THE CONSTRUCTION OF EFFICIENTLY COMPUTABLE ENDOMORPHISMS FOR SCALAR MULTIPLICATION ON SOME ELLIPTIC CURVES

SITI NOOR FARWINA MOHAMAD ANWAR ANTONY

UNIVERSITI SAINS MALAYSIA

2019

THE CONSTRUCTION OF EFFICIENTLY COMPUTABLE ENDOMORPHISMS FOR SCALAR MULTIPLICATION ON SOME ELLIPTIC CURVES

by

SITI NOOR FARWINA MOHAMAD ANWAR ANTONY

**Thesis submitted in fulfillment of the requirements
for the degree of
Doctor of Philosophy**

May 2019

ACKNOWLEDGEMENT

Alhamdulillah. In the name of Allah, the Most Beneficent and the Most Merciful. All praises to Him for giving me the strength to complete this thesis.

My sincere appreciation goes to my supervisor, Prof. Dr. Hailiza Kamarulhaili for her encouragement, support and guidance throughout my Ph.D journey. Thank you Prof., for not giving up on me.

I would like to express my gratitude to the Ministry of Higher Education (MOHE), and Universiti Sains Malaysia (USM) for funding me under RLKA scheme during my study. Special thanks to RUI grant for funding me to conferences and seminars throughout my study. Special thanks to Prof. Izani who gave me opportunity to continue my study under this sponsorship. I might faced difficulties in finishing my study without their financial supports.

I would also like to thank all the members of School of Mathematical Sciences, USM who have been parts of my journey. Not forgotten, thanks to Prof. Jamaludin Md. Ali who always encourage me to complete what I have started and reminds me of where I should stand. To all my friends, my lab-mates, my room-mate, and those whom I have been knowing for the past few years, whoever involves directly and indirectly, thanks for making my journey enjoyable.

My deepest appreciation and love go to my family who has been with me through my ups and downs especially to Mak and Papa. I know they can't wait for me to finish my PhD. Their prayers and patience give me incredible strength to finish this thesis. I love you all!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
DES	Data Encryption Standard
DH	Diffie-Hellman
EC	Elliptic curve
ECC	Elliptic Curve Cryptography
ECSM	Elliptic Curve Scalar Multiplication
EEA	Extended Euclidean Algorithm
GLS	Galbraith-Lin-Scott
GLV	Gallant-Lambert-Vanstone
ISD	Integer Sub-Decomposition
LLL	Lenstra, Lenstra, Lovasz
PKC	Public Key Cryptography
RSA	Rivest, Shamir, Adleman

LIST OF SYMBOLS

E	elliptic curve
E_{j_E}	elliptic curve with given j-invariant
K	number field
$\bar{K}$	algebraic closure of a number field K
K^*	multiplicative group of a number field K
$\cong$	isomorphic
mod	modulo
$\equiv$	congruent to
$\mathbb{R}$	real number
$\mathbb{C}$	complex number
$\mathbb{Q}$	rational number
$\mathbb{Z}$	integer number
$\mathbb{N}$	natural number
$\hat{\Phi}$	conjugate of endomorphism Φ
t_Φ	trace of endomorphism Φ
n_Φ	norm of endomorphism Φ
$\mathbb{Q}(\sqrt{-d})$	imaginary quadratic field
D	discriminant of quadratic field
$E(F_p)$	elliptic curve over finite prime field

$j(E)$	j-invariant of elliptic curve
$\mathcal{O}_E$	identity element of E or point at infinity of E
$\mathcal{O}_K$	maximal order of a field K
$E(\mathbb{Q})$	rational points of E
$E(\mathbb{Q})_{tors}$	rational torsion points of E
t	trace
$\#E$	order of E
Δ	discriminant of E
$C\ell(d)$	class group
$h(D)$	class number of discriminant, D
$\mathbb{Z}_n$	ring of integer modulo n
$a\|b$	a divides b
$\left(\frac{d}{p}\right)$	Legendre symbol of d and p
$\lfloor a \rceil$	nearest integer of a
$\langle a \rangle$	generator
ψ	division polynomial
ϕ	mapping
Ψ	Frobenius endomorphism quadratic twist of E on $char(K) = p$
π	Frobenius endomorphism of E on $char(K) = p$
τ	Frobenius endomorphism on $char(K) = 2$
t_Φ	trace of endomorphism Φ

n_Φ	norm of endomorphism Φ
$G \oplus H$	direct sum of two cyclic groups G and H
$G \times H$	direct product of two cyclic groups G and H
$\bar{E}$	twist of E
$\tilde{E}$	another twist of E
h	cofactor of E

PEMBINAAN ENDOMORFISMA YANG DAPAT DIHITUNG SECARA EFISIEN BAGI PENDARABAN SKALAR TERHADAP BEBERAPA LENGKUNG ELIPTIK

ABSTRAK

Pendaraban skalar lengkung eliptik (ECSM), dilambangkan sebagai kP, merupakan satu di antara cabaran terbesar dalam kriptografi yang melibatkan kriptografi lengkung eliptik (ECC). Suatu lengkung eliptik, E yang ditakrifkan pada suatu medan perdana terhingga, F_p mempunyai titik-titik terhingga bilangannya yang membentuk satu kumpulan abelan dan wujudnya satu subkumpulan perdana yang berkitar dengan bilangan n. ECSM melibatkan pendaraban skalar $k \in [1, n-1]$ dan titik P yang terdapat dalam subkumpulan perdana tersebut. ECSM memerlukan kos operasi yang tertinggi dalam ECC dan seterusnya akan mempengaruhi kecekapan sistem kriptografi ini. Untuk beberapa tahun kebelakangan ini, ramai penyelidik mencadangkan pelbagai kaedah, seperti kaedah Gallant, Lambert dan Vanstone (GLV) dan kaedah sub-penguraian integer (ISD), untuk mengurangkan kos operasi ECSM. Salah satu pendekatan untuk mengurangkan kos operasi ECSM ini adalah dengan menggunakan endomorfisma yang dapat dihitung secara efisien. Kajian ini bertujuan untuk membina endomorfisma yang dapat dihitung secara efisien terhadap beberapa lengkung eliptik, khusus kepada lengkung eliptik yang mempunyai j-invarians, $j(E) = 0, 1728, 8000, 54000$, yang mana lengkung-lengkung ini masing-masing berpadanan dengan medan kuadratik khayalan, $\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$ dengan pendiskriminasi $D = -3, -4, -8, -12$. Medan kuadratik khayalan ini masing-masing mempunyai bentuk turunan unik bagi nombor perdana dan mempunyai turutan maksimal unik. Turutan maksimal bagi setiap medan kuadratik khayalan memenuhi suatu bentuk khusus polinomial monik yang akan menjadi polinomial cirian bagi endomorfisma yang dapat dihitung secara efisien untuk mewakili pendaraban kompleks pada suatu lengkung eliptik. Memandangkan penjana untuk turutan maksimal bagi lengkung eliptik dengan $j(E) = 0, 1728$ memenuhi punca primitif keunitan, konsep isomorfisma digunakan dalam kajian ini bagi menerbitkan pemetaan bagi endomorfisma pertama tertakrif pada lengkung eliptik tersebut. Kajian ini juga membina pemetaan bagi endomorfisma selain daripada yang telah diterbitkan berdasarkan pemetaan terhadap isogeni, ϕ yang mana $\phi : E \to E$. Isogeni ini ditakrifkan menggunakan titik-titik kilasan yang terdapat pada E dan konsep formula Velu. Kajian ini mewakilkan pemetaan isogeni tersebut sebagai pemetaan bagi endomorfisma sekiranya ia mengekalkan struktur lengkung eliptik dan memenuhi bentuk terbatas bagi sesuatu isomorfima yang tertakrif pada medan kuadratik khayalan yang sama seperti medan kuadratik khayalan bagi suatu lengkung eliptik. Endomorfisma-endomorfisma yang dapat dihitung secara efisien ini kemudiannya digunakan dalam kaedah ISD untuk mengurangkan kos operasi ECSM. Kos operasi ECSM dikira menggunakan kaedah penambahan dan penggandaan titik berulang melalui algoritma Kanan-ke-Kiri. Perbandingan di antara kos operasi menggunakan kaedah penambahan dan penggandaan titik berulang, kaedah GLV dan kaedah ISD juga dibuat. Sebagai tambahan, kos operasi bagi setiap endomorfisma yang dapat dihitung secara efisien yang telah diterbitkan juga dibincangkan dalam kajian ini. Kos operasi ECSM dalam kaedah ISD dengan endomorfisma yang dapat dihitung secara efisien dan tanpa endomorfisma dapat dihitung secara efisien dikira bagi menunjukkan bahawa kewujudan endomorfisma dapat dihitung secara efisien mempercepatkan dan mengurangkan kos operasi ECSM dalam kaedah ISD.

THE CONSTRUCTION OF EFFICIENTLY COMPUTABLE ENDOMORPHISMS FOR SCALAR MULTIPLICATION ON SOME ELLIPTIC CURVES

ABSTRACT

Elliptic curves scalar multiplication (ECSM), denoted as kP, is one of the building blocks in Elliptic Curve Cryptography (ECC). An elliptic curve, E defined over a finite prime field, F_p have finitely many points which form an abelian group and there exists a prime subgroup with order n. ECSM involves the multiplication of scalar $k \in [1, n-1]$ and a point P which belongs to the prime subgroup. ECSM consumes the highest operating cost in ECC which later affects the efficiency of this cryptosystem. For the past few years, many researchers proposed various methods, such as the Gallant, Lambert and Vanstone (GLV) method and Integer Sub-Decomposition (ISD) method, to reduce the operation cost of ECSM. One of the approaches to reduce the operation cost of ECSM is by employing an efficiently computable endomorphism. This research aims to construct efficiently computable endomorphisms on selected elliptic curves, mainly elliptic curves with j-invariant, $j(E) = 0, 1728, 8000, 54000$, which corresponds to imaginary quadratic field $\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3})$, with discriminant, $D = -3, -4, -8, -12$, respectively. These imaginary quadratic fields correspond to a unique reduced form of prime numbers and a unique maximal order, respectively. The maximal order for each imaginary quadratic field satisfies a specific monic polynomial which becomes the characteristic polynomial for the endomorphisms that has been constructed to represent the complex multiplication on elliptic curves. Since the generator of maximal order for elliptic curves with $j(E) = 0, 1728$ satisfy the primitive roots of unity, the concept of isomorphism is used in this work to derive their first endomorphism mapping. This study also constructed the mapping for endomorphisms apart from those derived earlier, based on the mapping of isogeny, ϕ where $\phi : E \to E$. The isogeny is derived using the torsion points defined on E and from the concept of Velu's formulae. This work represents the isogeny mapping as the endomorphism mapping if it preserves the structure of elliptic curve and it satisfies the restricted form of isomorphism defined over the same imaginary quadratic field as the elliptic curves itself. These efficiently computable endomorphisms are being employed on the ISD method to reduce the operating cost of ECSM. The cost of computing ECSM is computed using repeated additions and doublings via Right-to-Left algorithm. The comparison of operation counts among the repeated additions and doublings approach, GLV method and ISD method is also discussed in this work. Additionally, the operation counts for each of the derived efficiently computable endomorphism is computed. The cost of computing ECSM in ISD method with and without using efficiently computable endomorphism is computed to show that the existence of efficiently computable endomorphism accelerates and reduces the cost of computing ECSM in the ISD method.

CHAPTER 1

INTRODUCTION

1.1 Introduction

This introductory chapter explains the background of cryptography and elliptic curves. Section 1.2 lists the basic concepts on elliptic curves. Next section is the literature review section which succinctly explains the previous works related to elliptic curve scalar multiplication. This is followed by Section 1.4 that highlights the problem statement. The last section, Section 1.5 lists the research objectives.

1.2 Background of the Study

Cryptography is a platform which provides secure communication between two parties to pass their secret messages and provide authentication of one party to another from being traced by the third parties, known as eavesdroppers (Galbraith, 2012). There are two main processes in cryptography which are encryption and decryption. The following figure describes how the secret messages being encrypted and decrypted.

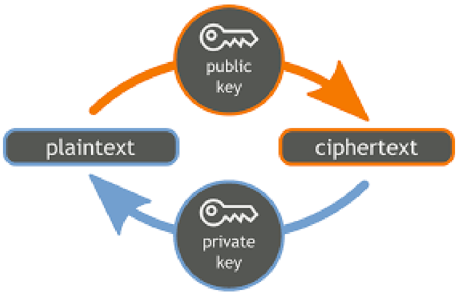

Figure 1.1: Cryptography processes

From Figure 1.1, the process where the first party namely Alice converts her plaintext (secret messages) into codes (ciphertext) that is unreadable by using an encryption key (or public key) and pass it to the second party namely Bob is called encryption. While decryption is the process where the second party Bob converts the unreadable messages (ciphertext) back into the plaintext by using a decryption key (or private key).

There are two types of cryptography which are symmetric cryptography and asymmetric cryptography. In symmetric cryptography, the encryption key and the decryption key are the same (Washington, 2007). This symmetric cryptography has been widely used in the Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Meanwhile, in asymmetric cryptography or also known as Public Key Cryptography (PKC), the encryption key is being public while the decryption key is being kept secret. This asymmetric encryption is being used by cryptographic protocols such as Diffie-Hellman (DH), Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC).

The use of elliptic curve in the cryptographic area was first discovered by Miller (1985) and Koblitz (1987). The security of ECC is based on the intractability of solving the discrete logarithm problem in the elliptic curve which is the problem of finding scalar k, given Q in the operation $Q = kP$ (Salah & Said, 2015). ECC attracted many attentions due to its effectiveness of having a shorter key as compared to other cryptosystems such as RSA at the same level of security (Salah & Said, 2014). For instance, a 160-bit ECC can have an equivalent security level as RSA 2048-bit (Park et al., 2005). Similarly, a 256-bit ECC equivalent to RSA 3072-bit (Kwon et al., 2018). The n-bit refers to the bit length of scalar k or the length of k in its binary representation.

An elliptic curve E is defined by the general Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

where a_1, a_2, a_3, a_4, a_6 are scalars defined in a field K (Silverman, 2009), then E is said to be defined over K and can be denoted as $E(K)$. The scalar a_i's are the coefficients of the elliptic curve in the given Weierstrass equation as defined in Eq. (1.1).

Let the following scalars be defined as

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= a_1a_3 + 2a_4 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_2a_3 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6
\end{aligned}$$

(Silverman, 2009). These scalars are useful to determine the discriminant and j-invariant of an elliptic curve.

The discriminant of E (Silverman, 2009) denoted as Δ is defined by

$$\begin{aligned}
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
&= \frac{c_4^3 - c_6^2}{1728}.
\end{aligned}$$

The value for Δ determines whether the curves is smooth or not smooth (Longa, 2011). Points on elliptic curves does not form a group when $\Delta = 0$. Thus, it is crucial to have $\Delta \neq 0$. The curve is said to be smooth if tangent line that touches any point on the elliptic curve is unique (Hankerson et al., 2004), which happened when $\Delta \neq 0$.

Meanwhile, the j-invariant of elliptic curves, $j(E)$ is defined as follows

$$j(E) = \frac{c_4^3}{\Delta} = 1728\frac{c_4^3}{c_4^3 - c_6^2}$$

(Silverman, 2009). The value for $j(E)$ determines the types of family of curves, as two elliptic curves with the same $j(E)$ are belong to the same family of curves and they are said to be isomorphic to each other over $\bar{K}$(Galbraith, 2012) where $\bar{K}$ is the algebraic closure of K. A homomorphism from E_1 to E_2 is a map $\phi : E_1 \to E_2$ which satisfy $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$ (Washington, 2007). While an isomorphism is a bijective homomorphism (Roman, 2006). Two elliptic curve $E(K)$ and $\bar{E}(K)$ are said to be isomorphic over $\bar{K}$ if every isomorphism satisfies the restricted form of change of variable where $\phi(x,y) = (u^2x + r, u^3y + su^2x + t)$ for $u \in \bar{K}$ and $r, s, t \in \bar{K}$, and they can be written as $E(K) \cong \bar{E}(K)$. The elements u, r, s, t are chosen to be defined in $\bar{K}$ since every element in $\bar{K}$ are called algebraic numbers, and every algebraic number satisfies a non-constant polynomial defined in K.

The field K can be either $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ or finite field F_p where p is prime(Washington, 2007). Since K is a field, it has two binary operations namely addition $(+)$ and multiplication $(\cdot)$ such that K an Abelian group under addition and the set of non-zero elements in K is an Abelian group under multiplication (Roman, 2008). Other than that, the elements in K should satisfy the distributive law where for $a, b, c \in K$ then $(a+b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b+c) = a \cdot b + a \cdot c$ (Roman, 2008).

The characteristic of a field K can be either 0 or a prime number (Roman, 2006). The characteristic of a field K denoted as $char(K)$ is equal to the characteristic of a ring $char(R)$ if $char(R)$ is a prime number. The $char(K) = 0$ if the field $K = \mathbb{Q}$ and $char(K)$ is a prime number if K is a finite field (Roman, 2006). A characteristic of a ring R is defined by the smallest positive number n where $n \cdot 1 = 0$ such that 1 is the multiplicative identity and 0 is the additive identity (Roman, 2006).

Elliptic curve cryptography always deal with finite prime field. The characteristic of finite field can be either be characteristic 2 where $char(K) = 2$ or $char(K) = 2^q$ (also known as binary field) (Roman, 2006), characteristic 3 where $char(K) = 3$ or $char(K) = 3^q$, or large prime characteristic specifically $char(K) = p$ or $char(K) = p^q$ where p is a prime number and $q \in \mathbb{N}$ (Hankerson et al., 2004). If $q = 1$, $K = F_p$ is called a finite prime field while if $q \geq 1$, $K = F_{p^q}$ is called the extension field (Roman, 2006).

It is known that $\{0, 1, 2, ..., p-1\}$ is the set of elements in F_p. These elements form an abelian group under addition with 0 as the additive identity. Meanwhile, the non-zero p-elements $\{1, 2, ..., p-1\}$ in F_p forms an abelian group under multiplication where 1 is considered as the multiplicative identity. Some arithmetic operations exist in F_p in shown in the example below.

Example 1.2.1. *A finite field F_p with $p = 17$ have the following arithmetic operations:*

1. ***Addition:*** $13 + 12 = 12 + 13 = 8$.

2. ***Substraction:*** $11-16=12$.

3. ***Multiplition;*** $13\cdot 2=26=9$.

4. ***Inversion:*** $12^{-1}=10$ *since* $12\cdot 10=120=1$.

Since $char(K)\neq 2,3$, one can transform Eq. (1.1) into

$$E: y^2 = x^3 + Ax + B, \tag{1.2}$$

where $A,B\in K$ (Silverman, 2009). The discriminant Δ of Eq. (1.2) (Cohen et al., 2006) is equal to the polynomial discriminant of $f(x)$ where

$$E: y^2 = x^3 + Ax + B := f(x),$$

which is the product of the differences of zeroes of $f(x)$, which endowed with the constant

$$\Delta = -16(4A^3 + 27B^2). \tag{1.3}$$

To make Δ is well-defined, it is important to consider it modulo 12-th power in K. Meanwhile, the j-invariant for Eq. (1.2) is defined by

$$j(E) = 12^3\frac{-4A^3}{\Delta} = 1728\frac{4A^3}{4A^3+27B^2} \tag{1.4}$$

(Silverman, 2009). An elliptic curve with a given j-invariant can be constructed by using Eq. (1.4), where $E_{j_E}: y^2 = x^3 + Ax + B$. Figure 1.2 shows a few types of elliptic curves based on Eq. (1.2) with respective values for A and B.

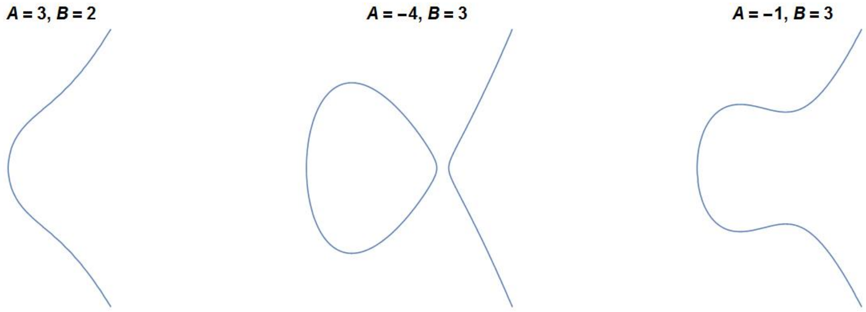

Figure 1.2: Examples of elliptic curves

The set of rational points in an affine coordinate in E defined over an extension field L of K is given by

$$E(L) = \left\{(x,y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_3x - a_6 = 0\right\} \cup \{\mathcal{O}_E\},$$

(Hankerson et al., 2004) where $\mathcal{O}_E$ is point at infinity or the identity element in E. Geometrically, $\mathcal{O}_E$ sits infinitely far up the y-axis (Koblitz, 1991).

The set of points in E form an abelian additive group satisfy the following properties (Washington, 2007):

1. **Commutative:** $P_1 + P_2 = P_2 + P_1$ for P_1, P_2 in E.

2. **Associative:** $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for P_1, P_2, P_3 in E.

3. **Existence of identity:** Given a point P in E. There exists $\mathcal{O}_E$ in E with $P + \mathcal{O}_E = \mathcal{O}_E + P = P$.

4. **Existence of inverse:** Given a point P in E. There exists $-P$ in E with $P +$

$(-P) = -P + P = \mathcal{O}_E$. $-P$ is called the inverse of P where it just a reflection of P over the x-axis. If $P = (x, y)$, then $-P = (x, -y)$.

The cardinality of this additive group denoted as $\#E(F_p)$ is given by $\#E(F_p) = nh$ where n is a prime number and h is the cofactor of elliptic curves. A cofactor h is a prime divisor of $\#E\left(F_p\right)$ where $h = \frac{\#E\left(F_p\right)}{n}$ (Galbraith, 2012). For cryptographic purpose, $h \leq 4$ (Longa & Sica, 2012). The additive group consists of points defined in the elliptic curve with coordinate (x, y) where $x, y \in F_p$. In other words, there are nh's points in additive group $E(F_p)$ including the identity element $\mathcal{O}_E$. In the additive group of $E(F_p)$, there exists a subgroup G with prime order n. In the subgroup G, there exists a cyclic subgroup which is generated by a where $a \in G$ and a is not the identity element. It is known that the order of the element divides the order of the group (Fraleigh, 2004). Since G has prime order n which is only divisible by 1 and itself, where the only element of order one is the identity element, this implies the order of a is equal to the order of G and a generates G. Thus, G is a cyclic subgroup. Since $G \subset E(F_p)$, where $E(F_p)$ consists of points defined in E over F_p, thus G also consists of points in $E(F_p)$. In other words, every point in G is the generator of G. Thus, the prime subgroup of $E(F_p)$ can be generated by knowing only a single point P which belongs the respected prime subgroup by using arithmetic operation defined in elliptic curve.

Two main point arithmetic operations in elliptic curve are point addition and point doubling. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on elliptic curve defined over F_p, where $P \neq Q$. The geometry of point addition $P + Q = R = (x_3, y_3)$ is as follows:

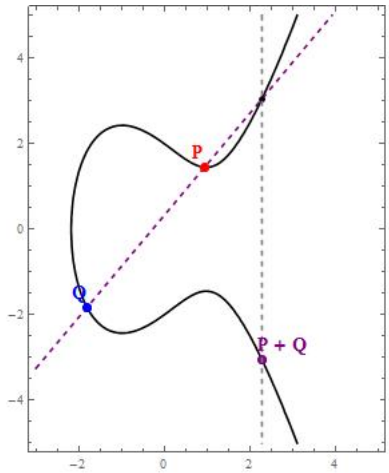

Figure 1.3: Point addition

The point addition $P+Q$ can be computed using this formula:

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

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

(Silverman, 2009). As can be seen, m needs one inversion operation, x_3 needs one squaring and y_3 needs two multiplications. Different operations require different running time. As the number of operation increases, the computational cost also increases. Thus, the computational cost is represented by the total number of operations. The cost of computing a point addition is $2M + 1S + 1I$ where M, S, I denote the multiplication, squaring and inversion operations, respectively.

By using same description, the geometry of point doubling $P+P = R = (x_3, y_3)$ for Eq. (1.2) where $E : y^2 = x^3 + Ax + B$ is as follows:

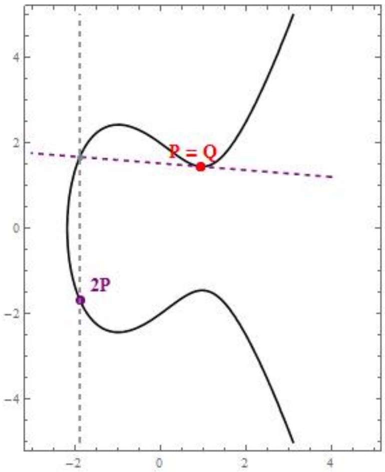

Figure 1.4: Point doubling

Point doubling (Silverman, 2009) can also be computed by using this formula:

$$m = \frac{3x_1^2 + A}{2y_1}$$

$$x_3 = m^2 - 2x_1$$

$$y_3 = m(x_1 - x_3) - y_1.$$

As can be seen, m needs one squaring and one inversion operation, x_3 needs one squaring and y_3 needs two multiplications. Thus, cost of computing a point doubling is $2M + 2S + 1I$ where M, S, I denote the multiplication, squaring and inversion operations, respectively.

The point addition and point doubling arithmetic operations are important in ECC, especially to generate the public key. The following steps ECC and point arithmetic operation play roles in public key cryptography:

1. Alice and Bob agree on certain parameters, such as an elliptic curve E defined

over the finite prime field F_p, a point P with large prime order n.

2. Alice chooses her secret key, $k_A \in [1, n-1]$.

3. Alice computes her own public key, $Q_A = k_A P$ and then she sends it to Bob.

4. Bob chooses his secret key, $k_B \in [1, n-1]$.

5. Bob computes his own public key, $Q_B = k_B P$ and then he sends it to Alice.

6. They both can compute $Q_A \cdot Q_B$ which are their shared secret key.

Every secret key and public key refer to points on an elliptic curve. In elliptic curve public key cryptography, the secret messages are being embedded on the points of elliptic curves. Only if Alice and Bob able to compute the shared secret key correctly, then they can read the secret messages. However, the cost of computing the shared secret key and also the public requires high computational time resulting in high computational cost. The process of computing these keys is called the elliptic curves scalar multiplication (ECSM) denoted as kP where $P \in E(F_p)$ and k is the secret key chosen from $[1, n-1]$. Generally, to compute kP, one needs $(k-1)$ addition processes where

$$kP = \underbrace{P + P + \cdots + P + P.}_{\text{adding } P \text{ by } k\text{-times}}$$

One can also use repeated point additions and point doublings to compute kP. In order to know the number of doubling and addition operations needed to compute kP, the scalar k needs to be changed into its binary form representation where the bit length and Hamming weight are determined. The bit length of k refers to the length of the binary representation of k. While, the Hamming weight of an integer k is defined as the number of ones in its binary expansion, denoted as w (Galbraith, 2012). The number of addition operations needed to compute kP depends on the Hamming weight of k in its binary representation, while the number of doubling operations needed depends on the bit length of k in its binary representations.

However, the problem arises when the subgroup has a very large prime order which causes the scalar multiplication to have high computational cost due to the higher number of operation needed to compute kP. As the number of operations getting bigger, the running time will be higher, resulted in higher computational cost. Hence, many researchers try to speed up and reduce the cost of computing kP so that it requires less running time and storage, and it can be beneficial to elliptic curve cryptosystem. One of the methods to speed up and reduce the cost of computing scalar computation is by employing the efficiently computable endomorphism such as the Frobenius endomorphism and endomorphism with complex multiplication.

An endomorphism is a homomorphism ϕ where $\phi : E \mapsto E$ which is given by rational function $\phi(x,y) = (R_1(x,y), R_2(x,y))$ (Washington, 2007). Every endomorphism satisfies a quadratic characteristic polynomial with integer coefficients (Galbraith, 2012). A Frobenius endomorphism for $char(K) = 2$ is the morphism from E to E which maps $\tau(x,y) = (x^2, y^2)$ (Park et al., 2002) with characteristic polynomial of $\tau^2 - t\tau + 2 = 0$. Meanwhile, Frobenius endomorphism for $char(K) = p$ maps $\pi(x,y) = (x^p, y^p)$ (Itjima et al., 2002). While, an endomorphism with complex multiplication is an endomorphism with characteristic polynomial of complex roots which is given by

$$\Phi^2 - t_\Phi + n_\Phi = 0 \tag{1.5}$$

where $t_\Phi = \Phi + \hat{\Phi}$ is the trace of endomorphism Φ and $n_\Phi = \Phi \cdot \hat{\Phi}$ is the norm of endomorphism Φ (Silverman, 2009).

The existence of the rational function of an endomorphism allows the scalar multiplication to skip the process of repeated additions and doublings. If the rational function is well-defined and requires a small number of operations, then the endomorphism is said to be efficiently computable. The existence of efficiently computable endomorphism accelerates the scalar multiplication kP in an elliptic curve since it allows the scalar multiplication to be computed easily with less number of operation.

1.3 Literature Review

Scalar multiplication, kP is one of the most critical operations in ECC, where k is the secret key and P belong to the prime subgroup with order n in $E(F_p)$. This operation consumes most of the operation time, especially when dealing with large prime field due to a higher number of operations. Other than that, it requires more storage as the field getting larger. In the past few years, many researchers proposed various methods to accelerate and reduce the cost of computing kP to overcome this problem. However, this operation still needs further improvement.

Previous studies show that the use of an efficiently computable endomorphism can be applied to improve the performance of scalar multiplication (Gallant et al., 2001; Part et al., 2005). One of the efficiently computable endomorphism is Frobenius endomorphism. In 1992, Neal Koblitz employed the Frobenius endomorphism on curves with characteristic 2 ($char(K) = 2$ or a binary field), which is known as the Koblitz curves (Koblitz, 1991) by using τ-adic expansion. Define the Koblitz curves as $E_a : y^2 + xy = x^3 + ax^2 + 1$ where $a \in \{0,1\}$. A Frobenius endomorphism is the morphism which maps $\tau(x,y) = (x^2, y^2)$ (Park et al., 2002). The characteristic polynomial of a Frobenius maps for $char(K) = 2$ is given by $\tau^2 - t\tau + 2 = 0$, where t is the trace of Frobenius and $t = (-1)^{1-a}$. The Frobenius map on elliptic curve with $char(K) = 2$ can be considered as the complex multiplication by $\tau = \frac{1+\sqrt{-7}}{2}$ or $\tau = \frac{-1+\sqrt{-7}}{2}$. This endomorphism was able to speed up computation on the elliptic curve defined over the binary field (Solinas, 2000; Yunos et al., 2015). The following example on the implementation of Frobenius endomorphism via τ-adic expansion.

Example 1.3.1. *Let the Frobenius endomorphism acted on a point $P \in E(F_p)$ be defined as $\tau^2(P) - \tau(P) + 2(P) = 0$. Then, $2P$ can be written as $2 = \tau - \tau^2$.*

$$\begin{aligned}
7 &= 1 + 3(2) \\
&= 1 + 3\left(\tau - \tau^2\right) = 1 + 3\tau - 3\tau^2 \\
&= 1 + \tau(3 - 3\tau) = 1 + \tau(1 + 2 - \tau - 2\tau) \\
&= 1 + \tau + \tau\left(\tau - \tau^2\right) - \tau^2 - \tau^2\left(\tau - \tau^2\right) \\
&= 1 + \tau - 2\tau^3 + \tau^4 \\
&= 1 + \tau - \tau^3\left(\tau - \tau^2\right) + \tau^4 \\
&= 1 + \tau + \tau^5
\end{aligned}$$

Since $\tau(x,y) = (x^2, y^2)$, then

$$\begin{aligned}
7P &= P + \tau(P) + \tau^5(P) \\
&= (x,y) + (x^2,y^2) + (x^2,y^2)^5 \\
&= (x,y) + (x^2,y^2) + (x^{32},y^{32}).
\end{aligned}$$

However, the Frobenius map only worked for the field with $char(K) = 2$. Later in 2001, Gallant et al. proposed a method to speed up the computation of kP that works on the large prime field, F_p. They work with elliptic curves with $char(K) \neq 2,3$ which is defined in Eq. (1.2), $E : Y^2 = X^3 + AX + B$. This method employs an efficiently computable endomorphism, and it is known as the Gallant, Lambert and Vanstone (GLV) method (Gallant et al., 2001). The key idea for this method is the scalar k is decomposed into two scalars, k_1 and k_2 where each of the decomposed scalars has half bit length of k (Ciet et al., 2003). The general formula of the GLV method is as follows:

$$kP = k_1 P + k_2 \Phi(P), \tag{1.6}$$

where Φ is the efficiently computable endomorphism acted on P with prime order n. The characteristic polynomial for Φ is $\Phi^2 + r\Phi + s = 0$ and has root λ. Following Eq. (1.5), $r = -t_\Phi$ and $s = n_\Phi$ where $t_\Phi = \Phi + \hat{\Phi}$ the trace of endomorphism Φ and $n_\Phi = \Phi \cdot \hat{\Phi}$ as the norm of endomorphism Φ (Silverman, 2009). The GLV method considers the group homomorphism :

$$f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_n \tag{1.7}$$

$$(i, j) \quad \mapsto i + \lambda j \pmod{n}. \tag{1.8}$$

GLV method needs two short vectors $v_1, v_2 \in \mathbb{Z} \times \mathbb{Z}$ such that $f(v_1) = f(v_2) = 0$. These vectors are independent toward k but dependent on λ. Such vectors can be obtained by using Extended Euclidean algorithm (EEA). Then, by using Babai's rounding to solve the closest vector problem, a vector $u = \mathbb{Z}v_1 + \mathbb{Z}v_2 = (k_1, k_2)$ that is closed to $(k,0)$ is computed, where

$$u=(k_1,k_2)=(k,0)-(\lfloor b_1 \rceil v_1+\lfloor b_2 \rceil v_2). \tag{1.9}$$

The vector $(k,0)$ is given by $(k,0)=b_1v_1+b_2v_2$ where $\lfloor b \rceil$ is the nearest integer to b.

The GLV method was able to accelerate the scalar computation roughly by 50% as long as the condition of GLV method where $max\{|k_1|,|k_2|\} \leq \sqrt{n}$ is satisfied, and the endomorphism is efficiently computable (Park et al., 2002). Since then, many researchers proposed various approaches extension to the GLV method.

Park et al. (2002) extended the GLV method by studying the algebraic structure of decomposing k. They used μ-Euclidean algorithm where they used the μ-Euclidean ring $\mathbb{Z}[\Phi]$ such that $\mathbb{Z}[\Phi] \subset End(E) \subset \mathbb{Q}\left(\sqrt{-D}\right)$. They proved that there exists an element $\alpha=a+b\Phi \in \mathbb{Z}(\Phi)$, such that the norm of alpha $n_\alpha=s_nn$ and $\alpha P=\mathcal{O}_E$ where $s_n \leq 3$, and $s_n=1$ if $\mathbb{Z}[\Phi]$ is the maximal order. The value for α can be found using Shanks' algorithm and lattice reduction method. Additionally, in the same year, Itjima et al. (2002) extended the GLV method; but instead of using the efficiently computable endomorphism Φ, they used the Frobenius endomorphism Ψ on the quadratic twist of the elliptic curve with genus one. They defined the p-th power Frobenius map over F_{p^n} where $\Psi_p=\phi\pi\hat{\phi}$ and $\Psi_p:\bar{E}(F_{p^n}) \rightarrow \bar{E}(F_{p^n})$ such that $\Psi_p:(x,y) \mapsto \left(c^{1-p}x^p, c^{\frac{3-3p}{2}}y^p\right)$. Note that, $\hat{\phi}$ is the isogeny from $\bar{E}$ to E defined over F_{p^n}, pi is the isogeny from E to E and ϕ is the isogeny from E to $\bar{E}$ defined over F_{p^n} (Galbraith et al., 2009).

The original GLV method did not come up with an explicit or clear upper bound for the decomposed scalars. This allows Sica et al. (2002) to fill the gap and they successfully obtained the explicit bound for the decomposed scalars in GLV method. Later, in 2009, Galbraith et al. extended the studies of GLV method on elliptic curves defined over F_{p^2}, their method is known as Galbraith, Lin and Scott (GLS) method. As mentioned in Section 1.2, F_{p^2} is the extension field of finite field F_p with $q = 2$. The $E(F_{p^2})$ curves are also known as the GLS curves. GLS used the p-Frobenius endomorphism with characteristic polynomial $\Psi^2 + 1 = 0$ to be applied on $E(F_{p^2})$ curves. In 2010, Zhou et al. came up with three-dimensional GLV method on some GLS curves, specifically on elliptic curves with j-invariant 0. They proposed the scalar k is decomposed into three scalars where

$$kP = k_0P + k_1\Phi(P) + k_2\Psi(P) \tag{1.10}$$

where $\Phi(P) = \lambda_1 P$ and $\Psi(P) = \lambda_2 P$. Besides, they defined the homomorphism for three-dimensional GLV as $f : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/n$. They used the Lenstra, Lenstra, Lovasz (LLL) algorithm on $w_0 = (n, 0, 0), w_1 = (\lambda_1, -1, 0)$ and $w_2 = (\lambda_2, 0, -1)$ to obtain the short vectors v_0, v_1 and v_2.

Later in 2012, Longa and Sica proposed a four-dimensional GLV scalar multiplication on a quadratic extension of the large prime field, F_{p^2} (Longa & Sica, 2012). They combined both Frobenius and efficiently computable endomorphism where the general formula is given as

$$kP = k_1P + k_2\Phi(P) + k_3\Psi(P) + k_4\Phi\Psi(P). \tag{1.11}$$

Since it is a four-dimensional scalar multiplication, they used the Cornacchia algorithm instead of using Extended Euclidean algorithm or LLL to compute the lattice basis v_1, v_2, v_3 and v_4. Also in the same year, Hu et al. (2012) studied the four-dimensional GLV on GLS curves with j-invariant 0 .

In the following year, Bos et al. (2013a) extended the four-dimensional GLV method on elliptic curves of genus two. Elliptic curves of genus two are also known as the Hyperelliptic curves, $E : y^2 = f(x)$ where $f(x)$ is a polynomial of degree five or six. They implemented the four-dimensional GLV method on Buhler-Koblitz curves, $y^2 = x^5 + B$ and Furukawa-Kawazoe-Takahashi curves, $y^2 = x^5 + Ax$. In the same year, Bos et al. (2013b) extended the GLV method to eight-dimensional GLV/GLS decomposition method and implemented it on genus two curves.

Later in 2014, Hernández et al. studied the efficient and secured algorithm for GLV scalar multiplication and implemented it on GLV-GLS curves. In the following year, Smith (2015) proposed an easy scalar decomposition for efficient scalar multiplication on elliptic curves and genus two Jacobian. He suggested the short basis in the integer lattice involving the eigenvalues of the endomorphism for the GLV, GLS and GLV+GLS curves. Lastly, Kwon et al. (2018) studied on the implementation of the four-dimensional GLV proposed by Longa and Sica (2012) on several bits of micro-controllers.

All these variants extensions of GLV method satisfy the same condition as the original GLV method where the bit length of the decomposed scalars k_1 and k_2 should be half of bit length k, such that $max\{|k_1|,|k_2|\} \leq \sqrt{n}$. However, not all k's can be successfully decomposed into k_1 and k_2 that fall within that condition. Thus, Ajeena and Kamarulhaili (2013) proposed a method known as the Integer Sub-Decomposition (ISD) method to solve the scalar multiplication problem when $min\{|k_1|,|k_2|\} > \sqrt{n}$. They were able to increase the number of successful decomposition of k's (Ajeena & Kamarulhaili, 2014a; 2014b). In 2017, Ajeena and Yaqoob implemented the ISD method on the elliptic el-gamal digital signature algorithm.

The ISD method proposed an additional layer of decomposition to the GLV method, such that when $min\{|k_1|,|k_2|\} > \sqrt{n}$, these scalars are being further decomposed into $k_{1,1}, k_{1,2}$ and $k_{2,1}, k_{2,2}$, respectively with the help of two other endomorphisms Φ_1 and Φ_2. The general formula for the ISD method is as follows:

$$\begin{aligned} kP &= k_1P + k_2\Phi(P) && (1.12) \\ &= k_{1,1}P + k_{1,2}\Phi_1(P) + k_{2,1}P + k_{2,2}\Phi_2(P) && (1.13) \end{aligned}$$

where $\Phi_1(P) = \lambda_1 P$ and $\Phi_2 P = \lambda_2 P$.

As it can be seen, Eq. (1.13) have similar form as Eq. (1.11). However, Eq. (1.11) is a four-dimensional problem while Eq. (1.13) is a two-dimensional problem. Since it is a two-dimensional problem, it uses the same group homomorphism as defined in Eq. (1.7), and the same approach as in the GLV method to solve the closest vector problem to obtain the decomposed scalars. By adopting the Extended Euclidean algorithm on $(n,\lambda),(n,\lambda_1)$ and (n,λ_2), they obtained the short vectors $(v_1,v_2),(v_3,v_4)$ and (v_5,v_6), respectively.

However, the ISD method uses trivial endomorphisms where the minimal polynomial for the endomorphism is given by $\Phi - \lambda = 0$. These endomorphisms are not efficiently computable since $\lambda, \lambda_1, \lambda_2$ in the ISD method are defined in $\mathbb{Z}$, where these values are chosen randomly from interval $[1, n-1]$, such that $\lambda_1 \neq \pm\lambda_2$ (Ajeena and Kamarulhaili, 2014a).

1.4 Problem Statement

For the past few years, researchers tried to reduce the cost of computing the scalar multiplication *kP* in elliptic curves cryptography by introducing methods and algorithms such as GLV and ISD method. The GLV method suggested that the multiplier k being decomposed into two mini scalars with condition $max\{|k_1|, |k_2|\} \leq \sqrt{n}$. This method is effective provided that the endomorphism can be evaluated at a constant time and the condition for mini-scalars is satisfied. It suffices to know that one can reduce the cost of computing *kP* if the decomposition is short and the endomorphism is efficiently computable (Smith, 2015). As mentioned in Section 1.2, the endomorphism is said to be efficiently computable if it costs less than a small number of point doubling where each point doubling costs 2 multiplications, 2 squarings and 1 inversion operation.

Nonetheless, the GLV method is unable to decompose all scalar $k \in [1, n-1]$ into k_1, k_2 which are less or equal to $\sqrt{n}$. To increase the number of successful decomposition of scalar k, Ajeena and Kamarulhaili (2013) proposed the ISD method. The ISD method employs a double layer decomposition, which extends the decomposition of GLV method when $min\{|k_1|, |k_2|\} > \sqrt{n}$. As a result, the ISD method has longer decomposition process and higher computational cost. The only way to lower down the computing cost is by using the endomorphism that is efficiently computable.

The ISD method proposed by Ajeena and Kamarulhaili (2014a) used trivial endomorphisms defined over $\mathbb{Z}$, with the characteristic polynomial of degree one, $X - \lambda = 0$. These endomorphisms could not be evaluated easily. The values for λ in the ISD method were selected randomly from $[1, n-1]$ which made these endomorphisms ring isomorphic to the ring of integers. Since the endomorphisms are defined over $\mathbb{Z}$, the ISD method was unable to solve complex multiplication on elliptic curves. These cause the ISD method to have higher computation cost.

Therefore, this thesis aims to improve the current ISD method and to reduce the cost of computing kP using the ISD method by implementing the efficiently computable endomorphism which represents the complex multiplication. In order for the ISD method to allow complex multiplication, the endomorphism ring defined in this method should be larger than $\mathbb{Z}$, where the endomorphism ring is defined over the imaginary quadratic field. Some elliptic curves are defined over specific imaginary quadratic field based on their j-invariant. These imaginary quadratic field have properties which later helps to define the endomorphism acted on these elliptic curves.

1.5 Research Objectives

The objectives of this study are as follows:

1. To determine the properties of elliptic curves with $j(E) = 0, 1728, 8000, 54000$.
2. To develop an efficiently computable endomorphism with complex multiplication acted on elliptic curves with $j(E) = 0, 1728, 8000, 54000$

3. To compare the number of operations needed to compute scalar multiplication kP among repeated additions and doublings approach (via Right-to-Left algorithm), GLV method and ISD method.

4. To evaluate the operation counts on each of the derived efficiently computable endomorphism for E_0, E_{1728}, E_{8000} and E_{54000}.

1.6 Thesis Outline

This thesis consists of seven chapters where the organization is as follows:

Chapter 1 discusses the definition of elliptic curves and the group law acting on the points on elliptic curves. It also includes the literature review which consists of previous studies on the elliptic curve scalar multiplication, problem statement and research objectives.

Chapter 2 is the preliminaries chapter which introduces all basic concepts about linear algebra, quadratic field, prime numbers, and elliptic curves relevant to this study. It also includes some preliminary results we obtained throughout this study.

Chapter 3 discusses the properties of the elliptic curves with j-invariant 0 and the construction of three efficiently computable endomorphisms defined on it. This chapter also includes the lower and upper bound for each of the decomposed scalars on this curve.

Chapter 4 explains the properties of the elliptic curves with j-invariant 1728 and the construction of efficiently computable endomorphisms defined on it. Similar to

Chapter 3, this chapter also discusses the lower and upper bound for each of the decomposed scalars on this curve.

Chapter 5 presents the result for efficiently computable endomorphism acting on the other elliptic curves namely elliptic curves j-invariant 8000 and 54000.

Chapter 6 discusses the operation counts among repeated additions and doublings (via Right-to-Left algorithm), GLV method and ISD method. This chapter evaluates the operation counts for each of efficiently computable endomorphism defined throughout this study. Next, a comparison is made between the operation counts of the ISD method with and without using efficiently computable endomorphism.

Chapter 7 is the final chapter which summarises and conclude the thesis.

1.7 Summary

This introductory chapter succinctly explains the background of elliptic curves and literature review on the elliptic curve scalar multiplication. Followed by the problem statements as well as the research objectives. Lastly, it describes the contents of each chapter in this thesis.

CHAPTER 2

PRELIMINARIES

2.1 Introduction

This chapter highlights the basic concepts related to the elliptic curves scalar multiplication. Section 2.2 recalls several facts on the algebraic structure of linear algebra which include group, ring, and field theory. Sections 2.3 and 2.4 discusses the facts related to the quadratic field and prime numbers. Section 2.5 highlights several important concepts related to elliptic curves. The following section discusses the concept of isogeny on the elliptic curve. Next section explains the concept of Frobenius endomorphism and endomorphism with complex multiplication on elliptic curves. The last section discusses previous results that are related to this study which includes some preliminary results that are obtained throughout this study. Also included, the Right-to-Left algorithm to compute scalar multiplication which applies repeated additions and doublings.

2.2 Group, Ring and Field

This section provides a mathematical background related to group, ring and field.

Definition 2.2.1. *(Humpreys, 1996) A group is a non-empty set G together with a binary operation, $\circ$, with the following properties:*

1. ***(Closure)*** *For $a,b \in G$, then $a \circ b$ is in G.*

2. ***(Associative)*** *For $a,b,c \in G$, then $(a \circ b) \circ c = a \circ (b \circ c)$.*