Identity Based Encryption, or IBE for short, is a form of public key encryption first proposed by Shamir in 1984 [Sha84]. Its major difference to a conventional public key encryption system is the elimination of the authenticity problem of public keys.

In general crypto schemes, a public key must be assigned to each user allowing for the encryption of messages. If a mistake had been made in the assigning of the public key, the encrypted messages would be decipherable by the wrong person and the intended recipient wouldn't have the according private key to decipher the message. The IBE system finds a solution to this problem by directly linking the digital identifier or ID with the public key. The public key can therefore be derived from the public information of the user, most importantly from the digital ID. Hence, the public key is readily available to anyone who knows the digital ID of the person with whom they wish to correspond.

The private key is then derived from the public key. However, private keys are not generated by users themselves. This is logical as if they could be derived, any user could compute the private keys from anyone else's public key and decipher all messages, leading to a very insecure cryptosystem. The fact that users cannot derive their own private keys calls for the necessity of a third party, commonly called the Trusted Authority (TA) or the Key Generation Center (KGC). The TA is able to generate the private keys for users as it has the privilege of knowing some secret information, called the master key. A user's private key is computed by means of some one-way function of the public key or, better said, the digital ID and the master key. For this system a secure communication channel between the TA and the user is necessary to share the private key with the intended user only.

For identity based encryption to work, the digital identity has to be unique and corresponding to the correct user. Most companies or communication systems make use of a Registration Authority, RA. An RA issues digital identifiers to all users in the system, securing uniqueness and authenticity of the user. An example for such a system is the emailing system used at our university, Rijksuniversiteit Groningen. As soon as a person enters the digital system, be it student or staff, they receive an email address based on their initials and last name. If two people have the exact same first, middle and last name a differentiation is made via use of numbers or extra specifications of the users identity in the email address. This allows for unique email addresses and a publicly known digital ID, accessible to all.

While Shamir's concept was innovative as the first concept of an identity based encryption scheme, it faced several practical limitations, including issues with efficiency, security, key management, and scalability. These limitations made his IBE scheme impractical for real-world use at the time. One can find his proposed system in his text [Sha84]. Yet an improvement was made by Boneh and Franklin, who utilised pairings on elliptic curves to overcome the previous limitations in identity based encryption systems.
The following section will give a brief overview of how Boneh and Franklin integrated pairings into their IBE scheme.

2.2.2 Boneh and Franklin's IBE

The scheme is built upon four major algorithms. The *set up* of the system and the parameters, the *extraction* of the private key, the *encryption* of the message and the *decryption* of the message.

The four algorithms will be briefly introduced here. A detailed description will be given in section 3 alongside the IBE system we are focused on presenting in this thesis. This is done because Boneh and Franklin's scheme is the foundation for the specific one described by Washington. It is obvious by context what parameters and specific functions can be interchanged with others that fulfill the same purpose. Therefore, Washington's description gives the necessary information about the general layout of the scheme. However, if the reader of this thesis wishes to see the general form, it can be found in Boneh and Franklin's paper [BF01].

The *set up* and *extraction* are run by the trusted authority. In the *set up* algorithm, all system parameters are established. This includes the master key, which stays secret to the trusted authority. The parameters are chosen according to the elliptic curve and pairing that will build the system, in our case the Weil pairing. The *extraction* algorithm entails a user asking the trusted authority for it to generate a private key for that user. This is done via a calculation performed on the public key with the master key. The *encryption* and *decryption* algorithms are comparable to other public key encryption schemes, the novelty being that they make use of the Weil pairing.

3 A Cryptosystem based on the Weil Pairing

3.1 A description of the system

Lawrence C. Washington describes a cryptosystem based on the Weil pairing in Chapter 6.9 of his book "Elliptic Curves. Number Theory and Cryptography", [Was08]. In Washington's own words "[...] we'll present a method, due to Boneh and Franklin, that uses the Weil pairing on these curves to obtain a cryptosystem [...]". This very cryptosystem is the one we wish to understand mathematically which is the motivation for this thesis.
Before diving into the analysis of the parameters we wish to transfer, we must first grasp what different components there are in the cryptosystem. A blueprint of the cryptosystem is necessary for the full development of this thesis. The parties involved are the trusted authority and two users who wish to communicate. We name them Alice and Bob for easy differentiation between the two and as it is a cryptographic tradition that the two are called as such. Recall the structure presented in section 2.2.2.

Set up. The TA does the following:

1. chooses a large prime, p
2. chooses an elliptic curve defined over a finite field, $E/\mathbb{F}_p$
3. chooses a large prime ℓ based on $\ell|\#E(K)$ for some field K
3. chooses a random point $P \in E(\mathbb{F}_p)$ of order ℓ
4. chooses two Hash functions (functions that will be described at the end of this section)

- $H_1 : \{0,1\}^{arb} \to E(\mathbb{F}_p)[\ell]$
- $H_2 : \mathbb{F}_{p^2}^{\times} \to \{0,1\}^n$, n being the length of the message being sent in binary

5. chooses a secret random $s \in \mathbb{F}_\ell^{\times}$ and computes $P_{pub} = [s]P$
6. makes p, H_1, H_2, n, P, P_{pub} public and keeps s private as the master key

Extraction. The TA does the following after a request by Bob to obtain his private key to allow for communication. Here Bob's digital identifier is simply denoted as ID:

1. computes $Q_{ID} = H_1(ID)$
2. computes $D_{ID} = [s]Q_{ID}$
3. after verifying that ID is Bob's identifier, sends D_{ID} to Bob

Encryption. If Alice wishes to send Bob a message, denoted as M, she does the following:

1. looks up Bob's ID and computes $Q_{ID} = H_1(ID)$
2. computes $g_{ID} = \tilde{e}_\ell(Q_{ID}, P_{pub})$. $\tilde{e}_\ell$ is the modified Weil pairing
3. chooses a random $r \in \mathbb{F}_\ell^{\times}$
4. produces the ciphertext $c = ([r]P, M \oplus H_2({g_{ID}}^r))$ where $\oplus$ denotes XOR, as in the bitwise addition modulo 2
5. sends the ciphertext c via public communication channels

Decryption. Once Bob receives the message from Alice, consisting of two parts (u, v), he proceeds as follows to decipher Alice's message using his private key:

- the ciphertext is $c = (u, v)$

1. using his private key, computes $h_{ID} = \tilde{e}_\ell(D_{ID}, u)$
2. finally he computes $m = v \oplus H_2(h_{ID})$

The success of the decryption is based on two parts. In the first the Weil pairing with the private key, D_{ID}, matches that with the public key, Q_{ID}. In the second, conditional on the first, the message is correctly decrypted (that is, successfully read). The following two lines show these two parts mathematically:

$$\tilde{e}_\ell(D_{ID}, u) = \tilde{e}_\ell([s]Q_{ID}, [r]P) = \tilde{e}_\ell(Q_{ID}, P)^{sr} = \tilde{e}_\ell(Q_{ID}, P_{pub})^r = g_{ID}^r$$

which uses a property of the Weil pairing. The equality of $\tilde{e}_\ell(D_{ID}, u)$ and g_{ID}^r leads to the deciphered message m equalling the original message M.

$$m = v \oplus H_2(\tilde{e}_\ell(D_{ID}, u)) = (M \oplus H_2({g_{ID}}^r)) \oplus H_2({g_{ID}}^r) = M$$

The Hash functions are functions commonly used in many different schemes in cryptography. Their main purpose is to ensure that data has not been altered. By comparing the output value of received data with its expected output, any changes in the data can be detected. Therefore, they are most commonly used as digital signatures.
A hash function is an easily computable map $f : x \to h$ from a very long or arbitrary input x to a much shorter and precise output h. This output, known as a hash value or hash code, uniquely represents the original data, ensuring that even the slightest change in input will result in a vastly different hash, meaning it is not computationally feasible to find two different inputs x and x' such that $f(x) = f(x')$.

This concludes the description of the cryptosystem. One missing piece of the puzzle is the definition of the function $\tilde{e}_\ell$ mentioned throughout the above description, which we have already identified as the Weil pairing.

3.2 The Weil Pairing

Bi-linear pairings are often found in cryptography. Their most common structure consists of a function mapping pairs of points on an elliptic curve to a finite field. The fact that they can "produce" finite fields that are large enough to make the discrete logarithm problem, DLP, hard to solve, yet small enough to make computations efficient, is the reason they are so commonly found in encryption schemes. Their security is based on the hardness of the "Bilinear Diffie Hellman" problem defined as follows:

$$\text{Given } [a]P, [b]P, [c]P \text{ compute } e(P, P)^{abc}$$

which is analogue to the DLP.
There are many such a pairing used in cryptography, such as the Tate-Lichtenbaum pairing or the Hyperelliptic Tate-Lichtenbaum pairing [Mef09]. Yet, we will devote our attention to the Weil pairing, first introduced by André Weil in 1940 [Wei79].

The Weil pairing is a function that maps a pair of points of an ℓ- torsion group of an elliptic curve to an ℓ^{th} root of unity in some extension field of the field over which the elliptic curve E is defined.

Definition 3. *Let $E/\mathbb{F}_p$ be an elliptic curve and let ℓ be a prime divisor of $\#E(\mathbb{F}_p)$, the order of the $\mathbb{F}_p$ points on E, and coprime to $char(\mathbb{F}_p)$. Let $\mathbb{F}_{p^k}$ be the splitting field of $x^\ell - 1 \in \mathbb{F}_p[x]$. The Weil pairing e_ℓ is a certain function*

$$e_\ell \colon E(\overline{\mathbb{F}_p})[\ell] \times E(\overline{\mathbb{F}_p})[\ell] \to \mathbb{F}_{p^k}^\times. \tag{1}$$

The image of the map e_ℓ consists of the ℓ^{th} roots of unity contained in the units $\mathbb{F}_{p^k}^\times$ of the field extension.

A precise constructive definition of the Weil pairing function includes mathematical objects, such as divisors (formal sums of points), which beyond the scope of this thesis. An interesting and well structured read on the topic is Victor S. Miller's paper on the formal definition of the Weil pairing [Mil04].

The following properties state that the Weil pairing is a bilinear, alternating and non-degenerate mapping. The proof of these can be found in Silverman's book [Sil86].

Lemma 1. *The Weil pairing is linear in both arguments:*

$$e_\ell(P+Q,R) = e_\ell(P,R)e_\ell(Q,R)\ \forall P,Q,R$$

and

$$e_\ell(P,R+S) = e_\ell(P,R)e_\ell(P,S)\ \forall P,Q,R$$

Lemma 2. *The Weil pairing is alternating:*

$$e_\ell(P,R) = e_\ell(R,P)^{-1}\ \forall P,R$$

Therefore, it also holds that:

$$e_\ell(P,P) = e_\ell(P,P)^{-1} = 1\ \forall P$$

Lemma 3. *The Weil pairing is non-degenerate:*

$$e_\ell(P,R) = 1\ \forall R \Leftrightarrow P = O$$

Some important conclusions can be made from the above listed Lemmas.
The first is crucial for the Bilinear Deffie Hellmann problem. Following from Lemma 1

$$e_\ell([a]P,[b]Q) = e_\ell(P+_{\cdot a\ times}..+P,[b]Q) = e_\ell(P,[b]Q)_{\cdot a\ times}..e_\ell(P,[b]Q) = e_\ell(P,[b]Q)^a = e_\ell(P,Q)^{ab}$$

If either $P,\ Q = O$ or both, $e_\ell([a]P,[b]Q) = e_\ell(P,Q)^{ab} = 1^{ab} = 1$

The second conclusion is instrumental to the use of the Weil pairing in cryptosystems.

Lemma 4. *If P,Q are multiples of one another meaning w.l.o.g. $[n]P = Q$ for $n \in \mathbb{Z}$, then $e_\ell(P,Q) = 1$.*

Proof. To prove the lemma we can discuss multiple scenarios.
Case 1 $\underline{P = Q = O}$ **or** $\underline{P = O}$
$e_\ell(P,Q) = \underline{e_\ell(P,[n]P) = e_\ell(O,[n]O)} = e_\ell(O,O) = 1$

Case 2 $\underline{Q = O}$ **and** $\underline{P \neq O}$
$e_\ell(P,Q) = \underline{e_\ell(P,[n]P) = e_\ell(P,O)} = 1$

Case 3 $\underline{P,Q \neq O}$
$e_\ell(P,Q) = \underline{e_\ell(P,[n]P)} = e_\ell(P,P)^n = 1^n = 1$ given the alternating property $e(P,P) = 1$ □

A cryptographic problem that comes to light after the conclusion of Lemma 4 is that one needs points of order ℓ that are not multiples of one another to ensure that the Weil pairing produces a nontrivial outcome. The problem lies in the fact that finding two points that are indeed not multiples of one another in the ℓ-torsion group is in general not an easy task. Even more difficult is developing an algorithm to do the task as part of a cryptosystem.

The solution we choose to use is introducing an endomorphism $\delta\colon E \to E$, in cryptography commonly known as the distortion map. This endomorphism plays the basic role of taking points of order ℓ as an input and mapping it to another point of order ℓ which is not a multiple of the original point. With such a tool, we redefine and rename definition 3 to

Definition 4. *Let $E/\mathbb{F}_p$ be an elliptic curve and let ℓ be a prime divisor of $\#E(\mathbb{F})$, the order of the $\mathbb{F}_p$ points on E, and coprime to $char(\mathbb{F}_p)$. Let $\mathbb{F}_{p^k}$ be the splitting field of $x^\ell - 1 \in \mathbb{F}_p[x]$. Together with the endomorphism δ the modified Weil Pairing is defined as such:*

$$\begin{aligned} \tilde{e_\ell} :& E(\mathbb{F}_{p^d})[\ell] \times E(\mathbb{F}_{p^d})[\ell] \to \mathbb{F}_{p^k}^\times \\ & \tilde{e_\ell}(P,Q) = e_\ell(P,\delta(Q)) \end{aligned} \tag{2}$$

Note, the extension $\mathbb{F}_{p^d}$ suffices to ensure the ℓ- torsion group is contained in $E(\mathbb{F}_{p^d})$. The image of $\tilde{e_\ell}$ remains the same as that of e_ℓ.

With that the Weil Pairing has been modified to suit the purposes it holds within a cryptosystem.

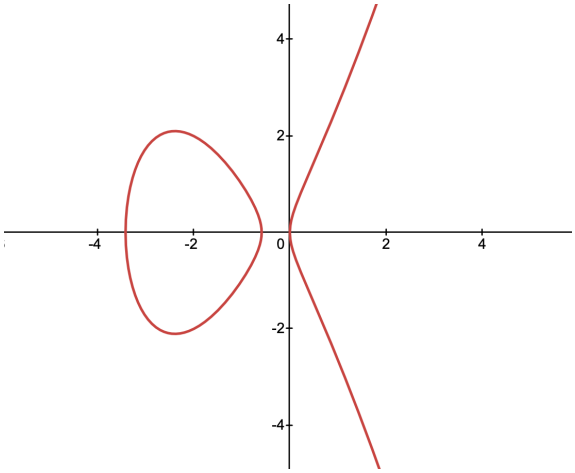


Figure 1: The elliptic curve E

4 Analysis of the New Parameters

As stated in the introduction of this text, we wish to look at all mathematical conditions necessary for the cryptosystem based on the Weil pairing to work. For that we will introduce the individual components one by one in combination with the reasoning for their specific condition in relation to the system, and the proof that the components either already suit the condition, or that a certain tweaking must be made in order to fit the system.

A simultaneous introduction of the elliptic curve and the endomorphism is appropriate due to their intertwining properties. This intertwining, though very interesting, is not the focus of this thesis. A full description is covered in Berno Reitsma's Bachelor's Thesis[Rei17]. Throughout the rest of the thesis we will use their close correlation, yet showcase other properties these two have, especially with respect to the cryptosystem we are focusing on.

Please note that other elliptic curves and endomorphism would have been a suitable choice for the system, yet all must correlate in the same way our two do. The choice was made as E, (4), and δ, (3), has not been discussed yet in application to the cryptosystem based on the Weil pairing.

The elliptic curve we will discuss is the curve depicted in Figure 1 and mathematically defined as follows

$$E : y^2 = x^3 + 4x^2 + 2x$$

with the endomorphism

$$\delta(P) = \left(-\frac{1}{2}(x + 4 + \frac{2}{x}), \frac{y}{2\sqrt{-2}}(1 - \frac{2}{x^2}) \right)$$

for some point $P = (x, y)$.

4.1 The Endomorphism δ

The map we have so far denoted δ is a prime focus of the thesis. It is of great value to the Weil pairing and hence the encryption system in paragraph 3.1. It was chosen in correlation to the elliptic curve E. We wish to show it fulfills its duty described in the definition of the modified Weil pairing (definition 4); to "find" points of order ℓ that are not multiples of one another for the Weil pairing.

We begin with a formal definition.
δ is a map with its domain equal the points of $E(K)$. K being an arbitrary field of characteristic $\text{char}(K) \neq 2$ and $E(K)$ the points of K over E: $y^2 = x^3 + 4x^2 + 2x$ as the elliptic curve.

$$\delta\colon E(K) \to E(K)$$
$$\delta(P) = \begin{cases} \left(-\frac{1}{2}(x+4+\frac{2}{x}), \frac{y}{2\sqrt{-2}}(1-\frac{2}{x^2})\right) & \text{if } P=(x,y) \text{ and } x \neq 0, \\ O & \text{if } P = O \text{ and if } P=(0,0). \end{cases} \tag{3}$$

We make the assumption that $X^2+2 \in K[X]$ is reducible, which means -2 is a square in K. A square root of it, as is used in the formula (3), we write as $\sqrt{-2} \in K$. This is a condition for the field K to be remembered when later narrowing down what precise field will be used in the cryptosystem.

4.1.1 δ is an endomorphism

An endomorphism is a homomorphism, in this case a group homomorphism, that takes a group to itself. This should not be confused with an automorphism, which also takes a group to itself with the added condition that the map must be an isomorphism. The endomorphism does not need to be isomorphic.
We show δ is indeed a group homomorphism and that the image of δ is contained in $E(K)$, meaning it indeed takes the group $E(K)$ to itself.

The image of δ is contained in $E(K)$

We proceed by showing that δ takes the group $E(K)$ to itself. Every point the map δ receives as an input is mapped to a point of $E(K)$ meaning the image of delta is contained in E(K).

Theorem 1. $\delta(E(K)) \subseteq E(K)$

Proof. There are three different points we must discuss.
Case 1 $\underline{P = O}$
By definition $\delta(O) = O \in E(K)$

Case 2 $\underline{P = (0,0)}$
By definition $\delta(0,0) = O \in E(K)$

Case 3 $\underline{P = (x,y) \in E(K)}$
Let P be any other point, so $x \neq 0$. $P=(x,y)$ is mapped to $\delta(x,y) = \left(-\frac{1}{2}(x+4+\frac{2}{x}), \frac{y}{2\sqrt{-2}}(1-\frac{2}{x^2})\right) = (X,Y)$, where the new coordinates receive the notation (X,Y). The following equation then shows us that the new coordinates also satisfy the equation of the elliptic curve E, [4], implying that $\delta(x,y) = (X,Y)$ are also points on the curve and therefore in $E(K)$.

$$\begin{gathered} Y^2 \\ = \\ \left(\frac{y}{2\sqrt{-2}}(1-\frac{2}{x^2})\right)^2 = \frac{y^2}{4(-2)}(1-\frac{2}{x^2})^2 = -\frac{y^2}{8}(1-\frac{4}{x^2}+\frac{4}{x^4}) = y^2(-\frac{1}{8}+\frac{1}{2x^2}-\frac{1}{2x^4}) \\ \text{substituting } y^2 \text{ for } x^3+4x^2+2x \\ = \\ x^3+4x^2+2x(-\frac{1}{8}+\frac{1}{2x^2}-\frac{1}{2x^4}) = -\frac{x^3}{8}-\frac{1}{x^3}-\frac{x^2}{2}-\frac{2}{x^2}+\frac{x}{4}+\frac{1}{2x}+2 \\ = \\ -\frac{x^3}{8}-\frac{1}{x^3}-\frac{3x^2}{2}-\frac{6}{x^2}-\frac{27x}{4}-\frac{27}{2x}-14+20+\frac{4}{x^2}+\frac{16}{x}+8x+x^2-x-4-\frac{2}{x} \\ = \\ \left(-\frac{1}{2}(x+4+\frac{2}{x})\right)^3+4\left(-\frac{1}{2}(x+4+\frac{2}{x})\right)^2+2\left(-\frac{1}{2}(x+4+\frac{2}{x})\right) \\ = \\ X^3+4X^2+2X \end{gathered} \tag{4}$$

We conclude that indeed $\delta(x,y) \in E(K)\ \forall P=(x,y) \in E(K)$, hence $\delta(E(K)) \subseteq E(K)$. □

δ is a homomorphism

The definition of a group homomorphism can be taken from the Group Theory reader of the University of Groningen [TM18]. The group homomorphism is a map between groups that satisfies $\delta(P_1 + P_2) = \delta(P_1) + \delta(P_2)$ with P_1 and P_2 being two elements of the group, so two points in $E(K)$.

To continue it is important to define point addition as it is a non-trivial definition of a group operation. Knowing the coefficients of E, the group operation can be described precisely. Given any two points P_1 and P_2 of $E(K)$ the following equations hold:

- For negation of $P_1 = (x_1, y_1)$: $-P_1 = -(x_1, y_1) = (x_1, -y_1)$
- For addition, if $x_1 = x_2$ and $y_1 + y_2 = 0$: $P_1 + P_2 = O$

  otherwise $P_1 + P_2 = P_3$ with $P_3 = (x_3, y_3) = (\lambda^2 - 4 - x_1 - x_2, -\lambda x_3 - \nu)$

where λ and ν are chosen according to the table

	λ	ν
$x_1 \neq x_2$	$\frac{y_2 - y_1}{x_2 - x_1}$	$\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$
$x_1 = x_2$	$\frac{3x_1^2 + 8x_1 + 2}{2y_1}$	$\frac{-x_1^3 + 2x_1}{2y_1}$

This definition of point addition is the group operation and used throughout the entire thesis.

Theorem 2. *$\delta\colon E(K) \to E(K)$ is a homomorphism. Meaning $\delta(P_1 + P_2) = \delta(P_1) + \delta(P_2)$ $\forall P_1, P_2 \in E(K)$.*

Proof. For this proof one has to consider 5 case distinctions for the points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$.
Case 1 $P_1 = P_2 = O$
$\delta(O) + \delta(O) = O + O = O = \delta(O) = \delta(O + O)$ by definition of δ.

Case 2 Either P_1 or $P_2 = O$
Without loss of generality we take $P_1 = O$. $E(K)$ is abelian, hence the order of the points in the group operation is insignificant.
$\delta(O + P_2) = \delta(P_2) = O + \delta(P_2) = \delta(O) + \delta(P_2)$ using the property of the identity element.

Case 3 $x_1 = x_2$ **and** $y_1 + y_2 = 0$
When two points satisfy the condition above it means that $P_1 + P_2 = O$. This is described by Silverman in his book [Sil86], yet one can also see it in the figure 1. Since E is symmetric along the x-axis, the condition $x_1 = x_2$ and $y_1 + y_2 = 0$ describes points that lie mirrored on the x-axis. A line connecting the two is therefore parallel to the y-axis and goes to the point at infinity or in other words, the identity element O. This also holds for the points of order two, where $y_1 = y_2 = 0$.

$\delta(P_1 + P_2) = \delta(O) = O$. What is left is to show $\delta(P_1) + \delta(P_2) = O$. We denote the components of the points as such $\delta(P_1) = \delta((x_1, y_1)) = (X_1, Y_1)$ and $\delta(P_2) = \delta((x_2, y_2)) = (X_2, Y_2)$. Since $x_1 = x_2$ it follows by definition that $X_1 = -\frac{1}{2}(x_1 + 4 + \frac{2}{x_1}) = -\frac{1}{2}(x_2 + 4 + \frac{2}{x_2}) = X_2$. Since $y_1 = -y_2$ it follows by definition that $Y_1 + Y_2 = \frac{y_1}{2\sqrt{-2}}(1 - \frac{2}{x_1^2}) + \frac{y_2}{2\sqrt{-2}}(1 - \frac{2}{x_2^2}) = \frac{y_1}{2\sqrt{-2}}(1 - \frac{2}{x_1^2}) - \frac{y_1}{2\sqrt{-2}}(1 - \frac{2}{x_1^2}) = 0$.
So indeed $\delta(P_1) + \delta(P_2) = O$.

Case 4 $x_1 = x_2$ **but** $y_1 + y_2 \neq 0$
Meaning $P_2 = P_1$ with $y \neq 0$. The proof via calculation using the definition of δ and that of addition is needed. Firstly, we calculate $\delta(P_1)$ and $\delta(P_2)$ individually and then their summation.

$$\delta(P_1) = (X_1, Y_1) = \left(-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right), \frac{y_1}{2\sqrt{-2}}\left(1 - \frac{2}{x_1^2}\right)\right)$$
$$\delta(P_2) = (X_2, Y_2) = \left(-\frac{1}{2}\left(x_2 + 4 + \frac{2}{x_2}\right), \frac{y_2}{2\sqrt{-2}}\left(1 - \frac{2}{x_2^2}\right)\right)$$
given that $X_1 = X_2$ but $Y_1 + Y_2 \neq 0$,
$$\delta(P_1) + \delta(P_2) = (X_3, Y_3) = \left(\left(\frac{3X_1^2 + 8X_1 + 2}{2Y_1}\right)^2 - 4 - 2X_1, -\left(\frac{3X_1^2 + 8X_1 + 2}{2Y_1}\right)X_3 - \frac{-X_1^3 + 2X_1}{2Y_1}\right)$$

Secondly, we calculate $\delta(P_1 + P_2)$ using the summation $P_1 + P_2$

$$\delta(P_1 + P_2) = (X_3, Y_3) = \left(-\frac{1}{2}(x_3 + 4 + \frac{2}{x_3}), \frac{y_3}{2\sqrt{-2}}\left(1 - \frac{2}{x_3^2}\right)\right)$$

using

$$P_1 + P_2 = (x_3, y_3) = \left(\left(\frac{3x_1^2 + 8x_1 + 2}{2y_1}\right)^2 - 4 - 2x_1, -\left(\frac{3x_1^2 + 8x_1 + 2}{2y_1}\right)x_3 - \frac{-x_1^3 + 2x_1}{2y_1}\right)$$

As the two final equation must be equated, yet they are both quite complex, we proceed by first showing the x-values are equal and then the y-values.
To start with the x-value we take the expressions shown above with X_1, x_3 substituted for their full expressions and after squaring Y_1^2 substituted for $X_1^3 + 4X_1^2 + 2X_1$

$$\frac{\left(3\left(-\frac{1}{2}\left(x + 4 + \frac{2}{x}\right)\right)^2 + 8\left(-\frac{1}{2}\left(x + 4 + \frac{2}{x}\right)\right) + 2\right)^2}{4\left(\left(-\frac{1}{2}\left(x + 4 + \frac{2}{x}\right)\right)^3 + 4\left(-\frac{1}{2}\left(x + 4 + \frac{2}{x}\right)\right)^2 + 2\left(-\frac{1}{2}\left(x + 4 + \frac{2}{x}\right)\right)\right)} - 4 - 2\left(-\frac{1}{2}\left(x + 4 + \frac{2}{x}\right)\right) =$$
$$-\frac{1}{2}\left(\left(\frac{(3x^2 + 8x + 2)^2}{4(x^3 + 4x^2 + 2x)} - 4 - 2x\right) + 4 + \frac{2}{\left(\frac{(3x^2+8x+2)^2}{4(x^3+4x^2+2x)} - 4 - 2x\right)}\right)$$

For the y-value one has the following equation after the same substitutions as in the x- value

$$-\left(\frac{3\left(-\frac{1}{2}(x_1 + 4 + \frac{2}{x_1})\right)^2 + 8\left(-\frac{1}{2}(x_1 + 4 + \frac{2}{x_1})\right) + 2}{2\left(\frac{y_1}{2\sqrt{-2}}(1 - \frac{2}{x_1^2})\right)}\right) \cdot$$
$$\left(\frac{\left(3\left(-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right)\right)^2 + 8\left(-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right)\right) + 2\right)^2}{4\left(\left(-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right)\right)^3 + 4\left(-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right)\right)^2 + 2\left(-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right)\right)\right)}\right.$$
$$- 4 - 2\left(-\frac{1}{2}\left(x + 4 + \frac{2}{x_1}\right)\right)$$
$$\left. - \frac{-\left(-\frac{1}{2}(x_1 + 4 + \frac{2}{x_1})\right)^3 + 2\left(-\frac{1}{2}(x_1 + 4 + \frac{2}{x_1})\right)}{2\left(\frac{y_1}{2\sqrt{-2}}(1 - \frac{2}{x_1^2})\right)}\right) =$$
$$\frac{\left(-\left(\frac{3x_1^2+8x_1+2}{2y_1}\right)\left(\left(\frac{3x_1^2+8x_1+2}{2y_1}\right)^2 - 4 - 2x_1\right) - \frac{-x_1^3+2x_1}{2y_1}\right)}{2\sqrt{-2}}\left(1 - \frac{2}{\left(\left(\frac{3x_1^2+8x_1+2}{2y_1}\right)^2 - 4 - 2x_1\right)^2}\right)$$

These equations are now solvable by radicals and one can therefore easily show that they are indeed equal. (The omission of the in between steps stems from the steps being plentiful yet there being no insight gained from showing these steps. The same holds for equations that are yet to follow.)

Case 5 $\underline{x_1 \neq x_2}$ **so** $\underline{P_1 + P_2 = P_3}$
The proof again is one of calculation using the definition of δ and of addition. $\delta(P_1)$ and $\delta(P_2)$ stay the same as in Case 4, however the definition of addition changes. Using a different formula comes from the fact that $x_1 \neq x_2$ which one can verify in the table 4.1.1. Hence we have the following equations

$$\delta(P_1) + \delta(P_2) = (X_3, Y_3) = \left(\left(\frac{Y_2 - Y_1}{X_2 - X_1} \right)^2 - 4 - X_1 - X_2, - \left(\frac{Y_2 - Y_1}{X_2 - X_1} \right) X_3 - \frac{Y_1 X_2 - Y_2 X_1}{X_2 - X_1} \right)$$

and $\delta(P_1 + P_2) = (X_3, Y_3)$ using

$$P_1 + P_2 = (x_3, y_3) = \left(\left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - 4 - x_1 - x_2, - \left(\frac{y_2 - y_1}{x_2 - x_1} \right) x_3 - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \right)$$

We again start with the x-value and take the expressions shown above with X_1, x_3 substituted for their full expressions and after squaring Y_1^2 substituted for $X_1^3 + 4X_1^2 + 2X_1$:

$$\left(\frac{\frac{y_2}{2\sqrt{-2}}(1 - \frac{2}{x_2^2}) - \frac{y_1}{2\sqrt{-2}} \left(1 - \frac{2}{x_1^2}\right)}{(-\frac{1}{2}\left(x_2 + 4 + \frac{2}{x_2}\right) - (-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right)} \right)^2 - 4 - (-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right) - (-\frac{1}{2}\left(x_2 + 4 + \frac{2}{x_2}\right) =$$

$$-\frac{1}{2}\left(\left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - 4 - x_1 - x_2 + 4 + \frac{2}{\left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - 4 - x_1 - x_2} \right)$$

And finally the y-value

$$-\left(\frac{\frac{y_2}{2\sqrt{-2}}\left(1 - \frac{2}{x_2^2}\right) - \frac{y_1}{2\sqrt{-2}}\left(1 - \frac{2}{x_1^2}\right)}{-\frac{1}{2}\left(x_2 + 4 + \frac{2}{x_2}\right) + \frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right)} \right) \left(\left(\frac{\frac{y_2}{2\sqrt{-2}}(1 - \frac{2}{x_2^2}) - \frac{y_1}{2\sqrt{-2}}\left(1 - \frac{2}{x_1^2}\right)}{(-\frac{1}{2}\left(x_2 + 4 + \frac{2}{x_2}\right) - (-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right)} \right)^2 \right.$$

$$\left. - 4 - (-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right) - (-\frac{1}{2}\left(x_2 + 4 + \frac{2}{x_2}\right) \right.$$

$$- \frac{\left(\frac{y_1}{2\sqrt{-2}}\left(1 - \frac{2}{x_1^2}\right)\right)\left(-\frac{1}{2}\left(x_2 + 4 + \frac{2}{x_2}\right)\right) - \left(\frac{y_2}{2\sqrt{-2}}\left(1 - \frac{2}{x_2^2}\right)\right)\left(-\frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right)\right)}{-\frac{1}{2}\left(x_2 + 4 + \frac{2}{x_2}\right) + \frac{1}{2}\left(x_1 + 4 + \frac{2}{x_1}\right)} =$$

$$\frac{-\left(\frac{y_2 - y_1}{x_2 - x_1}\right)\left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - 4 - x_1 - x_2\right) - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}}{2\sqrt{-2}} \left(1 - \frac{2}{\left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - 4 - x_1 - x_2\right)^2} \right)$$

This ultimately proves that $\delta(P_1) + \delta(P_2) = \delta(P_1 + P_2)$ and therefore δ is indeed a group homomorphism. □

4.1.2 The unique property of δ

A unique and important property of the endomorphism is one that, at first sight, does not transparently show how it can be useful nor does it reveal where its property comes from. Yet, in the further exploration of other properties of the endomorphism and the elliptic curve it will become clear that this property emerges everywhere.
If interested in how the property arose from the definition of the endomorphism, please refer to Silverman's book [Sil94](see proposition II.2.3.1 and the pages leading up to it).

Theorem 3. $\delta^2(P) = [-2]P \ \forall P \in E(K)$

Proof. We consider three cases:
Case 1 $\underline{P = O}$
$\delta(O) = O$ so $\delta^2(O) = \delta(O) = O$. Also $[-2]O = [-1][2]O = [-1]O = O$. Hence, $\delta^2(O) = [-2]O$.

Case 2 $\underline{P = (0,0)}$
When $P = (0,0)$, by definition of δ, $\delta^2(0,0) = \delta(\delta(0,0)) = \delta(O) = O$. And since we know $P = (0,0)$ is a point of order 2, we have $[-2](0,0) = [-1][2](0,0) = [-1]O = O$. Hence, $\delta^2(0,0) = [-2](0,0)$.

Case 3 $\underline{P = (x,y)}$ **with** $x \neq 0$ **and** $y = 0$
The points with $y = 0$ are, as already mentioned in the proof of δ being a homomorphism, the points of order 2. If P is of order 2, it holds that $[-2]P = [-1][2]P = [-1]O = O$, since $E(K)$ is abelian. Considering $\delta^2(P) = O$ must hold we look at the points that are mapped to O by δ. From this we conclude that $\delta(P) = \{(0,0), O\}$.
If $\delta(P) = O$ then $x = 0$ and our point is $P = (0,0)$.
If $\delta(P) = (0,0)$, then $\delta(P) = \left(-\frac{1}{2}(x + 4 + \frac{2}{x}), \frac{0}{2\sqrt{-2}}(1 - \frac{2}{x^2})\right) = (0,0)$. So $0 = -\frac{1}{2}(x + 4 + \frac{2}{x}) \Leftrightarrow x^2 + 4x + 2 = 0 \Leftrightarrow x = -2 \pm \sqrt{2}$ which is precisely the points of the elliptic curve E at $y = 0$.

Case 4 $\underline{P}$ **otherwise, so** $P = (x,y)$**,** $x \neq 0$ **and** $y \neq 0$
We use the definition of addition to prove $\delta^2(P) = [-1](P + P)$ To start with the x-value we have the following equation:

$$-\frac{1}{2}\left((-\frac{1}{2}(x + 4 + \frac{2}{x}) + 4 + \frac{2}{-\frac{1}{2}(x + 4 + \frac{2}{x})})\right) = \left(\frac{3x^2 + 8x + 2}{2y}\right)^2 - 4 - 2x$$

And for the y-value we have

$$(\frac{\frac{y}{2\sqrt{-2}}(1 - \frac{2}{x^2})}{2\sqrt{-2}}(1 - \frac{2}{(-\frac{1}{2}(x + 4 + \frac{2}{x^2}))^2}) = -(\frac{3x^2 + 8x + 2}{2y}\left(\left(\frac{3x^2 + 8x + 2}{2y}\right)^2 - 4 - 2x\right) - \frac{-x^3 + 2x}{2y}$$

With this we conclude that the unique property of $\delta^2(P) = [-2]P$ is true. □

4.1.3 The order of the point $\delta(P)$

The purpose of δ is to serve as the map required by the modified Weil pairing, definition 4 to take a point of a specific order ℓ to another point of order ℓ that was not a multiple of the original point. For our δ to be able to take on that role, we must ensure its image points are indeed of order ℓ if the input point is also of order ℓ.

We generalize the statement to say that δ takes points of order n, where n is odd, to points of order n. The reason why we do not generalize the statement to points of any order is because there are more exceptions to explain in the case where n is even. An example is $(0,0)$ being a point of order 2 and being mapped to O, the point of order 1. In this cryptosystem we also do not require δ to take points of even order therefore we can omit the description of what happens to the points of even order.

Theorem 4. *If $P \in E(K)[n]$ where n is odd, then $\delta(P) \in E(K)[n]$.*

Proof. $E(K)[n]$ containes all the points of order n. The order of a point in $E(K)$ is defined in the canonical way where $[n]P = O$ for the smallest of such $n \in \mathbb{Z}$. To verify that $\delta : E(K)[n] \to E(K)[n]$ we consider two cases as there are two different types of points to examine.

Case 1 $\underline{P = O}$
O has order 1. $\delta(O) = O$ by definition of δ, so $\delta(O)$ also has order 1.

Case 2 $\underline{P}$ **otherwise with order** n**, so** $P = (x,y)$**,** $x \neq 0$
$P = (x,y)$ has order n, meaning $[n]P = O$ where it is the smallest $n \in \mathbb{Z}$. Then, based on the fact that δ is a homomorphism it follows that $[n]\delta(P) = \delta(P) + ...{}_{\text{n times}} + \delta(P) = \delta(P + ...{}_{\text{n times}} + P) = \delta([n]P) = \delta(O) = O$. We conclude from this that the order of $\delta(P)$ must divide n, so lets say $t = \#\delta(P)$ and $t|n$.

With t being the order of $\delta(P)$ we know $[t]\delta(P) = O$. Meaning, $[t]\delta(P) = \delta(P) + ...{}_{\text{t times}} + \delta(P) = \delta(P + ...{}_{\text{t times}} + P) = \delta([t]P) = O$. There are two points that $[t]P$ could be.
If $[t]P = O$ then the order of P must divide t, so $n|t$. However, since we also stated that $t|n$ we deduce the equality $t = n$.
If $[t]P = (0, 0)$ then $[t]P$ has order 2, so $[2t]P = O$ taking us to the conclusion that $n|2t$. However n is odd $n|2t \Rightarrow n|t \Rightarrow n = t$. □

4.1.4 The multiplicity of the point $\delta(P)$

We recall the definition of the modified Weil Pairing 4 being $\tilde{e_\ell}(P, Q) = e_\ell(P, \delta(Q))$, so the endomorphism δ maps one of the points in the pairing to some other point in $E(K)$. In addition, we remember the Lemma 4 that states if $[m]P = Q$ then $\tilde{e_\ell}(P, Q) = 1$. For the cryptosystem to work the Weil pairing requires a non-trivial result. For this endomorphism to be appropriate for the pairing we require the point $\delta(Q)$ not to be a multiple of the point Q.

As will become clear in the proof of the theorem to follow, the prime ℓ is chosen with a specific condition, namely ℓ should be chosen is a way that the field with ℓ points does not contain the square of -2. In other words, $\sqrt{-2} \notin \mathbb{F}_\ell$. This condition ensures that δ takes a point P from the group of ℓ torsion points $E(K)[\ell]$ and maps it to a separate point $\delta(P)$ in $E(K)[\ell]$ which is not a multiple of the first point P.

Theorem 5. *If ℓ is a prime where $\sqrt{-2} \notin \mathbb{F}_\ell$, then $\delta(P) \neq [m]P$ for an arbitrary point P of order ℓ and $m \in \mathbb{Z}$.*

Proof. We use the method "proof by contradiction". Let ℓ be a prime such that $\sqrt{-2} \notin \mathbb{F}_\ell$. Assume $\delta(P) = [m]P$ for a point P of order ℓ.
Using the previous property, $\delta^2(P) = [-2]P$, we apply δ to our assumption.

$$\begin{aligned}\delta(P) =& [m]P \Leftrightarrow \delta^2(P) = \delta(\delta(P)) = \delta([m]P) = [m]\delta(P)\\ [-2]P =& \delta^2(P) = \delta([m]P) = [m]\delta(P) = [m][m]P = [m^2]P\end{aligned}$$

since $\delta(P) = [m]P$. If $[-2]P = [m^2]P$ then by the law of the group operation $[m^2 + 2]P = O$. Since ℓ is the order of P, ℓ must divide $m^2 + 2$, from which follows

$$m^2 + 2 \equiv 0 \pmod{\ell} \Leftrightarrow m^2 \equiv -2 \pmod{\ell}$$

Yet, $\sqrt{-2} \notin \mathbb{F}_\ell$ is equivalent to saying that $\nexists x \in \mathbb{Z}$ such that $x^2 \equiv -2 \pmod{\ell}$. Such an $m \in \mathbb{Z}$ can therefore not exist. We have come to a contradiction and can refute our assumption, leading to the conclusion that $\delta(P) \neq [m]P$ for a point P having order ℓ. □

We have hereby proven the relevant conditions of the endomorphism δ. In the following section, we analyse the conditions and properties of its counterpart E, the elliptic curve.

4.2 The Elliptic Curve E

We introduced the elliptic curve $E/\mathbb{F}_p$ as $E : y^2 = x^3 + 4x^2 + 2x$. As a reminder, $E/\mathbb{F}_p$ stands for E defined over $\mathbb{F}_p$ which means that E's coefficients lie in $\mathbb{F}_p$.

4.2.1 Supersingularity of E

Supersingularity is a special property that elliptic curves over finite fields can exhibit. Curves that do not exhibit this special property are referred to as ordinary. The exact definition of supersingularity and supersingular curves deals with the ring structure of the endomorphisms from $E(\overline{K})$ to itself. As this is not relevant for our cryptosystem no details will be mentioned in this text, however an acknowledgment of there being some property is important as to not be vague with the term "supersingular". For further reading on the topic Chapter 4.6 of Washington's book [Was08] is recommendable.

What is relevant are the implications that follow from the elliptic curve being supersingular. In our case, we are interested in the order of $E(K)$ which can be determined with the help of knowing E is supersingular. Without getting ahead of ourselves, we first show our E (4) is supersingular.

When coming to the fact the E over the $\mathbb{F}_p$ is supersingular it is important to mention what finite field $\mathbb{F}_p$ it is defined over, specifically what the characteristic of that field is.

Theorem 6. *If p is a prime such that $\sqrt{-2} \notin \mathbb{F}_p$, then the elliptic curve E over the finite field $\mathbb{F}_p$ of characteristic p is supersingular.*

Proof. $E(\mathbb{F}_p)$ is an abelian group. For every $n \in \mathbb{Z}$ the multiplication map $[n] : E(\mathbb{F}_p) \to E(\mathbb{F}_p)$ exists with the subgroup of the n- torsion points as its kernel, so $ker([n]) = E(\overline{\mathbb{F}_p})[n]$.

Let us take the characteristic of the finite field $\mathbb{F}_p$, being $p > 0$. A statement made by Washington in chapter 3.1 in [Was08] is

$$E(\overline{\mathbb{F}_p})[p] \cong \begin{cases} 0 & \text{if } E \text{ is supersingular} \\ \mathbb{Z}/p\mathbb{Z} & \text{if E is ordinary} \end{cases}$$

For proof by contradiction we claim $E(\mathbb{F}_p)[p] \cong \mathbb{Z}/p\mathbb{Z}$.
So the p- torsion points form a cyclic group. Therefore, any element $Q \in E(\overline{\mathbb{F}_p})$ of order p generates the subgroup $\{Q, [2]Q, ..., [p]Q = O\}$ which is equal to $E(\overline{\mathbb{F}_p})[p]$. Hence the points of order p are multiples of one another. If we think back to our endomorphism δ and apply it to the point Q of order p, we get $\delta(Q)$, another point of order p. Since all points of order p are multiples of one another, we have that $\delta(Q) = [m]Q$ for some $m \in \mathbb{Z}$.
Remember that$[-2]P = \delta^2(P) \forall P \in E(\mathbb{F}_p)$ so

$$[-2]Q = \delta^2(Q) = \delta([m]Q) = [m][m]Q = [m^2]Q \Leftrightarrow [m^2 + 2]Q = O$$

and with p being the order of Q it follows that

$$p|m^2 + 2 \Leftrightarrow m^2 + 2 \equiv 0 \pmod{p} \Leftrightarrow m^2 \equiv -2 \pmod{p}$$

Yet, $\sqrt{-2} \notin \mathbb{F}_p$ is equivalent to saying that $\nexists x \in \mathbb{Z}$ such that $x^2 \equiv -2 \pmod{p}$. Such an $m \in \mathbb{Z}$ can therefore not exist. We have come to a contradiction and can refute our assumption, concluding that $E(\overline{\mathbb{F}_p})[p] \cong 0$ and therefore $E((\mathbb{F}_p)$ is supersingular. □

4.2.2 The order of $E(\mathbb{F}_p)$

The expressed interest in $\#E(\mathbb{F}_p)$ and the reason in knowing whether $E(\mathbb{F}_p)$ was supersingular in the first place stems from the need of the Weil pairing for ℓ to be a prime divisor of $\#E(\mathbb{F}_p)$. To be explicit, the calculation of the order $\#E(\mathbb{F}_p)$ is a necessity.

The order of $E(\mathbb{F}_p)$, as first formulated by Hasse, is given by $\#E(\mathbb{F}_p) = p + 1 - a$ where $|a| \leq 2\sqrt{p}$. The supersingularity of E allows for the use of Proposition 3.3.3 stated in [VV15]. It goes as follows:

Proposition 1. *Let $E/\mathbb{F}_p$ be an elliptic curve [...]. Then E is supersingular [...] if and only if $\#E(\mathbb{F}_p) \equiv 1$ (mod p).*

Theorem 7. *$\#E(\mathbb{F}_p) = p + 1$ with p prime.*

Proof. Since E is supersingular, we know that $\#E(\mathbb{F}_p) \equiv 1 \pmod{p}$. This is to say that

$$\begin{aligned} \#E(\mathbb{F}_p) = p + 1 - a \equiv 1 \pmod{p} &\Leftrightarrow p - a \equiv 0 \pmod{p} \\ &\Leftrightarrow -a \equiv 0 \pmod{p} \Leftrightarrow a \equiv 0 \pmod{p} \Leftrightarrow p|a \end{aligned}$$

We rewrite $a = bp$ for some $b \in \mathbb{Z}$ and substitute $|bp| \leq 2\sqrt{p} \Leftrightarrow |b|p =\leq 2\sqrt{p}$ as p is a positive prime number. Note that $\frac{p}{\sqrt{p}} = \sqrt{p}$. It follows that

$$|b|p =\leq 2\sqrt{p} \Leftrightarrow |b|\sqrt{p} \leq 2 \Leftrightarrow \sqrt{p} \leq \frac{2}{|b|}$$

This means that either $b = 1$, such that $\sqrt{p} \leq 2$ and $p = 2, 3$, $b \geq 2$ and $\sqrt{p} \leq 1$, where there is no prime p that satisfies this condition or $b = 0$ and hence $a = bp = 0$, where p can be any prime. In our cryptographic system p is taken to be a large prime, also meaning $p \gg 2, 3$, so we must have the case where $a = 0$. Plugging this into Hasse's formulation of the order of $E(\mathbb{F}_p)$, we can finalise the proof stating $\#E(\mathbb{F}_p) = p + 1$. □

With this we conclude the conditions provided by the elliptic curve E and its order.

4.3 The primes p and ℓ

The following sub-chapter will be somewhat different to the previous sections as there is not so much analyzing the given structure of the parameters (such as with the endomorphism or the elliptic curve which already come with a complex algebraic structure) so much as providing guidelines with which p and ℓ must be chosen.

The primes p and ℓ have been a major focus throughout the thesis. The prime p being the characteristic of the finite field over which the elliptic curve is defined has influence over the finite field $\mathbb{F}_p$ itself which impacts the group $E(\mathbb{F}_p)$, the fact that it's supersingular and its order. Directly impacted by p is also the choice of ℓ, which in turn determines the ℓ- torsion group considered for the cryptosystem. Therefore, ℓ determines the input of the Weil pairing, and hence the construction of the pairing itself as that depends on the order of the points it takes in.

We collectionize the conditions given to the primes to finally determine what they must look like. The cryptosystem we are analyzing, described in section 3, states p is taken to be a large prime. With a large prime, what is meant is a prime with 100 or more digits. Theorem 6 specifies that the $\sqrt{-2}$ must not be contained in the finite field of p elements $\mathbb{F}_p$. This is equivalent to saying that there does not exist an $x \in \mathbb{Z}$ such that $x^2 \equiv -2 \pmod{p}$ or that the Legendre symbol must be $\left(\frac{-2}{p}\right) = -1$ (definition III.3.1 in [Top17]).
Having put a condition on the prime p, one can determine the prime ℓ. It must be coprime to p and a prime divisor of $\#E(\mathbb{F}_p)$ as by the definition of the Weil pairing 4. ℓ is also chosen to be a large prime. There are many ways to have ℓ be a large prime divisor of $\#E(\mathbb{F}_p) = p + 1$ but for the sake of simplicity we determine $p + 1 = 2\ell$ such that $\ell = \frac{p+1}{2}$ is a large prime. Similarly to p, theorem 5 specifies that the $\sqrt{-2}$ must not be contained in the finite field of ℓ elements $\mathbb{F}_\ell$. The Legendre symbol must also be $\left(\frac{-2}{\ell}\right) = -1$. By making a choice for ℓ we have therefore determined which ℓ- torsion group is to be considered for the Weil pairing.

4.3.1 The finite field $\mathbb{F}_p$ and its extensions

Recalling the modified Weil pairing that is used in the cryptosystem we can now address the field extensions necessary for the complete construction of the pairing for our system.

$$\tilde{e_\ell} : E(\mathbb{F}_{p^d})[\ell] \times E(\mathbb{F}_{p^d})[\ell] \to \mathbb{F}^\times_{p^k}$$

Firstly, the field extension d must be determined.
What is necessary to verify is that the ℓ- torsion group is indeed contained in the group of $E(K)$. For that we need that the field K contains a point of order ℓ.

What is required by the modified Weil pairing is that $\mathbb{F}_{p^d}$ must suffice as an extension of $\mathbb{F}_p$ to ensure the ℓ- torsion group is contained in $E(\mathbb{F}_{p^d})$. This is is equivalent to checking whether the ℓ^{th} roots of unity are contained in $\mathbb{F}^\times_{p^d}$, hence if there is a point of order $\ell \in \mathbb{F}^\times_{p^d}$. For the analysis of the degree of the extension d we start by taking $d = 1$, so $K = \mathbb{F}_p$. But $\ell \nmid p - 1 = \#\mathbb{F}_p$. With $d = 2$ it holds that $\ell | p^2 - 1 = \#\mathbb{F}_{p^2}$ since $(p^2 - 1)^2 = (2\ell - 1)^2 = 4\ell^2 - 4\ell$ which is obviously divisible by ℓ. So $d = 2$ suffices as a field extension for the ℓ- torsion group to be contained in $E(\mathbb{F}_{p^d})$.

An additional condition that is to be satisfied was mentioned in the first definition of the endomorphism δ, 3. An assumption made is that $X^2 + 2 \in K[X]$ is reducible, meaning that $\sqrt{-2} \in K$.
It was already mentioned that $\sqrt{-2} \notin \mathbb{F}_p$. So $X^2 + 2 \in \mathbb{F}_p[X]$ is irreducible. By the law of finite

fields, for a prime p and a monic irreducible polynomial $\pi(X) = X^2 + 2 \in \mathbb{F}_p$ of degree 2, the ring $\mathbb{F}_p/\pi(X)$ is a field of order p^2. We write $\mathbb{F}_{p^2}$ for the degree 2 extension of the finite field $\mathbb{F}_p$. Since $\sqrt{-2}$ is the root of $\pi(X)$ we know $\mathbb{F}_{p^2} \cong \mathbb{F}_p(\sqrt{-2})$. This verifies that $d = 2$ again suffices as a field extension for $\sqrt{-2} \in \mathbb{F}_{p^d}$ hence in $E(\mathbb{F}_{p^d})$.

Lastly, the field extension k must be determined.
$\mathbb{F}_{p^k}$ is the splitting field of $X^\ell - 1 \in \mathbb{F}_p[X]$ and the image of the modified Weil pairing consists of the ℓ^{th} roots of unity in the units $\mathbb{F}_{p^k}^\times$ of the field extension. We can therefore again verify that $\mathbb{F}_{p^k}^\times$ contains a point of order ℓ to verify those conclusions.
For the analysis of the degree of the extension d we start by taking $k = 1$, so $K = \mathbb{F}_p$. But $\ell \nmid p - 1 = \#\mathbb{F}_p$. With $k = 2$ it holds that $\ell | p^2 - 1 = \#\mathbb{F}_{p^2}$ since $(p^2 - 1)^2 = (2\ell - 1)^2 = 4\ell^2 - 4\ell$ which is obviously divisible by ℓ. So $k = 2$ suffices as a field extension for the ℓ^{th} roots of unity to be contained in $E(\mathbb{F}_{p^k})$.

We are finally left with the modified Weil pairing

$$\tilde{e_\ell} : E(\mathbb{F}_{p^2})[\ell] \times E(\mathbb{F}_{p^2})[\ell] \to \mathbb{F}_{p^2}^\times$$

with $\ell = \frac{p+1}{2}$ and p a large prime (such that $\sqrt{-2} \notin \mathbb{F}_\ell, \mathbb{F}_p$).

This concludes all necessary conditions of the parameters of the cryptosystem 3 and hence concludes the analysis of the new parameters.

5 Building the Cryptosystem

After the analysis of the new parameters adapted to the cryptosystem 3 following Washington's example, a demonstration of the IBE scheme can be executed on Magma, a Computational Algebra System. The Magma implementation preformed by Mak in his bachelors thesis [Mak14] is taken as a template. He implements the cryptosystem using the initial parameters that Washington had used. The Magma code to follow is adapted to the algorithm and parameters described in section 3 and discussed in the previous chapter.

For the choice of the primes p and ℓ a piece of code is implemented that requires a brief mathematical explanation in order to understand the algorithm. As already stated we have $\ell = \frac{p+1}{2}$ and $\sqrt{-2} \notin \mathbb{F}_p, \mathbb{F}_\ell$. $\sqrt{-2} \notin \mathbb{F}_p$ is equivalent to the Legendre symbol $\left(\frac{-2}{p}\right) = -1$. We make use of the following proposition which can be found in many text books such as [Bur11] but which was simply shown in [wik].

Proposition 2. *The Legendre symbol* $\left(\frac{-2}{p}\right) = -1 \Leftrightarrow p \equiv 5, 7 \ mod \ 8$

We choose $\ell = 5 + 8k$ for some $k \in \mathbb{Z}$. However, $p = 2\ell - 1 = 2(5 + 8k) - 1 = 9 + 16k \equiv 1 \bmod 8$. Hence p doesn't satisfy the above proposition. We choose $\ell = 7 + 8k$ for some $k \in \mathbb{Z}$. So $p = 2\ell - 1 = 2(7 + 8k) - 1 = 13 + 16k \equiv 5 \bmod 8$. Hence p does satisfy the above proposition. So we choose $\ell \equiv 7 \bmod 8$.
In order to make the algorithm some what more efficient, instead of increasing by a value of 8 to get to the next possible ℓ, we increase by a value of 24 which one can see in line 16 of the code. We look at when $k \equiv 1 \bmod 3$. $\ell = 7 + 8(3k + 1) = 7 + 8 + 8 \cdot 3k = 15 + 8 \cdot 3k = 3(5 + 8k)$ so ℓ is definitely not prime. It happens that $16 \equiv 1 \bmod 3$ and $24 \equiv 0 \bmod 3$.
One can go further with more conditions for finding the appropriate ℓ in the code yet this already delivers a code with time complexity low enough.

A few simplifications have been made in order to keep the time to execute the code low and to exclude unnecessary complications that do not facilitate the demonstration of the cryptosystem. Bob's digital ID is most likely in any real world scenario a string of characters. Yet in the code it will be presented as an integer. This is such that we can avoid having to transforming characters into binary strings. Including such a transformation would not add to the understanding of the new parameters and how they adapt to the cryptosystem. Similarly, the message M, which Alice wishes to send to Bob, is also an integer rather than a string of characters for the same reasons. The Hash functions are constructed appropriately to accepting an integer instead of a sting and outputting a point or vice versa. The Hash functions still serve the purpose they are meant to.

The Magma code follows

```
1  //SET UP
2  //Determining the primes p and l. starting with 2^400 for a very
       large number
3  // and checking for the first p and l after that. The starting
       value can be changed
4  // at will. 2^400 was chosen as it is a large number yet the
       computation time
5  //is kept reasonable
6  start:=2^400;
7  while (start mod 3) ne 0 do
8      start:=start+1;
9  end while;
10 ell:=7+8*start;
11 notfound:=true;
12 while notfound do
13     if IsPrime(ell) and IsPrime(2*ell-1)
14         then  p:= 2*ell-1;
15                 notfound:=false;
16         else ell:=ell+24;
```

```
    end if;
end while;

//Defining structures
// F_p is the finite field with p elements
// PR<x> is the polynomial ring over F_p
// F_p^2 is the finite field with p^2 elements
// E is the elliptic curve y^2 = x^3 + 4*x^2+2*x over F_p
// E2 is the same curve over F_p2

F_p:=GF(p);
PR<x>:=PolynomialRing(F_p);
F_p2 <a>:=ext<F_p | x^2 + 2>;
E:=EllipticCurve([F_p!0,F_p!4,F_p!0, F_p!2, F_p!0 ]);
E2:=EllipticCurve([F_p2!0,F_p2!4, F_p2!0, F_p2!2, F_p2!0]);

//Random point of order ell or 1 (but point 0 is very rare)
P:= 2*Random(E);
//Computing Ppub requires a random s in the units of F_ell so 0<s<
   ell
s:=Random(ell);
while s eq 0
    do s:=Random(ell);
end while;
Ppub:=s*P;

//EXTRACTION
//Bob's ID is taken as a number
ID:=55;

//Hash function 1 is constructed such that it creates a unique
//point of order ell based on the ID
H1IDy:=F_p!ID;
f:=x^3+4*x^2+2*x-H1IDy^2;
H1IDx:=Roots(f)[1][1];

QID:=2*E![H1IDx,H1IDy];

//The DID is Bobs private key. It is a point of E2 as it will later
// be used in the Weil pairing
DID:=s*QID;
DID:=E2!DID;

//ENCRYPTION
//the message is taken as a number
M:=123456789;

//the Weil pairing takes two points of order ell (which one
//specifies in the formula)
//For the construction of the endomorphism delta the point sqrt(-2)
    is necessary
//Note: a=sqrt(-2) as it is the adjoined number to F_p after the
   extension
// with x^2+2 such that we have F_p2

// Define the function delta(x, y)
```

```
delta:=func< x, y | E2![-(x+4+ 2/x)/2, y/(2*a)*(1-2/(x^2))]>;

QID:=E2!QID;
deltaPpub:=delta(Ppub[1],Ppub[2]);
gID:=WeilPairing(QID, deltaPpub, ell);
r:=Random(ell);
u:=r*P;
gIDr:=gID^r;

//Create the Hash function 2. The points of F_p^2 are of the form x
   +y*a where
//a is sqrt(-2) and the root of x^2+2
coefficients := Eltseq(gIDr);
xcoord:=Integers()!coefficients[1]; // Coefficient of 1 (x: the
   constant term)
ycoord:=Integers()!coefficients[2]; // Coefficient of a (y: the
   linear term)
H2gIDr := xcoord + p * ycoord;

//Take bitwise XOR of M and H2gIDr
v:=BitwiseXor(M, H2gIDr);
//cipher text c=(u,v) are sent to Bob


//DECRYPTION
//before computing Weil pairing the delta function must be applied
deltau:=delta(u[1],u[2]);
hID:=WeilPairing(DID, deltau, ell);

//applying Hash function 2 to hID
coefficients := Eltseq(hID);
xcoord:=Integers()!coefficients[1];
ycoord:=Integers()!coefficients[2];
H2hID := xcoord + p * ycoord;

m:=BitwiseXor(v, H2hID);

M;
m;
```

The code prints the values of M and m, which end up being the integer 123456789. M and m match meaning the encryption/ decryption process was successful. This concludes the demonstration of the cryptosystem analysed in this thesis and therefore shows a successful adaptation of the new parameters to the system.

6 Conclusion

This thesis builds upon Washington's IBE cryptosystem, which is based on Boneh and Franklin's encryption scheme. By selecting new parameters, specifically the elliptic curve (4) with an endomorphism δ given in (3), we have conducted an in-depth analysis of the cryptosystem's requirements. This analysis establishes the conditions necessary for these new parameters to function effectively within the cryptosystem.

The structure of the elliptic curve and its endomorphisms was a major focus due to their inherent algebraic properties. These algebraic structures were carefully compared to the requirements of the Weil pairing to construct a non-trivial modified Weil pairing. Conditions for the primes p and ℓ were determined to suit the modified Weil pairing and to establish essential structural properties for the cryptosystem. For instance, ensuring that $\sqrt{-2} \notin \mathbb{F}_p$ was necessary to confirm the supersingularity property of the elliptic curve E or $\sqrt{-2} \notin \mathbb{F}_\ell$ ensured δ fulfilled its purpose and "found" another point of order ℓ.

Having a comprehensive outline of all the conditions necessary for a cryptosystem not only provides mathematical proof of its functionality but also ensures its robustness and reliability. Should an error occur, this detailed mathematical outline facilitates the easier localization of faults. Furthermore, by presenting all conditions along with detailed descriptions of how new parameters are integrated, the thesis offers a blueprint for utilizing alternative parameters in future implementations. For example, alternative parameters could be drawn from Reitsma's Bachelor Thesis [Rei17], which provides multiple elliptic curves with suitable endomorphisms. Such parameters can be adapted and incorporated into the cryptosystem based on the methods outlined in this thesis.

This approach paves the way for further innovation and adaptation in the field of cryptography. With the advent of quantum cryptography, new parameters can be explored, or the presented encryption scheme can be further deconstructed. This thesis provides a comprehensive mathematical description of an elliptic curve IBE cryptosystem, detailing all its requirements and conditions, which facilitates future adaptations, such as incorporating quantum security levels.

Acknowledgements

I would like to express my deepest gratitude to my first supervisor, Professor Jaap Top. His understanding and supportive nature made this journey a rewarding experience. I thoroughly enjoyed our meetings, which were always insightful and filled with valuable guidance. His expertise and encouragement were crucial in shaping this work, and I am truly grateful for the time and effort he dedicated to helping me succeed.

I would also like to extend my heartfelt thanks to Professor Cecília Salgado, my second supervisor. Having her in this role was a true comfort, as her guidance was both supportive and encouraging. I not only had the pleasure of working with Cecília as my thesis supervisor but also as a professor in several courses. Her enthusiasm for the subjects she taught was contagious, and attending her lectures was always a pleasure. Her passion and dedication were truly inspiring, and I am deeply grateful for the positive impact she had on both my thesis and my overall academic experience.

I would like to extend my deepest thanks to both of my parents for being an incredible source of moral support throughout this journey. Their encouragement kept me motivated, and their assistance with the grammatical aspects of my thesis was invaluable. I am truly grateful for their unwavering support and guidance.

I would also like to thank Leo for being not only a wonderful partner but also a true friend. Throughout this journey of writing my thesis and the entire Bachelor's in Mathematics, he never stopped giving support and love. He offered encouragement when I needed to work and provided comfort and a safe place to rest when I needed a break. His unwavering support made a significant difference, and I am deeply grateful for everything he has done.

And to the truest of friends, Aylan. In both the best of times and the worst of times, she has been by my side. Her presence has made my experience in Groningen everything I could have wished for. She has provided me with such support, love, and insightful advice that I cannot thank her enough. From late-night study sessions working on our theses to moments of joyous, spontaneous laughter that brightened even the toughest days, she has made this journey feel effortless.

Finally, thank you to the city of Groningen for being such a beautiful and welcoming city which has allowed me to enjoy my Bachelor's of Mathematics to the fullest. I have made unforgettable memories here.

References

[BF01] Dan Boneh and Matthew Franklin. Identity-based encryption from the weil pairing. *SIAM J. of Computing*, 2001.

[Bur11] David M. Burton. *ELEMENTARY NUMBER THEORY*. McGraw-Hill, 2011.

[KMV00] Neal Koblitz, Alfred Menezes, and Scott Vanstone. The state of elliptic curve cryptography. *Designs, Codes and Cryptography*, 2000.

[Mak14] Richard Mak. Identity-based encryption using supersingular curves with the Weil pairing. Bachelor's thesis, University of Groningen, 2014. `https://fse.studenttheses.ub.rug.nl/12902/`.

[Mef09] Dennis Meffert. Bilinear pairings in cryptography. Master's thesis, Radboud Universiteit Nijmegen, 2009.

[Mil04] Victor S. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 2004.

[Rei17] Berno Reitsma. Endomorphisms of degree 2, 3 and 4 on elliptic curves. Bachelor's thesis, University of Groningen, 2017. `https://fse.studenttheses.ub.rug.nl/15691/`.

[RSA21] *What are the differences between RSA, DSA, and ECC encryption algorithms?*, 2021. `https://www.sectigo.com/resource-library/rsa-vs-dsa-vs-ecc-encryption#:~:text=The%20biggest%20difference%20between%20ECC,key%20of%20the%20same%20size.`

[Sha84] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Annual International Cryptology Conference*, 1984. `https://api.semanticscholar.org/CorpusID:1402295`.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[TM18] Jaap Top and Steffen Müller. Group theory. *Groningen University lecture notes*, 2018.

[Top17] Jaap Top. Advanced algebraic structures. *Groningen University lecture notes*, 2017.

[VV15] Gijsbert Van Vliet. The use of elliptic curves in cryptography. Master's thesis, Radboud University Nijmegen, 2015.

[Was08] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

[Wei79] André Weil. Sur les fonctions algébriques à corps de constantes fini. 1979. `https://api.semanticscholar.org/CorpusID:124985401`.

[wik] *Quadratic reciprocity*. `https://en.wikipedia.org/wiki/Quadratic_reciprocity`.