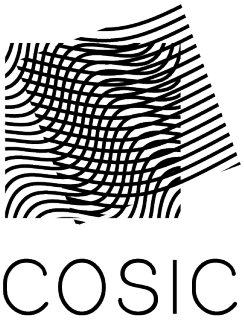
INDIAN STATISTICAL INSTITUTE (ISI), KOLKATA, INDIA
KATHOLIEKE UNIVERSITEIT (KU), LEUVEN, BELGIUM



The Monodromy Leak for a Generalized Montgomery Ladder

The thesis is submitted in partial fulfillment of the requirements for the degree of

Masters of Technology

to the

Department of Cryptology and Security Research Unit (CSRU)

By

Arani Raychaudhuri (CRS2302)

Supervisor: Dr. Wouter Castryck (KU Leuven)

Co-Supervisor: Prof. Dr. Mriganka Mandal (ISI Kolkata)

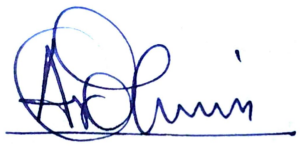
July, 2025

Declaration of Authorship

Date: 11th July, 2025

I, Mr. **Arani Raychaudhuri** (Registration No. **CRS2302**), a student of the **Department of Cryptology and Security Research Unit**, **M.Tech. in Cryptology and Security** at ISI Kolkata, hereby declare that this thesis entitled **"The Monodromy Leak for a Generalized Montgomery Ladder"** is my original work. To the best of my knowledge, it does not contain material previously published or written by any other individual, nor has it been submitted elsewhere for any degree, diploma, or academic award. I have used originality checking services to ensure the authenticity of the work and to prevent inappropriate copying. I further declare that all copyrighted materials included in this thesis comply with the Indian Copyright Act, 1957 (as amended in 2012), and that appropriate permissions have been obtained from the respective copyright holders for their use.

I hereby grant permission to the Indian Statistical Institute, Kolkata to store this thesis in a database accessible to others.

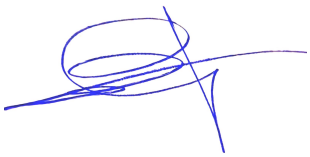


Arani Raychaudhuri
CRS2302
Department of Cryptology and Security Research Unit (CSRU)
Indian Statistical Institute, Kolkata
Kolkata 700108, West Bengal, India

Certificate from the Supervisor

Date: 11th July, 2025

This is to certify that the thesis titled **"The Monodromy Leak for a Generalized Montgomery Ladder"** submitted by **Mr. Arani Raychaudhuri**, Registration No. **CRS2302**, a student of the **Department of Cryptology and Security Research Unit** of the **M.Tech. in Cryptology and Security** program of ISI Kolkata, is based on his own research work under my supervision. I also certify, to the best of my knowledge, that neither the thesis nor any part of it has been submitted for any degree/diploma or any other academic award anywhere before. In my opinion, the thesis fulfills the requirement for the award of the degree of **Masters of Technology** in **Cryptology and Security**.



Dr. Wouter Castryck
Research Expert
Computer Security and Industrial Cryptography research group (COSIC)
Katholieke Universiteit, Leuven
Leuven, 752050, Belgium

Certificate from the Co-supervisor

Date: 11th July, 2025

This is to certify that the thesis titled **"The Monodromy Leak for a Generalized Montgomery Ladder"** submitted by **Mr. Arani Raychaudhuri**, Registration No. **CRS2302**, a student of the **Department of Cryptology and Security Research Unit** of the **M.Tech. in Cryptology and Security** program of ISI Kolkata, is based on his own research work under my co-supervision. I also certify, to the best of my knowledge, that neither the thesis nor any part of it has been submitted for any degree/diploma or any other academic award anywhere before. In my opinion, the thesis fulfills the requirement for the award of the degree of **Masters of Technology** in **Cryptology and Security**.

Mriganka Mandal.

Dr. Mriganka Mandal
Assistant Professor
Cryptology and Security Research Unit (CSRU)
Indian Statistical Institute, Kolkata
Kolkata, 700108, India

डॉ मृगांक मडल /Dr. MRIGANKA MANDAL
सहायक प्राचार्य /ASSISTANT PROFESSOR
क्रिप्टोलॉजी एवं सुरक्षा अनुसंधान यूनिट
CRYPTOLOGY & SECURITY RESEARCH UNIT
आर. सी. बोस कूटलिपि एवं सुरक्षा केंद्र
R. C. Bose Centre for Cryptology & Security
भारतीय सांख्यिकीय संस्थान
INDIAN STATISTICAL INSTITUTE
203, बैरकपुर ट्रंक रोड, कोलकाता-700 108
203, Barrackpore Trunk Road, Kolkata-700 108

Acknowledgements

At the very outset, I would like to express my heartfelt gratitude to everyone who has supported me, both academically and emotionally, throughout the course of this journey. Completing this thesis would not have been possible without the guidance, encouragement, and kindness of many individuals, each of whom has contributed in their own unique way.

I would like to express my deepest gratitude to my supervisor, **Dr. Wouter Castryck**, for his constant support and encouragement throughout my thesis journey. His motivational words, especially during the times when I felt like giving up, were instrumental in helping me find the strength to start again from the beginning. It took me a considerable amount of time to learn about the project and to navigate the challenges of independent research, particularly in learning Elliptic Curve Cryptography from scratch. I am immensely grateful to him for giving me the time and space to learn at my own pace, allowing me to grow both academically and personally. I would also like to thank him for always making time to discuss my project whenever I needed help. There were many moments when I was uncertain about the importance of my work, and his guidance helped me overcome these doubts and stay focused on the path forward. I am especially thankful for the opportunity he gave me to work in the field of ECC and Isogeny when I was struggling to find my footing and had nearly lost hope. His belief that it is always possible to learn something new, at any stage of life, is a lesson I will always carry with me. Finally, his constant effort to achieve 'Quality over Quantity' will be a lesson to me, which I will try all the time.

I am deeply grateful to my co-supervisor, **Dr. Mriganka Mandal**, not only for consistently coordinating with Dr. Castryck on my behalf throughout the year, but also for providing me with numerous opportunities to learn, grow and contribute. He has given me opportuinities to venture into research when I had no background and successfully guided and motivated me to flourish with my full potential. His support and guidance have been invaluable and I will remain thankful to him always.

I would also like to sincerely thank **Dr. Bimal Roy** and **Dr. Bart Preneel**, the professors who selected me for the project opportunity in COSIC, KU Leuven. This chance granted me this project, on which I am hoping to work on for rest of my life. I am immensely grateful to both of them.

I would like to thank **Dr. Krijn Reijnders** for all the discussions and suggestions he gave me for my Master's thesis. His insights and advice helped me significantly to complete my thesis and better understand the finer aspects of my work and proving the theorems.

My biggest thank you goes to my parents, **Mr. Subrata Raychaudhuri** and **Mrs. Nandini Raychaudhuri**, for guiding me towards the right path when I was unsure, for providing me with a life full of opportunities, and for instilling in me the confidence to strive for better. Thank you for never letting my education be a secondary priority, even when you faced your own hardships, and for protecting me from a world where aspirations for pure sciences are often questioned.

Finally, I would like to thank **Ms. Sudipta Mridha**, who has been with me since the beginning of this academic journey and has watched me grow through all its phases. Thank you for never losing hope and for being both the academic and emotional support I needed to complete this thesis, along with writing and correcting several parts of my thesis. Without your help, I could not complete this writing.

To everyone who has even walked a small part of this journey with me, your presence has meant more than I can express. This work is a testament not just to my efforts, but also to the love, patience, and encouragement that I have received. Thank you from the bottom of my heart.

Table of Contents

"There are more things in heaven and earth, Horatio, than are dreamt of in your philosophy."

— William Shakespeare (Hamlet)

Abstract

The Diffie-Hellman key exchange protocol using elliptic curves is the most wide-spread approach to the establishment of a secure internet connection. As an important subroutine, Alice and Bob need to perform multiplications of elliptic curve points by large scalars. The textbook method for scalar multiplication is the double-and-add algorithm. For the sake of efficiency, one usually performs x-coordinate only arithmetic using projective coordinates, and doubling-and-adding is done using the Montgomery ladder.

The advantage of using projective coordinates is that this avoids costly field inversions at each iteration. However, when Alice (say) uses the double-and-add algorithm for computing her public key $Q = [a]P$, it is a bad idea for her to publish the resulting projective coordinates of Q. Indeed, it was shown in 2003 by Naccache, Smart and Stern that these coordinates leak a few bits of the secret scalar a. Therefore, Alice must perform a final division deprojectivizing the coordinates of Q, and this division must be done in constant time so that side-channel analysis does not allow for a reconstruction of these projective coordinates. In 2019 Aldaya, Garcia and Brumley discovered that many real-life implementations violate this requirement.

New work by Robert from 2024 shows that the leak is much more devastating than assumed by Naccache et al.: one can easily recover the entire secret. Thus, bad implementations of elliptic curve scalar multiplication using the Montgomery ladder are a recipe for disaster. The goal of this thesis is to study the new method by Robert, which he calls "the monodromy leak". It stems from the deep fact that the set of all possible projective coordinates for points on an elliptic curve E (called "cubical points") still comes equipped with a natural scalar- multiplication map, despite this set not being a group. Robert shows that the cubical discrete logarithm problem reduces to a discrete logarithm problem in the underlying finite field, which is known to be easier (index-calculus). He then also shows that the Montgomery ladder essentially implements cubical scalar multiplication: whence the devastating conclusion.

Besides understanding how the attack works, the goal is also to study the relation between cubical arithmetic and other projective double-and-add algorithms (such as the standard double-and-add algorithm for Weierstrass curves, or Edwards curves). Our current conclusion is that the Monodromy Leak is specific to the Montgomery ladder, but not to Mont-

gomery curves : we generalize the attack to Partially-Long Weierstrass curves (PLWC). For the standard double-and-add algorithm on Edwards curves (as used in EdDSA), we report on some first explorations.

There are also other applications of cubical arithmetic, namely to the efficient computation of pairings, and to the efficient computation of isogenies. Isogeny-based cryptography is another booming branch in cryptography, which is supposed to remain hard even in the presence of quantum adversaries (unlike "classical" elliptic curve cryptography, which is based on the discrete logarithm problem and therefore broken by Shor's algorithm). However, these applications are not touched upon in this thesis.

Chapter 1
INTRODUCTION

1.1 Outline

Chapter 2 provides the algebraic geometry background necessary to analyze the arithmetic of elliptic curves in higher-dimensional coordinate models. It introduces non-singular varieties and local rings, offering a rigorous framework for understanding projective and affine varieties, their regularity conditions, and coordinate transformations. The foundational setup in this chapter prepares to explore more advanced arithmetic operations used in the thesis.

Chapter 3 moves on to the basics of elliptic curve cryptography, with emphasis on the Elliptic Curve Diffie–Hellman (ECDH) key exchange protocol. It formalizes the classical discrete logarithm problem (DLP) and shows how the elliptic curve version, the ECDLP, underpins the security of elliptic curve protocols. Importantly, it also introduces the MOV/ Frey–Rück attack, highlighting the vulnerability of certain curves to pairing-based reductions of the ECDLP to finite field DLPs.

Chapter 4 presents the core of the thesis: a detailed exposition of the Monodromy Leak discovered by Damien Robert. It shows that the Montgomery ladder for scalar multiplication which is a classical constant-time algorithm inherently carries information leakage, if projective coordinates would be leaked. This is done using cubical arithmetic, where scalar multiplication maps can be defined on cubical points that are not part of a group, yet still support a consistent multiplication mechanism.

Chapter 5 and **6** introduces the new ideas that have been worked out in this thesis. Chapter 5 generalizes elliptic curves in SHort-Weierstrass form or Montgomery form to Partially-Long Weierstrass Curves (PLWCs). It studies how the standard addition and doubling formulas adapt to this new form, including a common generalization of the Montgomery ladder and the Brier-Joye ladder. These generalizations are crucial in understanding Monodromy Leak for PLWCs.

Chapter 6 builds a bridge between the cubical arithmetic used in previous chapters and

the theory of Edwards Curves. It does a first exploration of cubical structures in the setting of Edwards curves. The chapter concludes with a high-level discussion on how the ideas presented throughout the thesis may contribute to leakage in cubical arithmetic in Edwards model in elliptic curve cryptographic protocols.

1.2 Project Target

The primary objective of this project is to investigate the newly proposed Monodromy Leak attack that exploits the leakage in projective coordinate scalar multiplications on elliptic curves. By analyzing how Montgomery ladder computations effectively realize cubical scalar multiplication, the project aims to expose the fundamental vulnerability in existing implementations. The goal of this project is build a generalized curve equation from Montgomery curves and Short-Weierstrass curves, calling them 'Partially-Long Weierstrass curves (PLWCs)' and understand the action of these curves on a 'Generalized Montgomery Ladder' setting. The arithmetic operations of PLWCs on Generalized Montgomery ladder will eventually lead us to the theory of Monodromy Leak for PLWCs. The study extends beyond identifying the attack to understanding the algebraic structure of cubical points and the resulting implications for the discrete logarithm problem. Furthermore, the project aspires to connect these insights with alternative coordinate models and arithmetic techniques, potentially influencing the future design of elliptic curve cryptographic systems. A secondary aim includes examining the relevance of cubical arithmetic in efficient pairing and Edwards curve computations, offering pathways to novel applications.

Chapter 2
Preliminaries

[Throughout all the sections k will denote a field and the algebraic closure of k will be denoted by $\bar{k}$.]

2.1 Non-Singular Varieties

2.1.1 Local Ring and Maximal Ideal

Definition 1. *Let X be a variety over a field k, and let $P \in X(k)$ be a point on the variety. The* local ring *of X at P, denoted $\mathcal{O}_{P,k}(X)$, is defined as the set*

$$\mathcal{O}_{P,k}(X) = \{f \in k(X) : f \text{ is regular at } P\}.$$

Furthermore, define the maximal ideal *at P as*

$$\mathfrak{m}_{P,k}(X) = \{f \in \mathcal{O}_{P,k}(X) : f(P) = 0\} \subseteq \mathcal{O}_{P,k}(X).$$

When the variety X and field k are understood from the context, we shall often abbreviate $\mathcal{O}_{P,k}(X)$ to $\mathcal{O}_P$, and $\mathfrak{m}_{P,k}(X)$ to $\mathfrak{m}_P$.

Lemma 1. *With the above definitions, we have:*

1. *$\mathcal{O}_{P,k}(X)$ is a ring.*
2. *$\mathfrak{m}_{P,k}(X)$ is an ideal in $\mathcal{O}_{P,k}(X)$.*
3. *$\mathfrak{m}_{P,k}(X)$ is a maximal ideal.*
4. *$\mathcal{O}_{P,k}(X)$ is a Noetherian local ring.*

Proof. The first three properties can be argued from the definitions of ring and ideal. For the fourth point, if X is affine, then $\mathcal{O}_{P,k}(X)$ is the localisation of the coordinate ring $k[X]$, which is Noetherian, at the maximal ideal $\mathfrak{m} = \{f \in k[X] : f(P) = 0\}$. Since localisation preserves the Noetherian property when localising at a maximal ideal, it follows that $\mathcal{O}_{P,k}(X)$ is Noetherian. In the projective case, a similar reasoning holds by working within affine charts that cover the point P. □

It is important to note that for an affine variety X, we always have the inclusions

$$k \subseteq k[X] \subseteq \mathcal{O}_P(X) \subseteq k(X),$$

where $k(X)$ denotes the function field of the variety.

Remark 1. *The definitions of $\mathcal{O}_{P,k}(X)$ and $\mathfrak{m}_{P,k}(X)$ depend only on the function field $k(X)$, not on a specific presentation of the variety. This makes them birational invariants: if $\phi : X \to Y$ is a birational map defined at $P \in X(k)$, then $\mathcal{O}_{P,k}(X) \cong \mathcal{O}_{\phi(P),k}(Y)$ as rings, and likewise for the maximal ideals.*

To study local properties, we can often reduce to the affine case. This is justified by the fact that if X is projective and covered by affine open sets U_i, then the behavior at $P \in X(k)$ can be understood from the affine variety $\varphi_i^{-1}(X \cap U_i)$ for suitable i.

2.1.2 Singular Points and Non-Singular Varieties

Lemma 2. *Let $X \subseteq \mathbb{A}^n$ be an affine variety defined over k, and let $P \in X(k)$. Then:*

1. *The quotient ring $\mathcal{O}_{P,k}(X)/\mathfrak{m}_{P,k}(X)$ is isomorphic to k.*
2. *The quotient $\mathfrak{m}_{P,k}(X)/\mathfrak{m}_{P,k}(X)^2$ is a finite-dimensional k-vector space with dimension at most n.*

The dimension of this quotient vector space provides insight into the local geometry of the variety at the point P. This leads to a foundational definition:

Definition 2. *Let X be a variety (either affine or projective) over k, and let $P \in X(k)$. We say that P is a* non-singular *point of X if*

$$\dim_k \left(\mathfrak{m}_{P,k}(X)/\mathfrak{m}_{P,k}(X)^2\right) = \dim(X).$$

If this condition fails, then P is said to be a singular *point. The variety X is said to be* non-singular *or* smooth *if every point in $X(\bar{k})$ is non-singular.*

Let $X = V(f_1, \ldots, f_m) \subseteq \mathbb{A}^n$ be an affine variety defined by polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$, and let $P \in X(k)$. Consider the Jacobian matrix

$$J_{X,P} = \left(\frac{\partial f_i}{\partial x_j}(P)\right)_{1 \le i \le m,\ 1 \le j \le n}.$$

Theorem 1. *Let* $d_1 = \dim_k \left(\mathfrak{m}_{P,k}(X)/\mathfrak{m}_{P,k}(X)^2\right)$*, and let* $d_2 = rank(J_{X,P})$*. Then,*

$$d_1 + d_2 = n.$$

Proof. By translation, we may assume without loss of generality that $P = (0, \ldots, 0)$. Let $m = \{f \in k[X] : f(P) = 0\}$ and note that $m/m^2 \cong \mathfrak{m}_{P,k}(X)/\mathfrak{m}_{P,k}(X)^2$. Define a linear map $\theta : k[x_1, \ldots, x_n] \to k^n$ by sending a polynomial f to the vector of partial derivatives evaluated at P:

$$\theta(f) = \left(\frac{\partial f}{\partial x_1}(P), \ldots, \frac{\partial f}{\partial x_n}(P)\right).$$

Then $\ker(\theta) = (x_1, \ldots, x_n)^2$ and θ induces an isomorphism $(x_1, \ldots, x_n)/(x_1, \ldots, x_n)^2 \cong k^n$. Through this identification, we find that

$$\dim_k(m/m^2) + \dim_k(\theta(I(X))) = n,$$

and $\dim_k(\theta(I(X))) = \operatorname{rank}(J_{X,P})$, so the result follows. □

Corollary 1. *Let* $X = V(f_1, \ldots, f_m) \subseteq \mathbb{A}^n$ *be an affine variety of dimension* d*, and let* $P \in X(k)$*. Then* P *is a non-singular point if and only if the Jacobian matrix* $J_{X,P}$ *has rank equal to* $n - d$*.*

Corollary 2. *Let* $X = V(f) \subseteq \mathbb{A}^n$ *be an irreducible affine variety defined by a single polynomial* f*, and let* $P \in X(k)$*. Then* P *is a singular point if and only if*

$$\frac{\partial f}{\partial x_j}(P) = 0 \quad \textit{for all } 1 \leq j \leq n.$$

Definition 3. *A* curve *is defined to be a projective non-singular variety of dimension one. A* plane curve *is a curve defined by a homogeneous polynomial* $F(x, y, z)$ *in* $\mathbb{P}^2$*.*

Lemma 3. *Let* C *be a curve over* k*, and let* $P, Q \in C(k)$*. If* $\mathcal{O}_{P,k} \subseteq \mathcal{O}_{Q,k}$*, then* $P = Q$*.*

Proof. Assume $P \neq Q$. In affine coordinates, suppose $P = (a_1, \ldots, a_n)$ and $Q = (b_1, \ldots, b_n)$. Then $a_i \neq b_i$ for some i, and the function $f = 1/(x_i - b_i)$ is regular at P, but has a pole at Q. Thus, $f \in \mathcal{O}_{P,k}$, but $f \notin \mathcal{O}_{Q,k}$, contradicting the inclusion $\mathcal{O}_{P,k} \subseteq \mathcal{O}_{Q,k}$. □

2.2 Divisors

In the theory of algebraic curves, divisors play a central role as formal sums of points on the curve, equipped with integer coefficients. The notion captures information about zeros

and poles of rational functions, and allows us to formulate many geometric and arithmetic properties of curves.

We work over an algebraically closed field k, and consider a smooth, projective, irreducible algebraic curve C defined over k.

Definition 4. *Let C be a curve over k. A **divisor** D on C is a formal finite sum:*

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

where $n_P \in \mathbb{Z}$, and only finitely many coefficients n_P are nonzero.

This means that a divisor is essentially a formal linear combination of the k-rational points of the curve with integer weights, with only finitely many of these weights being non-zero.

The set of all divisors on C is denoted by $\mathrm{Div}_k(C)$.

The zero divisor, denoted 0, is the unique divisor with all coefficients $n_P = 0$.

The **support** of a divisor D, denoted $\mathrm{Supp}(D)$, is the set of all points $P \in C(\bar{k})$ such that $n_P \neq 0$. That is,

$$\mathrm{Supp}(D) = \{P \in C(\bar{k}) : n_P \neq 0\}.$$

The notation $|D|$ is sometimes used for the support in the literature.

Given two divisors

$$D = \sum_P n_P(P), \quad D' = \sum_P n'_P(P),$$

their sum is defined pointwise by

$$D + D' = \sum_{P \in C(\bar{k})} (n_P + n'_P)(P).$$

The additive inverse of a divisor D is defined as:

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

We define a partial ordering on divisors as follows:

$$D \geq D' \quad \text{if and only if} \quad n_P \geq n'_P \text{ for all } P \in C(k).$$

A divisor D is said to be **effective** if $D \geq 0$, that is, all the coefficients $n_P \geq 0$. These divisors correspond to finite formal sums of points with non-negative multiplicities.

Definition 5. *The* ***degree*** *of a divisor* $D = \sum_{P \in C(\bar{k})} n_P(P)$ *is defined to be the integer:*

$$\deg(D) = \sum_{P \in C(\bar{k})} n_P.$$

This sum is always finite since only finitely many n_P are nonzero. The degree is an additive map from $\mathrm{Div}(C)$ to $\mathbb{Z}$. The subset of divisors of degree zero is denoted:

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}_k(C) : \deg(D) = 0\}.$$

Lemma 4. *The set* $\mathrm{Div}(C)$ *of all divisors on* C *forms an abelian group under addition. Moreover, the set of divisors of degree zero,* $\mathrm{Div}^0(C)$*, forms a subgroup of* $\mathrm{Div}(C)$*.*

Definition 6. *Let* C *be a curve over* k*, and let* $D = \sum_{P \in C(\bar{k})} n_P(P)$ *be a divisor. For* $\sigma \in \mathrm{Gal}(\bar{k}/k)$*, define:*

$$\sigma(D) := \sum_{P \in C(\bar{k})} n_P \cdot (\sigma(P)).$$

We say that the divisor D *is* ***defined over*** k *if* $\sigma(D) = D$ *for all* $\sigma \in \mathrm{Gal}(\bar{k}/k)$*.*

That is, a divisor is defined over the base field k if it is invariant under the action of the absolute Galois group $\mathrm{Gal}(\bar{k}/k)$. This corresponds to a natural condition that the divisor does not "move" under field automorphisms of $\bar{k}$, that fix k.

We denote by $\mathrm{Div}_k(C)$ the set of all divisors on C that are defined over k. We write $Div_k^0(C)$ for $Div^0(C) \cap Div_k(C)$.

Even though the Galois group $\mathrm{Gal}(\bar{k}/k)$ is generally enormous and abstract, checking whether a given divisor is defined over k is often computationally manageable. The key observation is that the coordinates of the finitely many points in $\mathrm{Supp}(D)$ lie in a finite extension k' of k, say k'/k. Let k'' be the Galois closure of k'/k, which is then a finite Galois extension. Since every $\sigma \in \mathrm{Gal}(\bar{k}/k)$ stabilizes k'', we only need to verify the equality $\sigma(D) = D$ for those $\sigma \in \mathrm{Gal}(k''/k)$, which is a finite group.

2.3 Principal Divisors

This section discusses an important theoretical result concerning rational functions on curves: namely, that the number of poles and the number of zeroes of a non-zero rational function (each counted with multiplicity) are both finite and equal. This result is essential because it ensures that we can express both poles and zeroes as a divisor, and that these divisors belong to a special class known as *principal divisors*. Additionally, this balance between zeroes and

poles shows that the divisors associated to rational functions lie in the subgroup of divisors of degree zero.

In this section, we prove the result about the finiteness of zeroes and poles only for plane curves. The fact that the degree of the divisor of a function is zero will be shown explicitly for elliptic curves.

Theorem 2. *Let C be a curve over a field k, and let $f \in k(C)^*$ be a nonzero rational function on C. Then f has only finitely many poles and finitely many zeroes.*

Proof. We prove this in the special case where C is a plane affine curve. Suppose C is defined as $V(F(x, y, z)) \subset \mathbb{P}^2$, where F is an irreducible homogeneous polynomial over k. If $F(x, y, z) = z$, then C lies entirely in the plane at infinity, and the finiteness of poles and zeroes follows directly from known results.

To proceed, we reduce to the affine case $C = V(F(x, y)) \subset \mathbb{A}^2$. Let $f = f_1(x, y)/f_2(x, y)$, where $f_1, f_2 \in k[x, y]$ are polynomials. The poles of f occur at those points $P \in C$ for which $f_2(P) = 0$. Therefore, the set of poles of f is a subset of the intersection $C \cap V(f_2)$.

To show this intersection is finite, we can assume without loss of generality that $f_2(x, y)$ includes a monomial involving x. Then we can form the resultant of $f_2(x, y)$ and $F(x, y)$ with respect to x, denoted $R_x(f_2(x, y), F(x, y))$. This is a polynomial in y, and as such, it has only finitely many roots. Hence the variety $C \cap V(f_2)$ is finite, so f has only finitely many poles.

A similar argument applies to the zeroes of f, since they are contained in $C \cap V(f_1)$, which is also finite. Therefore, f has finitely many zeroes and poles. □

Definition 7. *Let $f \in k(C)^*$ be a nonzero rational function on a curve C over k. The* divisor *of f, denoted* $\mathrm{div}(f)$*, is defined as:*

$$\mathrm{div}(f) = \sum_{P \in C(\bar{k})} v_P(f) \cdot (P),$$

where $v_P(f)$ is the valuation of f at the point P. This divisor is called a ***principal divisor****, also denoted as (f). The set of all such principal divisors on C is denoted by*

$$\mathrm{Prin}_k(C) := \{\mathrm{div}(f) \,:\, f \in k(C)^*\}.$$

Lemma 5. *Let C be a curve over k and let $f, f' \in k(C)^*$ be rational functions. Then:*

1. $\mathrm{div}(ff') = \mathrm{div}(f) + \mathrm{div}(f')$,
2. $\mathrm{div}(1/f) = -\mathrm{div}(f)$,

3. $\operatorname{div}(f+f') \geq \sum_P \min\{v_P(f), v_P(f')\} \cdot (P)$,

4. $\operatorname{div}(f^n) = n \cdot \operatorname{div}(f)$ *for all integers* n,

5. *For any* $\sigma \in \operatorname{Gal}(\bar{k}/k)$, $\operatorname{div}(\sigma(f)) = \sigma(\operatorname{div}(f))$.

Lemma 6. *The set* $\operatorname{Prin}_k(C)$ *of principal divisors is a subgroup of the group of all divisors* $\operatorname{Div}_k(C)$.

Lemma 7. *Let* $D = \sum_{i=1}^n e_i(x_i : z_i)$ *be a divisor of degree zero on the projective line* $\mathbb{P}^1(k)$, *so that* $\sum_{i=1}^n e_i = 0$. *Then* D *is a principal divisor.*

Proof. Define the function

$$f(x,z) = \prod_{i=1}^n (xz_i - zx_i)^{e_i}.$$

Since the total exponent sum is zero, $f(x,z)$ is a homogeneous rational function of degree zero (a ratio of polynomials of the same degree). This ensures that $f(x,z)$ is a well-defined function on $\mathbb{P}^1$. Using known uniformizers on $\mathbb{P}^1$, it can be verified that for each point $P_i = (x_i : z_i)$, we have $v_{P_i}(f) = e_i$. Thus,

$$\operatorname{div}(f) = \sum_{i=1}^n e_i(x_i : z_i) = D.$$

□

Lemma 8. *Let* E *be an elliptic curve over* k *given by the Weierstrass equation* $y^2 + H(x)y = F(x)$. *Let* $P = (x_i, y_i) \in E(k)$ *be a non-singular point. Then:*

$$\operatorname{div}(x - x_i) = (P) + (\iota(P)) - 2(O_E),$$

where $\iota(P)$ *denotes the inverse point of* P *on the elliptic curve and* O_E *is the point at infinity.*

Proof. There are one or two points on $E(k)$ having the x-coordinate x_i: namely $P = (x_i, y_i)$ and $\iota(P) = (x_i, -y_i - H(x_i))$. These are the roots of the equation $x = x_i$ on the curve. Depending on whether $2y_i + H(x_i) = 0$, the point P could equal $\iota(P)$.

In the case where $2y_i + H(x_i) \neq 0$, the function $x - x_i$ has a simple zero at both P and $\iota(P)$ and a double pole at O_E, so its divisor is:

$$\operatorname{div}(x - x_i) = (P) + (\iota(P)) - 2(O_E).$$

In the case where $P = \iota(P)$, $x - x_i$ has a double zero at that point and a double pole at O_E, again leading to the same result. □

Theorem 3. *Let C be a curve over k, and let $f \in k(C)^*$. Then the degree of the divisor of f is zero:*

$$\deg(\mathrm{div}(f)) = 0.$$

Proof. It can be shown that the sum of valuations over all points equals zero, the divisor of any nonzero function f always has degree zero. □

Corollary 3. *Let $f \in k(C)^*$ be a nonzero rational function. Then for every $\sigma \in \mathrm{Gal}(\bar{k}/k)$, we have:*

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

Proof. For any automorphism $\sigma \in \mathrm{Gal}(k/k)$, the valuation at a point satisfies:

$$v_{\sigma(P)}(\sigma(f)) = v_P(f).$$

Thus, the divisor transforms under Galois action as:

$$\sigma(\mathrm{div}(f)) = \sum_P v_P(f) \cdot \sigma(P) = \sum_Q v_{\sigma^{-1}(Q)}(f) \cdot Q = \sum_Q v_Q(\sigma(f)) \cdot Q = \mathrm{div}(\sigma(f)).$$

□

Definition 8. *According to the theorem.3, we get $\mathrm{Prin}_k(C) \subset \mathrm{Div}_k^0(C)$. From this property, the Picard-0 Group is defined as*

$$\mathrm{Pic}_k^0(C) \ := \ \frac{\mathrm{Div}_k^0(C)}{\mathrm{Prin}_k(C)}.$$

Corollary 4. *Let C be a curve over k and let $f \in k(C)^*$. The following conditions are equivalent:*

1. $\mathrm{div}(f) \geq 0$,
2. $f \in k^*$,
3. $\mathrm{div}(f) = 0$.

2.4 General Weierstrass Equations

Definition 9. *Let a_1, a_2, a_3, a_4, a_6 be elements of a field k. A **Long Weierstrass equation** is defined as a projective algebraic set E over k, described by the following homogeneous equation in projective coordinates $(x : y : z)$:*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

The corresponding affine version of this equation (obtained by setting $z = 1$) is:

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

Lemma 9. *Let $H(x), F(x) \in k[x]$ be polynomials where $\deg(F) = 3$ and $\deg(H) \leq 1$. Then the curve $E(x, y)$ defined by the equation*

$$y^2 + H(x)y - F(x)$$

is irreducible over k.

Proof. Suppose by contradiction that $E(x, y)$ is reducible over k. Then it can be factored in the ring $k[x, y]$ as:

$$E(x, y) = (y + M(x))(y + N(x)),$$

for some polynomials $M(x), N(x) \in k[x]$. Expanding this product, we get:

$$y^2 + (M(x) + N(x))y + M(x)N(x).$$

Comparing with $y^2 + H(x)y - F(x)$, we find that:

$$M(x) + N(x) = H(x), \quad M(x)N(x) = -F(x).$$

But since $\deg(F) = 3$, and the product $M(x)N(x)$ has degree 3, one of $M(x), N(x)$ must have degree at least 2. Without loss of generality, assume $\deg(M) \geq 2$ and hence $\deg(N) \leq 1$. Then $\deg(M + N) \geq 2$, which contradicts $\deg(H) \leq 1$. Therefore, such a factorization is not possible, and $E(x, y)$ is irreducible over k. □

Definition 10. *Let E be a Weierstrass equation over the field k. Then the point $(0 : 1 : 0)$ in projective coordinates is always a solution to the Weierstrass equation. This point is referred to as the **point at infinity** on E, and we denote it by $\mathcal{O}_E$. It plays a key role in defining the group structure on the curve.*

Definition 11. *An **elliptic curve** over a field k is a projective algebraic curve defined by a Weierstrass equation that is* non-singular*. That is, the curve has no singular points over the algebraic closure of k.*

Lemma 10. *Let E be an elliptic curve defined over k by a Weierstrass equation. Then every function f in the function field $k(E)$ can be expressed as a rational function on the affine model of E in the form:*

$$f(x, y) = \frac{a(x) + b(x)y}{c(x)}, \tag{7.5}$$

where $a(x), b(x), c(x) \in k[x]$. Conversely, any such expression defines a unique function on the projective model of E.

Proof. Let U denote the affine algebraic set obtained from the projective curve E by setting $z = 1$. Since E is non-singular and projective, it contains at least one affine point, hence $U(k) \neq \emptyset$. Then, the function fields $k(E)$ and $k(U)$ are isomorphic. Therefore, we may restrict attention to functions on the affine curve U.

Any function $f \in k(U)$ can be represented as a rational expression in x and y. Because the defining equation of E expresses y^2 in terms of x and y, we can eliminate any higher powers of y (i.e., y^n for $n > 1$) using substitutions based on the equation:

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

By repeated substitution and clearing denominators, every function can be written in this form. The uniqueness claim refers to the fact that two distinct such expressions will define the same rational function on the projective curve if and only if their difference is the zero function in $k(E)$. □

2.5 Elliptic Curves

Let E be an elliptic curve, and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the affine part of E. Consider the line $l(x, y) = 0$ that passes through both P_1 and P_2. If $P_1 \neq P_2$, then this is an ordinary chord; if $P_1 = P_2$, then the line is defined to be the tangent to the curve at P_1 (see (1)).

This line will intersect the curve in a third point R, which we count with appropriate multiplicity. Then, we consider a vertical line $v(x) = 0$ connecting the identity element $\mathcal{O}_E$ (the point at infinity) and the point R. The third intersection point of this vertical line with the curve is denoted S, and we define

$$P_1 + P_2 := S.$$

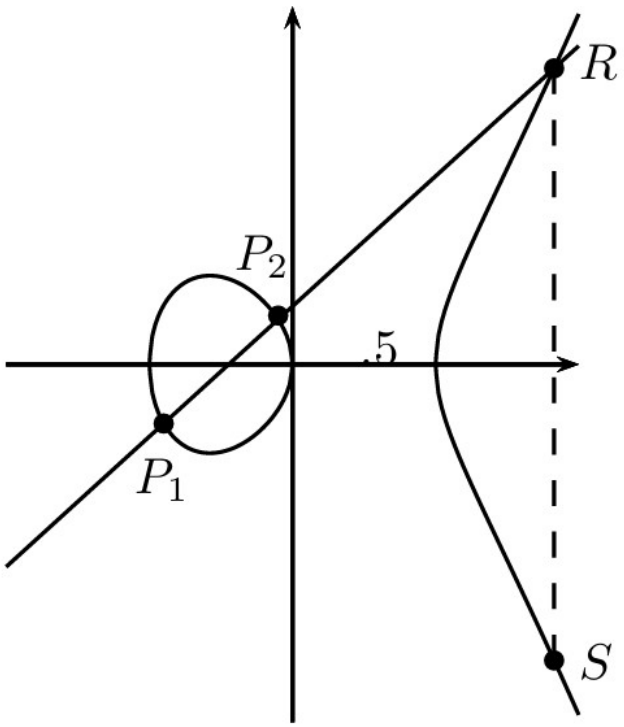


Figure 2.1: Chord and tangent rule for elliptic curve addition.

Definition 12. *Let $E(x, y)$ be a Weierstrass equation for an elliptic curve over a field k. Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(k) \cap \mathbb{A}^2$. Then:*

- *If $P_1 = \iota(P_2)$, i.e., P_2 is the additive inverse of P_1, then the line between them is vertical, given by $v(x) = x - x_1$.*
- *If $P_1 \neq \iota(P_2)$, there are two subcases:*
  - *If $P_1 = P_2$, define*
$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4}{2y_1 + a_1x_1 + a_3}.$$
  - *If $P_1 \neq P_2$, define*
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

  Then the line between P_1 and P_2 is given by:

$$l(x, y) = y - \lambda(x - x_1) - y_1.$$

We emphasize that $l(x, y)$ is only defined in the non-vertical case.

Lemma 11. *Let $P_1, P_2 \in E(k) \cap \mathbb{A}^2$. Then the function $l(x,y)/v(x)$, as defined in Definition 11, satisfies:*

$$\operatorname{div}\left(\frac{l(x,y)}{v(x)}\right) = (P_1) + (P_2) + (R) - 3(\mathcal{O}_E),$$

where R is the third point of intersection (with multiplicities) of the line $l(x,y) = 0$ with the curve E.

Theorem 4. *Let E be a Weierstrass equation for an elliptic curve over a field k. Let $P_1, P_2 \in E(k) \cap \mathbb{A}^2$. Define R as the third intersection point of the line through P_1 and P_2, and define $S = \iota(R)$, the inverse of R in the group law. Then:*

$$[(P_1) - (\mathcal{O}_E)] + [(P_2) - (\mathcal{O}_E)] = [(S) - (\mathcal{O}_E)] \in \operatorname{Pic}^0_k(E).$$

Proof. We know that the function $l(x,y)/v(x)$ has divisor:

$$\operatorname{div}\left(\frac{l(x,y)}{v(x)}\right) = (P_1) + (P_2) + (R) - 3(\mathcal{O}_E).$$

This implies:

$$(P_1) + (P_2) - 2(\mathcal{O}_E) = (\iota(R)) - (\mathcal{O}_E),$$

since $\iota(R)$ is the third intersection point of the vertical line through R and $\mathcal{O}_E$.

Hence, as elements of the degree-zero divisor class group $\operatorname{Pic}^0_k(E)$, we have:

$$[(P_1) - (\mathcal{O}_E)] + [(P_2) - (\mathcal{O}_E)] = [(\iota(R)) - (\mathcal{O}_E)] = [(S) - (\mathcal{O}_E)].$$

□

Remark 2. *The traditional geometric rule for adding points on an elliptic curve coincides with the group law derived from the theory of divisors. This confirms that the set of points $E(k)$, together with this addition, indeed forms an abelian group, with identity element $\mathcal{O}_E$ and inverses given by $\iota(P)$.*

2.6 Edwards Model

The origin of the Edwards model dates back to Euler and Gauss, who considered the genus 1 curve

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

This model was later generalized by Harold Edwards to encompass a broader class of elliptic curves. Further enhancements were introduced by Bernstein, Birkner, Joye, Lange, and Peters. The Edwards model has gained prominence due to several desirable properties: it offers a complete group law over $E(\mathbb{F}_q)$ for certain finite fields $\mathbb{F}_q$, meaning that a single rational function $+ : E \times E \to E$ suffices for all possible additions in $E(\mathbb{F}_q) \times E(\mathbb{F}_q)$. Furthermore, the addition law in this model can be computed with high efficiency, making it particularly suitable for cryptographic implementations.

Definition 13. *Let k be a field with char$(k) \neq 2$, and let $a, d \in k$ satisfy $a \neq 0$, $d \neq 0$, and $a \neq d$. The* twisted Edwards model *(see (2)) is the plane affine curve defined by:*

$$ax^2 + y^2 = 1 + dx^2y^2.$$

While Weierstrass models express elliptic curves over k (with $\text{char}(k) \neq 2$) in the form $y^2 = F(x)$, the twisted Edwards model can also be rearranged as

$$y^2 = \frac{1 - ax^2}{1 - dx^2},$$

suggesting that the natural inverse of a point (x, y) is $(x, -y)$, and the identity element becomes $(x, y) = (1/\sqrt{a}, 0)$. However, due to historical conventions, it is more common to reparametrize the curve as

$$x^2 = \frac{1 - y^2}{a - dy^2},$$

which sets the identity at $(0, 1)$, and defines the inverse of a point (x, y) as $(-x, y)$.

Group Law: The group operation in the twisted Edwards model is defined as:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

A geometric interpretation of this group law, particularly on singular models, has been studied by Arène, Lange, Naehrig, and Ritzenthaler (see (3)).

Projective Model: To analyze points at infinity, a projective model of the twisted Edwards curve is introduced. Let $\phi(x, y) = (X_0 = xy, X_1 = x, X_2 = y, X_3 = 1)$, mapping the affine point (x, y) to a projective 4-tuple. The projective variety X is then defined in $\mathbb{P}^3$ by:

$$X = V(aX_1^2 + X_2^2 - X_3^2 - dX_0^2, X_1X_2 - X_0X_3).$$

This variety is irreducible and of dimension 1. The points at infinity correspond to the case $X_3 = 0$, and are given by the tuples:

$$(1 : \pm\sqrt{d/a} : 0 : 0), \quad (1 : 0 : \pm\sqrt{d} : 0).$$

Lemma 12. *Let k be a field with $char(k) \neq 2$, and let $a, d \in k$ with $a, d \neq 0$. Then the projective twisted Edwards model has four points at infinity over k, each of which has order dividing 4.*

Proof. We consider the map $\phi(x, y)$ as described above and analyze the projective variety X. Points at infinity correspond to $X_3 = 0$. These yield the points $(1 : \pm\sqrt{d/a} : 0 : 0)$ and $(1 : 0 : \pm\sqrt{d} : 0)$. We verify these are non-singular by evaluating the Jacobian matrix:

$$\begin{pmatrix} 2aX_1 & 2X_2 & -2X_3 \\ X_2 & X_1 & -1 \end{pmatrix}$$

at each of these points and confirming that the rank is 2.

The group law in projective coordinates uses the expressions:

$$\begin{aligned} S_1 &= X_1Z_2 + Z_1X_2, \\ S_2 &= X_2Z_2 - aX_1Z_1, \\ S_3 &= X_3Z_3 + dX_0Z_0, \\ S_4 &= X_3Z_3 - dX_0Z_0. \end{aligned}$$

Then the group addition is given by:

$$(X_0 : X_1 : X_2 : X_3) + (Z_0 : Z_1 : Z_2 : Z_3) = (S_1S_2 : S_1S_4 : S_2S_3 : S_3S_4).$$

It can be checked that $(0 : 0 : 1 : 1)$ acts as the identity element. Furthermore, by evaluating the group law at points $(0 : 0 : -1 : 1)$, $(1 : \pm\sqrt{d/a} : 0 : 0)$, and $(1 : 0 : \pm\sqrt{d} : 0)$, one confirms they have order dividing 2 and 4 respectively. □

Lemma 13. *Let k be a field of characteristic not equal to 2, and let $a, d \in k$ be such that $a \neq 0$, $d \neq 0$, and $a \neq d$. Suppose a is a square in k^* but d is not a square in k^*. Then the affine group law given by equation (9.14) is defined for all points over k.*

Proof. Let $\epsilon = dx_1x_2y_1y_2$. Suppose, for contradiction, that $\epsilon = \pm 1$. This implies all x_1, x_2, y_1, y_2 are non-zero. Substituting from the curve equation $ax^2 + y^2 = 1 + dx^2y^2$,

one gets:

$$dx_1^2y_1^2(ax_2^2 + y_2^2) = ax_1^2 + y_1^2.$$

Now add $\pm 2\sqrt{a}\epsilon x_1y_1$ to both sides:

$$(\sqrt{a}x_1 \pm \epsilon y_1)^2 = dx_1^2y_1^2(\sqrt{a}x_2 \pm y_2)^2.$$

If either $\sqrt{a}x_2 + y_2 \neq 0$ or $\sqrt{a}x_2 - y_2 \neq 0$, then we conclude that d must be a square, contradicting the assumption. If both expressions are 0, then $x_2 = 0$, contradicting the initial assumption that $x_2 \neq 0$. Hence, no such ϵ can exist, and the group law is defined for all k-points. □

Lemma 14. *Let $M : By^2 = x^3 + Ax^2 + x$ be a Montgomery model for an elliptic curve over k, where $B \neq 0$ and $A^2 \neq 4$. Define*

$$a = \frac{A+2}{B}, \qquad d = \frac{A-2}{B}.$$

Then $a \neq 0$, $d \neq 0$, and $a \neq d$. The map $(x, y) \mapsto (X = x/y, Y = (x-1)/(x+1))$ is a birational equivalence over k from M to the twisted Edwards curve

$$E : aX^2 + Y^2 = 1 + dX^2Y^2.$$

Conversely, define $A = 2(a+d)/(a-d)$, $B = 4/(a-d)$. Then the map $(X, Y) \mapsto \left(x = \frac{1+Y}{1-Y}, y = \frac{1+Y}{X(1-Y)}\right)$ is a birational equivalence over k from E to M.

2.7 Pairings

2.7.1 Weil Reciprocity

A divisor on a curve C over a field k is a finite sum $D = \sum_{P \in C(\bar{k})} n_P(P)$ (i.e., $n_P = 0$ for all but finitely many $P \in C(\bar{k})$). The support of a divisor D is the set of points $\mathrm{Supp}(D) = \{P \in C(\bar{k}) : n_P \neq 0\}$. If f is a function on a curve and D is a divisor such that the support of D and the support of $\mathrm{div}(f)$ are disjoint, then

$$f(D) = \prod_{\substack{P \in C(\bar{k}) \\ n_P \neq 0}} f(P)^{n_P}.$$

Theorem 5 (Weil reciprocity)**.** *Let C be a curve over a field k. Let $f, g \in k(C)$ be functions*

such that $Supp(div(f)) \cap Supp(div(g)) = \emptyset$. *Then*

$$f(div(g)) = g(div(f)).$$

2.7.2 The Weil Pairing

Let E be an elliptic curve defined over a field k, and suppose $n \in \mathbb{N}$ is such that $\gcd(n, \mathrm{char}(k)) = 1$. Take two points $P, Q \in E[n]$, i.e., both are of order dividing n.

We begin by choosing a function $f \in \bar{k}(E)$ whose divisor satisfies:

$$\mathrm{div}(f) = n(Q) - n(\mathcal{O}_E),$$

where $\mathcal{O}_E$ is the identity element on the elliptic curve. Such a function exists because $Q \in E[n]$.

Next, let $Q' \in E(\bar{k})$ be any point such that $[n]Q' = Q$, which implies $[n^2]Q' = \mathcal{O}_E$. We consider the pullback divisor:

$$D = [n]^*((Q) - (\mathcal{O}_E)) = \sum_{R \in E[n]} (Q' + R) - (R).$$

We know that this divisor D is principal. Hence, there exists a function $g \in \bar{k}(E)$ such that:

$$\mathrm{div}(g) = D = [n]^*((Q) - (\mathcal{O}_E)).$$

Now consider the composition $f \circ [n]$, i.e., the function $[n]^* f$. Its divisor becomes:

$$\mathrm{div}(f \circ [n]) = [n]^*(\mathrm{div}(f)) = [n]^*(n(Q) - n(\mathcal{O}_E)) = nD.$$

Thus, $f \circ [n]$ and g^n have the same divisor, and by multiplying f by an appropriate constant, we can ensure that $f \circ [n] = g^n$.

Now, choose any point $U \in E(\bar{k})$ such that $[n]U \notin E[n^2]$. Then we have:

$$g(U + P)^n = f([n]U + [n]P) = f([n]U) = g(U)^n,$$

which implies that the ratio $g(U + P)/g(U)$ is an n-th root of unity in $\bar{k}$.

Lemma 15. *Let the notation be as above. Then* $g(U+P)/g(U)$ *is independent of the choice of the point* $U \in E(\bar{k})$.

Definition 14. *Let* E *be an elliptic curve over a field* k, *and let* $n \in \mathbb{N}$ *be such that*

$\gcd(n, char(k)) = 1$. *Define*

$$\mu_n = \{z \in \bar{k}^* : z^n = 1\}.$$

The ***Weil pairing*** *is the function*

$$e_n : E[n] \times E[n] \to \mu_n,$$

defined by $e_n(P, Q) = g(U + P)/g(U)$*, where* g *is as above with* $div(g) = [n]^*((Q) - (\mathcal{O}_E))$*, and* $U \in E(\bar{k})$ *is any point such that* $[n]U \notin E[n^2]$.

Theorem 6. *The Weil pairing satisfies the following properties:*

1. ***(Bilinear)*** *For* $P_1, P_2, Q \in E[n]$*, one has*

$$e_n(P_1 + P_2, Q) = e_n(P_1, Q) \cdot e_n(P_2, Q), \quad \text{and} \quad e_n(Q, P_1 + P_2) = e_n(Q, P_1) \cdot e_n(Q, P_2).$$

2. ***(Alternating)*** *For all* $P \in E[n]$*, one has*

$$e_n(P, P) = 1.$$

3. ***(Non-degenerate)*** *If* $e_n(P, Q) = 1$ *for all* $Q \in E[n]$*, then* $P = \mathcal{O}_E$.

4. ***(Galois invariant)*** *If* E *is defined over* k *and* $\sigma \in Gal(\bar{k}/k)$*, then*

$$e_n(\sigma(P), \sigma(Q)) = \sigma(e_n(P, Q)).$$

5. ***(Compatible)*** *If* $P \in E[nm]$ *and* $Q \in E[n]$*, then*

$$e_{nm}(P, Q) = e_n([m]P, Q).$$

Finally, there exists an alternative and often more computationally useful expression for the Weil pairing. Let $P, Q \in E[n]$, and let $D_P \sim (P) - (\mathcal{O}_E)$, $D_Q \sim (Q) - (\mathcal{O}_E)$, be degree-zero divisors with disjoint support. Then choose functions $f_P, f_Q \in \bar{k}(E)$ such that:

$$\text{div}(f_P) = nD_P, \quad \text{div}(f_Q) = nD_Q.$$

Then the Weil pairing can also be defined as:

$$e_n(P, Q) = \frac{f_Q(D_P)}{f_P(D_Q)}.$$

2.7.3 The Tate-Lichtenbaum Pairing

The Tate pairing, originally introduced by Tate for abelian varieties over local fields, was further developed by Lichtenbaum, who showed how to compute it for Jacobians of curves. Later, Frey and Rück adapted the pairing to elliptic curves over finite fields and highlighted its cryptographic significance. This pairing has become the fundamental component in most pairing-based cryptographic constructions.

Suppose E is an elliptic curve over the finite field $\mathbb{F}_q$, and let n be a positive integer such that $\gcd(n, q) = 1$ and n divides $\#E(\mathbb{F}_q)$. Define the subgroup

$$nE(\mathbb{F}_q) = \{[n]Q : Q \in E(\mathbb{F}_q)\}.$$

Then, $nE(\mathbb{F}_q)$ is a group. Also, we consider the quotient group $E(\mathbb{F}_q)/nE(\mathbb{F}_q)$ and the multiplicative group $\mathbb{F}_q^*/(\mathbb{F}_q^*)^n$, which are both finite groups of exponent n.

Let $P \in E(\mathbb{F}_q)[n]$ and $Q \in E(\mathbb{F}_q)$. Since $n(P) - n(\mathcal{O}_E)$ is a principal divisor, defined over $\mathbb{F}_q$, there exists a function $f \in \mathbb{F}_q(E)$ such that

$$\mathrm{div}(f) = n(P) - n(\mathcal{O}_E).$$

Choose a divisor D such that its support does not intersect the support of $\mathrm{div}(f)$ (i.e., equal upto a principal divisor) and such that D is linearly equivalent to $(Q) - (\mathcal{O}_E)$. A typical choice could be $D = (Q + R) - (R)$ for some $R \in E(\mathbb{F}_q)$ not equal to any of the points $P, Q, -Q, P - Q, \mathcal{O}_E$.

Using this setup, we define the Tate-Lichtenbaum pairing.

$$t_n(P, Q) = f(D).$$

This defines a pairing of the form

$$t_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \longrightarrow \mathbb{F}_q^*/(\mathbb{F}_q^*)^n.$$

The pairing is well-defined due to properties of divisors and Weil reciprocity.

Theorem 7. *The Tate-Lichtenbaum pairing has the following properties:*

1. ***Bilinearity**: For $P_1, P_2 \in E(\mathbb{F}_q)[n]$ and $Q \in E(\mathbb{F}_q)$,*

$$t_n(P_1 + P_2, Q) = t_n(P_1, Q)t_n(P_2, Q).$$

Similarly, for $P \in E(\mathbb{F}_q)[n]$ and $Q_1, Q_2 \in E(\mathbb{F}_q)$,

$$t_n(P, Q_1 + Q_2) = t_n(P, Q_1)t_n(P, Q_2).$$

2. ***Non-degeneracy**: If $\mathbb{F}_q^*$ contains a nontrivial n-th root of unity and $P \in E(\mathbb{F}_q)[n]$ such that $t_n(P, Q) = 1$ for all $Q \in E(\mathbb{F}_q)$, then $P = \mathcal{O}_E$. Conversely, if $Q \in E(\mathbb{F}_q)$ and $t_n(P, Q) = 1$ for all $P \in E(\mathbb{F}_q)[n]$, then $Q \in nE(\mathbb{F}_q)$.*

3. ***Galois invariance**: If E is defined over $\mathbb{F}_q$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, then*

$$t_n(\sigma(P), \sigma(Q)) = \sigma(t_n(P, Q)).$$

Definition 15 (**Reduced Tate-Lichtenbaum Pairing**). *Let k be the embedding degree, i.e., the smallest positive integer such that $n \mid (q^k - 1)$. Then the reduced Tate-Lichtenbaum pairing is defined by*

$$\hat{t}_n(P, Q) = t_n(P, Q)^{(q^k-1)/n},$$

which maps into the group of n-th roots of unity $\mu_n \subseteq \mathbb{F}_{q^k}^*$.

This final exponentiation ensures that the pairing value lies in μ_n and uniquely represents the coset of $t_n(P, Q)$ modulo n-th powers.

Chapter 3
ECDH and ECDLP

3.1 Diffie-Hellman Key Exchange on Elliptic Curves

Elliptic curves play a prominent role in modern cryptographic systems, with one of their earliest and simplest applications being the **Diffie-Hellman key exchange protocol**. This protocol allows two parties to establish a shared secret over an insecure channel, such that an eavesdropper cannot feasibly determine the secret. The security relies on the hardness of the *discrete logarithm problem* in a suitably chosen group.

3.1.1 Classical Diffie-Hellman Protocol

The original Diffie-Hellman protocol, proposed by Whitfield Diffie and Martin Hellman in the 1970s, operates in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ for a large prime p. The setup consists of:

- A large prime number p such that $p-1$ has at least one large prime factor (to avoid attacks by Pohling-Hellman reduction, (see (4))).
- A generator $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ of the multiplicative group.

The key exchange proceeds as follows:

1. Alice and Bob each pick secret integers $a, b \in (1, p-1)$ respectively.
2. They compute their public keys: $A = g^a \mod p$ and $B = g^b \mod p$.
3. They exchange A and B over a public channel.
4. Each party computes the shared secret: $S = B^a = A^b = g^{ab} \mod p$.

3.1.2 Generalization to Other Groups

The protocol can be generalized to any cyclic group $G = \langle g \rangle$ of known order. The security hinges on the computational difficulty of the following:

Definition 16 (Discrete Logarithm Problem)**.** *Let G be a cyclic group generated by g. Given an element $A \in G$, the* discrete logarithm *of A with respect to g, denoted $\log_g(A)$, is the unique integer $x \in \{0, 1, \ldots, |G| - 1\}$ such that $g^x = A$.*

If an eavesdropper can compute $\log_g(A)$ or $\log_g(B)$, they can recover the shared secret. Hence, the protocol's security relies on the intractability of computing discrete logarithms in G.

3.1.3 Elliptic Curve Diffie-Hellman (ECDH)

In the 1980s, Miller and Koblitz proposed using elliptic curve groups in place of $(\mathbb{Z}/p\mathbb{Z})^\times$, leading to what we now call **Elliptic Curve Diffie-Hellman** (ECDH).

Let E be an elliptic curve defined over a finite field $\mathbb{F}_p$, such that the number of rational points $\#E(\mathbb{F}_p)$ is a large prime (in practice, a small cofactor is often tolerated). Let $P \in E(\mathbb{F}_p)$ be a generator of the group.

The protocol proceeds as follows:

- **Public Parameters:**
  - A large prime p (typically with $\log_2 p \approx 256$).
  - An elliptic curve $E/\mathbb{F}_p$ such that $\#E(\mathbb{F}_p)$ is prime.
  - A generator point $P \in E(\mathbb{F}_p)$.
- **Key Exchange:**
  1. Alice chooses a secret integer a, computes $A = [a]P$.
  2. Bob chooses a secret integer b, computes $B = [b]P$.
  3. They exchange A and B over a public channel.
  4. Alice computes $[a]B$, and Bob computes $[b]A$; both equal the shared secret $[ab]P$.

This setup is shown in the following table:

Alice	**Bob**
Pick $a \in \mathbb{Z}_{\#E(\mathbb{F}_p)}$	Pick $b \in \mathbb{Z}_{\#E(\mathbb{F}_p)}$
Compute $A = [a]P$	Compute $B = [b]P$
Send A to Bob	Send B to Alice
Compute $S = [a]B$	Compute $S = [b]A$

3.1.4 Security Considerations

No sub-exponential algorithm is known for computing discrete logarithms in elliptic curve groups over finite fields. This contrasts with $(\mathbb{Z}/p\mathbb{Z})^\times$, where index calculus methods allow for faster attacks. As a result, ECDH achieves equivalent security with significantly smaller parameter sizes (e.g., 256-bit elliptic curve vs 3072-bit multiplicative group).

The strength of the ECDH protocol relies on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP). To date, no efficient classical algorithm is known that solve ECDLP in general elliptic curve groups.

3.2 Index Calculus Method

3.2.1 Introduction

In this section, we explore the **index calculus method**, which is a non-generic algorithm for computing discrete logarithms in finite fields. This leads to discussions of **smooth numbers**, the **Canfield-Erdős-Pomerance theorem**, and two integer factorization techniques: the **Pollard $p-1$ method** ([5]) and the **elliptic curve method** (ECM) ([6]). These methods form the basis for many cryptanalytic attacks and provide insight into the structure of number-theoretic problems.

3.2.2 Overview

The index calculus algorithm is a powerful method to compute discrete logarithms in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. It relies on the idea of representing group elements as products of small primes, known as *smooth numbers*, and reducing the problem to solving linear systems.

3.2.3 Factor Base and Smoothness

Let p be a prime and fix a generator α of $(\mathbb{Z}/p\mathbb{Z})^\times$. Define a *factor base*:

$$\mathcal{P}_B = \{p_i \text{ prime} : p_i \leq B\}$$

where B is a *smoothness bound*. An integer is B-smooth if all its prime factors lie in $\mathcal{P}_B$.

3.2.4 Algorithm Outline

Given $\beta \in \langle \alpha \rangle$, we attempt to find $\log_\alpha \beta$ via the following steps:

1. Choose a bound B and construct $\mathcal{P}_B$.
2. Randomly select exponents e and compute $\alpha^e \beta^{-1} \bmod p$.
3. If the result is B-smooth, factor it and write
$$\alpha^e \beta^{-1} = \prod p_i^{e_i}$$
4. Taking logs yields linear equations:
$$\sum e_i \log_\alpha p_i + \log_\alpha \beta = e$$
5. Collect $b+1$ such relations and solve the resulting system to recover $\log_\alpha \beta$.

3.2.5 Remarks

- The matrix is typically sparse, aiding fast linear algebra.
- If $\log_\alpha \beta$ is not determined uniquely, adding a few more relations usually suffices.
- The method also computes $\log_\alpha p_i$ for primes in $\mathcal{P}_B$, which can be reused.

3.3 Smooth Numbers and Theorem

3.3.1 Smooth Numbers

A positive integer is called y-smooth if all of its prime divisors are $\leq y$. Let $\psi(x, y)$ count the number of y-smooth integers in $[1, x]$. The smoothness probability of a random integer in this range is roughly:
$$\frac{\psi(x, y)}{x}$$

3.3.2 Canfield–Erdős–Pomerance Theorem

Let $u = \frac{\log x}{\log y}$. Then:
$$\frac{\psi(x, x^{1/u})}{x} = u^{-u+o(u)} \quad \text{uniformly as } u, x \to \infty$$

This asymptotic estimate is crucial for choosing the optimal B in index calculus and factorization algorithms.

3.4 Optimizing the Smoothness Bound

3.4.1 Expected Time Complexity

Assume smoothness testing dominates computation. The expected time is:

$$(b+1) \cdot u^u \cdot b \cdot M(\log N)$$

where:

- $b = \pi(B) \sim \frac{B}{\log B}$
- $u = \frac{\log N}{\log B}$
- $M(\log N)$ is cost per trial division

Ignoring log factors, we simplify to:

$$\text{Time} \sim B^2 u^u = N^{2/u} u^u$$

3.4.2 Optimal Choice of B

Minimizing this expression leads to:

$$u = 2\sqrt{\frac{\log N}{\log \log N}}, \quad B = N^{1/u} = L_N[1/2, 1/2]$$

$$L_N[\alpha, c] := \exp\left((c + o(1))(\log N)^\alpha (\log \log N)^{1-\alpha}\right)$$

3.4.3 Final Complexity

The optimized running time becomes:

$$L_N[1/2, 2]$$

3.5 ECDLP Reduction to Finite Fields

One of the earliest and most important applications of bilinear pairings in elliptic curve cryptography is the reduction of the elliptic curve discrete logarithm problem (ECDLP) to the discrete logarithm problem in finite fields. This reduction makes it possible, in certain circumstances, to attack the ECDLP by solving a potentially easier problem in a multiplicative group of a finite field. This idea was pioneered by Menezes, Okamoto, and Vanstone using the Weil pairing, and later refined by Frey and Rück using the reduced Tate-Lichtenbaum pairing.

The general strategy involves a non-degenerate bilinear pairing e defined on a subgroup of $E(\mathbb{F}_q)$ of order n, where $\gcd(n, q) = 1$. Suppose we are given an instance of the ECDLP: given $P, Q = [a]P \in E(\mathbb{F}_q)[n]$, compute the scalar a. By selecting another point $R \in E(\mathbb{F}_q)$ such that $e(P, R) \neq 1$, we can compute the pairing values $z = e(P, R)$ and $e(Q, R) = e([a]P, R) = z^a$. In this way, the discrete logarithm a is revealed through the logarithm base z of the value $e(Q, R)$, now entirely within the multiplicative group of a finite field.

The crucial observation is that the target of the pairing, $\mu_n \subset \mathbb{F}_{q^k}^*$, lies in an extension field of $\mathbb{F}_q$, where k is the smallest positive integer for which $n \mid (q^k - 1)$; this k is called the *embedding degree*. If k is small, then the discrete logarithm problem in $\mathbb{F}_{q^k}^*$ can be solved significantly faster using index calculus techniques than the ECDLP in the elliptic curve group.

This process, often referred to as the **MOV (Menezes–Okamoto–Vanstone)** ([7]) or **FR (Frey–Rück)** ([8]) attack, poses a substantial threat only when the embedding degree is small. In practice, for a given q, one determines the smallest k such that the group $\mu_n \subset \mathbb{F}_{q^k}^*$ contains the image of the pairing. If this k is small, the security of the elliptic curve group is compromised.

Interestingly, the original approach by Menezes et al. using the Weil pairing required finding a point R possibly defined over an extension field of $\mathbb{F}_q$. Frey and Rück improved this by showing that, in the case of the reduced Tate-Lichtenbaum pairing, it suffices to take $R \in E(\mathbb{F}_{q^k})$, where k is the embedding degree. Later, Balasubramanian and Koblitz demonstrated that even when using the Weil pairing, one can usually stay within the same extension field $\mathbb{F}_{q^k}$, thereby making the reduction more practical.

Theorem 8. *Let E be an elliptic curve over $\mathbb{F}_q$ and let r be a prime dividing $\#E(\mathbb{F}_q)$. Suppose $r \nmid (q - 1)$ and $\gcd(r, q) = 1$. Then $E[r] \subset E(\mathbb{F}_{q^k})$ if and only if $r \mid (q^k - 1)$.*

This theorem justifies the use of pairings for reducing the ECDLP to a finite field DLP

when the embedding degree k is small. So, it is important for certain special classes of elliptic curves. In particular, supersingular curves always have small embedding degrees, which makes them vulnerable to this form of reduction. For this reason, supersingular curves are often avoided in protocols requiring long-term security against discrete logarithm attacks, unless the system is designed to exploit pairings directly, such as in pairing-based cryptography (or in Isogeny-based cryptography, which is not based on the discrete logarithm problem).

3.6 The MOV/Frey–Rück Attack on the ECDLP

3.6.1 The Attack

Suppose E is an elliptic curve defined over the finite field $\mathbb{F}_q$ and $P \in E(\mathbb{F}_q)$ is a point of prime order r, where r is coprime to q. Let Q be another point in $E(\mathbb{F}_q)$ which is a multiple of P, i.e., $Q = [\lambda]P$ for some unknown scalar λ. The goal is to recover λ, i.e., solve the ECDLP: find λ such that $Q = [\lambda]P$.

Algorithm 1 MOV/Frey–Rück Attack

Require: Points $P, Q \in E(\mathbb{F}_q)$ of prime order r, such that $Q = [\lambda]P$ for unknown λ.
Ensure: The discrete logarithm λ such that $Q = [\lambda]P$.
1: Construct the extension field $\mathbb{F}_{q^k}$ such that $r \mid (q^k - 1)$.
2: Find a point $S \in E(\mathbb{F}_{q^k})$ such that $e(P, S) \neq 1$.
3: Compute $\zeta_1 \leftarrow e(P, S)$.
4: Compute $\zeta_2 \leftarrow e(Q, S)$.
5: Use index-calculus (or any DLP algorithm) in $\mathbb{F}_{q^k}^*$ to find λ such that $\zeta_1^\lambda = \zeta_2$.
6: **return** λ.

- **Step 1: Embedding into a Finite Field.** The embedding degree k is the smallest positive integer such that $r \mid (q^k - 1)$. This ensures that the r-torsion subgroup of E can be mapped injectively into the multiplicative group $\mathbb{F}_{q^k}^*$ using a bilinear pairing.

- **Step 2: Pairing Setup.** We choose a point $S \in E(\mathbb{F}_{q^k})$ such that the pairing $e(P, S)$ is non-trivial (i.e., not equal to 1). In practice, a random S will satisfy this condition with overwhelming probability, so this step is usually straightforward.

- **Step 3-4: Compute Pairings.** The Weil or Tate pairing is evaluated for the pairs (P, S) and (Q, S), giving us $\zeta_1 = e(P, S)$ and $\zeta_2 = e(Q, S) = e([\lambda]P, S) = e(P, S)^\lambda = \zeta_1^\lambda$.

- **Step 5: Solve DLP in Finite Field.** We now need to solve the equation $\zeta_1^\lambda = \zeta_2$ in $\mathbb{F}_{q^k}^*$. This is a standard discrete logarithm problem in a finite field, for which subexponential-time index-calculus algorithms exist.

3.6.2 Practical Considerations

- The attack's efficiency hinges on the size of the embedding degree k. While solving the DLP in $\mathbb{F}_{q^k}^*$ is theoretically faster due to subexponential algorithms, the attack is only practical if k is small.

- A crucial observation made by Menezes, Okamoto, and Vanstone is that *supersingular* elliptic curves tend to have small embedding degrees (often $k \leq 6$), making them more vulnerable to this type of attack.

- However, there exist ordinary (non-supersingular) curves that are also susceptible. For instance, some curves over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q - 1$ may have $r \mid (q-1)$, implying that $k = 1$ and no extension field is even needed.

Remark 3. *When designing secure elliptic curve cryptographic systems, one must choose curves with large embedding degrees to avoid such attacks, effectively ruling out vulnerable supersingular and specific ordinary curves (see ([9])).*

Chapter 4
Monodromy Leak from Montgomery Ladder and Cubical Arithmetic

4.1 Montgomery Ladder

The details of Montgomery Ladder can be found in ([10])

4.1.1 Introduction to Montogomery Ladder

The Montgomery ladder provides an elegant and efficient algorithm to compute scalar multiples of points on a wide family of elliptic curves. It operates through a recurrence involving sequences $(X_1, X_2, \ldots)$ and $(Z_1, Z_2, \ldots)$, which are constructed from an initial point (X_1, Z_1) and a curve parameter A. The method works on Montgomery curves defined by the equation

$$By^2 = x^3 + Ax^2 + x,$$

and enables one to compute the scalar multiplication nP with high speed and regularity.

Given the initial point (X_1, Z_1), the recursive sequences are defined by the relations

$$X_{2n} = (X_n^2 - Z_n^2)^2, \quad Z_{2n} = 4X_nZ_n(X_n^2 + AX_nZ_n + Z_n^2),$$

$$X_{2n+1} = \frac{4(X_nX_{n+1} - Z_nZ_{n+1})^2}{Z_1}, \quad Z_{2n+1} = \frac{4(X_nZ_{n+1} - Z_nX_{n+1})^2}{X_1},$$

for all $n \geq 1$. The projective coordinates (X_n, Z_n) represent the multiple nP as a point on the curve via the ratio X_n/Z_n, which corresponds to the affine x-coordinate of the point. The associated y-coordinate, up to sign, can also be recovered if needed using the curve equation.

More precisely, under mild assumptions on the parameters and the initial point, the expression

$$\left(\frac{X_n}{Z_n}, \pm\sqrt{\frac{1}{B}\left(\frac{X_n^3}{Z_n^3} + A\frac{X_n^2}{Z_n^2} + \frac{X_n}{Z_n}\right)}\right)$$

gives the affine form of the scalar multiple nP. The ladder structure ensures that at every

iteration, two points are maintained: one corresponding to kP and the other to $(k+1)P$. This structure allows for a uniform, constant-time algorithm that is particularly beneficial for cryptographic applications where side-channel resistance is crucial.

A more optimized version of the Montgomery ladder further reduces the number of operations. By defining $A' = \frac{A+2}{4}$, the ladder can be executed using only 11 field multiplications per bit of the scalar n. The optimized recurrence relations are:

$$X_{2n} = (X_n - Z_n)^2 (X_n + Z_n)^2,$$

$$Z_{2n} = \left[(X_n + Z_n)^2 - (X_n - Z_n)^2\right] \left[(X_n + Z_n)^2 + A' \cdot \left((X_n + Z_n)^2 - (X_n - Z_n)^2\right)\right],$$

$$X_{2n+1} = \left[(X_n - Z_n)(X_{n+1} + Z_{n+1}) + (X_n + Z_n)(X_{n+1} - Z_{n+1})\right]^2 Z_1,$$

$$Z_{2n+1} = \left[(X_n - Z_n)(X_{n+1} + Z_{n+1}) - (X_n + Z_n)(X_{n+1} - Z_{n+1})\right]^2 X_1.$$

4.1.2 The Montgomery Ladder Step

In Projective coordinate, the x-coordinates of $2P_2$ and $P_3 + P_2$ can be computed as $x(2P_2) = X_4/Z_4$ and $x(P_3 + P_2) = X_5/Z_5$, respectively. These values were derived from the inputs $x(P_2) = X_2/Z_2$, $x(P_3) = X_3/Z_3$, and $x(P_3 - P_2) = X_1/Z_1$, where it is assumed that $X_1 \neq 0$ and $Z_1 \neq 0$.

The Montgomery ladder iteratively computes X_n starting from the base values X_0 and X_1, using one point doubling and one differential addition for each bit of the scalar n. In this optimized version, the doubling and differential addition are now combined into a single operation per iteration, which highlights the efficiency gains achieved by merging the two steps.

To formalize this combined operation, we define a function step0 which, for a fixed pair (X_1, Z_1), takes the inputs (X_2, Z_2, X_3, Z_3) and returns the outputs (X_4, Z_4, X_5, Z_5), defined as follows:

$$X_4 = (X_2^2 - Z_2^2)^2, \quad Z_4 = 4X_2Z_2(X_2^2 + AX_2Z_2 + Z_2^2),$$

$$X_5 = \frac{4(X_2X_3 - Z_2Z_3)^2}{2Z_1}, \quad Z_5 = \frac{4(X_2Z_3 - Z_2X_3)^2}{2X_1}.$$

Note that in this context, Z_1 is fixed and assumed to be 1 for optimization purposes, simplifying the divisions.

We also define a companion function step1 that simply reverses the roles of the inputs

for compatibility with bit-serial scalar multiplication. Specifically,

$$\mathsf{step1}(X_3, Z_3, X_2, Z_2) = (X_5, Z_5, X_4, Z_4),$$

ensuring that the ladder remains consistent when updating across iterations.

4.1.3 Constant-Time Ladders

In elliptic curve cryptography, a common operation is computing the scalar multiple nP, where n is a secret scalar in the range $\{0, 1, \ldots, 2^{256} - 1\}$. The traditional Montgomery ladder, though efficient, reveals timing information that can potentially leak the position of the most significant bit of n, since the number of iterations depends on that position. This variation in runtime opens up the possibility of side-channel attacks based on timing analysis.

To mitigate this issue, one approach is to ensure that the scalar n always has a fixed top bit, which can be achieved by adding a suitable multiple of the order of P. A more general way is to adopt a version of the Montgomery ladder where the number of steps is predetermined and does not depend on the bit-length of n.

Crucially, this variant of the ladder must allow computation to begin from the pair $(0P, 1P)$ instead of the usual $(1P, 2P)$, and it must maintain the correctness of the representation of the scalar multiple throughout all ladder steps. In this setup, it is essential that each ladder step follows an identical and constant sequence of operations, regardless of the value of each bit in n. Any branching or conditional behavior based on secret data must be avoided to maintain constant-time execution and resist timing attacks.

A key component of this constant-time behavior is the conditional swap operation, denoted $\mathtt{cswap}_b$. For a bit $b \in \{0, 1\}$, the operation $\mathtt{cswap}_b(X_2, Z_2, X_3, Z_3)$ performs either the identity operation when $b = 0$, or swaps the pairs (X_2, Z_2) and (X_3, Z_3) when $b = 1$. To implement this without branching, one uses arithmetic expressions such as

$$\begin{aligned}\mathtt{cswap}_b(X_2, Z_2, X_3, Z_3) = (&b(X_3 - X_2) + X_2,\ b(Z_3 - Z_2) + Z_2,\\ &(1-b)(X_3 - X_2) + X_2,\ (1-b)(Z_3 - Z_2) + Z_2),\end{aligned}$$

or other mathematically equivalent expressions that compute the same effect in constant time.

When multiple ladder steps are composed, a sequence of operations such as `cswap`–step–`cswap`–`cswap`–step–`cswap` naturally arises. It is possible to optimize this by merging adjacent swaps: for instance, two successive conditional swaps can be reduced to a single

swap governed by the XOR of the two controlling bits. As a result, a full Montgomery ladder with many steps can be implemented efficiently using a repeating pattern of `cswap`–step–`cswap`–step–`cswap` and so on, maintaining both correctness and constant-time execution throughout.

4.1.4 Completeness of the Ladder

In Montgomery ladder computations, the final step involves calculating $x(nP)$ as the ratio X_n/Z_n. Typically, when the scalar k is finite, this ratio is computed as $X_n Z_n^{\#k-2}$, where $\#k$ denotes the size of the field. However, when $Z_n = 0$, this computation outputs 0, whereas the correct value might be the point at infinity ∞. This discrepancy becomes problematic, especially when the Montgomery ladder receives $x(P) = X_1/Z_1$ as an input where either $X_1 = 0$ or $Z_1 = 0$, i.e., when $x(P) = 0$ or ∞.

When the ladder is allowed to accept 0 or ∞ as input, it yields $X_n Z_n = 0$ for all n. Nonetheless, it does not guarantee that $x(nP) = X_n/Z_n$. In fact, one may encounter situations where $X_n/Z_n = \infty$ while $x(nP) = 0$, or even where both $X_n = 0$ and $Z_n = 0$, making the output ambiguous.

To resolve this ambiguity, we define a modified x-coordinate function, denoted $x_0 : M(k) \to k$, where $x_0(x, y) = x$ for any affine point, and $x_0(\infty) = 0$. This function essentially treats the point at infinity ∞ as 0 in terms of its x-coordinate. By adopting $x_0(nP)$ as the output of the ladder instead of $x(nP)$, we merge the cases of 0 and ∞ and thus eliminate the need for case-by-case distinctions. Furthermore, using $x_0(P)$ instead of $x(P)$ as the input also becomes safe, because both inputs 0 and ∞ yield the same outputs under this formulation. This idea of utilizing the function x_0 in the Montgomery ladder context originates from (11).

Theorem 9. *Fix a field k not of characteristic 2. Fix $A, B \in k$ with $B(A^2 - 4) \neq 0$. Define M as the Montgomery curve*

$$By^2 = x^3 + Ax^2 + x.$$

Define $x_0 : M(k) \to k$ as follows: $x_0(x, y) = x$; $x_0(\infty) = 0$.

Let P be an element of $M(k)$. Let X_1, Z_1 be elements of k such that $Z_1 \neq 0$ and $x_0(P) = X_1/Z_1$. Let c be a nonnegative integer. Let $n_0, \ldots, n_{c-1}$ be elements of $\{0, 1\}$. Define

$$n = 2^{c-1} n_{c-1} + 2^{c-2} n_{c-2} + \cdots + 2^0 n_0.$$

Define

$$(X, Z, X', Z') = step_{n_0} step_{n_1} \cdots step_{n_{c-1}}(1, 0, X_1, Z_1).$$

If $Z = 0$, then $x_0(nP) = 0$; otherwise $x_0(nP) = X/Z$.

4.2 Banegas-Gilchrist-Smith Exponent

4.2.1 Montgomery Arithmetic

Most isogeny-based cryptographic systems, such as CSIDH, operate on elliptic curves given in the Montgomery form. These curves are typically expressed as

$$E_A : y^2 = x(x^2 + Ax + 1),$$

where the parameter A is referred to as the Montgomery coefficient. The group law on these curves is denoted by $\oplus$ and $\ominus$, representing addition and subtraction of points, respectively. Given any three among the four values $x(P), x(Q), x(P \oplus Q), x(P \ominus Q)$, the fourth can be uniquely determined. This property allows us to define a differential addition map

$$\text{xADD} : (x(P), x(Q), x(P \ominus Q)) \mapsto x(P \oplus Q),$$

as well as a pseudo-doubling map

$$\text{xDBL}_A : x(P) \mapsto x([2]P).$$

In practice, computations on Montgomery curves are usually performed using projective coordinates. Given points P and Q on E_A, we write their x-coordinates in projective form as $(X_P : Z_P) = x(P)$, $(X_Q : Z_Q) = x(Q)$, $(X_\oplus : Z_\oplus) = x(P \oplus Q)$, and $(X_\ominus : Z_\ominus) = x(P \ominus Q)$. Recall that the affine x-coordinate corresponding to a projective point $(X : Y : Z)$ is given by $(X : Z)$ when $Z \neq 0$, and defined to be $(1 : 0)$ when $Z = 0$.

Using these projective representations, the differential addition map xADD is computed via the following relations:

$$X_\oplus = Z_\ominus \cdot (U + V)^2,$$
$$Z_\oplus = X_\ominus \cdot (U - V)^2,$$

where

$$U = (X_P - Z_P)(X_Q + Z_Q),$$
$$V = (X_P + Z_P)(X_Q - Z_Q).$$

These formulas are homogeneous and hence compatible with projective equivalence. Specifi-

cally, replacing (X_P, Z_P) and (X_Q, Z_Q) with $(\lambda_P X_P, \lambda_P Z_P)$ and $(\lambda_Q X_Q, \lambda_Q Z_Q)$, respectively, results in $(X_\oplus, Z_\oplus)$ being scaled by a factor of $(\lambda_P \lambda_Q)^2$, preserving their projective equivalence class.

Similarly, the pseudo-doubling operation xDBL_A, which maps $x(P) \mapsto x([2]P)$, can also be computed in projective coordinates. Writing $(X_{[2]P} : Y_{[2]P} : Z_{[2]P})$ for the projective coordinates of the doubled point, the corresponding formulas are:

$$\begin{aligned} X_{[2]P} &= R \cdot S, \\ Z_{[2]P} &= T \cdot (S + \tfrac{A+2}{4} T), \end{aligned}$$

where the intermediate variables are defined as

$$\begin{aligned} R &= (X_P + Z_P)^2, \\ S &= (X_P - Z_P)^2, \\ T &= 4 X_P Z_P. \end{aligned}$$

These expressions also behave well under projective scaling. That is, if we replace (X_P, Z_P) with $(\lambda_P X_P, \lambda_P Z_P)$, then the resulting coordinates $(X_{[2]P}, Z_{[2]P})$ are scaled by λ_P^4, ensuring projective consistency.

These operations are the foundation for the Montgomery ladder algorithm, which computes scalar multiplications of the form $(m, x(P)) \mapsto x([m]P)$ efficiently and securely, using only x-coordinate arithmetic and without the need for full point recovery.

4.2.2 Division Polynomials

For a non-negative integer m, the m-th division polynomial $\psi_{E,m}$ associated with an elliptic curve E plays a crucial role in identifying torsion points. Specifically, we have:

$$\psi_{E,m}(x(P), y(P)) = 0 \quad \Longleftrightarrow \quad P \in E[m] \setminus \{\mathcal{O}\},$$

where $E[m]$ denotes the group of m-torsion points on E, and $\mathcal{O}$ is the point at infinity.

For a Montgomery curve of the form

$$E : y^2 = x(x^2 + Ax + 1),$$

the first few division polynomials take the following explicit forms:

$$\psi_{E,0} = 0, \quad \psi_{E,1} = 1, \quad \psi_{E,2} = 2y,$$

and for higher degrees:

$$\psi_{E,3} = 3x^4 + 4Ax^3 + 6x^2 - 1,$$

$$\psi_{E,4} = 4y(x^2 - 1)(x^4 + 2Ax^3 + 6x^2 + 2Ax + 1).$$

For general m, the division polynomials obey standard recurrence relations. For even indices $2m$ with $m \geq 3$, the recurrence is given by:

$$\psi_{E,2m} = \frac{\psi_{E,m-1}^2 \psi_{E,m} \psi_{E,m+2} - \psi_{E,m-2} \psi_{E,m} \psi_{E,m+1}^2}{\psi_{E,2}}.$$

For odd indices $2m + 1$ with $m \geq 2$, the recurrence is:

$$\psi_{E,2m+1} = \psi_{E,m}^3 \psi_{E,m+2} - \psi_{E,m-1} \psi_{E,m+1}^3.$$

It is important to observe that for any $m > 0$, the square $\psi_{E,m}^2$ lies in the polynomial ring $\mathbb{F}_p[A][x]$. In particular, the division polynomial $\psi_{E,m}$ itself lies in $\mathbb{F}_p[A][x]$ whenever m is odd.

Lemma 16. *Let p be a prime. The p-th division polynomial of a Montgomery curve satisfies*

$$\psi_{E,p}(x) = \left(\tilde{\psi}_{E,p}(x)\right)^p,$$

where $\tilde{\psi}_{E,p}(x) \in \mathbb{F}_p[A][x]$ is a polynomial of degree $\frac{p-1}{2}$ when the curve E is ordinary, and is equal to ± 1 when E is supersingular. In particular, the identity

$$\psi_{E,p}^2(x) = 1$$

holds if and only if the curve E is supersingular.

4.2.3 The Exponent

Scalar multiplication on an elliptic curve can be expressed using rational functions involving the so-called division polynomials (see (12)). For a point (x, y) on an elliptic curve E, the multiplication-by-m map can be written as:

$$[m](x, y) = \left(\frac{\phi_{E,m}(x)}{\psi_{E,m}^2(x)}, \frac{\omega_{E,m}(x, y)}{\psi_{E,m}^3(x)}\right),$$

where the polynomials involved are defined as follows:

$$\phi_{E,m}(x) := x\psi_{E,m}^2(x) - \psi_{E,m+1}(x)\psi_{E,m-1}(x),$$

$$\omega_{E,m}(x,y) := (4y)^{-1}\left(\psi_{E,m+2}(x)\psi_{E,m-1}^2(x) - \psi_{E,m-2}(x)\psi_{E,m+1}^2(x)\right).$$

Although the full expression for $\omega_{E,m}(x,y)$ is included here, it will not be needed for the purposes that follow.

In Montgomery form, we begin with a point $(u : v : 1) \in E_A$. If we apply the Montgomery ladder algorithm to compute the scalar multiple $[p](u : v : 1)$, then from the above relation, we know that the resulting projective coordinates (X, Z) must be proportional to $(\phi_{E,p}(u), \psi_{E,p}^2(u))$, up to a common projective scaling factor. This factor can be explicitly computed and, in many contexts, can also be normalized or removed. The following proposition makes this relationship precise for general values of m and $\mathrm{len}(m) := \lfloor \log_2 m \rfloor + 1$.

Proposition 1. *On input A, m, and $(x, 1)$, Algorithm 1 (the Montgomery ladder) returns*

$$(X_m, Z_m) = \left(\phi_{E,m}(x) \cdot f_m(x),\ \psi_{E,m}^2(x) \cdot f_m(x)\right)$$

where

$$f_m(x) := (4x)^{m(2^{\mathrm{len}(m)} - m)}.$$

Proof. The proof is given in Proposition 2 in ([13]) □

4.3 Overview of Cubical Arithmetic

In this section, we discuss cubical arithmetic, which modifies elliptic curve arithmetic by preserving extra information contained in affine representatives of projective points. Specifically, it uses a chosen coordinate function Z to track projective scaling. For a positive integer n, the coordinate Z_n is chosen as a non-trivial section of the line bundle associated with the divisor $n(0_E)$, and cubical points built using Z_n are said to be of level-n. In practice, we often set $Z_n = Z_1^n$, and for this part, we focus on the case $n = 1$. The details are described in ([14])).

4.3.1 Cubical Points of Level 1

Let $E/\mathbb{F}_q$ be an elliptic curve defined by the Weierstrass equation

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

We choose a projective coordinate Z_1, which is a nonzero section vanishing to order 1 at the identity point 0_E. This choice defines the notion of a level-1 cubical point.

Definition 17. *Let $P = (x_P, y_P) \in E(\mathbb{F}_q) \setminus \{0_E\}$. A* level-1 cubical point $\widetilde{P}$ *above P is a pair $(P, Z_1(\widetilde{P}))$, where $Z_1(\widetilde{P}) \in \mathbb{F}_q^*$ encodes a projective scaling.*

Remark 4. *At the identity 0_E, the coordinate Z_1 vanishes, so we define a cubical point above 0_E using the ratio $Z_1/(x/y)$, which is nonvanishing at 0_E. We then define $\widetilde{0}_E = (0_E, 1)$ by normalizing this expression.*

4.3.2 Cubical Arithmetic

For points $P_1, P_2 \in E$, define the function g_{P_1,P_2} with divisor:

$$(-P_1 - P_2) + (0_E) - (-P_1) - (-P_2).$$

We define the cubical function:

$$\mathrm{cub}_1(P_1, P_2, P_3) := \frac{g_{P_1,P_2}(P_3)}{g_{P_1,P_2}(0_E)}. \tag{4.1}$$

This quantity is well-defined regardless of the choice of g_{P_1,P_2}, and it can also be expressed as:

$$\mathrm{cub}_1(P_1, P_2, P_3) = \frac{x(P_1 + P_2) - x(P_3)}{\ell_{P_1,P_2}(-P_3)},$$

where ℓ_{P_1,P_2} is the line through P_1 and P_2.

Definition 18. *Let $P_1, P_2, P_3 \in E$, and construct the cube of 8 points:*

$$0_E, P_1, P_2, P_3, P_1 + P_2, P_1 + P_3, P_2 + P_3, P_1 + P_2 + P_3.$$

We say that their cubical lifts $\widetilde{P}_i$ form a cubical cube *if:*

$$\mathrm{cub}_1(P_1, P_2, P_3) = \frac{Z_1(\widetilde{P}_1 + \widetilde{P}_2 + \widetilde{P}_3) \cdot Z_1(\widetilde{P}_1)Z_1(\widetilde{P}_2)Z_1(\widetilde{P}_3)}{Z_1(\widetilde{0}_E)Z_1(\widetilde{P}_1 + \widetilde{P}_2)Z_1(\widetilde{P}_1 + \widetilde{P}_3)Z_1(\widetilde{P}_2 + \widetilde{P}_3)}. \tag{4.2}$$

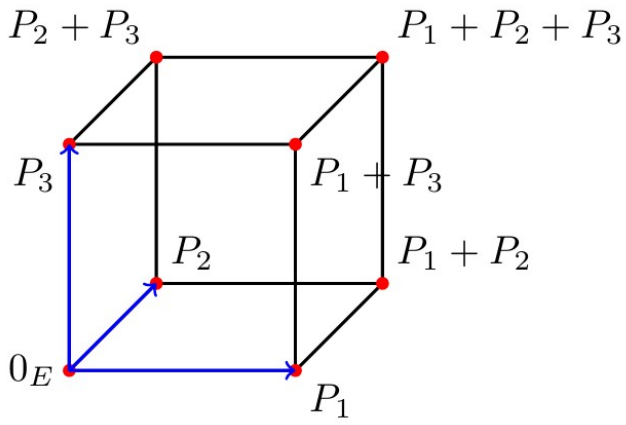


Figure 4.1: A cubical cube of points in the elliptic curve group law.

Remark 5. *Strictly speaking, Equation (4) lacks full definition due to the fact that* $Z_1(\widetilde{0}_E) = 0$*, and we evaluate* g_{P_1,P_2} *at this point. Nonetheless, the equation becomes meaningful once we multiply both sides by a uniformizer, such as* x/y*. As previously mentioned, we normalize* $\widetilde{0}_E$ *so that* $(Z_1/(x/y))(\widetilde{0}_E) = 1$*.*

We note that Z_1 is a level-1 cubical function with a simple zero at the identity 0_E, and x/y similarly has a simple zero at this point. Hence, their ratio yields a cubical function that remains non-vanishing and well-defined at 0_E.

From the perspective of line bundle rigidifications, the selection of $\widetilde{0}_E$ essentially fixes a rigidification, allowing us to interpret Z as a local section $\varphi_Z \in \mathcal{O}_{E,0_E}$, and hence the quotient $\varphi_Z/(x/y) \in \mathcal{O}^*_{E,0_E}$ becomes well-defined. The normalization condition then ensures this value at 0_E is exactly one.

The central and powerful feature provides a mechanism to determine $Z_1(\widetilde{P}_1 + P_2 + P_3)$ from the known values at the seven other vertices of a cube. In essence, given any seven vertices of a cubical configuration, we can compute the eighth.

Of particular importance in this article is the cube formed by choosing $(P_1, P_2, P_3) = (P, Q, -Q)$. This specific arrangement gives rise to a cube with vertices at:

$$0_E, \quad P, \quad Q, \quad -Q, \quad P+Q, \quad P-Q, \quad 0_E, \quad P.$$

By applying Equation (4), we derive a key identity involving the cubical values at these points, leading directly to the following result.

Lemma 17. *Given* $Z_1(\widetilde{P})$*,* $Z_1(\widetilde{Q})$*, and the difference* $x(Q) - x(P)$*, the above cube structure*

yields the following cubical differential addition formula:

$$Z_1(\widetilde{P}+Q)\cdot Z_1(\widetilde{P}-Q) = Z_1(\widetilde{P})^2\cdot Z_1(\widetilde{Q})^2\cdot(x(Q)-x(P)).$$

Specializing further to the case $P=Q$, we obtain the cubical doubling formula:

$$Z_1(2\widetilde{P}) = Z_1(\widetilde{P})^4\cdot 2y(P).$$

Proof. To establish the cubical differential addition, we appeal to Definition 2, which yields:

$$\frac{Z_1(\widetilde{P}+Q)Z_1(\widetilde{P}-Q)Z_1(\widetilde{0}_E)^2}{Z_1(\widetilde{P})^2Z_1(\widetilde{Q})Z_1(-\widetilde{Q})} = \frac{g_{Q,-Q}(0_E)}{g_{Q,-Q}(P)}.$$

The equation follows directly from the fact that $Z_1(-\widetilde{Q}) = -Z_1(\widetilde{Q})$, and choosing the rational function $g_{Q,-Q} = 1/(x-x(Q))$, which is normalized at infinity such that $(g_{Q,-Q}/(x/y)^2)(0_E)=1$. The normalization of $\widetilde{0}_E$ ensures that $(Z_1^2/g_{Q,-Q})(\widetilde{0}_E)=1$.

For the doubling case, an extra $Z_1(\widetilde{0}_E)$ appears in the numerator, necessitating the computation of the inverse of $Z(\widetilde{0}_E)\cdot g_{P,-P}(P)$. Taking $g_{P,-P} = 1/(x-x(P))$, which is also normalized at 0_E, we define $g' = t_P^* g_{P,-P}$, meaning $g'(R) = g_{P,-P}(R+P)$. Hence,

$$Z(\widetilde{0}_E)\cdot g_{P,-P}(P) = (g'\cdot x/y)(0_E).$$

Analyzing the addition law gives:

$$\frac{1}{g'\cdot x/y} = \frac{(y-y(P))^2}{(x-x(P))^2 - x - 2x(P)}/(x/y),$$

leading to the evaluation:

$$(g'\cdot x/y)(0_E)^{-1} = -2y(P).$$

The result then follows from the fact that $Z_1(-\widetilde{P}) = -Z_1(\widetilde{P})$. □

4.3.3 Properties

Theorem 10 (Cubical Arithmetic Identities)**.** *Let $P_1, P_2, P_3, P_4 \in E$ be points on an elliptic curve E. Then the following properties hold for the cubical function* cub_1*:*

1. ***Neutral Element:***

$$\mathrm{cub}_1(0_E, 0_E, 0_E) = 1.$$

2. ***Symmetry:*** *For any permutation $\sigma \in S_3$ (the symmetric group on 3 elements),*

$$\mathrm{cub}_1(\sigma(P_1, P_2, P_3)) = \mathrm{cub}_1(P_1, P_2, P_3).$$

3. ***Associativity:*** *The following multiplicative identity holds:*

$$\mathrm{cub}_1(P_1 + P_2, P_3, P_4) \cdot \mathrm{cub}_1(P_1, P_2, P_4) = \mathrm{cub}_1(P_1, P_2 + P_3, P_4) \cdot \mathrm{cub}_1(P_2, P_3, P_4).$$

4. ***Anti-symmetry:***

$$\mathrm{cub}_1(P_1, P_2, -P_1 - P_2) = -1.$$

Proof. Let g_{P_1,P_2} be a rational function on E with divisor

$$\mathrm{div}(g_{P_1,P_2}) = (-P_1 - P_2) + (0_E) - (-P_1) - (-P_2),$$

and suppose g_{P_1,P_2} is normalized so that $\dfrac{g_{P_1,P_2}}{x/y}(0_E) = 1$. Then, using the definition of the cubical function from Equation (3),

$$\mathrm{cub}_1(P_1, P_2, P_3) = g_{P_1,P_2}(P_3),$$

and this identity makes it straightforward to derive each of the properties:

- **Neutrality:** Setting $P_1 = P_2 = P_3 = 0_E$, we have $g_{0_E,0_E}(0_E) = 1$ by normalization, hence $\mathrm{cub}_1(0_E, 0_E, 0_E) = 1$.
- **Commutativity:** The symmetry in the arguments arises because, up to projective equivalence and divisor class, the function $g_{P_1,P_2}(P_3)$ remains invariant under permutation of its inputs. Thus:

  $$g_{P_1,P_2}(P_3) = g_{P_2,P_3}(P_1) = g_{P_3,P_1}(P_2),$$

  which implies the cubical function is invariant under any permutation in S_3.
- **Associativity:** This follows from the identity:

  $$g_{P_1+P_2,P_3} \cdot g_{P_1,P_2} = g_{P_1,P_2+P_3} \cdot g_{P_2,P_3},$$

  which holds since both sides define rational functions with identical divisors and the same normalization at 0_E. Evaluating both sides at P_4 yields the associativity identity.

- **Anti-symmetry:** When evaluated at $-P_1 - P_2$, we find:

$$g_{P_1,P_2}(-P_1 - P_2) = -1,$$

which directly gives $\mathrm{cub}_1(P_1, P_2, -P_1 - P_2) = -1$.

The proof for commutativity and anti-symmetry, while deduced from the function-theoretic identities, also aligns with more abstract results involving symmetric biextensions ([15]) and cubical torsor structures on abelian varieties ([16]). The full exposition can be found in ([17]). □

Corollary 5. *Let $P_1, \ldots, P_m \in E$, and choose cubical points $\widetilde{P}_i$, $\widetilde{P}_i + \widetilde{P}_j$ for all $1 \leq i, j \leq m$. Then, for $n_1, \ldots, n_m \in \mathbb{Z}$, we are free to compute a cubical point above the elliptic point $\sum n_i P_i$ using any choice of cubes and inversions: we always obtain the same cubical point $\widetilde{\sum n_i P_i}$.*

Note: This result tells us that, regardless of how we combine cubes and use inversions to compute a linear combination of elliptic points, the resulting cubical point is uniquely determined. In particular, the cubical representative $\widetilde{\sum n_i P_i}$ does not depend on the order in which we perform the additions, nor on the intermediate cubical points we choose. Because of this uniqueness, it is conventional to denote the cubical point simply as $\sum n_i \widetilde{P}_i$.

Proof. In the special case where all $n_i \geq 0$ and no inversions are needed, the result follows directly from the associativity and commutativity properties of cubical arithmetic. In the general case, where n_i may be negative, we must account for inversions. Here, anti-symmetry comes into play.

Specifically, suppose we have a cube with third vertex $P_3 = -P_1 - P_2$. Then by the anti-symmetry property and the formula, we obtain the following identity:

$$\frac{Z_1(\widetilde{P}_1)Z_1(\widetilde{P}_2)Z_1(\widetilde{-P_1 - P_2})}{Z_1(-\widetilde{P}_1)Z_1(-\widetilde{P}_2)Z_1(\widetilde{P}_1 + P_2)} = \mathrm{cub}_1(P_1, P_2, -P_1 - P_2) = -1,$$

and the inversion relation $Z_1(-\widetilde{P}) = -Z_1(\widetilde{P})$ confirms the expression is consistent with anti-symmetry. □

Remark 6. *Even though $\sum n_i \widetilde{P}_i$ is uniquely defined in a cubical sense, it still depends on the specific choices of cubical representatives $\widetilde{P}_i$ and their pairwise sums $\widetilde{P}_i + \widetilde{P}_j$. Changing these choices can introduce a projective scaling factor.*

Lemma 18. *Let $\widetilde{P}_i'$, $\widetilde{P}_i+P_j'$ be other choices of cubical points above P_i, P_i+P_j. If $\lambda_i, \lambda_{i,j} \in \mathbb{F}_q^*$ are such that*

$$Z_1(\widetilde{P}_i') = \lambda_i \cdot Z_1(\widetilde{P}_i) \quad \textit{and} \quad Z_1(\widetilde{P}_i + P_j') = \lambda_i\lambda_j\lambda_{i,j} \cdot Z_1(\widetilde{P}_i + P_j),$$

then

$$Z_1\left(\sum n_i\widetilde{P}_i'\right) = \lambda \cdot Z_1\left(\sum n_i\widetilde{P}_i\right),$$

where

$$\lambda := \prod_{i=1}^{m} \lambda_i^{n_i^2} \prod_{1\le i<j\le m} \lambda_{i,j}^{n_i n_j}.$$

This lemma precisely quantifies the effect of choosing different cubical representatives for the same underlying elliptic points. The result indicates that all such changes scale the resulting cubical combination by a predictable factor $\lambda \in \mathbb{F}_q^*$ that depends quadratically on the coefficients n_i. The formula shows a precise structure resembling bilinear and quadratic forms, ensuring that any such rescaling is consistent and can be systematically understood.

4.3.4 Translated Cubes

Consider the set of eight points derived from a base point P_0: namely,

$$P_0, \quad P_0+P_1, \quad P_0+P_2, \quad P_0+P_3, \quad P_0+P_1+P_2, \quad P_0+P_1+P_3, \quad P_0+P_2+P_3, \quad P_0+P_1+P_2+P_3.$$

We may express the cubical ratio associated with this translated cube by the formula:

$$\frac{\mathrm{cub}_1(P_1, P_2, P_0+P_3)}{\mathrm{cub}_1(P_1, P_2, P_0)} = \frac{Z_1(P_0+\widetilde{P_1+P_2}+P_3)\cdot Z_1(\widetilde{P_0+P_1})\cdot Z_1(\widetilde{P_0+P_2})\cdot Z_1(\widetilde{P_0+P_3})}{Z_1(\widetilde{P_0})\cdot Z_1(P_0+\widetilde{P_2+P_3})\cdot Z_1(P_0+\widetilde{P_1+P_3})\cdot Z_1(P_0+\widetilde{P_1+P_2})}.$$

This expression is based on analyzing two related cubes: the original cube generated from points P_1, P_2, P_3 and the translated one constructed from P_1, P_2, P_0+P_3. We can interpret this ratio as the evaluation of the cubical function g_{P_1,P_2} at $(P_0+P_3)-P_0$, so that

$$\frac{\mathrm{cub}_1(P_1, P_2, P_0+P_3)}{\mathrm{cub}_1(P_1, P_2, P_0)} = g_{P_1,P_2}((P_0+P_3)-P_0).$$

To make the symmetry in the input points more explicit, we may re-parameterize the

points as follows:

$$U_1 = P_0 + P_1, \quad U_2 = P_0 + P_2, \quad U_3 = P_0 + P_3, \quad U_4 = P_0 + P_1 + P_2 + P_3,$$
$$W = 2P_0 + P_1 + P_2 + P_3, \quad V_1 = W - U_2 = P_0 + P_2 + P_3,$$
$$V_2 = W - U_3 = P_0 + P_1 + P_3, \quad V_3 = W - U_4 = P_0 + P_1 + P_2, \quad V_4 = W - U_1 = P_0.$$

With this notation, we can express the translated cubical relation in an entirely symmetric form:

$$\frac{\mathrm{cub}_1(U_1 - V_4, U_2 - V_4, U_3)}{\mathrm{cub}_1(U_1 - V_4, U_2 - V_4, V_4)} = \frac{Z_1(\widetilde{U_1}) \cdot Z_1(\widetilde{U_2}) \cdot Z_1(\widetilde{U_3}) \cdot Z_1(\widetilde{U_4})}{Z_1(\widetilde{V_1}) \cdot Z_1(\widetilde{V_2}) \cdot Z_1(\widetilde{V_3}) \cdot Z_1(\widetilde{V_4})}.$$

This formulation not only provides elegance through symmetry but also simplifies computations when dealing with translated cubical configurations.

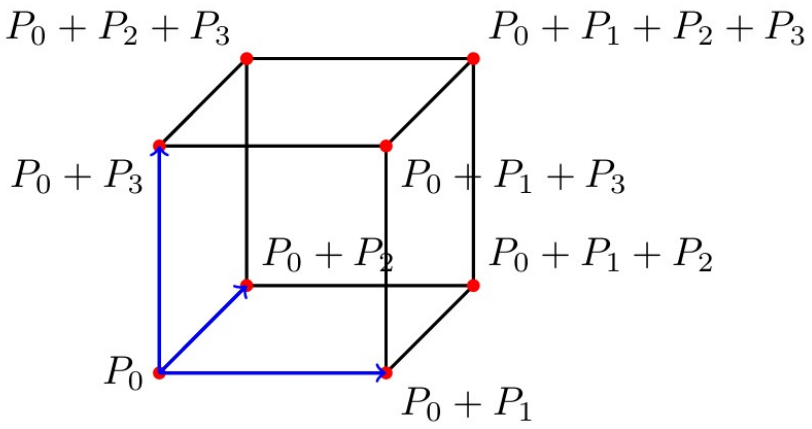


Figure 4.2: A cube of points P_1, P_2, P_3 translated by a base point P_0.

Remark 7. *An even more symmetric form is possible by defining the points* $U_1 = P_0 + P_1$, $U_2 = P_0 + P_2$, $U_3 = P_0 + P_3$, *and* $U_4 = P_0 + P_1 + P_2 + P_3$, *and similarly defining* V_1, V_2, V_3, V_4. *Then:*

$$\frac{\mathrm{cub}_1(U_1 - V_4, U_2 - V_4, U_3)}{\mathrm{cub}_1(U_1 - V_4, U_2 - V_4, V_4)} = \frac{Z_1(\widetilde{U}_1)Z_1(\widetilde{U}_2)Z_1(\widetilde{U}_3)Z_1(\widetilde{U}_4)}{Z_1(\widetilde{V}_1)Z_1(\widetilde{V}_2)Z_1(\widetilde{V}_3)Z_1(\widetilde{V}_4)}.$$

4.4 Monodromy Leak

4.4.1 Motivation

Let $P \in E(\mathbb{F}_q)$ be a point on an elliptic curve defined over a finite field $\mathbb{F}_q$, and suppose that P is of ℓ-torsion, where ℓ is a prime number. When computing the scalar multiplication $[m]P$ using projective coordinates, the result is often represented in the form $(X(mP) : Y(mP) : Z(mP))$. A subtle yet powerful side-channel vulnerability was identified in the foundational work of Naccache, Smart, and Stern ([18]), where it was demonstrated that leaking these individual projective coordinates during the scalar multiplication process—what is known as a *projective coordinate leak*—can reveal partial information about the secret scalar m.

In their 2004 paper, NSS introduced a novel attack showing that under certain conditions, even partial leakage of intermediate values like $X(mP)$ or $Z(mP)$ could expose bits of the scalar m. Though the technique is not strong enough to recover the full scalar directly, the authors observed that the leak could be particularly dangerous in the context of digital signatures. In the case of ECDSA, where a new scalar is generated for every signature, gathering a small number of leaked bits from each scalar allows an attacker to assemble a system of inequalities. These inequalities can be processed using lattice-based techniques, such as the Hidden Number Problem (HNP) framework, to reconstruct the long-term private key.

The danger of such leakage was revisited and further elaborated in the recent work of Aldaya, García, and Brumley ([19]). Their research revealed that many cryptographic libraries and implementations in the wild still fail to properly mask or protect intermediate projective coordinates, especially when using algorithms like the Montgomery ladder for scalar multiplication. Unlike traditional double-and-add methods, the Montgomery ladder was previously assumed to be safer against certain side-channel attacks due to its regular structure. However, AGB showed that coordinate-based leakage could still be exploited in this setting if care is not taken during the implementation.

More critically, they demonstrated real-world exploits and presented practical results showing that the theoretical risks outlined in ([18]) by NSS were far from academic. The Montgomery ladder, although designed for constant-time execution, still involves intermediate coordinate values that can be inferred through timing, power, or electromagnetic analysis. Once these values are compromised, the attack techniques by NSS can be adapted to recover bits of the secret scalar even in supposedly hardened implementations.

4.4.2 Monodromy from Cubical Arithmetic

In the context of side-channel attacks, the Monodromy Leak attack (see ([20])) on the Montgomery ladder is particularly powerful. Unlike other attacks, it can completely recover the secret key from a single leakage, by reducing the discrete logarithm problem on an elliptic curve to discrete logarithms in the multiplicative group $\mathbb{F}_q^*$.

To analyze this, we first assume that the group of ℓ-th roots of unity μ_ℓ is not contained in $\mathbb{F}_q$. If $\mu_\ell \subseteq \mathbb{F}_q$, then pairings already provide an efficient reduction from the discrete logarithm problem on $E(\mathbb{F}_q)$ to one in $\mathbb{F}_q^*$. For simplicity, we will also assume that ℓ is an odd prime.

Under this assumption, consider a point $P \in E[\ell](\mathbb{F}_q)$. There exists a unique rational point $\hat{P}$, called the **canonical cubical lift** of P, which lies in the space of cubical points and still satisfies $\ell\hat{P} = \widetilde{0}$. The lift $\hat{P}$ can be computed efficiently. Starting from any rational cubical point $\widetilde{P}$ lying above P, we define

$$\hat{P} = u \cdot \widetilde{P},$$

where the scalar $u \in \mathbb{Z}$ satisfies the congruences

$$u \equiv 1 \pmod{\ell}, \quad u \equiv 0 \pmod{q-1}.$$

Such a u always exists since ℓ and $q-1$ are coprime by assumption (by Chinese Remainder Theorem). Furthermore, this canonical lift respects scalar multiplication in the sense that for any integer m,

$$\widehat{mP} = m \cdot \hat{P}.$$

Lemma 6.2. *Assume that $\mu_\ell(\mathbb{F}_q) = 1$, that is, ℓ is coprime to $q-1$. Then, for every point $P \in E[\ell](\mathbb{F}_q)$, there exists a unique rational cubical point $\hat{P}$ of order ℓ, called the canonical lift of P.*

This canonical lift satisfies $\ell\hat{P} = \widetilde{0}$, and for any rational cubical point $\widetilde{P}$ above P, we have

$$\hat{P} = u \cdot \widetilde{P},$$

for some integer u such that $u \equiv 1 \pmod{\ell}$ and $u \equiv 0 \pmod{q-1}$. Moreover, scalar multiplication commutes with canonical lifting: for any $m \in \mathbb{Z}$,

$$\widehat{mP} = m \cdot \hat{P}.$$

4.4.3 DLP with BGS Exponent

It uses the relations:

$$\begin{aligned} U &= (X(P) - Z(P))(X(Q) + Z(Q)), \\ V &= (X(P) + Z(P))(X(Q) - Z(Q)), \\ X(P+Q) &= Z(P-Q)(U+V)^2, \\ Z(P+Q) &= X(P-Q)(U-V)^2. \end{aligned}$$

This differs from the cubical differential addition by a multiplicative factor of $4X(P-Q)Z(P-Q)$, which must be taken into account when analyzing ladder leakage.

As a result, recovering the scalar m from a projective coordinate leakage requires solving a modified degree-two equation. Let $[\widetilde{mP}]$ denote the cubical point obtained through the standard Montgomery ladder. Then, according to Proposition 2 from (13), we have

$$[\widetilde{mP}] = (4x(P))^{m(2^{\mathrm{len(m)}}-m)} \cdot \widetilde{mP},$$

where $len(m)$ denotes the bit-length of the scalar m. This relation links the projective and cubical representations via the action of division polynomials.

Suppose $\widetilde{P} = \lambda_1 \hat{P}$, $Q = mP$, and $\widetilde{mP} = \lambda_1^{m^2} \hat{mP}$, then the leaked projective output can be written as $[\widetilde{mP}] = \lambda_2 \hat{mP}$. Since the values P, Q, and therefore $\hat{P}, \hat{Q}$, as well as $\widetilde{P}$ and $[\widetilde{mP}]$, are known through the leakage, one can solve for λ_2 in the equation

$$(4x(P))^{m(2^{\mathrm{len(m)}}-m)} \cdot \lambda_1^{m^2} = \lambda_2.$$

Assuming that the bit-length $len(m)$ of m is also known, we fix a primitive root $\zeta \in \mathbb{F}_q^*$ and reduce the above relation to a discrete logarithm problem with respect to ζ. Letting $\mathrm{dlp}_\zeta(\cdot)$ denote the discrete logarithm base ζ, we define:

$$\alpha = \mathrm{dlp}_\zeta(4x(P)), \quad \beta = \mathrm{dlp}_\zeta(\lambda_1), \quad \gamma = \mathrm{dlp}_\zeta(\lambda_2).$$

Substituting into the logarithmic form of the equation, we obtain a quadratic in m:

$$X^2(\beta - \alpha) + 2^{\mathrm{len(m)}}\alpha X - \gamma = 0,$$

where the integer solution $X = m$ is the unknown we aim to recover.

Theorem 11. *Let $P = (X(P), Z(P))$ be a known public point of order ℓ on a Montgomery Kummer line associated to a Montgomery curve $E/\mathbb{F}_q$ (here we assume that we know not only P, but $X(P), Z(P)$; in practice, P is normalised via $Z(P) = 1$). Assume that ℓ is prime to $q - 1$.*

Let $m \leq \ell$, and let $mP = (X(mP), Z(mP))$ be computed by the standard projective Montgomery ladder. Assume that we obtain a projective coordinate leak of mP, i.e., we not only know $x(mP) = X(mP)/Z(mP)$, but also $X(mP), Z(mP)$.

Let u be the number of distinct prime factors of $q - 1$. Let $\hat{P} = (X(\hat{P}), Z(\hat{P}))$ be the unique canonical cubical rational point above P, $N \mid (q - 1)$ be the multiplicative order of $Z(P)/Z(\hat{P})$, and let $v = (q - 1)/N$.

Then one can recover m by solving three discrete logarithms in $\mathbb{F}_q^*$ (two of which can be seen as a precomputation depending only on P, not m), followed by an algorithm polynomial in $\log q, 2^u$, and v.

Chapter 5
Partially-Long Weierstrass Curve Arithmetic

5.1 Montgomery Form

The Montgomery form of an elliptic curve over a finite field $\mathbb{F}_p$ is defined as:

$$E_M : By^2 = x^3 + Ax^2 + x$$

where $A, B \in \mathbb{F}_p$ and $B \neq 0$. This form is particularly useful because it supports efficient computation of scalar multiplication using only the x-coordinates of points. This x-only arithmetic is more efficient and, importantly, can be implemented in a way that provides resistance to side-channel attacks such as Simple Power Analysis (SPA).

Let $P = (x_1, y_1)$ be a point on the curve E_M. We represent it in projective coordinates as $P = (X_1 : Y_1 : Z_1)$. For scalar multiplication, we compute $[n]P = (X_n : Y_n : Z_n)$ using a ladder-like structure. The formulas used for point addition and doubling in this Montgomery form avoid computing with y-coordinates entirely.

5.1.1 Addition ($n \neq m$)

Let $P_n = (X_n : Z_n)$ and $P_m = (X_m : Z_m)$, then their sum $P_{n+m} = (X_{n+m} : Z_{n+m})$ is computed by:

$$X_{n+m} = Z_{m-n} \left[(X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)\right]^2$$
$$Z_{n+m} = X_{m-n} \left[(X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)\right]^2$$

Note that P_{m-n} is required in the computation, making this formula suitable for structured ladder algorithms.

5.1.2 Doubling ($n = m$)

Let $P_n = (X_n : Z_n)$, then we compute $[2]P_n = (X_{2n} : Z_{2n})$ as:

$$\begin{aligned} 4X_nZ_n &= (X_n + Z_n)^2 - (X_n - Z_n)^2 \\ X_{2n} &= (X_n + Z_n)^2(X_n - Z_n)^2 \\ Z_{2n} &= 4X_nZ_n \left[(X_n - Z_n)^2 + \left(\frac{A+2}{4}\right)(4X_nZ_n)\right] \end{aligned}$$

In this representation:

- Each addition requires approximately $4M + 2S$ operations,
- Each doubling needs about $3M + 2S$ operations.

(M denotes a field multiplication, S a squaring.)

5.1.3 Recovering the y-coordinate

In some applications like digital signatures, it is necessary to recover the y-coordinate from the computed x-coordinates. If $[n]P = (x_n, y_n)$ and $[n+1]P = (x_{n+1}, y_{n+1})$, the following formula allows us to reconstruct y_n:

$$y_n = \frac{(x_1x_n + 1)(x_1 + x_n + 2A) - 2A - (x_1 - x_n)^2x_{n+1}}{2By_1}$$

This formula assumes knowledge of $P = (x_1, y_1)$ and requires x_n and x_{n+1}.

5.2 Generalization to Weierstrass Curves

While the Montgomery ladder is most efficient on curves in Montgomery form, Brier and Joye ([21]) extended the idea to elliptic curves in short Weierstrass form:

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

They proposed x-coordinate-based formulas which also make use of projective coordinates to reduce costly inversion operations.

5.2.1 Addition ($n \neq m$)

Given two projective points $P_n = (X_n : Z_n)$ and $P_m = (X_m : Z_m)$, their sum P_{n+m} is:

$$X_{n+m} = Z_{m-n}\left[-4a_6 Z_m Z_n (X_m Z_n + X_n Z_m) + (X_m X_n - a_4 Z_m Z_n)^2\right]$$
$$Z_{n+m} = X_{m-n}(X_m Z_n - X_n Z_m)^2$$

5.2.2 Doubling ($n = m$)

Let $P_n = (X_n : Z_n)$, then the doubling $[2]P_n$ is computed as:

$$X_{2n} = (X_n^2 - a_4 Z_n^2)^2 - 8a_6 X_n Z_n^3$$
$$Z_{2n} = 4Z_n\left[X_n(X_n^2 + a_4 Z_n^2) + a_6 Z_n^3\right]$$

5.2.3 Cost Analysis

- Addition: approximately $9M + 2S$
- Doubling: approximately $6M + 3S$

5.2.4 Recovering the y-coordinate

To obtain the y-coordinate for a computed multiple $[n]P = (x_n, y_n)$ when using the x-coordinate-only method in this generalized setting, the formula is:

$$y_n = \frac{2a_6 + (x_1 x_n + a_4)(x_1 + x_n) - (x_1 - x_n)^2 x_{n+1}}{2y_1}$$

This generalization enables the Montgomery ladder approach to be used even on curves not initially in Montgomery form. Although it is not as efficient as the native Montgomery setting, it still retains the benefits of uniformity and side-channel resistance.

5.3 Generalization for Partially-Long Weierstrass Curves(PLWC)

By the PLWC, we mean the curve,

$$y^2 \;=\; x^3 + Ax^2 + Bx + C$$

and for this group of elliptic curves, we have generalized the addition and doubling formulas. In PLWC, if we input $A = 0$, we get Short-Weierstrass curves and putting $B = 1$ and $C = 0$, we obtain Montgomery curves. So, in our formulas, inputing the constants accordingly, we can obtain the formulas for Montgomery and Short-Weierstrass curves.

We start with the affine coordinates (x, y) on our PLWC and it satisfies the curve equation.
Starting with two points on the curve (x_m, y_m) and (x_n, y_n) and they obey

$$y_m^2 \;=\; x_m^3 + Ax_m^2 + Bx_m + C$$

$$y_n^2 \;=\; x_n^3 + Ax_n^2 + Bx_n + C$$

5.3.1 Addition of (x_m, y_m) and (x_n, y_n)

As shown in the figure, the addition of two points on elliptic curve will be the reflection with respect to X-axis of the point where the line joining (x_m, y_m) and (x_n, y_n) cuts the elliptic curve. We call the points to be $P_m = (x_m, y_m)$ and $P_n = (x_n, y_n)$.

From the coordinates, we can get the slope of the line joining P_m and P_n will be (calling it λ)

$$\lambda \;=\; \frac{(y_m - y_n)}{(x_m - x_n)}$$

We denote $P_m + P_n \;=\; P_{m+n} \;=\; (x_{m+n}, y_{m+n})$ under the elliptic curve addition law.

Now, the line joining P_m and P_n passes through P_m, so the equation of the line can be formulated as

$$(y - y_m) \;=\; \lambda \cdot (x - x_m)$$

which implies

$$y \;=\; y_m \;+\; \lambda \cdot (x - x_m)$$

$$\implies \; y^2 \;=\; (y_m \;+\; \lambda \cdot (x - x_m))^2 \;=\; \lambda^2 x^2 \;-\; 2\lambda x x_m \;+\; h$$

where h is some constant. Now replacing y^2 by the curve equation, we get

$$x^3 \;+\; Ax^2 \;+\; Bx \;+\; C \;=\; \lambda^2 x^2 \;-\; 2\lambda x x_m \;+\; h$$

$$\implies x^3 \;+\; (A - \lambda^2)x^2 \;+\; (B + 2\lambda x_m)x \;+\; (C - h) \;=\; 0$$

But on the other hand, this equation of the line must satisfy the three points P_m, P_n,

$-P_{m+n} = (x_{m+n}, -y_{m+n})$. Thus,

$$(x - x_m) \cdot (x - x_n) \cdot (x - x_{m+n}) \;=\; x^3 \;+\; (A - \lambda^2)x^2 \;+\; (B + 2\lambda x_m)x \;+\; (C - h).$$

By compairing the coefficient of x^2 in above equality, we get

$$x_m + x_n + x_{m+n} \;=\; -(A - \lambda^2)$$

which implies

$$x_{m+n} \;=\; \lambda^2 - (A + x_m + x_n) \;=\; (\frac{(y_m - y_n)}{(x_m - x_n)})^2 - (A + x_m + x_n)$$

Correspondingly, to evaluate x_{m-n}, we can get this from the addition of the two points P_m and $-P_n$ and $-P_n = (x_n, -y_n)$. Thus we can directly compute x_{m-n} from the above formula by replacing y_n with $-y_n$ which will give us

$$x_{m-n} \;=\; (\frac{(y_m + y_n)}{(x_m - x_n)})^2 - (A + x_m + x_n).$$

From the above two equations we can evaluate

$$x_{m+n} \times x_{m-n} \;=\; [(\frac{(y_m - y_n)}{(x_m - x_n)})^2 - (A + x_m + x_n)] \times [(\frac{(y_m + y_n)}{(x_m - x_n)})^2 - (A + x_m + x_n)]$$

$$=\; (\frac{(y_m^2 - y_n^2)}{(x_m - x_n)^2})^2 + (A + x_m + x_n)^2 - (A + x_m + x_n)(\frac{2(y_m^2 + y_n^2)}{(x_m - x_n)^2})$$

Substituting $y_i^2 = x_i^3 + Ax_i^2 + Bx_i + C$ for $i \in \{m, n\}$ and simplying the whole expression we finally get

$$x_{m+n} \times x_{m-n} \;=\; \frac{-4C(x_m + x_n) - 4AC + (x_m x_n - B)^2}{(x_m - x_n)^2}$$

which ensures x-coordinate only addition as desired.

Now, as we want our formulas to be in projective coordinates, we substitute $x_i = \frac{X_i}{Z_i}$ for $i \in \{m, n, m - n, m + n\}$ and replacing them in the equation will give

$$\frac{X_{m+n}}{Z_{m+n}} \times \frac{X_{m-n}}{Z_{m-n}} \;=\; \frac{[-4C(\frac{X_m}{Z_m} + \frac{X_n}{Z_n}) - 4AC + (\frac{X_m}{Z_m}\frac{X_n}{Z_n} - B)^2]}{(\frac{X_m}{Z_m} - \frac{X_n}{Z_n})^2}$$

$$\implies \;\; \frac{X_{m+n}}{Z_{m+n}} \;=\; \frac{Z_{m-n}[-4CZ_mZ_n(X_mZ_n + X_nZ_m) - 4ACZ_m^2Z_n^2 + (X_mX_n - BZ_mZ_n)^2]}{X_{m-n}(X_mZ_n - X_nZ_m)^2}$$

Separating the numerator and denominator, we get our targeted projective x-coordinate only addition formulas to be

$$X_{m+n} \;=\; Z_{m-n}[-4CZ_mZ_n(X_mZ_n + X_nZ_m) - 4ACZ_m^2Z_n^2 + (X_mX_n - BZ_mZ_n)^2]$$

and

$$Z_{m+n} \;=\; X_{m-n}(X_mZ_n - X_nZ_m)^2.$$

Clearly, in this formulas, putting $A = 0$, we get addition formulas for Brier-Joye ladder and putting $B = 1$ and $C = 0$, we get Montgomery addition formulas.

Another way we can look at the addition formulas by taking $x_{m+n} + x_{m-n}$, which will give

$$x_{m+n} + x_{m-n} \;=\; [(\frac{(y_m - y_n)}{(x_m - x_n)})^2 - (A + x_m + x_n)] + [(\frac{(y_m + y_n)}{(x_m - x_n)})^2 - (A + x_m + x_n)]$$

$$\iff x_{m+n} + x_{m-n} \;=\; \frac{2(y_m^2 + y_n^2)}{(x_m - x_n)^2} - 2(A + x_m + x_n).$$

Upon replacing y_m^2 and y_n^2 by the curve equation, we get

$$x_{m+n} + x_{m-n} \;=\; \frac{2(x_m + x_n)(2B + x_mx_n) + 4(Ax_mx_n + C)}{(x_m - x_n)^2}$$

To make this projective x-coordinate only formulas we replace x_i by $\frac{X_i}{Z_i}$ and will get

$$\frac{X_{m+n}}{Z_{m+n}} + \frac{X_{m-n}}{Z_{m-n}} \;=\; \frac{Z_mZ_n[2(X_mZ_n + X_nZ_m)(2BZ_mZ_n + X_mX_n) + 4(AX_mX_n + CZ_mZ_n)]}{(X_mZ_n - X_nZ_m)^2}$$

upon simplifying, we get another addition formulas

$$X_{m+n} \;=\; -X_{m-n}(X_mZ_n - X_nZ_m)^2 + 2Z_mZ_n[(X_mZ_n + X_nZ_m)$$
$$(2BZ_mZ_n + X_mX_n) + 2(AX_mX_n + CZ_mZ_n)]$$

and

$$Z_{m+n} \;=\; Z_{m-n}(X_mZ_n - X_nZ_m)^2.$$

5.3.2 Doubling of (x_n, y_n)

As shown in the figure, the double of a point on the elliptic curve will be the reflection with respect to the X -axis of the point where the tangent at the point (x_n, y_n) cuts the elliptic curve. We call the point to be $P_n = (x_n, y_n)$.

The slope of the tangent at the point P_n will be (denoted by λ)

$$\lambda = \frac{3x_n^2 + Ax_n + B}{2y_n}.$$

The doubling of the point P_n will be done by $P_{2n} = 2P_n$, under the doubling of the elliptic curve.

Now, by the same calculation as addition, we get (replacing x_m by x_n and x_{m+n} by x_{2n})

$$x_n + x_n + x_{2n} \;=\; -(A - \lambda^2)$$

which implies

$$x_{2n} \;=\; (\frac{3x_n^2 + Ax_n + B}{2y_n})^2 - (A + 2x_n)$$

simplifying this, along with substituting from y_n^2 from the curve equation, we will get

$$x_{2n} \;=\; \frac{(x_n^2 - B)^2 - 8Cx_n - 4AC}{4(x_n^3 + Ax_n^2 + Bx_n + C)}.$$

Finally, as our desired formulas have to be in projective coordinate, we replace x_i by $\frac{X_i}{Z_i}$ for $i \in \{n, 2n\}$ (homogenization), we achieve

$$\frac{X_{2n}}{Z_{2n}} \;=\; \frac{(X_n^2 - BZ_n^2) - 8CX_nZ_n^3 - 4ACZ_n^4}{4Z_n(X_n^3 + AX_n^2Z_n + BX_nZ_n^2 + CZ_n^3)}$$

which gives the doubling formulas to be

$$X_{2n} \;=\; (X_n^2 - BZ_n^2) - 8CX_nZ_n^3 - 4ACZ_n^4$$

$$Z_{2n} \;=\; 4Z_n(X_n^3 + AX_n^2Z_n + BX_nZ_n^2 + CZ_n^3).$$

5.3.3 Monodromy Leak from Generalized Montgomery Ladder

Recall that for a point $P = (x, y)$ on an elliptic curve E, the multiplication-by-m map $[m]P$ can be expressed as:

$$[m](x, y) = \left(\frac{\phi_{E,m}(x)}{\psi_{E,m}(x)^2}, \frac{\omega_{E,m}(x, y)}{\psi_{E,m}(x)^3} \right),$$

where the rational functions $\phi_{E,m}, \psi_{E,m}, \omega_{E,m}$ are built from the division polynomials. Specifically,

$$\phi_{E,m}(x) = x \cdot \psi_{E,m}(x)^2 - \psi_{E,m+1}(x)\psi_{E,m-1}(x),$$

and $\psi_{E,m}(x)$ satisfies well-known recursive formulas.

Now, consider using the Generalized Montgomery ladder to compute $[m]P$ with x-coordinate $(x : 1)$ for a point P on a PLWC $E_A : y^2 = x^3 + Ax^2 + Bx + C$. The output projective coordinates (X_m, Z_m) then correspond to x-coordinates of $[m]P$ in projective form.

Proposition 2. *On input $A \in \mathbb{F}_p$, $m \in \mathbb{Z}_{>0}$, and $(x, 1)$, the Generalized Montgomery ladder returns*

$$(X_m, Z_m) = \left(\phi_{E,m}(x) \cdot f_m(x), \psi_{E,m}(x)^2 \cdot f_m(x)\right),$$

where

$$f_m(x) := (\delta \cdot x)^{m(2^{\mathrm{len}(m)} - m)},$$

$\delta = \delta(A, B, C)$ is a constant and $\mathrm{len}(m) := \lfloor \log_2 m \rfloor + 1$ is the bitlength of m.

Proof. Let P be a point on E_A with affine x-coordinate $x \neq 0$. The Generalized Montgomery ladder computes a pair of projective coordinates (X_m, Z_m) such that

$$\frac{X_m}{Z_m} = x([m]P).$$

From the formula for scalar multiplication, we know that:

$$x([m]P) = \frac{\phi_{E,m}(x)}{\psi_{E,m}(x)^2},$$

so the ladder must produce (X_m, Z_m) proportional to $(\phi_{E,m}(x), \psi_{E,m}(x)^2)$, up to a common projective factor $f_m(x)$. That is,

$$(X_m, Z_m) = (\phi_{E,m}(x) \cdot f_m(x), \psi_{E,m}(x)^2 \cdot f_m(x)).$$

We aim to determine the exact expression of $f_m(x)$ in terms of x and m. Through

experimentation and base case analysis:

$$f_m(x) = (\delta \cdot x)^{m(2^{\text{len}(m)}-m)}.$$

This is established by induction. For the base case $m = 1$, the ladder computes:

$$(X_1, Z_1) = (\delta \cdot x^2, \delta \cdot x),$$

which matches:

$$\phi_{E,1}(x) = 1, \quad \psi_{E,1}(x)^2 = 1, \quad f_1(x) = \delta \cdot x.$$

For the inductive step, the ladder computes scalar multiples using differential addition and doubling formulas, which recursively define the next projective factor. The recurrence relations for f_m and a second factor g_m (for $m + 1$) are:

$$\begin{aligned} f_{2m}(x) &= f_m(x)^4, \\ f_{2m+1}(x) &= \delta \cdot x \cdot f_m(x)^2 \cdot g_m(x)^2, \\ g_{2m+1}(x) &= g_m(x)^4. \end{aligned}$$

Assuming the hypothesis holds for m, direct substitution shows that the recurrence is satisfied and the inductive claim holds. The explicit closed-form expression for $f_m(x)$ is therefore valid. □

Remark 8. *This proof coincides with the proof given in the paper (13), as for the induction base cases $\phi_{E,1}(x), \phi_{E,2}(x), \psi^2_{E,1}(x) = \psi_{E,1}(x), \psi^2_{E,2}(x)$ remain unchanged and we prove the proposition by recurssion in the exponent.*
More importantly, putting $\delta = 4$, we retrieve the formula for Montgomery model and for $\delta = 1$, we achieve the factor for Brier-Joye model. So δ will depend on the values of the parameters A, B, C in PLWC but while applying this for Monodromy Leak, the second-degree equation will involve δ in case of PLWC, such as the second degree euqation remains

$$X^2(\beta - \alpha) + 2^{\text{len(m)}}\alpha X - \gamma = 0,$$

but in this case $\alpha = dlp_\zeta(\delta \cdot x(P))$.

Chapter 6
Edwards Curve Arithmetic

6.1 Introduction to Edwards Curves

Let k be a field of characteristic not equal to 2. An *Edwards curve* (see ([22])) over k is a special type of elliptic curve, typically described in the projective space $\mathbb{P}^3$ by the following system of equations:

$$E_{a,d} : \begin{cases} xy - zw = 0, \\ ax^2 + y^2 - z^2 - dw^2 = 0, \end{cases}$$

where $a, d \in k \setminus \{0\}$ are distinct constants. The curve is equipped with a distinguished base point $O = (0 : 1 : 1 : 0)$.

Most literature simplifies this representation by projecting $E_{a,d}$ onto $\mathbb{P}^2$ using the map:

$$\pi : \mathbb{P}^3 \setminus \{(0 : 0 : 0 : 1)\} \to \mathbb{P}^2, \quad (x : y : z : w) \mapsto (x : y : z).$$

To understand the image $\pi(E_{a,d})$, we eliminate w using $w = xy/z$ and substitute into the second equation, yielding:

$$\pi(E_{a,d}) : ax^2z^2 + y^2z^2 - z^4 - dx^2y^2 = 0.$$

Note, however, that this projection is not an isomorphism. Certain points, like $(1 : 0 : 0)$ and $(0 : 1 : 0)$, are singular points of $\pi(E_{a,d})$, each with two preimages:

$$P_x^{\pm} = (\pm\sqrt{d} : 0 : 0 : \sqrt{a}),$$
$$P_y^{\pm} = (0 : \pm\sqrt{d} : 0 : 1).$$

Thus, the projection separates branches at these singularities, and away from them, π behaves as a bijection. The base point O remains in the affine chart and maps to $\pi(O) = (0 : 1 : 1)$.

One typically dehomogenizes the projected equation with respect to z to obtain an affine model:

$$E_{a,d}^{\text{aff}} : ax^2 + y^2 = 1 + dx^2y^2,$$

with affine base point $(0, 1)$. Every point (x, y) on $E^{\text{aff}}_{a,d}$ corresponds to a point $(x : y : 1 : xy)$ on $E_{a,d}$, but the exceptional points at infinity are not included in the affine model.

Unlike Weierstrass curves that omit a single point at infinity, Edwards curves miss four such points. Fortunately, when d and d/a are non-squares in k, these points live in an extension of k and do not interfere with computations over k (e.g., $k = \mathbb{F}_p$ in cryptographic applications). This is foundational to the completeness of the Edwards group law.

6.2 The Formula and Proof of Exponent

This theorem investigates how the scalar multiplication of a point on an Edwards elliptic curve behaves under uniform projective scaling. Specifically, it shows that if a point $P = (X : Y : Z : W)$ is scaled by a constant λ, then the m-multiple of the scaled point, denoted by $m(\lambda \cdot P)$, is equivalent to the original mP scaled by an explicit power of λ, namely $\lambda^{m'}$, where the exponent m' depends on the binary expansion of the scalar m. The proof proceeds by induction on the bit-length of m, relying on the recursive structure of the double-and-add algorithm (denoted **SCALMULT**) used for scalar multiplication in Edwards curves. The main technical achievement of the proof lies in the recursive computation of the exponent m', showing that it satisfies a specific recurrence relation derived from the structure of the addition formula. This result plays a critical role in understanding the algebraic behavior of point multiplication under coordinate transformations.

Theorem 12. *Let the projective coordinate of an Elliptic (Edwards) Curve is given by $P = (X : Y : Z : W)$ and the scaling of the point by λ is denoted by $\lambda \cdot P = (\lambda X : \lambda Y : \lambda Z : \lambda W)$ and we denote the m multiple of the point P by mP. Then, if $m(\lambda \cdot P) = \lambda^{m'}.P$, m' is given by*

$$m' = (\prod_{i=1}^{r}(1 + a_{r-i})) \cdot 2^{2r} + \sum_{j=1}^{r}(\prod_{i=j}^{r}(1 + a_{r-i})) \cdot a_{r-j} \cdot 2^{2(r-j)},$$

where $m = a_r \cdots a_1 a_0$.

Proof. We will prove this by induction on r (the bit lenth of m).

We use the function **SCALMULT** to denote the Double and Add algorithm for Edward's curve, which is well established and **SCALMULT**$(P, m = a_r \cdots a_1 a_0)$ will give us the m multiple of point P in the Edward's Curve Double and Add algorithm.

Now, we observe that, **SCALMULT**$(P, m = a_r \cdots a_1 a_0) = 2($**SCALMULT**$(P, \bar{m} = a_r \cdots a_1) + a_0 P$, where $\overline{m} = a_r \cdots a_1$ denotes one-bit short expression of m, excluding a_0.

Our goal is to show that,

$$\mathbf{SCALMULT}(\lambda \cdot P, m) \;=\; \lambda^{m^{'}} \cdot \mathbf{SCALMULT}(P, m),$$

where $m^{'}$ is given by the expression in the theorem. But this is equivalent to show that

$$2(\mathbf{SCALMULT}(\lambda \cdot P, \overline{m} = a_r \cdots a_1)) + a_0(\lambda \cdot P) \;=\; \lambda^{m^{'}} \cdot (2(\mathbf{SCALMULT}(P, \overline{m})) + a_0 P)$$

$$\equiv 2\lambda^{\overline{m}^{'}} \cdot (\mathbf{SCALMULT}(P, \overline{m})) + a_0(\lambda \cdot P) \;=\; 2\lambda^{m^{'}} \cdot (\mathbf{SCALMULT}(P, \overline{m})) + \lambda^{m^{'}} \cdot (a_0 P).$$

So it suffices to show that :

- Base case, i.e. for $r = 0$, we have $m \in \{0, 1\}$, we get only a_0 and $a_0 P$ will be either exactly point 0 or point P. So, the scaling factor is trivially satisfied.

- For all points $P, Q \in E$ (E is the Edward's Curve), we have

$$\lambda^{4\overline{m}^{'}} \cdot 2Q + a_0(\lambda \cdot P) \;= \lambda^{m^{'}} \cdot (2Q + a_0 P)$$

  which is immediate from the above equivalence, replacing $\mathbf{SCALMULT}(P, \overline{m})$ by the point Q on E.

Finally, the above equality suggests it is enough to show :

1. If $a_0 = 0$, if should follow $m^{'} = 4\overline{m}^{'}$,
2. If $a_0 = 1$, it should follow $m^{'} = 8\overline{m}^{'} + 2$.

Now, from our given expression,

$$m^{'} \;=\; (\prod_{i=1}^{r}(1 + a_{r-i})) + \sum_{j=1}^{r}(\prod_{i=j}^{r}(1 + a_{r-i})) \cdot a_{r-j} \cdot 2^{2(r-j)}$$

$$= (1+a_0)\cdot 2^2 \cdot (\prod_{i=1}^{r-1}(1+a_{r-i}))\cdot 2^{r-1} + \sum_{j=1}^{r-1}(\prod_{i=j}^{r-1}(1+a_{r-i}))\cdot a_{r-j}\cdot 2^{2(r-j)} + (\text{for} j = r)\ (1+a_0)\cdot a_0 \cdot 2^{2(r-r)}$$

$$= 4(1 + a_0)[(\prod_{i=1}^{r-1}(1 + a_{r-i})) \cdot 2^{2(r-1)} + \sum_{j=1}^{r-1}(\prod_{i=j}^{r-1}(1 + a_{r-i})) \cdot a_{r-j} \cdot 2^{2(r-j)}] + (1 + a_0) \cdot a_0$$

$$= 4(1 + a_0)\overline{m}^{'} + (1 + a_0) \cdot a_0.$$

Clearly, this satisfies the two required condition for $a_0 = 0, 1$ and thus it verifies the expression for the exponent is accurate, via induction on the bit length of m. $\square$

6.3 Group Law on Edwards Curves

On the affine curve $E^{\text{aff}}_{a,d}$, the group inverse of (x, y) is $(-x, y)$ (see ([23])). In projective coordinates, this becomes:

$$-(x : y : z : w) = (-x : y : z : -w).$$

6.3.1 Cyclic Subgroup of Order 4

Consider the following points on the affine model:

$$R_+ = (1/\sqrt{a}, 0), \quad T = (0, -1), \quad R_- = (-1/\sqrt{a}, 0), \quad O = (0, 1).$$

These form a cyclic group of order 4 under the curve's group law:

$$T = 2R_+, \quad R_- = 3R_+, \quad O = 4R_+.$$

Their projective versions are:

$$R_+ = (1 : 0 : \sqrt{a} : 0), \quad T = (0 : -1 : 1 : 0), \quad R_- = (-1 : 0 : \sqrt{a} : 0).$$

The group law has elegant expressions:

$$\begin{aligned}
(x, y) + R_+ &= \left(\frac{y}{\sqrt{a}}, -\sqrt{a}x\right), \\
(x, y) + T &= (-x, -y), \\
(x, y) + R_- &= \left(\frac{-y}{\sqrt{a}}, \sqrt{a}x\right), \\
(x, y) + O &= (x, y).
\end{aligned}$$

6.3.2 Points at Infinity and Torsion Structure

Points $P^{\pm}_x$ have order 2, so the 2-torsion subgroup is:

$$E_{a,d}[2] = \{O, T, P^+_x, P^-_x\}.$$

Points $P^{\pm}_y$ have order 4 and are halves of T:

$$P^{\pm}_y = R_+ + P^{\pm}_x.$$

We have:

$$\begin{aligned} R_+ + O &= R_+, \\ R_+ + T &= R_-, \\ R_+ + P_x^+ &= P_y^+, \\ R_+ + P_x^- &= P_y^-. \end{aligned}$$

Translation rules for these special points include:

$$\begin{aligned} (x,y) + P_x^+ &= \left(\frac{1}{\sqrt{a}\sqrt{d}x}, \frac{\sqrt{a}}{\sqrt{d}y} \right), \\ (x,y) + P_x^- &= \left(\frac{-1}{\sqrt{a}\sqrt{d}x}, \frac{-\sqrt{a}}{\sqrt{d}y} \right), \\ (x,y) + P_y^+ &= \left(\frac{1}{\sqrt{d}y}, \frac{-1}{\sqrt{d}x} \right), \\ (x,y) + P_y^- &= \left(\frac{-1}{\sqrt{d}y}, \frac{1}{\sqrt{d}x} \right). \end{aligned}$$

6.4 Function Field of the Curve $E_{a,d}$

Functions on $E_{a,d}$ are of the form:

$$\frac{F(x,y,z,w)}{G(x,y,z,w)}$$

where F and G are homogeneous polynomials of the same degree, and all expressions are modulo the defining equations $xy - zw$ and $ax^2 + y^2 - z^2 - dw^2$.

The set of such functions forms the field $k(E_{a,d})$. Each non-zero function $f \in k(E_{a,d})$ has a *divisor*:

$$\operatorname{div}(f) = \sum_{P \in E_{a,d}} \operatorname{ord}_P(f)(P),$$

where $\operatorname{ord}_P(f)$ represents the order of vanishing or pole at P. The degree of a function's divisor is always zero.

For the function z/x, we find:

$$\operatorname{div}(z/x) = (P_x^+) + (P_x^-) - (O) - (O'),$$

where $O' = (0 : 1 : -1 : 0)$.

The affine function field is isomorphic to:

$$k(E_{a,d}) \cong \mathrm{Frac}\left(\frac{k[x,y]}{ax^2+y^2-1-dx^2y^2}\right),$$

via $f(x,y,z,w) \mapsto f(x,y,1,xy)$. Under this map, z/x becomes $1/x$.

6.5 Divisor at Infinity and Riemann–Roch Space

The intersection of $E_{a,d}$ with the hyperplane at infinity $H_\infty : z = 0$ yields the divisor:

$$D = (P_x^+) + (P_x^-) + (P_y^+) + (P_y^-),$$

a symmetric divisor of degree 4.

The Riemann–Roch space associated to D is:

$$\Gamma(D) = \{f \in k(E_{a,d}) \setminus \{0\} \mid \mathrm{div}(f) + D \geq 0\} \cup \{0\},$$

a k-vector space of dimension 4. A basis is:

$$\Gamma(D) = \langle x, y, 1, xy \rangle.$$

Their divisors are:

$$\begin{aligned}
\mathrm{div}(1) &= 0,\\
\mathrm{div}(x) &= (O) + (O') - (P_x^+) - (P_x^-),\\
\mathrm{div}(y) &= (O) + (O') - (P_y^+) - (P_y^-),\\
\mathrm{div}(xy) &= 2(O) + 2(O') - (P_x^+) - (P_x^-) - (P_y^+) - (P_y^-).
\end{aligned}$$

In projective terms, the functions $x, y, 1, xy$ correspond to:

$$\frac{x}{z}, \quad \frac{y}{z}, \quad \frac{z}{z}, \quad \frac{w}{z}.$$

Chapter 7
CONCLUSION

This thesis began with a comprehensive investigation of the foundational concepts in Elliptic Curve Cryptography (ECC), particularly emphasizing the role of scalar multiplication in secure key exchange protocols. We analyzed both classical approaches and modern optimizations, including Montgomery laddering and projective coordinate systems, to understand their computational advantages and cryptographic implications. These studies laid the groundwork for exploring deeper vulnerabilities inherent in ECC implementations.

The core contribution of this work was an in-depth examination of the Monodromy Leak, a powerful attack that exploits structural properties of cubical arithmetic and projective scalar multiplication. By showing how the Montgomery ladder inadvertently aligns with cubical scalar multiplication, and by connecting this to the BGS exponent and the function field of the curve, the thesis demonstrates a critical reduction from the ECDLP to a DLP in the finite field. This exposes a severe risk in implementations that do not rigorously protect against coordinate leakage and reinforces the need for constant-time, side-channel resilient procedures in cryptographic systems.

Beyond the attack itself, the thesis explored how cubical arithmetic could extend to other models, including Weierstrass and Edwards curves, and its potential applications in pairing and isogeny computations. These investigations not only highlight the vulnerabilities but also suggest novel avenues for optimizing and analyzing ECC arithmetic. Overall, this work provides both a cautionary perspective on cryptographic implementation and a constructive outlook on the deeper algebraic structures that govern secure computation.

An important direction for future work lies in the open problem of developing a complete theory of cubical arithmetic for Edwards curves. While translation formulas have been successfully derived and verified using `MAGMA`, formal proofs are still pending. Moreover, the precise connection between the Ed-curve double-and-add algorithm and the Monodromy Leak remains unproven. A central challenge lies in understanding how to derive the cubical function—and consequently the cubical scalar multiplication formula, from the divisor at infinity for Ed-curves. These questions will form the natural continuation of this thesis.

References

[1] J. W. S. Cassels, *Lectures on elliptic curves*. Cambridge University Press, 1991.

[2] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, "Twisted edwards curves," in *Progress in Cryptology – AFRICACRYPT 2008* (S. Vaudenay, ed.), (Berlin, Heidelberg), pp. 389–405, Springer Berlin Heidelberg, 2008.

[3] C. Arene, T. Lange, M. Naehrig, and C. Ritzenthaler, "Faster computation of the tate pairing," 2010.

[4] P. Gaudry, "The discrete logarithm problem. 1 – generic algorithms." Presentation Slides at Caramel – LORIA, CNRS, Université de Lorraine, Inria, 2013-2014, https://www.lix.polytechnique.fr/ morain/MPRI/2013/lecture1.pdf.

[5] B. Źrałek, "A deterministic version of pollard's $p-1$ algorithm," *Mathematics of Computation*, vol. 79, p. 513–513, Jan. 2010.

[6] P. Zimmermann, *Elliptic Curve Method for Factoring*, pp. 401–403. Boston, MA: Springer US, 2011.

[7] A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory*, vol. 39, no. 5, pp. 1639–1646, 1993.

[8] K. E. Lauter and K. E. Stange, "The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences," in *Selected Areas in Cryptography* (R. M. Avanzi, L. Keliher, and F. Sica, eds.), (Berlin, Heidelberg), pp. 309–327, Springer Berlin Heidelberg, 2009.

[9] A. V. Sutherland, "Identifying supersingular elliptic curves," *LMS Journal of Computation and Mathematics*, vol. 15, pp. 317–325, 2012.

[10] D. Bernstein and T. Lange, *Montgomery curves and the Montgomery ladder*. Cryptology ePrint Archive, IACR, 2017.

[11] D. J. Bernstein, "Curve25519: New diffie-hellman speed records," in *Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography*, vol. 3958 of *Lecture Notes in Computer Science*, pp. 207–228, Springer, 2006.

[12] J. Doliskani, "On division polynomial pit and supersingularity," *Applicable Algebra in Engineering, Communication and Computing*, vol. 29, no. 5, pp. 393–407, 2018.

[13] G. Banegas, V. Gilchrist, and B. Smith, "Efficient supersingularity testing over $\mathbb{F}_p$ and CSIDH key validation." Cryptology ePrint Archive, Paper 2022/880, 2022.

[14] G. Pope, K. Reijnders, D. Robert, A. Sferlazza, and B. Smith, "Simpler and faster pairings from the montgomery ladder." Cryptology ePrint Archive, Paper 2025/672, 2025.

[15] A. Grothendieck, *Groupes de monodromie en geometrie algebrique / (dirige par A. Grothendieck).* Lecture notes in mathematics ; 288, Berlin: Springer-Verlag, 1972.

[16] L. Breen, *Fonctions thêta canoniques*, pp. 67–71. Berlin, Heidelberg: Springer Berlin Heidelberg, 1983.

[17] D. Robert, "Fast pairings via biextensions and cubical arithmetic." Cryptology ePrint Archive, Paper 2024/517, 2024.

[18] D. Naccache, N. Smart, and J. Stern, "Projective coordinates leak." Cryptology ePrint Archive, Paper 2003/191, 2003.

[19] A. C. Aldaya, C. P. García, and B. B. Brumley, "From a to z: Projective coordinates leakage in the wild." Cryptology ePrint Archive, Paper 2020/432, 2020.

[20] D. Robert, "Cubical arithmetic on abelian varieties." Presentation Slides at Inria Bordeux, 2025, https://www.math.u-bordeaux.fr/ damienrobert/pro/publications/slides/2025-02-Cubical.pdf.

[21] É. Brier and M. Joye, "Weierstraß elliptic curves and side-channel attacks," in *Public Key Cryptography* (D. Naccache and P. Paillier, eds.), (Berlin, Heidelberg), pp. 335–345, Springer Berlin Heidelberg, 2002.

[22] H. Edwards, "A normal form for elliptic curves," *Bulletin of The American Mathematical Society - BULL AMER MATH SOC*, vol. 44, pp. 393–423, 07 2007.

[23] J. H. Silverman, *The Arithmetic of Elliptic Curves.* Graduate texts in mathematics, Dordrecht: Springer, 2009.