Mathematical Aspects of Elliptic Curve Cryptography

Ronal Pranil Chand

A thesis submitted for the degree of
Master of Science
of Fiji National University

October 2020

We certify that, as the assessors, we have read this thesis and that in our opinion it is fully appropriate, in scope and in quality, as this thesis for the degree of Master of Science.

Assessors: Signature:

I declare that this thesis has been composed solely by myself and has not been submitted, in whole or in part, in any previous application for a degree, except where states otherwise by reference or acknowledgment, the work presented is entirely my own.

Ronal Pranil Chand

23rd October, 2020.

Previously Published Content

This thesis contains materials on the following paper which was presented at the Number-Theoretic Methods in Cryptology 2019 (NutMic 2019).

Chand, R.P., Valluri, M.R. (2018). Elliptic Curves in Generalized Huff's Model. Cryptology ePrint Archive, Report 2018/1179. https://eprint.iacr.org/2018/1179

Acknowledgements

I want to offer my profound thanks to my supervisor Dr. Maheswara Rao Valluri, for his unending tolerance and support. He has been a patient mentor for both my academic learning and teaching. Without his help and mentorship, it would be unimaginable for me to accomplish my objective.

Special thanks also goes to Sandeep Ameet Kumar and Alveen Aditya Chand for their advice and technical support in compiling this thesis.

Finally, I would like to thank my loved ones for their support in my personal life and encouragement to pursue my dreams. My parents and my sister Pretika Kumar have constantly supported me in times of hardships and always believed in me for everything I did. It would have been impossible for me to achieve anything without them. Special thanks to my wife, Devika Rani. She has been understanding, a supportive and useful distraction for removing my stress, and Shaneel Chand and Prashneel Chand for their endless support and encouragement throughout my thesis journey.

Abstract

With the development and fast growth in information technology, data share security is an essential component. Cryptography is the general area of study associated with establishing different types of information security. One of the famous cryptography fields is the public key cryptosystem, which uses elliptic curves to construct key exchange protocols, encryption, authentication protocols, and digital signatures.

The purpose of this thesis is to investigate Huff's elliptic curves over finite fields. Huff's curve has not been used in cryptography as they are not fast even when compared to other well-known elliptic curves. Moreover, there is not much research done on Huff's model of elliptic curves. This thesis reflects on Weierstrass elliptic curves and a few of Huff's elliptic curves in literature and their essentials towards cryptography. The main contribution of this thesis is to introduce a new form of generalized Huff's model of elliptic curves and their arithmetic for point addition and doubling point. These new curves endowed with the addition are shown to be a group over a finite field. The computational cost of point addition and doubling point using projective, Jacobian, Lopez-Dahab coordinate systems, and embedding of the curves into $\mathbb{P}^1 \times \mathbb{P}^1$ system was compared . The new form of generalized Huff's model of elliptic curves are birationally equivalent to Weierstrass form of elliptic curves. It is noted that the computational cost on the curves for point addition and doubling point is lowest by embedding the curves into $\mathbb{P}^1 \times \mathbb{P}^1$ system than the other mentioned coordinate systems. It is noted that the introduced curve is nearly optimal to other known Huff's models but has not shown any improvement in computational cost.

Contents

Chapter 1

Introduction

The plane curves of degree 3 are known as cubics and have the general form of

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0.$$

Elliptic curves are non-singular cubic curves and have points defined over a finite field $\mathbb{K}$ [16, 36]. Elliptic curves are one of the most basic instances of group varieties, which are algebra geometric objects that may be adorned with a group structure. Their idea has been applied to significant issues in number theory, and it has lately found a practical application in the area of cryptography. In, the first cryptosystem was developed that was based on the so-called Diffie-Hellman problem on group varieties [13]. Following that, several additional writers were motivated to develop cryptosystems based on the same issue, thus addressing a range of difficulties in public-key cryptography. These cryptosystems were traditionally developed using the multiplicative group $F_q^{\times}$, which may be thought of as the affine plane curve $xy = 1$ over F_q. Replacing this group variety with an elliptic curve results in more secure cryptosystems than traditional equivalents, making this option extremely popular in recent years.

1.1 Background

Elliptic curves have been widely studied as a subject of almost pure mathematical interest. The study of elliptic curves could be of various areas: Algebra, Algebraic Geometry, Number Theory, Diophantine problems, etc. Lang

[27] mentions in his book that

> *"It is possible to write endlessly on elliptic curves. (This is not a treat.)"*

Elliptic curves have broad applications in cryptography, for which we introduce some of the technical cryptographic terms. Cryptography in the current internet world means sending data securely to the receiver without any third party able to decode and access the message sent. One of the methods is to use a secret-key cryptosystem. In the secret-key cryptosystem (also known as symmetric-key cryptosystem), two parties who wish to communicate through an unsecured channel have to use a single shared key to encrypt and decrypt the message. The secret-key cryptosystem is relatively faster because it has a high data transfer rate, and users usually use shorter keys to encrypt and decrypt data. This method's downfall is that the secret-key must be shared securely, and both parties must keep the key secret. A new era in cryptography started with a public-key cryptosystem (also known as asymmetric-key cryptosystem). Diffie and Hellman's groundbreaking idea in 1976 [13] got a lot of attention in the cryptographic world. In the public-key cryptosystem, encryption and decryption are done by two different keys. We here discuss public-key encryption by assuming that Bob wishes to send a scrambled message to Alice. Alice has a pair of keys, one key is called public-key, and the other is called secret-key or private-key. These keys are mathematically related, but the private-key is extremely difficult to deduce from the public-key. The public-key of Alice could be accessed by any user on the same network. Bob uses Alice's public-key to encrypt the message. Finally, Alice uses her secret-key to decrypt the encrypted message sent by Bob.

One of the exciting properties of elliptic curves is that we can define a group structure on them. The field of elliptic curve became interesting in the mid-1980s when Koblitz and Miller independently proposed Elliptic Curve Cryptography (ECC) using Elliptic Curve Discrete Logarithmic Problem (ECDLP) [25, 29].

The ECC offers better security compared to Rivest-Shamir-Adleman (RSA) cryptosystem using substantially lower-key sizes for a security parameter ϵ. Still, the underlying arithmetic group is more tedious, which makes the

study particularly interesting for systems with confined computing power and memory (such as cell phone) [26]. It is not surprising that small devices such as cell phones have increased in popularity in recent years, which regularly interact with the internet. These small devices have improved with better security due to ECC. The ECDLP does not have a ring structure; hence it is not vulnerable to attacks like the index calculus attack, which is the most efficient algorithm to solve both the problem of factoring the product of two large primes [20].

In 1995, elliptic curves played a vital role in the fascinated celebrations of Fermat's Last Theorem, whereby Andrew Wiles proved *Fermat's Last Theorem* using the proof of the modularity conjecture for semistable elliptic curves [38]. This led to renewed interest in elliptic curves and it's study. The uses of elliptic curves have commercialized and are studied extensively for their application in number theory and cryptography [17, 9, 10]. Following the separate contributions of Miller Miller [29] and Koblitz Koblitz [25], elliptic curve cryptography (ECC) began to be employed for commercial applications.

As a result, a significant amount of research has been devoted to analyzing the performance of various forms of elliptic curves proposed in the mathematical literature, such as Weierstra cubics Hoffstein et al. [20], Jacobi intersections Billet and Joye [8], Hessian curves Bernstein et al. [4], or the more recent forms of elliptic curves due to Montgomery Montgomery [30], or Edwards Edwards [15]. In addition, a long-forgotten model of elliptic curves suggested by Huff's in 1948 was addressed in 2010 Joye et al. [24]. This thesis is written on the fundamentals of Huff's model of elliptic curves.

1.2 Motivation

The following observations led to an emphasis on using elliptic curves in cryptography: The computation of discrete logarithms may be made intractable by present technology. Computing an elliptic curve discrete logarithm in a large prime order subgroup of an elliptic curve in exponential time using Pollard's rho method, the best algorithm known to date for calculating generic

discrete logarithms. The quest of a lower-cost elliptic curve is a perennially fascinating research subject. The computational cost determines the security of the ECC. Smaller key sizes are a significant characteristic of ECC, which prompted the initial motivation for this thesis. It is worth mentioning that the comparable RSA key sizes for "the same degree of security" increase at a faster rate since subexponential time attacks apply to the RSA cryptosystem. The "traditional" Weierstrass form of an elliptic curve may be rapidly computed in the case of cryptographic operations that include multiplications. One of the most frequent tools of the elliptic curve based cryptographic operations is scalar multiplication, which comprises addition operations on the points on an elliptic curve. As a result, increasing the speed of point addition also increases the speed of scalar multiplication and dependent protocols, and it is an excellent area of investigation. Huff's elliptic curves have not received much attention, and there may be some spectacular discoveries in this topic.

1.3 Aims and Outcome

The primary aim of this thesis is to provide a new generalized Huff's model of elliptic curves that is helpful for cryptography and give the efficiency of group operations on the new generalized Huff's curve. Multiplication, squaring, multiplication by a constant, addition/subtraction, and inversion is examples of group operation formulae. Inversion operations are much more expensive than others. As a result, removing the inversion operation is the first step toward improving the efficiency of scalar multiplication. Inversions are included in affine point addition formulae for elliptic curve points. When the curve is embedded in a projective space, however, the formulae become inversion-free. Thus, different projective spaces have varying degrees of efficiency for each curve shape. Even though Homogeneous Projective Coordinates are being presented more broadly in related research, the efficiency diversity is noteworthy. The derivation of the several formulas in this work were aided by computer software MATHEMATICA.

1.4 Outline of the thesis

This thesis is organized as follows: the next chapter gives an overview of cryptography and elliptic curves. In chapter 3, a brief study on Huff's model of elliptic curves. Chapter 4 introduces a new form of elliptic curves in generalized Huff's model and presents formulae for point addition and doubling point on the curves, and evaluates the computational cost of point addition and doubling. Chapter 5 shows that the new form of elliptic curves is birationally equivalent to the Weierstrass form of elliptic curves. Finally, the conclusion of the thesis with remarks and recommendations in the last chapter.

Chapter 2

Cryptography and Elliptic Curves

Researchers spent considerable effort investigating cryptographic systems based on more trustworthy trapdoor functions and succeeded in 1985 with the discovery of a new approach [29], specifically one based on elliptic curves, which were suggested as the foundation for the discrete logarithm group. Thus this chapter provides an overview of the elliptic curves and their application in cryptography.

2.1 History of Public-key Cryptography

In 1974, a proposal by Ralph Merkle [2] in an undergraduate project about public-key construction was rejected as it was little understood at that time. Two years later, the famous paper [13] entitled "New Directions in Cryptography" by Whitfield Diffie and Martin Hellman expressed the concept of a public-key cryptosystem. This paper contained groundbreaking contributions to the field of cryptography. After this breakthrough by Whitfield Diffie and Martin Hellman, Merkle's research appeared in 1982 as titled "Secure communication over insecure channels" [28].

It is worth noting that the idea of a public-key cryptosystem was initially discovered by James Ellis in 1969 and was kept a secret by the British government until after his death in 1997 [1, 20]. Similarly, Malcolm Williamson and Clifford Cocks at British Government Communication Headquarters discovered Diffie-Hellman key exchange algorithm and the Rivest–Shamir–Adleman (RSA)

[34, 35] public-key encryption system, respectively, before their rediscovery by Diffie, Hellman, Rivest, Shamir, and Adleman [20].

Alice, Bob, and Eve are users on the same channel network. Suppose Alice wants to communicate with Bob over the same channel without Eve knowing the message. As Eve is an adversary user and wants to know what message is communicated, Alice has to use some encryption that is hard for Eve to solve to secure her message. In this scenario, Alice's message could be encrypted by secret-key or public-key. If Alice wishes to use a secret-key cryptosystem, she must secretly share the same key to Bob. We can describe the procedure of Alice using a secret-key cryptosystem to communicate her message to Bob. Firstly, Alice and Bob have to choose a secret-key k only known to them and secret to other users on the channel.

Provided that Alice wants to send a plaintext message m, she would require a function $f(m,k)$ to produce a ciphertext c. Alice then publicly sends the ciphertext c. To recover the plaintext message m, Bob uses the function $g(c,k)$. The main advantage of a secret-key cryptosystem is that it is fast as it uses only one key in encryption and decryption. However, the main disadvantage of a secret-key cryptosystem is that the shared secret-key itself. This secret-key could be discovered by an adversary and must be changed very often with secure communication.

The second option for Alice is to use a public-key cryptosystem to encrypt her message. We will now give an overview of how the Public-Key Cryptosystem (PKC) is used. In [13], Diffie and Hellman define what PKC was and provided its associated components known as a one-way function. One-way functions are easy to compute; however, their inverse is challenging to compute. If one knows the trapdoor information, then finding the inverse function becomes easy. PKC consists of two keys, one is a private-key (k_{priv}), and the other is a public-key (k_{pub}). k_{pub} is computed by some key generation algorithms associated with k_{priv}. If Alice and Bob want to communicate a secret message, they must use the same key exchange algorithm. Bob shares his public-key $(k_{pub\,Bob})$ to Alice. Any users on the same network could access $k_{pub\,Bob}$. Its private key could only decrypt any message encrypted by a public-key since computing the inverse function is relativity as difficult without the trapdoor

information. Thus, Alice encrypts the message with $k_{pub\,Bob}$, and the ciphertext c sends to Bob. Upon receiving the ciphertext c, Bob uses his private-key $(k_{priv\,Bob})$ to decrypt the message. We note that even if Eve has c and $k_{pub\,Bob}$, she would not be able to decrypt the message as she does not have $k_{priv\,Bob}$. Thus the security of private-keys is not compromised in PKC. The security of PKC relies on hard computational problems. Now, let us explore some of the computational problems.

2.2 Discrete Logarithm Problem

The structure for the discrete logarithm issue is now defined. To begin, we shall define a group.

Definition 2.1. A set G is called a *group* on a binary operation $*$, denoted by $(G, *)$ if it satisfies the following four properties:

[Closure Law] For every $a, b \in G$, $a * b \in G$.

[Identity Law] There is an element $e \in G$ such that $e * a = a * e = a$ for every $a \in G$, e is an identity.

[Inverse Law] For every $a \in G$ there is a (unique) $b \in G$ such that $a * b = b * a = e$, where $b = a^{-1} \in G$.

[Associative Law] $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

If, in addition, it satisfies the

[Commutative Law] $a * b = b * a$ for all $a, b \in G$, then the group $(G, *)$ is called a commutative group or an abelian group [20].

The discrete logarithm problem is used in many cryptographic protocols. One such protocol is key exchange protocol. In the paper [13], Diffie and Hellman introduced a key exchange protocol based on the discrete logarithmic problem over a finite field $\mathbb{F}_p$, where p is at least 1024 bits length prime.

Theorem 2.2. ***(Primitive Root Theorem).*** *Let p be a prime number. Then, there exists an element $g \in \mathbb{F}_p^*$ whose powers give every element of $\mathbb{F}_p^*$, i.e. $\mathbb{F}_p^* = \{1, g, g^2, g^3, ..., g^{p-2}\}$, where $\mathbb{F}_p^*$ is a finite field. Elements with this property are called primitive roots of $\mathbb{F}_p^*$ or generators of F_p^*. The order of $\mathbb{F}_p^*$ is $p-1$.*

Proof. Proof. See [20] page 126. □

By the Theorem 2.2, it means that for every nonzero element of $\mathbb{F}_p$ is equal to some power of g. Here g is the generator of all nonzero elements of $\mathbb{F}_p$. Then, the Discrete Logarithm Problem (DLP) is to find $x \in \mathbb{F}_p$ which satisfies the following:

$$g^x \equiv h \bmod p \iff x \equiv log_g h \,(\bmod\, p),$$

where h is an element of $\mathbb{F}_p$.

Definition 2.3. Let G be a group whose group law is defined by $*$. The *Discrete Logarithm Problem* for G is to be determined, for $a, b \in G$ such that there is an integer x satisfying the following:

$$\underbrace{a * a * a * ... * a}_{x \text{ times}} = b.$$

2.3 Diffie–Hellman key Exchange Protocol

Again, take that Alice wants to publicly share a secret message to Bob through an unsecured channel where Eve is an adversary of the same channel and wants to know what Alice is communicating to Bob. To share the secret message, both Alice and Bob have to agree on a large prime p and a generator $g \in \mathbb{F}_p$. This ensures that there is no risk of sharing information publicly. Alice then picks a secret integer $a \in \mathbb{F}_p$ and does not reveal it to anyone. Likewise, Bob also chooses a secret integer $b \in \mathbb{F}_p$ and keeps it secret to himself. They both use their secret-key to compute their public-keys A and B, respectively.

$$\underbrace{A \equiv g^a \pmod{p}}_{\text{Alice computes}} \quad \text{and} \quad \underbrace{B \equiv g^b \pmod{p}}_{\text{Bob computes}}.$$

After computing their public-keys A and B, Alice and Bob share these on an unsecured communication channel. Again, the adversary Eve gets to see their computed values. Finally, Alice and Bob again use their secret integer to compute:

$$\underbrace{A^{'} \equiv B^a \pmod{p}}_{\text{Alice computes}} \quad \text{and} \quad \underbrace{B^{'} \equiv A^b \pmod{p}}_{\text{Bob computes}}.$$

Note that it is clear that $A^{'}$ and $B^{'}$ are the same shared secret-key since,

$$A^{'} \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B^{'} \mod p.$$

Example 2.4. Suppose Alice and Bob agree to use $p = 13441$ and $g = 781$. Alice chooses her secret-key as $a = 520$ and Bob chooses his secret-key as $b = 830$. They then compute their public-keys.

$$A \equiv \underbrace{977 \equiv 781^{520} \pmod{13441}}_{\text{Alice computes}} \quad \text{and} \quad \underbrace{B \equiv 13345 \equiv 781^{830} \pmod{13441}}_{\text{Bob computes}}.$$

Alice and Bob then share their computed value $A = 977$ and $B = 13345$ publicly. Now their shared secret-key would be

$$7201 \equiv 781^{(520\times 830)} \equiv 977^{830} \equiv 13345^{520} \pmod{13441}.$$

To see the communicated message Eve has to solve

$$781^a \equiv 977 \,(\mathrm{mod}\, 13441) \text{ or } 781^b \equiv 977 \,(\mathrm{mod}\, 13441).$$

Eve can solve these values of a and b if p is small prime. In practical, the p value must be at-least 1024 bits length ($p \approx 2^{1024}$ bits) [36]. Then it will be difficult for Eve to find the secret-keys of Alice and Bob.

2.4 Weierstrass Long Form of Elliptic Curve

Definition 2.5. Let $\mathbb{K}$ be a finite field and $\overline{\mathbb{K}}$ be its algebraic closure. Then the elliptic curve defined in the projective plane $\mathbb{P}^2(\mathbb{K})$ of a homogeneous Weierstrass equation is of the form

$$E(\mathbb{K}) : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

with $a_1, a_2, a_3, a_4 \in \mathbb{K}$.

The curve could be written in the form

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \tag{2.2}$$

and is smooth if the partial derivatives of the equation curve $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$ and $\frac{\partial F}{\partial Z}$ does not vanish simultaneously at any point on the curve. If all three partial derivatives of the curve vanish at a particular point P on $E(\mathbb{K})$ then the equation is singular, and point $P \in E(\mathbb{K})$ is called a singular point. The curve has one point at infinity namely $(0 : 1 : 0)$ and is represented by $\mathcal{O}$.

For simplicity, Weierstrass equation for the elliptic curve $E(\mathbb{K})$ could be transformed by using non-homogeneous coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ to the affine form as

$$E(\mathbb{K}) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.3}$$

If E is defined over a finite field $\mathbb{K}$ and $\text{char}(\overline{\mathbb{K}})$ represent characteristic of $\overline{\mathbb{K}}$ then with $a_1, a_2, a_3, a_4 \in \mathbb{K}$ and $\text{char}(\overline{\mathbb{K}}) \neq 2$, the equation could be simplified by substitution $y \longmapsto \frac{1}{2}(y - a_1x - a_3)$,and get as follows:

$$\begin{aligned}\frac{1}{4}\left(y^2 - x^2a_1^2 - 2xa_1a_3 - a_3^2\right) &= x^3 + a_2x^2 + a_4x + a_6\\ y^2 &= 4x^3 + (4a_2 + a_1^2)x^2 + \\ &\quad 2(2a_4 + a_1a_3)x + a_3^2 + 4a_6.\end{aligned}$$

For

$$b_2 = 4a_2 + a_1^2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6$$

gives a curve equation of

$$E:\ y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

The other quantities as defined as follows:

$$\begin{aligned}b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_2a_3 + a_2a_3^2 - a_4^2,\\ c_4 &= b_2^2 - 24b_4,\\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\ j &= \frac{c_4^3}{\Delta},\\ \omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.\end{aligned}$$

Moreover, if $\mathrm{char}(\overline{\mathbb{K}}) \neq 2, 3$, the substitution $(x, y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$ removes the x^2 term and yields a simpler equation

$$E:\ y^2 = x^3 + Ax + B, \tag{2.4}$$

where $A = -27c_4$ and $B = -54c_6$

Definition 2.6. The quantity Δ is the *discriminant* of the Weierstrass equation and j is the *j-invariant* of the elliptic curve. ω is the *invariant differential* associated to the Weierstrass equation.

The Weierstrass equation is singular if $\Delta = 0$. The *j-invariant* is related to an isomorphism between elliptic curves. Two elliptic curves are isomorphic over $\overline{\mathbb{K}}$ if and only if they have the same *j-invariant*.

Theorem 2.7. *Let E be an elliptic curve over a finite filed $\mathbb{K}$. Then the addition law on $E(\mathbb{K})$ has the following properties:*

1. $P + Q \in E(\mathbb{K})$ for all $P, Q \in E(\mathbb{K})$. [Closure Law]
2. $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E(\mathbb{K})$. [Identity Law]
3. $P + (-P) = \mathcal{O}$ for all $P \in E(\mathbb{K})$. [Inverse Law]
4. $(P + Q) + R = P + (Q + R)$ for all $P, Q, R \in E(\mathbb{K})$. [Associative Law]
5. $P + Q = Q + P$ for all $P, Q \in E(\mathbb{K})$. [Commutative Law]

Proof. For proof see [20]. □

2.5 The Group Law on Weierstrass Elliptic Curve

Let $E(\mathbb{K})$ be an elliptic curve over a finite field $\mathbb{K}$ given by the Weierstrass equation. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on $E(\mathbb{K})$ such that the line intersecting P and Q intersects the third point on $E(\mathbb{K})$, namely $R = (x_3, -y_3)$. The point R is then reflected across the x-axis and it yields another point $R' = (x_3, y_3)$. If we define the addition law by $\oplus$, then $P \oplus Q = R'$.

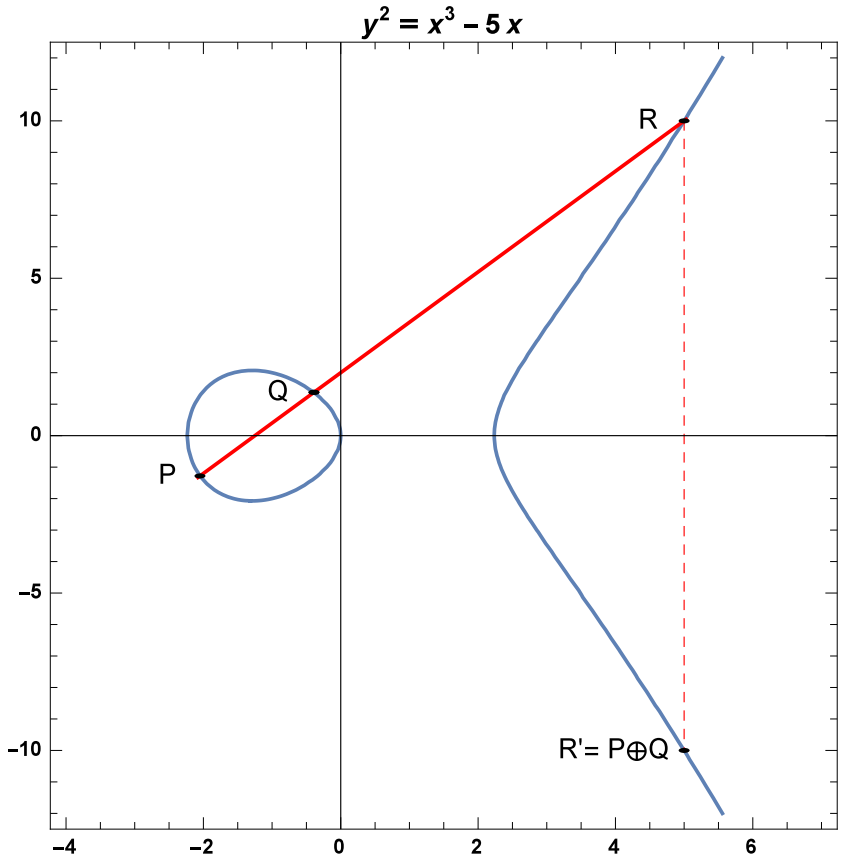

Figure 2.2: The additional law on a Weierstrass elliptic curve

Figure 2.2 shows that P and Q are two different points on $E(\mathbb{K})$. To add P to itself, noting that point Q on the curve could be moved as close to point P. In the sense of limit, as Q approaches P, the line becomes a tangent to $E(\mathbb{K})$ at P.

$$\begin{aligned} P \oplus Q &= P \oplus P \\ &= 2P. \end{aligned}$$

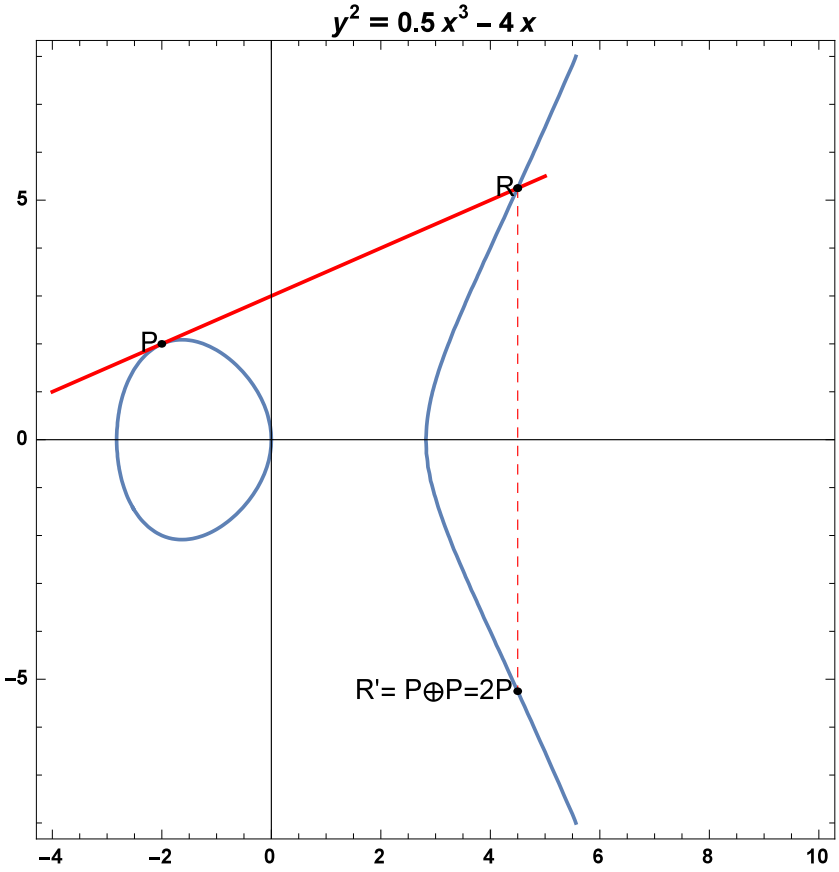

Figure 2.3: Adding a point P to itself on a Weierstrass elliptic curve

It is noted that addition of points on $E(\mathbb{K})$ is possible, but there is another scenario which is provided, that is $P \oplus P'$. This is where an additional point $\mathcal{O}$, which is at infinity is described. It is noted that $\mathcal{O}$ acts as the identity element of $E(\mathbb{K})$ under addition. Thus,

$$\begin{aligned} P \oplus P' &= \mathcal{O}, \\ P \oplus \mathcal{O} &= P. \end{aligned}$$

Definition 2.8. An *elliptic curve* $E(\mathbb{K})$ is the set of solutions to a short Weierstrass equation

$$E(\mathbb{K}) : Y^2 = X^3 + AX + B, \tag{2.5}$$

together with an extra point $\mathcal{O}$, where the constants A and B must satisfy $4A^3 + 27B^2 \neq 0$.

Take two points P and Q on $E(\mathbb{K})$; if they are added, then it produces another point $R^{'}$. We have a zero element $\mathcal{O}$ at infinity, which satisfies identity law (that is, $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$). Now, suppose there is another point Q (that is, $P, Q \neq \mathcal{O}$) on the same line which intersects the curve at another point known as R, then the following addition is correct:

$$P \oplus Q = Q \oplus P.$$

Furthermore, it could be shown that

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

Finally, repeated addition could be described by

$$\underbrace{P \oplus P \oplus P \oplus P \oplus P \oplus P ... \oplus P}_{\text{n times}} = nP,$$

where $n \in \mathbb{K}$ an integer. Thus, the elliptic curve E an additive group.

2.5.1 Affine Formulae

Let E be a non-singular elliptic curve over the field $\mathbb{K}$ defined by the Weierstrass equation

$$E(\mathbb{K}) : \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$. As mentioned that there is an additional point $\mathcal{O}$ which does not lie on $E(\mathbb{K})$ but is used to fulfill the group axioms. The additional formulas are as follow:

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two different points on E such that $P \neq \mathcal{O}$ and $Q \neq \mathcal{O}$,

$$\lambda = \begin{cases} \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } P = Q, \\ \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq \pm Q, \end{cases}$$

and then $x_3 = \lambda^2 + a_1\lambda - x_1 - x_2 - a_2$, and $y_3 = -\lambda(x_3 - x_1) - y_1 - a_1x_3 - a_3$. Then $P + Q = (x_3, y_3)$.

To achieve addition on short Weierstrass equation, one can set $a_1, a_2, a_3 = 0$, $a_4 = A$, and $a_6 = B$ on the above formulae of x_3, y_3 and λ. Thus, addition on short Weierstrass equation is given by the same conditions as above with

$P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two different points on short Weierstrass equation elliptic curve such that $P \neq \mathcal{O}$ and $Q \neq \mathcal{O}$,

$$\lambda = \begin{cases} \dfrac{3x_1^2 + A}{2y_1} & if \;\; P = Q, \\ \dfrac{y_2 - y_1}{x_2 - x_1} & if \;\; P \neq \pm Q, \end{cases}$$

and then $x_3 = \lambda^2 + x_1 - x_2$ and $y_3 = -\lambda(x_3 - x_1) - y_1$. Then $P + Q = (x_3, y_3)$.

2.5.2 Projective Coordinates

In regards to cryptography, projective coordinates are used to avoid the inversion that appears in the affine form. Using projective coordinates, one can reduce computational cost since inversion is costly. There are many varieties of projective form.

The short Weierstrass form of elliptic curve defined by equation (2.5) could be rewritten as

$$E(\mathbb{K})_\omega : Y^2Z = X^3 + AX^2Z + BZ^3.$$

The point $(X_1 : Y_1 : Z_1)$ is on $E(\mathbb{K})_\omega$ with $X_1, Y_1 \in E(\mathbb{K})$, $\text{char}(\mathbb{K}) \neq 2, 3$, and $Z_1 \in E(\mathbb{K})$. The projective point $(X_1 : Y_1 : Z_1)$ is equivalent to the affine form $(X_1/Z_1, Y_1/Z_1)$ and the point at infinity is $\mathcal{O} = (0 : 1 : 0)$.

2.6 Elliptic Curve Diffie-Hellman Key Exchange Protocol

If Alice and Bob want to communicate a secret message using Elliptic Diffie-Hellman key exchange protocol, then they have to agree to a particular elliptic curve $E(\mathbb{F}_p)$ and a specific point P on $E(\mathbb{F}_p)$. Alice then picks a secret integer n_A and does not reveal it to anyone. Likewise, Bob also chooses a secret integer n_B and keeps it confidential to himself. They both use their secret-key to compute their public-key Q_A and Q_B.

$$\underbrace{Q_A = n_A P}_{\text{Alice computes}} \qquad \text{and} \qquad \underbrace{Q_B = n_B P}_{\text{Bob computes}}.$$

After computing Q_A and Q_B, Alice and Bob share this on an unsecured communication channel. Finally, Alice and Bob again use their secret integer to compute

$$n_A Q_B = (n_A n_B)P = n_B Q_A,$$

which is the commonly shared secret-key of Alice and Bob.

2.7 Other Cryptographic Schemes and Models for Elliptic Curves

Elliptic curves can be used to construct other cryptographic schemes such as encryption schemes, digital signatures, and hash functions. But, their creations are not discussed in this write-up.

Other famous forms of elliptic curves existing in literature are Hessian curves [4, 23], Jacobi quartics [8], Montgomery [30, 6], Edwards [3, 7, 15], Doubling-oriented Doche–Icart–Kohel [14, 5] and Huff's curve [21]. The next chapter will visit Huff's model of elliptic curves, however there is no intention to place other elliptic curves models literature but are equally important to mathematical aspects and cryptography.

2.8 Computational Cost on Elliptic Curves

To analyze the efficiency of the arithmetic on an elliptic curve, one must compute the computational cost. To get optimal computational cost, one must analyse the cost of point addition and doubling point on the curve $E(\mathbb{K})$. In this thesis, m represents multiplication between two curve variables, s represents squaring of a curve variable, a represents addition/subtraction of two curve constants, and d represents multiplication by two curve constants.

Chapter 3

Huff's Model

There has been a lot of development to Huff's model of elliptic curves in [11, 19, 24, 39, 32]. For instance, Joye et al. studied Huff's elliptic curves in 2010 [23]. In 2012, Wu and Feng also carried out research on Huff's curves in [39]. A year later, Binary Huff's curves were investigated by Devigne and Joye [12]. In 2015, He et al. [19] studied generalized Huff's curves. In 2018, Orhon and Hisil also studied speeding of Huff's model of elliptic curve [32]. This chapter, studies Huff's Model of the elliptic curves as discussed by Joye et al [12, 24]. We intend to study and summarize the work of the authors mentioned above. However, there is no intention to deliver every aspect of each paper or content of every paper.

3.1 Elliptic Curves by Gerald Huff and Peeples

In 1948, to study a diophantine problem, Huff considered the distance of subsets of set S of the plane $\mathbb{R}^2$such that for all s_1,$s_2 \in S$, the distance between s_1 and s_2 is a rational number [21]. Given that if $a, b \in \mathbb{Q}$, S contains four points $(0, \pm a)$ and $(0, \pm b)$ on the y-axis, and $(x, 0)$ on the x-axis for some $x \in \mathbb{Q}$. The point $(x, 0)$ must satisfy the equation $x^2 + a^2 = u^2$ and $x^2 + b^2 = v^2$ with $u, v \in \mathbb{Q}$. The homogeneous equation is of the form $x^2 + a^2z^2 = u^2$ and $x^2 + b^2z^2 = v^2$ defines a curve of genus 1 in $\mathbb{P}^3$. Later Huff and his student Peeples [33] provided examples of curves that had positive rank over $\mathbb{Q}$. These examples provided large rational set distances of cardinality $k > 4$ such that there are $k - 4$ points on a line.

The non-homogeneous form of these genus 1 curve is equivalent to the curve

$$ax(y^2 - 1) = by(x^2 - 1), \tag{3.1}$$

where $a, b \in \mathbb{Q}$. It is clearly seen that equation (3.1) over any finite field $\mathbb{K}$ of odd characteristic defines an elliptic curve if $a^2 \neq b^2$ and $a, b \neq 0$. In the projective plane $\mathbb{P}^2(\mathbb{K})$ equation (3.1) could be defined as

$$F(X, Y, Z) = aX(Y^2 - Z^2) - bY(X^2 - Z^2). \tag{3.2}$$

One could verify that the partial derivatives $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$ and $\frac{\partial F}{\partial Z}$, of the curve equation does not vanish simultaneously at three points of infinity $(1 : 0 : 0)$, $(0 : 1 : 0)$, and $(a : b : 0)$, however, vanish at a finite point $(x : y : 1)$ if and only if, $ax = by$ together with equation (3.1) which suggest that $x^2 = y^2$ and therefore $a^2 = b^2$. The point $(1 : 1 : 1)$ in character 2, is always singular and the families of curve defined by equation (3.1) does not contain any smooth curve.

3.1.1 List of Huff's Model of Elliptic Curves

The different families of Huff's elliptic curves studied over the past decade are listed below.

1. The curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Joye et al. in [24] are of the form:
$$ax(y^2 - 1) = by(x^2 - 1), \text{where } a^2 - b^2 \neq 0.$$

2. The generalized Huff's curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Joye et al. in [24] are of the form:
$$ax(y^2 - d) = by(x^2 - d), \text{where } abd(a^2 - b^2) \neq 0.$$

3. The generalized Huff's curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Wu and Feng in [39] are of the form:
$$x(ay^2 - 1) = y(bx^2 - 1), \text{where } ab(a - b) \neq 0.$$

4. The binary Huff curves over a field $\mathbb{K}$, char($\mathbb{K}$) $= 2$ by Joye et al. in [24] are of the form:

$$ax(y^2 + y + 1) = by(x^2 + x + 1), \text{where } ab(a - b) \neq 0.$$

5. The generalized binary Huff curves over a field $\mathbb{K}$, char($\mathbb{K}$) $= 2$ by Joye et al. in [24] are of the form:

$$ax(y^2 + fy + 1) = by(x^2 + fx + 1), \text{where } abf(a - b) \neq 0.$$

6. The generalized Huff's curves over a field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Ciss and Sow in [11] are of the form:

$$ax(y^2 - c) = by(x^2 - d), \text{where } abcd(a^2c - b^2d) \neq 0.$$

7. The generalized Huff's curves over finite field $\mathbb{K}$, char($\mathbb{K}$) $\neq 2$ by Orhon and Hisil in [32] are of the form:

$$y(1 + ax^2) = cx(1 + dy^2), \text{where } acd(a - c^2d) \neq 0.$$

3.1.2 Huff's Model of Elliptic Curves by Joye, Tibouchi and Vergnaud

Let $\mathbb{K}$ be a field of characteristic $\neq 2$. Huff's model of an elliptic curve satisfying the set of projective points $(X : Y : Z) \in \mathbb{P}^2(\mathbb{K})$ is of the form

$$E(\mathbb{K}) \;:\; aX(Y^2 - Z^2) = bY(X^2 - Z^2), \tag{3.3}$$

where $a, b \in \mathbb{K}$ and $a^2 \neq b^2$.

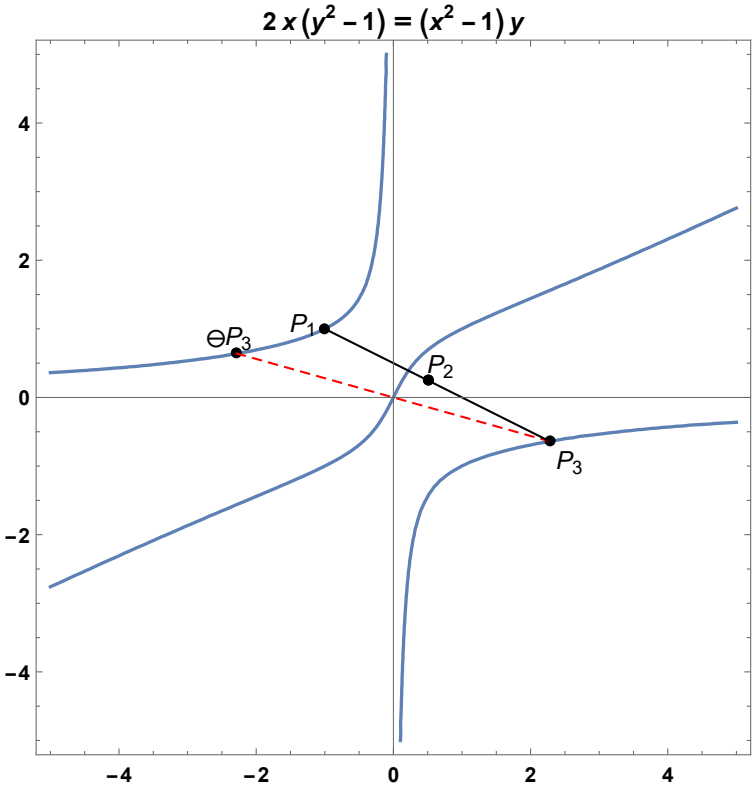

Figure 3.1: An Example of Huff's curve over $\mathbb{R}$

For equation (3.3), the neutral element is $\mathcal{O} = (0 : 0 : 1)$, which intersects the curve with multiplicity 3. The tangent line at $\mathcal{O}$ is $aX = bY$; thus $\mathcal{O}$ is a point of inflection. Then the elliptic curve $E(\mathbb{K})$ could be described; with the identity $\mathcal{O}$ and whose group law, defined by $\oplus$.

For any line intersecting $E(\mathbb{K})$ at three points as P_1, P_2 and, P_3 the following property $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$ is true. Figure 3.1 shows the line intersection at points P_1, P_2 and, P_3. The inverse of point $P_1 = (X_1 : Y_1 : Z_1)$ is $P_1 = (X_1 : Y_1 : -Z_1)$. Finally, the sum of P_1 and P_2 is $P_1 \oplus P_2 = \ominus P_3$. This elliptic curve have three points at infinity, $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(a : b : 0)$.

3.1.3 Affine Formula

Given that points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are on

$$E(\mathbb{K}) : ax(y^2 - 1) = by(x^2 - 1), \tag{3.4}$$

the line intersects the third point $P_3 = (x_3, y_3)$. Then the following is true:

1. Dedicated addition: $P_1 \oplus P_2$ where $P_1 \neq P_2$.,

$$x_3 = \frac{(x_1 - x_2)(y_1 + y_2)}{(1 - x_1x_2)(y_1 - y_2)} \text{ and } y_3 = \frac{(x_1 + x_2)(y_1 - y_2)}{(x_1 - x_2)(1 - y_1y_2)}.$$

2. Unified addition

$$x_3 = \frac{(x_1 + x_2)(1 + y_1y_2)}{(1 + x_1x_2)(1 - y_1y_2)} \text{ and } y_3 = \frac{(y_1 + y_2)(1 + x_1x_2)}{(1 - x_1x_2)(1 + y_1y_2)}\ .$$

3. Doubling: $2P_1$

$$2x_1 = \frac{2x_1(1 + y_1^2)}{(1 + x_1^2)(1 - y_1^2)} \text{ and } 2y_1 = \frac{(2y_1(1 + x_1^2)}{(1 - x_1^2)(1 + y_1^2)}$$

Chapter 4

Generalized Huff's Model of Elliptic Curves

The search for a new form of elliptic curves is fascinating, and if one gets a considerably faster curve, other models would be an outstanding achievement. This chapter introduces a new form of elliptic curve in generalized Huff's model. These models of Huff's elliptic curves endow with addition are group over a finite field. We provide point addition, doubling point, and computation cost comparison with other Huff's families of the elliptic curve.

4.1 Introduction to Generalized Huff's Model of Elliptic Curves

Let $\mathbb{K}$ be a finite field of $char(\mathbb{K}) \neq 2$. Let's define an elliptic curve, denoted by E, over $\mathbb{K}$ as

$$E(\mathbb{K}) : ax\left(y^2 + xy + f\right) = by\left(x^2 + xy + g\right), \tag{4.1}$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$. The j-invariant of $E(\mathbb{K})$ is given by $\frac{256\left(a^2f^2+abfg+b^2g^2\right)^3}{a^2b^2f^2g^2(af+bg)^2}$. The inflection point $(0:0:1)$ of $E(\mathbb{K})$ has the tangent line

$bgy = afx$ that passes through the curve with multiplicity 3; thus $\mathcal{O} = (0 : 0 : 1)$ is a neutral point of $E(\mathbb{K})$. Furthermore, group law is defined as

$\oplus$. Figure 4.1 shows that the line passing through the points P and Q, and intersecting at third point R on $E(\mathbb{K})$.

Let $P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, and $R = (X_3 : Y_3 : Z_3)$ be three points on $E(\mathbb{K})$. Then, $P \oplus Q$ could be obtained by the line connecting R and O that intersects at third point $\ominus R$ on $E(\mathbb{K})$ such that
$P \oplus Q = \ominus R$ which implies that $P \oplus Q \oplus R = \mathcal{O}$. In particular, the inverse of the point P is $\ominus P = (X_1 : Y_1 : -Z_1)$. It is clear that the curve $E(\mathbb{K})$ posses commutative law. There are three points at infinity, namely $(1 : 0 : 0)$, $(0 : 1 : 0)$, and $(a : b : 0)$ on $E(\mathbb{K})$, and the sum of any two points at infinity equals to the third point. For any point $(X_1 : Y_1 : Z_1)$, when $Z_1 \neq 0$, for some real number α and γ bounded by the field $\mathbb{K}$, it is observed that

$$(1 : 0 : 0) \oplus (X_1 : Y_1 : Z_1) = (\alpha Z_1^2 : -X_1 Y_1 : X_1 Z_1) \text{ and}$$

$$(0 : 1 : 0) \oplus (X_1 : Y_1 : Z_1) = (-X_1 Y_1 : \gamma Z_1^2 : Y_1 Z_1).$$

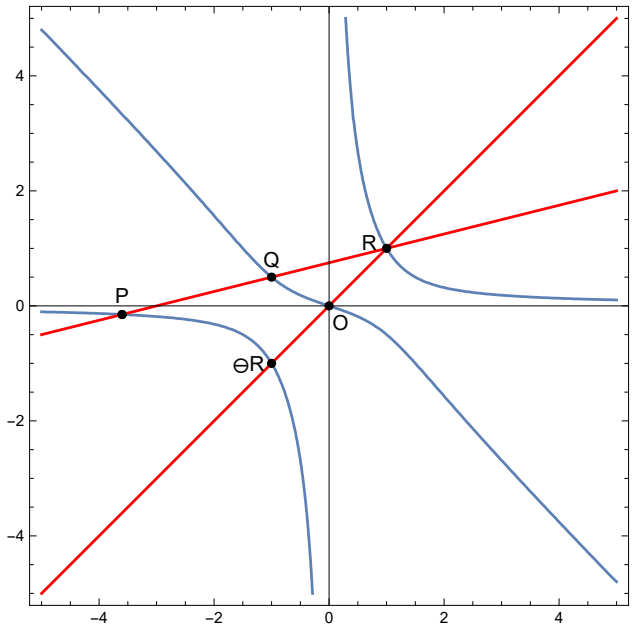

Figure 4.1: An example of the elliptic curve $E(\mathbb{K})$

Furthermore, note that

$$(a : b : 0) \oplus (X_1 : Y_1 : Z_1) = (0 : 1 : 0) \oplus (\alpha Z_1^2 : -X_1 Y_1 : X_1 Z_1),$$

therefore

$$(a : b : 0) \oplus (X_1 : Y_1 : Z_1) = \begin{cases} (a : b : 0) \text{ if } (X_1 : Y_1 : Z_1) = (0 : 0 : 1) \\ (-\alpha Y_1 Z_1 : -\gamma X_1 Z_1 : X_1 Y_1) \quad \text{otherwise} \end{cases}.$$

Doubling point is achieved if $P = Q$, thus the line connecting P and Q is the tangent at the point P.

4.2 Affine Formulae

This subsection provides explicit formulae for the group law for the elliptic curve defined by equation (4.1).

Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$, and $R = (x_3, y_3)$ be the three different points on $E(\mathbb{K})$ such that R is obtained by connecting a line through P and Q. Let the secant line joining P and Q has the slope defined as $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$. Thus, $y = \lambda x + \beta$ is the equation of the secant line passing through the points P, Q, and R, where $\beta = y_1 - \lambda x_1$. For the curve equation (4.1), replace y with $\lambda x + \beta$. Then,

$$\begin{aligned} ax((\lambda x + \beta)^2 + x(\lambda x + \beta) + f) &= b(\lambda x + \beta) \\ &\quad (x^2 + x(\lambda x + \beta) + g). \end{aligned}$$

This implies that (4.2)

$$\begin{aligned} x\left(af + a\beta^2\right) + x^2(a\beta + 2a\beta\lambda) \\ + x^3\left(a\lambda + a\lambda^2\right) &= (bg\beta + x\left(b\beta^2 + bg\lambda\right) \\ &\quad + x^2(b\beta + 2b\beta\lambda) + x^3\left(b\lambda + b\lambda^2\right). \end{aligned} \quad (4.3)$$

Let

$$A = a\beta - b\beta + 2a\beta\lambda - 2b\beta\lambda$$

and

$$B = a\lambda - b\lambda + a\lambda^2 - b\lambda^2.$$

Then, equation (4.2) becomes

$$-bg\beta + x\left(af + a\beta^2 - b\beta^2 - bg\lambda\right) + Ax^2 + Bx^3 = 0. \tag{4.4}$$

.

Note that

$$x_1 + x_2 + x_3 = -\frac{A}{B} \tag{4.5}$$

$$-x_3 = x_1 + x_2 + \frac{a\beta - b\beta + 2a\beta\lambda - 2b\beta\lambda}{a\lambda - b\lambda + a\lambda^2 - b\lambda^2},$$

substituting $\beta = y_1 - \lambda x_1$ and $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ yields

$$\begin{aligned} x_3 &= -\left(x_1 + x_2 + \frac{(x_1 - x_2 + 2y_1 - 2y_2)(-x_2y_1 + x_1y_2)}{(y_1 - y_2)(x_1 - x_2 + y_1 - y_2)}\right) \\ &= -x_1 - x_2 - \frac{(x_1 - x_2 + 2y_1 - 2y_2)(-x_2y_1 + x_1y_2)}{(y_1 - y_2)(x_1 - x_2 + y_1 - y_2)}, \end{aligned}$$

which simplifies to

$$x_3 = -\frac{(x_1 - x_2)(y_1(x_1 + y_1) - y_2(x_2 + y_2))}{(y_1 - y_2)(x_1 - x_2 + y_1 - y_2)}. \tag{4.6}$$

By symmetry that it could be claimed that,

$$y_3 = -\frac{(y_1 - y_2)\left(x_1^2 + x_1 y_1 - x_2\left(x_2 + y_2\right)\right)}{(x_1 - x_2)\left(x_1 - x_2 + y_1 - y_2\right)}. \tag{4.7}$$

Thus, this is an evidence that the curve $E(\mathbb{K})$ has three points $P = (x_1, y_1)$, $Q = (x_2, y_2)$, and $R = (x_3, y_3)$. Observe that the inverse of the point R is $\ominus R = (-x_3, -y_3)$. Note that point $R = (x_3, y_3)$ is computed only when $x_1 \neq x_2$, $y_1 \neq y_2$, and $x_1 - x_2 + y_1 - y_2 \neq 0$ and the addition formula used in the affine coordinate system could not be employed for doubling points since $x_1 \neq x_2$ and $y_1 \neq y_2$.

Theorem 4.1. *Let $E(\mathbb{K})$ be a elliptic curve defined by equation (4.1) with $abfg(a - b) \neq 0$ and points P, Q, and $\mathcal{O} = (0, 0)$ on $E(\mathbb{K})$. $\mathcal{O}$ is a neutral point. Then E has the following properties.*

1. *If $P = \mathcal{O}$, then $P \oplus Q = Q$.*
2. *Otherwise, if $Q = \mathcal{O}$, then $P \oplus Q = P$.*
3. *Otherwise, let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.*
4. *If $-x_1 = x_2$ and $-y_1 = y_2$, then $P \oplus Q = \mathcal{O}$.*
5. *Otherwise, let*

   $$x_3 = -\frac{(x_1 - x_2)(y_1(x_1 + y_1) - y_2(x_2 + y_2))}{(y_1 - y_2)(x_1 - x_2 + y_1 - y_2)} \text{ and } y_3 = -\frac{(y_1 - y_2)\left(x_1^2 + x_1 y_1 - x_2(x_2 + y_2)\right)}{(x_1 - x_2)(x_1 - x_2 + y_1 - y_2)}.$$

   Then $P \oplus Q = (-x_3, -y_3)$

Proof. Parts (1.) and (2.) are a similar concept and is easy to see. For (1.), P is the neutral point (0,0), then the line through P and Q intersects E with the of 3, as P, Q and $-Q$. To obtain $P \oplus Q$, one must take the inverse of the third point of the intersection. Thus, $-(-Q) = Q$. The similar proof follows for (2.). Part (4.) is also easily obtained. If $P = (x_1, y_1)$ and $Q = (x_2, y_2) = (-x_1, y_1)$ then the third point of intersection of P and Q is $\mathcal{O}$. The inverse of $\mathcal{O}$ is $-\mathcal{O}$=$\mathcal{O}$. To prove (5.), it is necessary to take algebraic step. If points $P = (x_1, y_1)$ and

$Q = (x_2, y_2)$ are two distinct points on E and neither of them equal to $\mathcal{O}$, then the line through points P and Q has the slope λ. The line equation could be written as $y = \lambda x + \beta$, where $\beta = y_1 - \lambda x_1$. Substituting the line equation in $E(\mathbb{K})$ gives us the equation (4.3). It is clear that x_1 and x_2 are two roots of the above cubic equation; thus, it could be written that,

$$\begin{aligned}(x - x_1)(x - x_2)(x - x_3) = x^3 + (-x_1 - x_2 - x_3)x^2 \\ + (xx_2 + x_3x_2 + x_1x_3)x - x_1x_2x_3.\end{aligned}$$

Then the proof follows the from equation (4.5) and equation (4.6) (See section 4.1). □

We now define a point of infinity on $E(\mathbb{K})$ as $\mathcal{O} = (0, 0)$. For the point $P = (x_1, y_1)$, $\ominus P = (-x_1, -y_1)$. Thus, it follows that

$$\begin{aligned}x_3 &= -\frac{(x_1 - x_2)\,(y_1\,(x_1 + y_1) - y_2\,(x_2 + y_2))}{(y_1 - y_2)\,(x_1 - x_2 + y_1 - y_2)} \\ &= -\frac{(x_1 - -x_1)\,(y_1\,(x_1 + y_1) - -y_2\,(-x_2 - y_2))}{(y_1 - -y_2)\,(x_1 - -x_2 + y_1 - -y_2)} \\ &= -\frac{(x_1 + x_1)\,(y_1\,(x_1 + y_1) + y_1\,(-x_1 - y_1))}{(y_1 - -y_1)\,(x_1 - -x_1 + y_1 - -y_1)} \\ &= -\frac{(2x_1)\,(0)}{(2y_1)\,(2x_1 + 2y_1)} \\ &= 0\end{aligned}$$

and

$$\begin{aligned} y_3 &= -\frac{(y_1-y_2)\left(x_1^2+x_1y_1-x_2\left(x_2+y_2\right)\right)}{(x_1-x_2)\left(x_1-x_2+y_1-y_2\right)} \\ &= -\frac{(y_1--y_1)\left(x_1^2+x_1y_1--x_1\left(-x_1-y_1\right)\right)}{(x_1--x_1)\left(x_1--x_1+y_1--y_1\right)} \\ &= -\frac{(2y_1)\left(x_1^2+x_1y_1+x_1\left(-x_1-y_1\right)\right)}{(x_1+x_1)\left(x_1+x_1+y_1+y_1\right)} \\ &= -\frac{(2y_1)\,(0)}{(2x_1)\left(2x_1+2y_1\right)} \\ &= 0. \end{aligned}$$

Thus $P \oplus (\ominus P) = \mathcal{O}$.

Corollary 4.2. *The identity $\mathcal{O}$ is always on the elliptic curve defined by*

$$E:\ ax(y^2+xy+f) = by(y^2+xy+g),$$

where $abfg(a-b) \neq 0$.

Theorem 4.3. *A line cutting $E(\mathbb{K})$ at three distinct points namely P,Q, and R. The associative law on these points is equivalent to $\mathcal{O} = (0,0)$.*

Proof. To show that the curve $E(\mathbb{K})$ holds associative law, that is
$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$.
For x-coordinates, the addition becomes,

$$Q \oplus R = \frac{(x_2-x_3)\left(y_2\left(x_3+y_2\right)-y_3\left(x_3+y_3\right)\right)}{(y_2-y_3)\left(x_2-x_3+y_2-y_3\right)},$$

and by equation (4.1),

$$P = \frac{(x_2-x_3)\left(y_2\left(x_3+y_2\right)-y_3\left(x_3+y_3\right)\right)}{(y_2-y_3)\left(x_2-x_3+y_2-y_3\right)},$$

then

$$\begin{aligned} P \oplus (Q \oplus R) &= -\frac{(x_2 - x_3)\,(y_2\,(x_3 + y_2) - y_3\,(x_3 + y_3))}{(y_2 - y_3)\,(x_2 - x_3 + y_2 - y_3)} + \\ &\quad \frac{(x_2 - x_3)\,(y_2\,(x_3 + y_2) - y_3\,(x_3 + y_3))}{(y_2 - y_3)\,(x_2 - x_3 + y_2 - y_3)} \\ &= 0. \end{aligned}$$

It follows that,

$$\begin{aligned} (P \oplus Q) \oplus R &= -\frac{(x_1 - x_2)\,(y_1\,(x_1 + y_1) - y_2\,(x_2 + y_2))}{(y_1 - y_2)\,(x_1 - x_2 + y_1 - y_2)} + \\ &\quad \frac{(x_1 - x_2)\,(y_1\,(x_1 + y_1) - y_2\,(x_2 + y_2))}{(y_1 - y_2)\,(x_1 - x_2 + y_1 - y_2)} \\ &= 0. \end{aligned}$$

For y-coordinates, the following addition holds,

$$\begin{aligned} P \oplus (Q \oplus R) &= -\frac{(y_2 - y_3)\,\left(x_2^2 + x_2 y_2 - x_3\,(x_3 + y_3)\right)}{(x_2 - x_3)\,(x_2 - x_3 + y_2 - y_3)} \\ &\quad + \frac{(y_2 - y_3)\,\left(x_2^2 + x_2 y_2 - x_3\,(x_3 + y_3)\right)}{(x_2 - x_3)\,(x_2 - x_3 + y_2 - y_3)}. \\ &= 0, \end{aligned}$$

and

$$\begin{aligned} (P \oplus Q) \oplus R &= -\frac{(y_1 - y_2)\,\left(x_1^2 + x_1 y_1 - x_2\,(x_2 + y_2)\right)}{(x_1 - x_2)\,(x_1 - x_2 + y_1 - y_2)} + \\ &\quad \frac{(y_1 - y_2)\,\left(x_1^2 + x_1 y_1 - x_2\,(x_2 + y_2)\right)}{(x_1 - x_2)\,(x_1 - x_2 + y_1 - y_2)} \\ &= 0. \end{aligned}$$

In both scenarios the addition gives $\mathcal{O}$. Now to get final point one must reflect

$\mathcal{O}$ on $\mathcal{O}$ (that is, $\mathcal{O} \oplus \mathcal{O}$), however $\mathcal{O}$ is the neutral point thus, we have

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

□

4.2.1 Doubling Point

The slope of the tangent line to the curve defined by equation (4.1) could be computed by implicit differentiation. Thus, by differentiation of $E(\mathbb{K})$ with respect to x, the equation (4.1) becomes,

$$\begin{aligned} af + 2axy + ay^2 + ax^2y' + 2axyy' &= 2bxy + by^2 + bgy' + bx^2y' + 2bxyy' \\ y' &= \frac{af + 2axy + ay^2 - 2bxy - by^2}{bg - ax^2 + bx^2 - 2axy + 2bxy}. \end{aligned}$$

For the point $P = (x_1, y_1)$, the slope could be describe as

$$\lambda_p = \frac{af + 2ax_1y_1 + ay_1^2 - 2bx_1y_1 - by_1^2}{bg - ax_1^2 + bx_1^2 - 2ax_1y_1 + 2bx_1y_1} = \frac{af + (a-b)y_1\,(2x_1 + y_1)}{bg - (a-b)x_1\,(x_1 + 2y_1)}.$$

Let

$$A_1 = afx_1 + \left(2af + bg + (a-b)x_1^2\right) y_1,\ A_2 = 3(a-b)x_1y_1^2 + 2(a-b)y_1^3,$$
$$A_3 = (bg - (a-b)x_1\,(x_1 + 2y_1))$$

and

$$B_1 = (af + (a-b)y_1\,(2x_1 + y_1)),\ B_2 = 2(-a+b)x_1^3 + bgy_1 + 3(-a+b)x_1^2y_1,$$
$$B_3 = x_1\left(af + 2bg + (-a+b)y_1^2\right).$$

We claim that

$$x_2 = -\frac{A_3\,(A_1 + A_2)}{\left(af + bg + (-a+b)x_1^2 + (a-b)y_1^2\right)\left(af + (a-b)y_1\,(2x_1 + y_1)\right)} \tag{4.8}$$

and

$$y_2 = -\frac{B_1\,(B_2 + B_3)}{\left(af + bg + (-a+b)x_1^2 + (a-b)y_1^2\right)\left(bg - (a-b)x_1\,(x_1 + 2y_1)\right)} \tag{4.9}$$

are the second coordinates of the point of intersection for the tangent line at P.

The claim could be proven simply by checking the slope given by

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

and by simplification, the slope could be obtain as

$$\lambda \;=\; \frac{af + (a-b)y_1\,(2x_1 + y_1)}{bg - (a-b)x_1\,(x_1 + 2y_1)}$$

which have the same slope as λ_p.

4.3 Projective Coordinates Formulae

Let $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, and $Z = 1$ [16, 36], then the affine coordinate of equation (4.1), becomes

$$a\frac{X}{Z}\left(\frac{Y^2}{Z^2}+\frac{XY}{Z^2}+f\right) \;=\; b\frac{Y}{Z}\left(\frac{X^2}{Z^2}+\frac{XY}{Z^2}+g\right).$$

Finally, multiplying by Z^3 on both the sides to get rid of denominators and achieve the projective form of the curve equation

$$E(\mathbb{K}) : aX\left(Y^2+XY+fZ^2\right) = bY\left(X^2+XY+gZ^2\right), \tag{4.10}$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$.

For the points $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$, the third point of intersection known as $R = (U_3, V_3, W_3)$ of the line joining P and Q has the coordinates as follow:

$$\begin{aligned}
U_3 =&(X_2Z_1 - X_1Z_2)^2(Y_2Z_1^2(X_2+Y_2) - Y_1Z_2^2(X_1+Y_1)),\\
V_3 =&(Y_2Z_1 - Y_1Z_2)^2(X_2Z_1^2(X_2+Y_2) - X_1Z_2^2(X_1+Y_1)),\\
W_3 =&- Z_1Z_2(X_2Z_1 - X_1Z_2)(Y_2Z_1 - Y_1Z_2)(Z_1(X_2+Y_2) - Z_2(X+Y_1)).
\end{aligned} \tag{4.11}$$

For doubling points, the coordinates are as follows:

$$\begin{aligned}
U_2 \;=\;& -(X_1(a-b)(X+2Y_1) - bgZ_1^2)^2\\
&(Y_1(a-b)(X_1+Y_1)(X_1+2Y_1) + Z_1^2(afX_1 + (2af+bg)Y_1)),\\
V_2 \;=\;& -(Y_1(a-b)(2X_1+Y_1) + afZ_1^2)^2\\
&(-X_1(a-b)(X_1+Y_1)(2X_1+Y_1) + Z_1^2(X_1(af+2bg) + bgX_1)),\\
W_2 \;=\;& Z_1(Y_1(a-b)(2X_1+Y_1) + afZ_1^2)(-X_1(a-b)(X_1+2Y_1) + bgZ_1^2)\\
&(-(a-b)(X_1^2 - Y_1^2) + (af+bg)Z_1^2).
\end{aligned} \tag{4.12}$$

Theorem 4.4. *Let $\mathbb{K}$ be a finite field of char($\mathbb{K}$) $\neq 2$. Let $P_1 = (X_1, Y_1, Z_1)$ and $P_2 = (X_2, Y_2, Z_2)$ be two points on the elliptic curve defined by equation (4.10). Then, the addition formula given by equation (4.8) is valid provided that $X_1Z_2 \neq X_2Z_1$, $Y_1Z_2 \neq Y_2Z_1$, and $X_1Z_2 + Y_1Z_2 \neq X_2Z_1 + Y_2Z_1$.*

Proof. Let P_1 and P_2 be finite points, then $P_1 = (x_1, y_1)$, and $P_2 = (x_2, y_2)$, where $(x_1, y_1) \neq (0, 0)$ and $(x_2, y_2) \neq (0, 0)$. The point addition given by the equations (4.5) and (4.6) is only valid if $x_1 \neq x_2$, $y_1 \neq y_2$ and $x_1 - x_2 + y_1 - y_2 \neq 0$, which translate to projective coordinates as $X_1Z_2 \neq X_2Z_1$, $Y_1Z_2 \neq Y_2Z_1$, and $X_1Z_2 + Y_1Z_2 \neq X_2Z_1 + Y_2Z_1$, respectively.

It remains to analyze that the condition is satisfied at the infinity points. The points at infinity are $(1 : 0 : 0)$, $(0 : 1 : 0)$, and $(a, b, 0)$, if P_1 or $P_2 \in \{(1 : 0 : 0), (0 : 1 : 0)\}$; then $X_1Z_2 \neq X_2Z_1$, $Y_1Z_2 \neq Y_2Z_1$, and $X_1Z_2 + Y_1Z_2 \neq X_2Z_1 + Y_2Z_1$ is not satisfied. Since $P_1 \notin \{O, (1 : 0 : 0), (0 : 1 : 0)\}$, then the addition law is valid for $P_2 = (a : b : 0)$ as mentioned earlier. □

4.3.0.1 Computational Cost Analysis on Projective Coordinates

We evaluate the efficiency of point addition and doubling point on the curve $E(\mathbb{K})$. The computational cost ratio between a square (s) and multiplication (m) is typically $s = 0.8m$. Other operations such as addition/subraction (a) and (d) are omitted as computation cost is lower for these operations.

Projective coordinates may be preferred for faster arithmetic than the affine formula. The affine formulae are given by equations (4.5) and (4.6) for the addition of two different points on $E(\mathbb{K})$ is described by equation (4.10).

The cost of a multiplication be m and the cost of a square be s in the field $\mathbb{K}$. Then, following is achieved,

$$m_1 = X_1Z_2,\ m_2 = X_2Z_1,\ m_3 = Y_1Z_2,\ m_4 = Y_2Z_1,$$

$$m_5 = m_4(m_2 + m_4),\ m_6 = m_3(m_1 + m_3),\ m_7 = m_2(m_2 + m_4),$$
$$m_8 = m_1(m_1 + m_3),\ m_9 = -Z_1Z_2,$$

$$s_1 = (m_2 - m_1)^2,\ s_2 = (m_4 - m_3)^2, \text{and}$$

$$U_3 = s_1(m_5 - m_6),\ V_3 = s_2(m_7 - m_8),$$
$$W_3 = m_9(m_2 - m_1)(m_4 - m_3)(m_2 + m_4 - m_1 - m_3).$$

Therefore, the total cost of point addition on the curve $E(\mathbb{K})$ is $14m + 2s$.

For the doubling point as described by equation (4.5), we have

$$s_1 = Z_1^2,\ s_2 = X_1^2,\ s_3 = Y_1^2,$$

$$m_1 = X_1(a-b)(X_1+2Y_1),\ m_2 = (X_1+Y_1)(X_1+2Y_1),$$
$$m_3 = s_1(afX_1 + Y_1(2af+bg)),\ m_4 = (a-b)Y_1m_2,\ m_5 = Y_1(a-b)(2X_1+Y_1)$$

$$m_6 = (X_1+Y_1)(2X_1+Y_1),\ m_7 = s_1((af+2bg)X_1 + bgY_1),$$
$$m_8 = -X_1m_6(a-b),\ m_9 = (m_5+afs_1)((a-b)(s_2+s_3) + s_1(af+bg))$$

$$U_2 = -(m_1 - bgs_1)^2(m_3+m_4),\ V_2 = -(m_5+afs_1)^2(m_7+m_8), \text{ and}$$

$$W_2 = -m_1m_9Z_1.$$

Therefore, the total cost of doubling points on the curve $E(\mathbb{K})$ is $13m + 5s$.

4.4 Jacobian Coordinates Formulae

Let $x = \frac{X}{Z^2}$, $y = \frac{Y}{Z^3}$, and $Z = 1$ [16, 36]. Then the affine coordinate of equation (4.1), after simplification becomes,

$$E(\mathbb{K}):\ aX(Y^2 + XYZ + fZ^6) = bY(XZ^2 + XYZ + gZ^6), \tag{4.13}$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$.

For the points $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$, the third point of intersection known as $R = (U_3, V_3, W_3)$ of the line joining P and Q has the coordinates as follow:

$$\begin{aligned}
U_3 &= -Z_1Z_2(X_2Z_1^2 - X_1Z_2^2)^2(Y_2^2Z_1^6 + X_2Y_2Z_1^6Z_2 - Y_1Z_2^6(Y_1 + X_1Z_1)),\\
V_3 &= -(Y_2Z_1^3 - Y_1Z_2^3)^2(X_2Y_2Z_1^5 + X_2^2Z_1^5Z_2 - X_1Z_2^5(Y_1 + X_1Z_1)),\\
W_3 &= Z_1^2Z_2^2\left((Y_2Z_1^3 - Y_1Z_2^3)\right)\\
&\quad (X_2Z_1^3Z_2 - X_1Z_1Z_2^3)(Y_2Z_1^3 + X_2Z_1^3Z_2 - Z_2^3(Y_1 + X_1Z_1)). \qquad (4.14)
\end{aligned}$$

For doubling points, the coordinates are as follows:

$$\begin{aligned}
U_2 &= -Z_1\left((2X_1Y_1(-a+b) + (-a+b)X_1^2Z_1 + bgZ_1^5)\right)^2\\
&\quad (2(a-b)Y_1^3 + 3(a-b)X_1Y_1^2Z_1 + afX_1Z_1^7\\
&\quad +Y_1Z_1^2((a-b)X_1^2 + (2af+bg)Z_1^4)),\\
V_2 &= -((a-b)Y_1^2 + 2(a-b)X_1Y_1Z_1 + afZ_1^6)^2\\
&\quad (3(-a+b)X_1^2Y_1Z_1 + 2(-a+b)X_1^3Z_1^2 +\\
&\quad bgY_1Z_1^5 + X_1((-a+b)Y_1^2 + (af+2bg)Z_1^6)),\\
W_2 &= Z_1^3(2(-a+b)X_1Y_1 + (-a+b)X_1^2Z_1 + bgZ_1^5)\\
&\quad ((a-b)Y_1^2 + 2(a-b)X_1Y_1Z_1 + afZ_1^6)\\
&\quad \left((a-b)Y_1^2 + (-a+b)X_1^2Z_1^2 + (af+bg)Z_1^6\right). \qquad (4.15)
\end{aligned}$$

The costs of point addition and doubling points on the curve $E(\mathbb{K})$ are $32m + 4s$ and $29m + 5s$, respectively.

4.5 Lopez-Dahab Coordinates Formuale

Let $x = \frac{X}{Z}$, $y = \frac{Y}{Z^2}$, and $Z = 1$ [16, 36]. Then the affine coordinate of equation (4.1) becomes

$$E(\mathbb{K}) : aX(Y^2 + XYZ + fZ^5) = bY(XZ^2 + XY + gZ^6), \qquad (4.16)$$

where $a, b, f, g \in \mathbb{K}$ and $abfg(a-b) \neq 0$.

For the points $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$, the third point of intersection known as $R = (U_3, V_3, W_3)$ of the line joining P and Q has the coordinates as follow:

$$\begin{aligned}
U_3 &= -Z_1Z_2(X_2Z_1 - X_1Z_2)^2(Y_2^2Z_1^4 + X_2Y_2Z_1^4Z_2 - Y_1Z_2^4(Y_1 + X_1Z_1)),\\
V_3 &= -\Big((Y_2Z_1^2 - Y_1Z_2^2)\Big)^2(X_2Y_2Z_1^3 + X_2^2Z_1^3Z_2 - X_1Z_2^3(Y_1 + X_1Z_1)), \text{ and}\\
W_3 &= Z_1^2Z_2^2(X_2Z_1 - X_1Z_2)(Y_2Z_1^2 - Y_1Z_2^2)\\
&\quad (Y_2Z_1^2 + Z_2(X_2Z_1^2 - Z_2(Y_1 + X_1Z_1))).
\end{aligned} \tag{4.17}$$

For doubling points, the coordinates are as follow:

$$\begin{aligned}
U_2 &= -Z_1(2(-a+b)X_1Y_1 + (-a+b)X_1^2Z_1 + bgZ_1^3)^2\\
&\quad (2(a-b)Y_1^3 + 3(a-b)X_1Y_1^2Z_1 + afX_1Z_1^5\\
&\quad + Y_1Z_1^2((a-b)X_1^2 + (2af+bg)Z_1^2)),\\
V_2 &= -((a-b)Y_1^2 + 2(a-b)X_1Y_1Z_1 + afZ_1^4)^2\\
&\quad (3(-a+b)X_1^2Y_1Z_1 + 2(-a+b)X_1^3Z_1^2 + bgY_1Z_1^3 +\\
&\quad X_1((-a+b)Y_1^2 + (af+2bg)Z_1^4)), \text{and}\\
W_2 &= Z_1^2(2(-a+b)X_1Y_1 + (-a+b)X_1^2Z_1 + bgZ_1^3)\\
&\quad ((a-b)Y_1^2 + 2(a-b)X_1Y_1Z_1 + afZ_1^4)\\
&\quad ((a-b)Y_1^2 + (-a+b)X_1^2Y_1^2 + (af+bg)Z_1^4).
\end{aligned} \tag{4.18}$$

The costs of point addition and doubling point on the curve $E(\mathbb{K})$ are $32m + 6s$ and $26m + 5s$, respectively.

4.6 Embedding of Huff's Model of Elliptic Curves into $\mathbb{P}^1 \times \mathbb{P}^1$

It is noted that computational cost is higher while using projective, Jocobian or Lopez-Dahab. Thus changing the form of the curve could yield a better result.

Theorem 4.5. *The elliptic curve* $E(\mathbb{K}) : ax(y^2 + xy + f = by(x^2 + xy + g)$ *could be written as* $E(\mathbb{K}) : x(y^2 - c) = y(x^2 - d)$, *where* $c = \dfrac{-af}{a-b}$ *and* $d = \dfrac{bg}{a-b}$.

Proof. First note that $E(\mathbb{K}) : ax(y^2 + xy + f = by(x^2 + xy + g)$ has

$$\begin{aligned} axy^2 + ax^2y + afx - bx^2y - bxy^2 - bgy &= 0, \\ axy^2 - bxy^2 + afx + ax^2y - bxy^2 - bgy &= 0, \\ x(ay^2 - by^2 + af) + y(ax^2 - bx^2 - bg) &= 0\,, \text{and} \\ x((a-b)y^2 + af) - y(-x^2(a-b) + bg) &= 0. \end{aligned}$$

Finally, by scaling the equations by $a - b$ since $a - b \neq 0$. Then $E(\mathbb{K})$ has the following forms,

$$\begin{aligned} \frac{x((a-b)y^2 + af)}{a-b} - \frac{y(-x^2(a-b) + bg)}{a-b} &= 0, \\ x\left(y^2 + \frac{af}{a-b}\right) - y\left(-x^2 + \frac{bg}{a-b}\right) &= 0. \end{aligned}$$

Let $c = \dfrac{-af}{a-b}$ and $d = \dfrac{bg}{a-b}$ then the equation could be simplify as follows,

$$xy^2 - cx - yx^2 + yd = 0$$

and finally,

$$E(\mathbb{K}) : x(y^2 - c) = y(x^2 - d).$$

□

Note that the elliptic curve given by $E(\mathbb{K}) : ax(y^2 - c) = by(x^2 - d)$ is a generalized Huff's elliptic curve by Ciss and Sow [11].

4.6.1 Efficiency of Elliptic Curve $E(\mathbb{K}) : x(y^2 - c) = y(x^2 - d)$

According to Ciss and Sow [11], their model of Huff's elliptic curve is

$$E(\mathbb{K}) : ax(y^2 - c) = by(x^2 - d), \tag{4.19}$$

where $abcd(a^2c - b^2d) \neq 0$. It is evident that the proposed curve given by equation (4.18) has unified formulas for point addition and doubling point. The model by Ciss and Sow has unified formulas for point addition and doubling point. According to Ciss and Sow [11], the point addition on the curve is given by equation (4.19) and the doubling point is given by equation (4.20).

$$(x_1, y_1) + (x_2, y_2) = \begin{cases} x_3 = \dfrac{d(x_1 + x_2)(c + y_1y_2)}{(d + x_1x_2)(c - y_1y_2)}, \\ y_3 = \dfrac{c(y_1 + y_2)(d + x_1x_2)}{(c + y_1y_2)(d - x_1x_2)}. \end{cases} \tag{4.20}$$

$$[2](x_1, y_1) = \begin{cases} x_3 = \dfrac{2dx_1(c + y_1^2)}{(d + x_1^2)(c - y_1^2)}, \\ y_3 = \dfrac{2cy_1(d + x_1^2)}{(c + y_1^2)(d - x_1^2)}. \end{cases} \tag{4.21}$$

As shown by Ciss and Sow in [11] the total cost of point addition and doubling point is 12m+4d and 7m+5s+4d. The same results will be there for the proposed curve since point addition, and doubling point formulas do not include curve constant $'a'$ and $'b'$.

4.6.2 Embedding of $E(\mathbb{K}) : ax(y^2 - c) = by(x^2 - d)$ into $\mathbb{P}^1 \times \mathbb{P}^1$

The projective closure of elliptic curve defined by equation (4.1) in $\mathbb{P}^1 \times \mathbb{P}^1$ is given by

$$E(\mathbb{K}) = \{(X : Z), (Y : T) \in \mathbb{P}^1 \times \mathbb{P}^1 : aXZ(Y^2 - cT^2) = bTY(X^2 - dZ^2)\}. \tag{4.22}$$

The formula for point addition and doubling point then corresponds to the following:

$$((X_1 : Z_1), (Y_1 : T_1)) + ((X_2 : Z), (Y_2 : T_2)) =$$

$$\begin{aligned}\{&(d(XZ_1 + X_1Z_2)(cT_1T_2 + Y_1Y_2) : (cT_1T_2 - Y_1Y_2)(dZ_1Z_2 + X_1X_2)),\\ &(c(T_2Y_1 + T_1Y_2)(dZ_1Z_2 + X_1X_2) : (cT_1T_2 + Y_1Y_2)(X_1X_2 - dZ_1Z_2))\}.\end{aligned} \tag{4.23}$$

$$[2]((X_1 : Z_1), (Y_1 : T_1)) =$$

$$\begin{aligned}\{&(2dX_1Z_1(cT_1^2 + Y_1^2) : (cT_1^2 - Y_1^2)(dZ_1^2 + X_1^2)),\\ &(2cT_1Y_1(dZ_1^2 + X_1^2) : -(cT_1^2 + Y_1^2)(X_1^2 - dZ_1^2))\}.\end{aligned} \tag{4.24}$$

Cost for Point Addition

$$\begin{aligned}m_1 = X_1X_2,\ m_2 = dZ_1Z_2,\ m_3 = cT_1T_2,\ m_4 = Y_1Y_2,\\ m_5 = T_1Y_2,\ m_6 = X_2Z_1,\ m_7 = X_1Z_2,\ m_8 = T_2Y_1,\end{aligned}$$

$$\begin{aligned}X_3 &= d(XZ_1 + X_1Z_2)(cT_1T_2 + Y_1Y_2) = d(m_3 + m_4)(m_6 + m_7),\\ Z_3 &= cT_1T_2 - Y_1Y_2)(dZ_1Z_2 + X_1X_2) = (m_3 - m_4)(m_1 + m_2),\\ Y_3 &= c(T_2Y_1 + T_1Y_2)(dZ_1Z_2 + X_1X_2) = c(m_8 - m_5)(m_6 + m_7),\\ T_3 &= cT_1T_2 + Y_1Y_2)(X_1X_2 - dZ_1Z_2) = -(m_3 + m_4)(m_1 - m_2).\end{aligned} \tag{4.25}$$

The total cost is $12m + 6a + 4d$ which is same as using projective coordinates.

Cost for Doubling Point

$$s_1 = X_1^2,\ s_2 = Y_1^2,\ s_3 = T_1^2,\ s_4 = Z_1^2,$$

$$\begin{aligned}
X_3 &= 2dX_1Z_1(cT_1^2 + Y_1^2) = 2dX_1Z_1(cs_3 + s_2),\\
Z_3 &= (cT_1^2 - Y_1^2)(dZ_1^2 + X_1^2) = (cs_3 - s_2)(s_1 + ds_4),\\
Y_3 &= 2cT_1Y_1(dZ_1^2 + X_1^2) = 2cT_1Y_1(s_1 + ds_4), \text{and}\\
T_3 &= -(cT_1^2 + Y_1^2)(X_1^2 - dZ_1^2) = -(cs_3 + s_2)(s_1 - ds_4). \qquad (4.26)
\end{aligned}$$

The total cost comes to $6m + 4s + 4a + 4d$, which is less than the cost given by Ciss and Sow and other coordinate systems. Using embedding of $E(\mathbb{K})$: $ax(y^2 - c) = by(x^2 - d)$ into $\mathbb{P}^1 \times \mathbb{P}^1$ and $c = \dfrac{-af}{a-b}$ and $d = \dfrac{bg}{a-b}$ have improved the proposed elliptic curves computational cost. One can notice that the curve described by Ciss and Sow has higher cost when computing $2P$ then found by embedding $E(\mathbb{K})$ into $\mathbb{P}^1 \times \mathbb{P}^1$.

4.7 Rational Points on $E(\mathbb{F}_q)$

The new form of Huff's model of elliptic curves is defined as

$$E(\mathbb{F}_q) : ax\left(y^2 + xy + f\right) = by\left(x^2 + xy + g\right), \qquad (4.27)$$

where $a, b, f, g \in \mathbb{F}_q$ and $abfg(a - b) \neq 0$ by replacing the field $\mathbb{K}$ by $\mathbb{F}_q$, where q is a prime in the equation (4.1). Observe that for each x, the curve (4.24) yields at most two values for y; and the point of infinity $(0, 0)$ is always on the curve $E(\mathbb{F}_q)$. Thus, an upper bound could be set for the number of rationals on $E(\mathbb{F}_q)$ as

$$\#E(\mathbb{F}_q) \leq 2q + 1.$$

However, computing the exact number of points on the curve $E(\mathbb{F}_q)$ is a challenge to us. However, Hasse's Theorem [18] on elliptic curve $E(\mathbb{F}_q)$ provides an estimate for the number of rational points over a finite field $\mathbb{F}_q$ as

$$| \#E(\mathbb{F}_q) - (q+1) | \leq 2\sqrt{q}.$$

For the understanding purpose, let's discuss the following method:

The curve (4.24) can be written be as

$$E(\mathbb{F}_q) : afx + \left(-bg + ax^2 - bx^2\right) y + (ax - bx)y^2 = 0. \tag{4.28}$$

This may be seen as a quadratic equation in y. The discriminant of (4.27) can be calculated by

$$\Delta = -4afx(ax - bx) + \left(-bg + ax^2 - bx^2\right)^2 \tag{4.29}$$

and y can be rational if and only if $\Delta = r^2$ for some rational r. In this senario, one can easily find some points on the curve (4.24) by simply assigning values of a, f, and g and solving for b. The following toy example shows how one can obtain y coordinates and compute point addition and doubling point.

Example 4.6. Let $q = 11$. Then use fixed values; $a = 1$, $f = 1$, $x = 1$, and $g = -1$ and substitute in the curve equation (4.24). Then the discriminant of (4.24) becomes

$$\begin{aligned} r^2 &= -4a(ax - bx) + (-bg + ax^2 - bx^2)^2 \\ r^2 &= -4(1 - b) + 1 \\ r^2 &= 4b - 3. \end{aligned} \tag{4.30}$$

Note that $4b-3$ must be a rational square to obtain rational points on the elliptic curve. When $r=1$, the equation (4.27) gives $b=1$ but this value is omitted due to the initial condition $abfg(a-b)\neq 0$ of the elliptic curve $E(\mathbb{F}_{11})$. When $r=2$, the equation (4.27) gives $b=3$. Now the curve equation (4.24) becomes $E(\mathbb{F}_{11}):\ x\left(y^2+xy+1\right)=3y\left(x^2+xy-1\right)$. It is easy to check that

$$\begin{aligned}E(\mathbb{F}_{11})=&\{\mathcal{O},(0,1),(1,0),(1,1),(1,5),(3,7),(4,1),(4,5),(5,7),(6,4),\\&(7,6),(7,10),(8,4),(10,1),(10,6),(10,10)\},\end{aligned}$$

so, $\#E(\mathbb{F}_{11})=16$. Since $P=(1,1)\in E(\mathbb{F}_{11})$ and $Q=(10,10)\in E(\mathbb{F}_{11})$, one can easily compute doubling point $2P=(8,4)$ and $2Q=(3,7)$ and point addition of the point $P+2Q=(10,6)$ and $2P+Q=(1,5)$ on the curve $E(\mathbb{F}_{11})$ by using the equations (4.5), (4.6), (4.7), and (4.8).

Lemma 4.7. *If (x,y) is a rational point on*

$$E(\mathbb{K}):ax\left(y^2+xy+f\right)-by\left(x^2+xy+g\right)=0$$

and $x\neq 0$, $y\neq 0$, then $(-x,-y)$ is also a rational point on $E(\mathbb{K})$.

Proof. It is clear that if (x,y) is rational, then $(-x,-y)$ is also rational. All one has to do is to show that $(-x,-y)$ is also on $E(\mathbb{K})$. Substituting $(-x,-y)$ in $E(\mathbb{K})$ gives the following.

$$\begin{aligned}a(-x)\left((-y)^2+(-x)(-y)+f\right)-b(-y)\left((-x)^2+(-x)(-y)+g\right)&=0\\-ax\left(y^2+xy+f\right)+by\left(x^2+xy+g\right)&=0\\E(\mathbb{K}):\ ax\left(y^2+xy+f\right)-by\left(x^2+xy+g\right)&=0\end{aligned}$$

Thus, $(-x,-y)$ is also rational point on $E(\mathbb{K})$. □

4.8 Computational Cost Analysis

Each coordinate system cost is summarized in the Table 1 for point addition and doubling point on standard coordinates for the elliptic curve (4.1).

Table 1: Computational cost comparison

Coordinates	Cost	
	Addition	Doubling
Projective	$14m + 2s$	$13m + 5s$
Jacobian	$32m + 4s$	$29m + 5s$
Lopez-Dahab	$32m + 6s$	$26m + 5s$
Embedding $E(\mathbb{K})$ into $\mathbb{P}^1 \times \mathbb{P}^1$	$12m$	$6m + 4s$

Note that the computational cost using the embedding $E(\mathbb{K})$ into $\mathbb{P}^1 \times \mathbb{P}^1$ is lower than the projective, Jacobian, and Lopez-Dahab coordinate systems. Thus, it is recommend to proceed with embedding of $E(\mathbb{K})$ into $\mathbb{P}^1 \times \mathbb{P}^1$ system as the cost is lower for point addition and doubling point on this curve.

To compare our results with other Huff's models, extra operations as a to be addition/subtraction of curve constants and d as multiplication by curve constants is taken.

Table 2: Computational cost comparison of other forms of Huff's curve

Source and the curve equation	Addition	Doubling
Wu, Feng [39] plus assuming b=1, $X(aY^2 - Z^2) = Y(X^2 - Z^2)$	11m+d+14a	6m+5s+d+12a
Joye, Tibouchi, Vergnaud [24], $aX(Y^2 - Z^2) = bY(X^2 - Z^2)$	6m+5s+13a	11m+14a
Orhon and Hisil [32], $YT(Z^2 + 2X^2) = cXZ(T^2 + 2Y^2)$	10m+14a	8m+10a
Orhon and Hisil [32], $YT(Z^2 + X^2) = cXZ(T^2 + 2Y)$	10m+12a	8m+8a
This work using projective coordinate, $aX(Y + XY + fZ^2) = bY(X^2 + XY + gZ^2)$	14m+2s+2d+12a	13m+5s+2d+3a
This work by embedding $aXZ(Y^2 - cT^2) = bTY(X^2 - dZ^2)$ into $\mathbb{P}^1 \times \mathbb{P}^1$	12m+6a+4d	6m+4s+4a+4d

Note that the computational cost on the curve described in this chapter is almost equivalent to other known Huff's model of elliptic curves [See in Table 2] by embedding the curve into $\mathbb{P}^1 \times \mathbb{P}^1$. The results shown by Ciss and Sow on their curves [11] could be improved from $7m + 5s + 4a + 4d$ to $6m + 4s + 4a + 4d$ for the doubling point by embedding the curve into $\mathbb{P}^1 \times \mathbb{P}^1$.

Chapter 5

Birational Equivalence to Weierstrass Form of Elliptic Curves

When two curves E_1 and E_2 are isomorphic, they are said to be "same." Another approach to equate things is to remark that they are "nearly identical." This chapter shows that the generalized Huff's model of an elliptic curve is birationally equivalent (nearly identical) to the Weierstrass form of elliptic curves. This chapter first look at birational equivalence of Huff's curves to Weierstrass curves in the literature provided by [21, 24], and then show how to achieve birational equivalence of our model of Huff's curve to Weierstrass curves.

5.1 Birational Equivalence of Huff's Curve to Weierstrass Curve

The affine Huff's curve defined by $E(\mathbb{K})_H : ax(y^2-1) = by(x^2-1)$ in [24] could be extended to a binary field as $E(\mathbb{K}) : ax(y^2+y+1) = by(x^2+x+1)$. The birationally equivalent to Weierstrass curve was found to be

$$v(v+(a+b)u = u(u+a^2)(u+b^2).$$

The inverse map are as

$$(x,y) = \left(\frac{b(u+a^2)}{v}, \frac{a(u+b^2)}{v+(a+b)u}\right) \text{ and } (u,v) = \left(\frac{ab}{x}, \frac{ab(axy+b)}{x^2y}\right)$$

with the neutral element as $O = (0, 0)$. The method of achieving the above results was not discussed in detail [24].

In 1928, Nagell proposed a simpler procedure to construct birational equivalence in the specific case of plane curves. Nagell's method failed in even characteristics. In [37], the author describes how Nagell's method [31] could be modified to suit any characteristics. One can visit chapter 8 of [22] for the details of Nagell's algorithm.

5.1.1 Nagell's Algorithm

Let E be a smooth curve defined by affine formulae, for some field $\mathbb{K}$ of any characteristics. Let the O be a rational point of E which isn't an inflection point. To construct an birational equivalence of the elliptic curve from (E, O) to a Weierstrass elliptic curve of affine form as

$$E(\mathbb{K}) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x^2 + a_6,$$

and mapping O to the point at infinity $(0 : 1 : 0)$. As O is not an inflection point, the tangent at O cuts $E(\mathbb{K})$ again at second point $P \neq O$. The point at infinity on the y-axis could be regarded as $O = (0 : 1 : 0)$ and $P = (0 : 0 : 1)$ to the projective transformation of origin.

The affine equation of $E(\mathbb{K})$ could be written as $F(x, y) = 0$. The polynomial F is of a total degree of 3 and satisfies $F(0, 0) = 0$ since the origin is on $E(\mathbb{K})$. The polynomial F could be written as the following:

$$F = F_1 + F_2 + F_3, \text{ where } F_i, i \text{ is the homogeneous degree.}$$

Let $y = tx$, then the equation of $F(x, y)$ becomes

$$xF_1(1, t) + x^2F_2(1, t) + x^3F_3(1, t) = 0.$$

Multiplying the above equation by $\dfrac{F_3(1, t)}{x}$ yields,

$$x^2F_3(1,t)^2 + xF_2(1,t)F_3(1,t) = -F_1(1,t)F_3(1,t).$$

Setting $u = xF_3(1,t)$, yields

$$u^2 + F_2(1,t)u = -F_1(1,t)F_3(1,t).$$

Note that the line $x = 0$ cuts E at infinity with multiplicity 2. This implies that

$$F(0,y) = yF_1(0,1) + y^2F_2(0,1) + y^3F_3(0,1)$$

is of degree $3-2 = 1$ in y. Therefore, $F_2(0,1) = F_3(0,1) = 0$, and it follows that polynomial $F_2(1,t)$ and $F_3(1,t)$ are of degree at most 1 and 2 in t, respectively. The following equation is obtained:

$$u^2 + G_1(t)u = G_3(t)$$

with G_1 of degree at most 1 and G_3 exactly 3. The rational map then is of the following form:

$$(x,y) \to (t,u) = \left(\frac{x}{y}, \frac{F_3(x,y)}{x^2}\right)$$

and

$$(t,u) \to (x,y) = \left(\frac{u}{F_3(1,t)}, \frac{tu}{F_3(1,t)}\right).$$

The point O is sent to itself under the map, which are isogenies. One can visit [37] for more detail.

5.1.2 Birational Equivalence of a New Form of Huff's Curves to Weierstrass Form.

Theorem 5.1. *Let $E(\mathbb{K})$ be a non-singular elliptic curve defined by the affine formulae defined by equation* (4.1). *$E(\mathbb{K})$ is birational equivalence to a Weierstrass form*

of $y^2 = t^3 + a_2t^2 + a_4t + a_6$, *where* $t = x - \frac{A}{BC}$, $A = a(a-b)f(af+bg), B = (a-b)bg(2af+bg)$, *and* $C = b^3g^3$.

Proof. It is easy to see that equation (4.1) is also equivalent to

$$axy^2 + ax^2y + axf = bx^2y + bxy^2 + byg.$$

The signs of a, b, f, and g are either positive or negative and never equal to zero. The curve has $O = (0,0)$ as the point of inflection. The curve has $(0 : 1 : 0)$, the point at infinity in projective transformation. For simplicity, take $E(\mathbb{K})$ in the following form:

$$E(\mathbb{K}) : (a-b)XY^2 + (a-b)X^2Y + afXZ^2 - bgYZ^2 = 0.$$

In chapter 8 of [22] as Cassels states that an elliptic curve genus 1 with at least a rational point on the curve and Weierstrass form is enough to get the birational equivalence to curve and where $\mathcal{O}$ is a rational point on the Weierstrass curve. If the curve has an inflectional tangent at point O, then let $\mathcal{O} = (0 : 1 : 0)$. The linear transformation of co-ordinates is enough to take O to $\mathcal{O}$ and the tangent the line at infinity. Define $O = (0 : 0 : 1)$ to be an inflection point on $E(\mathbb{K})$. O is firstly mapped to curve $E(\mathbb{K})_M$.

Let

$$\psi = (X : Y : Z) \longmapsto (U : V : W) = (U : \frac{af}{bg}U + W, V).$$

Then with a little bit of help from MATHEMATICA, the following parameters are achieved:

$$\begin{aligned} A &= a(a-b)f(af+bg), \\ B &= (a-b)bg(2af+bg), \\ C &= b^3g^3 \text{, and} \\ D &= (a-b)b^2g^2. \end{aligned}$$

Then, $E(\mathbb{K})_M = AU^3 + BU^2W + DUW^2 - CV^2W = 0$ is obtained. One can note that E_M could be easily changed to the Weierstrass form. To return to Huff's elliptic curve from $E(\mathbb{K})_M$, one may apply the following map:

$$\psi^{-1} = (U : V : W) \longmapsto (X : Y : Z) = (X : Z : \frac{-af}{bg}X + Y).$$

It is noted that $(0 : 0 : 1)$ on E is mapped to $(0 : 1 : 0)$ on $E(\mathbb{K})_M$ through ψ.

To obtain the Weierstrass affine form, let

$X = x$, $V = \frac{A}{C}y$, and $Z = \frac{C}{A}$ then the equation $E(\mathbb{K})_M$ could be simplified as

$$E(\mathbb{K})_M : y^2 = x^3 + \frac{BC}{A^2}x^2 + \frac{DC^2}{A^3}x.$$

After obtaining affine equation of E_M, let $x = t + \frac{A}{BC}$ to get the following Weierstrass form equation,

$$E(\mathbb{K})_w : y^2 = t^3 + a_2t^2 + a_4t + a_6,$$

where

$$\begin{aligned} a_2 &= \frac{3A^3 + B^2C^2}{A^2BC}, \\ a_4 &= \frac{3A^5 + 2A^2B^2C^2 + B^2C^4D}{A^3B^2C^2}, \text{and} \\ a_6 &= \frac{A^5 + A^2B^2C^2 + B^2C^4D}{A^2B^3C^3}. \end{aligned}$$

□

Chapter 6

Conclusion and Further Work

When compared to the previous several decades, technological advancements have been significant. Communicating over the internet, and ideally utilizing any device, is a common part of everyday life. As a result, the internet is one of the most widely used platforms for sharing knowledge with people all over the globe. Some material, on the other hand, is classified, and the transmission may be hazardous if it is intercepted by an unwelcome party. Consequently, encryption has become more important in our lives as a means of protecting information sent via the internet.

At the outset of this thesis, we addressed the theoretical foundations of public-key cryptography, which included the discrete logarithm issue and the elliptic curve discrete logarithmic problem over a finite field, respectively. When using public-key encryption, it is thought that obtaining the decryption key in a reasonable amount of time is virtually difficult. Public-key cryptography is based on the use of elliptic curves, which are very useful. Elliptic curves are capable of being utilized in cryptography. The selection of an elliptic curve is dictated by the purpose for which it is to be used. The majority of the time, the decision is made for the sake of speeding up the calculation of point addition and doubling point. While there are certain single curves and anomalous elliptic curves that should not be used for cryptography, there are others that should not be utilized because algorithms can solve the elliptic curve discrete logarithm issue on these curves.

This thesis has introduced a new form of elliptic curves in generalized Huff's model. Formulae for point addition and doubling on the affine, projective, Jacobian, Lopez-Dahab coordinates, and embedding of the curve into $\mathbb{P}^1 \times \mathbb{P}^1$

system is presented. It is observed that the computational cost for point addition and doubling point on the new form of Huff's model of elliptic curves is lowest by embedding the curve into $\mathbb{P}^1 \times \mathbb{P}^1$ system than other mentioned coordinate systems. The results shown by Ciss and Sow in Ciss and Sow [11]on their curves have been improved from $7m + 5s + 4a + 4d$ to $6m + 4s + 4a + 4d$ for the doubling point by embedding the curves into $\mathbb{P}^1 \times \mathbb{P}^1$ system. The computational cost of the contributed curve is nearly optimal to other known Huff's models.

Despite the fact that the Huff's curves does not become the quickest curve model, the efficiency gain of the Huff curve itself may be very significant. In comparison to a classical computer, a quantum computer is much quicker, and if this is taken into consideration, the Huff's curve may be an option in the near future. In this way, the results may be significant and represent a new field of investigation. future work is required to compare computational cost with other Huff's, Weierstrass, Montgomery, and Edwards curves. Furthermore, the study could be extended to supersingular elliptic curves and isogeny-based cryptography.

References

1. Adhikari, M. R. and Adhikari, A., 2014. *Basic modern algebra with applications*. Springer. 7

2. Bauer, C. P., 2016. *Secret history: The story of cryptology*. Chapman and Hall/CRC. 7

3. Bernstein, D. J.; Birkner, P.; Joye, M.; Lange, T.; and Peters, C., 2008. Twisted Edwards curves. In *International Conference on Cryptology in Africa*, 389–405. Springer. 19

4. Bernstein, D. J.; Chuengsatiansup, C.; Kohel, D.; and Lange, T., 2015. Twisted Hessian curves. In *International Conference on Cryptology and Information Security in Latin America*, 269–294. Springer. 3, 19

5. Bernstein, D. J. and Lange, T., 2007. Analysis and optimization of elliptic-curve single-scalar multiplication. http://eprint.iacr.org/2007/455. Tanja@hyperelliptic.org 13854 received 7 Dec 2007. 19

6. Bernstein, D. J. and Lange, T., 2017. Montgomery curves and the montgomery ladder. Cryptology ePrint Archive, Report 2017/293. https://eprint.iacr.org/2017/293. 19

7. Bernstein, D. J.; Lange, T.; and Farashahi, R. R., 2008. Binary Edwards curves. In *International Workshop on Cryptographic Hardware and Embedded Systems*, 244–265. Springer. 19

8. Billet, O. and Joye, M., 2003. The Jacobi model of an elliptic curve and side-channel analysis. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, 34–42. Springer Berlin Heidelberg, Berlin, Heidelberg. 3, 19

9. Bos, J.; Costello, C.; Longa, P.; and Naehrig, M., 2014. Specification of curve selection and supported curve parameters in MSR ECCLib. Technical report, Technical Report MSR-TR-2014-92, Microsoft Research. 3

10. Bos, J. W.; Costello, C.; Longa, P.; and Naehrig, M., 2016. Selecting elliptic curves for cryptography: An efficiency and security analysis. *Journal of Cryptographic Engineering*, 6, 4 (2016), 259–286. 3

11. Ciss, A. A. and Sow, D., 2011. On a new generalization of Huff curves. *IACR Cryptology ePrint Archive*, 2011 (2011), 580. 21, 23, 43, 49, 58

12. Devigne, J. and Joye, M., 2011. Binary Huff curves. In *Cryptographers Track at the RSA Conference*, 340–355. Springer. 21

13. Diffie, W. and Hellman, M., 1976. New directions in cryptography. *IEEE Transactions on Information Theory*, 22, 6 (Nov. 1976), 644–654. doi: 10.1109/TIT.1976.1055638. 1, 2, 7, 8, 9

14. Doche, C.; Icart, T.; and Kohel, D. R., 2006. Efficient scalar multiplication by isogeny decompositions. In *Public Key Cryptography - PKC 2006*, Lecture Notes in Computer Science, 191–206. Springer, Berlin, Heidelberg. doi:10.1007/11745853_13. 19

15. Edwards, H., 2007. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44, 3 (2007), 393–422. 3, 19

16. Galbraith, S. D., 2012. *Mathematics of public key cryptography*. Cambridge University Press. 1, 36, 39, 40

17. Gallagher, P., 2013. Digital signature standard (dss). *Federal Information Processing Standards Publications, volume FIPS*, (2013), 186–3. 3

18. Hasse, H., 1936. Zur theorie der abstrakten elliptischen funktionenkrper iii. die struktur des meromorphismenrings. die riemannsche vermutung. *Journal fr die reine und angewandte Mathematik*, 175 (1936), 193–208. http://eudml.org/doc/149968. 46

19. He, X.; Yu, W.; and Wang, K., 2015. Hashing into generalized Huff curves. In *International Conference on Information Security and Cryptology*, 22–44. Springer. 21

20. Hoffstein, J.; Pipher, J.; Silverman, J. H.; and Silverman, J. H., 2008. *An introduction to mathematical cryptography*, vol. 1. Springer. 3, 7, 8, 9, 10, 14

21. Huff, G. B., 1948. Diophantine problems in geometry and elliptic ternary forms. *Duke Mathematical Journal*, 15, 2 (1948), 443–453. 19, 21, 51

22. Jackson, T., 1995. Lectures on elliptic curves, london mathematical society student texts 24, by jws cassels. pp 137.£ 13-95 (paper)£ 27-95 (hard). 1991. isbn 0-521-42530-1,-41517-9.(cambridge university press). *The Mathematical Gazette*, 79, 484 (1995), 216–216. 52, 54

23. Joye, M. and Quisquater, J., 2001. Hessian elliptic curves and side-channel attacks. In *International Workshop on Cryptographic Hardware and Embedded Systems*, 402–410. Springer. 19, 21

24. Joye, M.; Tibouchi, M.; and Vergnaud, D., 2010. Huff's model for elliptic curves. In *Algorithmic Number Theory*, 234–250. Springer Berlin Heidelberg, Berlin, Heidelberg. 3, 21, 22, 23, 48, 51, 52

25. Koblitz, N., 1987. Elliptic curve cryptosystems. *Mathematics of computation*, 48, 177 (1987), 203–209. 2, 3

26. Koblitz, N. and Menezes, A. J., 2004. A survey of public-key cryptosystems. *SIAM review*, 46, 4 (2004), 599–634. 3

27. Lang, S., 1978. *Elliptic curves: Diophantine analysis*, vol. 231. Springer. 2

28. Merkle, R. C., 1978. Secure communications over insecure channels. *Communications of the ACM*, 21, 4 (1978), 294–299. 7

29. Miller, V. S., 1985. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, 417–426. Springer. 2, 3, 7

30. Montgomery, P. L., 1987. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48, 177 (1987), 243–264. 3, 19

31. Nagell, T., 1929. Sur les propriétés arithmétiques des cubiques planes du premier genre. *Acta Mathematica*, 52, 1 (Dec 1929), 93–126. doi:10.1007/BF02592681. https://doi.org/10.1007/BF02592681. 52

32. Orhon, N. G. and Hisil, H., 2018. Speeding up Huff form of elliptic curves. *Designs, Codes and Cryptography*, 86, 12 (2018), 2807–2823. 21, 23, 48

33. Peeples, W., 1954. Elliptic curves and rational distance sets. *Proceedings of the American Mathematical Society*, 5, 1 (1954), 29–33. 21

34. Rivest, R. L.; Shamir, A.; and Adleman, L., 1977. On digital signatures and public-key cryptosystems. Technical report, MASSACHUSETTS INST OF TECH CAMBRIDGE LAB FOR COMPUTER SCIENCE. 8

35. Rivest, R. L.; Shamir, A.; and Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21, 2 (1978), 120–126. 8

36. Silverman, J. H., 2009. *The arithmetic of elliptic curves*, vol. 106. Springer Science & Business Media. 1, 11, 36, 39, 40

37. Tibouchi, M., 2012. A nagell algorithm in any characteristic. In *Cryptography and Security: From Theory to Applications*, 474–479. Springer. 52, 53

38. Wiles, A., 1995. Modular elliptic curves and fermat's last theorem. *Annals of mathematics*, 141, 3 (1995), 443–551. 3

39. Wu, H. and Feng, R., 2012. Elliptic curves in Huff's model. *Wuhan University Journal of Natural Sciences*, 17, 6 (Dec 2012), 473–480. doi:10.1007/s11859-012-0873-9. https://doi.org/10.1007/s11859-012-0873-9. 21, 22, 48