IMPROVED ALGORITHMS OF ELLIPTIC CURVE POINT MULTIPLICATION OVER BINARY AND PRIME FIELDS USING ELLIPTIC NET

By

NORLIANA BINTI MUSLIM

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

June 2022

IPM 2022 16

DEDICATIONS

This thesis is dedicated to

My dear husband:
Zuhairy

My lovely kids:
Luqman and Umar

My beloved parents:
Mak, abah, mama, babah

With love, respect and a bunch of memories
Indeed, we belong to Allah and indeed to Him we will return

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

IMPROVED ALGORITHMS OF ELLIPTIC CURVE POINT MULTIPLICATION OVER BINARY AND PRIME FIELDS USING ELLIPTIC NET

By

NORLIANA BINTI MUSLIM

June 2022

Chairman : Faridah Yunos, PhD
Institute : Mathematical Research

The elliptic curve cryptosystem (ECC) is applied to meet the requirement for public-key cryptosystem, mainly because ECC has shorter key lengths, and its algorithms are more efficient than Rivest-Shamir-Adleman (RSA) cryptosystem. The elliptic curve point multiplication (ECPM) operation in ECC faces, however, major computational efficiency issue. The primary objective of this study is to improve the performance of ECPM algorithm of ECC using the elliptic net (EN) method in affine coordinate over binary and prime fields. In particular, this study looked into point and field arithmetic levels over the elliptic curve. The literature depicts that point multiplication (PM) can be computed using double (DBL) and double add (DBLADD) via binary method (BM), but this method rely on the Hamming weight of scalar. As a consequence, PM computation via BM is costly. The EN method is an alternative in ECPM computation since the first DBL and DBLADD via EN in the literature appear to dismiss the Hamming weight of scalar. In this study, the proposed DBL and DBLADD algorithm using the Karatsuba method for non-supersingular Koblitz curve over *m* bits binary field with $gcd(2^m–1, 3)=1$ that incorporates eight blocks of EN with three temporary variables saved two multiplications or 9.09% in DBL and DBLADD algorithms, in comparison to the recent literature pertaining to EN. For safe curves of 283, 409, and 571 bits over binary field, upon comparison with BM algorithm, the developed ENPM algorithm to enhance computational efficiency of ECC displayed better performance in overall multiplications based on the following average values; 8.70%, 8.79%, and 8.85% respectively, thus successfully speeding up the running time by an average of 9.00%. The designed ENPM algorithm over binary field gained 9.06%, 9.07%, and 9.07% respectively, and 9.06% average rapid time in comparison to eight blocks of EN method. The proposed DBL and DBLADD algorithm via EN using Karatsuba method for Twisted Edwards curve over *p* prime field with $gcd(p–1, 3)=1$ that embeds seven blocks of EN and three temporary variables saved two multiplications and squaring or 12.5% multiplication and 20% squaring in DBL, while one multiplication and two squaring or 6.25% multiplication and 20% squaring in DBLADD, in comparison

to EN with 10 temporary variables. For safe curves of 384 and 512 bits, the developed ENPM algorithm over prime field outperformed the BM algorithm in terms of overall multiplications with 57.60% and 59.16% average running time. The developed ENPM method performed better than eight blocks of EN for short Weierstrass curve with averages of 31.26% and 31.02%. The designed ENPM algorithm also exhibited better performance in terms of overall multiplication and running time by averages 13.17% and 13.22%, in comparison to EN with 10 temporary variables for short Weierstrass curve.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

TAMBAH BAIK ALGORITMA PENDARABAN SKALAR KELUK ELIPTIK MERANGKUMI MEDAN BINARI DAN PERDANA MENGGUNAKAN JEJARING ELIPTIK

Oleh

NORLIANA BINTI MUSLIM

Jun 2022

Pengerusi : Faridah Yunos, PhD
Institut : Penyelidikan Matematik

Sistem kripto keluk eliptik (ECC) digunakan untuk memenuhi keperluan sistem kripto kekunci awam, terutamanya kerana sistem ECC memiliki kunci yang lebih pendek dan algoritma-algoritma yang lebih berkesan berbanding sistem kripto Rivest-Shamir-Adleman (RSA). Namun begitu, operasi pendaraban titik keluk eliptik (ECPM) dalam sistem ECC menghadapi masalah kecekapan pengiraan. Objektif utama kajian ini adalah untuk menambahbaik prestasi algoritma ECPM menggunakan kaedah jejaring eliptik (EN) dalam koordinat afin ke atas medan binari dan perdana. Kajian ini secara khusus menyasar pada tahap aritmetik titik dan aritmetik medan ke atas keluk eliptik. Berdasarkan kajian lepas, pendaraban titik (PM) boleh dikira menggunakan kaedah berganda (DBL) dan penambahan berganda melalui binari (BM), tetapi kaedah ini bergantung kepada pemberat Hamming skalar. Oleh itu, pengiraan PM melalui BM mempunyai kos pengiraan yang tinggi. Kaedah EN adalah alternatif kepada pengiraan ECPM memandangkan kaedah pertama yang dibangunkan dalam kajian lepas tidak bergantung kepada pemberat Hamming skalar. Dalam kajian ini, algoritma DBL dan DBLADD yang dicadangkan melalui EN menggunakan kaedah Karatsuba melalui keluk Koblitz tak-super-tunggal untuk medan binari dengan bit m berserta $pst(2^m - 1, 3)=1$ yang menggunakan lapan blok EN dengan tiga pembolehubah sementara telah menjimatkan kos sebanyak dua pendaraban atau 9.09% dalam algorithma DBL dan DBLADD berbanding dengan kajian EN yang lepas. Untuk keluk selamat bagi 283, 409, dan 571 bit ke atas medan binari, ENPM yang dibangunkan bagi meningkatkan kecekapan pengiraan ECC menunjukkan prestasi lebih baik berbanding kaedah binari (BM) bagi keseluruhan pendaraban berdasarkan nilai purata masing-masing sebanyak 8.70%, 8.79%, dan 8.85% serta berjaya mempercepatkan masa dengan purata 9.00%. Jika dibandingkan dengan kaedah lapan blok EN, algoritma ENPM yang direka bentuk ke atas medan binari masing-masing memperolehi 9.06%, 9.07%, dan 9.07% dengan purata masa yang lebih laju sebanyak 9.06%. Algoritma DBL dan DBLADD yang dicadangkan melalui EN menggunakan kaedah Karatsuba

ke atas keluk Twisted Edwards untuk medan perdana *p* berserta *pst*(*p* – 1, 3)=1 berdasarkan tujuh blok EN dengan tiga pembolehubah sementara telah menjimatkan kos dua operasi pendaraban dan dua operasi kuasa dua iaitu sebanyak 12.5% pendaraban dan 20% kuasa dua dalam DBL, manakala satu operasi pendaraban dan dua operasi kuasa dua atau 6.25% pendaraban dan 20% kuasa dua dalam DBLADD, berbanding dengan EN bersama 10 pembolehubah sementara. Untuk keluk selamat bagi 384 dan 512 bit, algoritma ENPM yang dibangunkan ke atas medan perdana mengatasi algoritma BM bagi keseluruhan pendaraban dengan purata tempoh perlaksanaannya sebanyak 57.60% dan 59.16%. Pada panjang bit yang serupa, bagi jumlah pendaraban dan masa perlaksanaan, algorithma ENPM yang dibangunkan berprestasi lebih baik daripada lapan blok EN keluk Weierstrass pendek dengan purata sebanyak 31.26% dan 31.02%. Algorithma yang direka bentuk juga menunjukkan prestasi lebih baik bagi keseluruhan pendaraban dan masa perlaksanaan dengan purata sebanyak 13.17% dan 13.22%, berbanding dengan lapan blok EN bersama 10 pembolehubah sementara untuk keluk pendek Weierstrass.

ACKNOWLEDGEMENTS

With the name of Allah, the Most Compassionate and Most Merciful.

All praise and thanks to Almighty Allah, His blessing has given me the strength and passion to complete my research work and compile this thesis successfully.

To my mentor, Assoc. Prof. Dr. Mohamad Rushdan bin Md. Said, I would like to express my sincere gratitude for the continuous support given for my study, as well as for his patience, inspiration, enthusiasm, and vast expertise. His advice had helped me throughout this period of research work and writing. My gratitude also goes to my supervisor, Dr. Faridah binti Yunos, as well as committee members Prof. Dr. Mohamed Rezal bin Kamel Ariffin and Dr. Mohamat Aidil bin Mohamat Johari for valuable advice.

I am thankful to my husband and parents, who showered me moral and emotional support, especially when I was facing my weakest moments. I am also grateful to all my family members and friends who had helped me along my academic journey.

Last but not least, my special appreciation goes out to all members of the Institute for Mathematical Research for providing exceptional research facilities to students, myself alike.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Faridah binti Yunos, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Mohamed Rezal bin Kamel Ariffin, PhD
Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Member)

Mohamat Aidil bin Mohamat Johari, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Member)

Mohamad Rushdan bin Md Said, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

ZALILAH BINTI MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 12 January 2023

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ________________________ Date: __________________

Name and Matric No.: Norliana Binti Muslim

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature:	
Name of Chairman of Supervisory Committee:	Dr. Faridah binti Yunos
Signature:	
Name of Member of Supervisory Committee:	Prof. Dr. Mohamed Rezal bin Kamel Ariffin
Signature:	
Name of Member of Supervisory Committee:	Dr. Mohamat Aidil bin Mohamat Johari
Signature:	
Name of Member of Supervisory Committee:	Assoc. Prof. Dr. Mohamad Rushdan bin Md Said

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AS	Addition-Subtraction
AES	Advanced Encryption Standard
ANOVA	Analysis of Variance
BM	Binary Method
DBL	Double
DBLADD	Double add
DLP	Discrete Logarithm Problem
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellman
ECDL	Elliptic Curve Discrete Logarithm
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECPM	Elliptic Curve Point Multiplication
EDS	Elliptic Divisibility Sequences
EN	Elliptic Net
ENPM	Elliptic Net Point Multiplication
LHS	Left-hand Side
NIST	National Institute of Standard and Technology
NUMS	Microsoft Nothing Up My Sleeve
PM	Point Multiplication
RHS	Right-hand Side
RSA	Rivest-Shamir-Adleman

LIST OF NOTATIONS

F_p	Prime field
F_q	Finite field of *q* elements
F_{2^m}	Binary field
K	Field K
$\#E$	Number of points on the curve
$\mathbf{Z}$	Set of integers
N	Set of natural numbers
Q	Set of rational numbers
E(Q)	Elliptic curve over rational numbers
R	Set of real numbers
C	Set of complex numbers
O	Point at infinity
Δ	Discriminant
C_f	Co-factor
N_p	Order of point
$\tilde{\alpha}$	Second term elliptic net
$\langle W(\mu_i) \rangle$	Block centred at μ_i
h	Hamming weight
l	Bit length
r	Pearson correlation
N	Sample size
df	Degrees of freedom
R^2	Coefficient of determination
F	Variance ratio

t	Test statistic for t-test
α	Significance level
CT_0	Explicit formulae related cost of Chen et al. (2017) method
CT_1	Explicit formulae related cost of second proposed over binary field
CT_2	Explicit formulae related cost of Kanayama et al. (2014) and Rao et al. (2019) methods
CT_3	Explicit formulae related cost of second proposed over prime field
CF_{283}	Field operation cost for 283 bits in second proposed over binary field
CF_{409}	Field operation cost for 409 bits in second proposed over binary field
CF_{571}	Field operation cost for 571 bits in second proposed over binary field
CF_{384}	Field operation cost for 384 bits in second proposed over prime field
CF_{512}	Field operation cost for 512 bits in second proposed over prime field
TM_{283}	Total multiplications for 283 bits in second proposed over binary field
TM_{409}	Total multiplications for 409 bits in second proposed over binary field
TM_{571}	Total multiplications for 571 bits in second proposed over binary field
TM_{384}	Total multiplications for 384 bits in second proposed over prime field
TM_{512}	Total multiplications for 512 bits in second proposed over prime field
Y_{HK}	Point multiplication via Hankerson et al. (2004)
Y_{CH}	Point multiplication via Chen et al. (2017)
Y_{SP}	Point multiplication via second proposed over binary field
Y_{HI}	Point multiplication via Hisil et al. (2008)
RT_{SP283}	Running time for 283 bits in second proposed over binary field
RT_{SP409}	Running time for 409 bits in second proposed over binary field

RT_{SP571}	Running time for 571 bits in second proposed over binary field
RT_{FP384}	Running time for 384 bits in second proposed over prime field
RT_{FP512}	Running time for 512 bits in second proposed over prime field

CHAPTER 1

INTRODUCTION

1.1 Overview

The internet is the most effective and valuable knowledge-sharing platform used for communication purposes. To date, not only conventional computers are connected to the internet, but devices such as televisions, tablets, electrical appliances, automobiles, and smartphones are also substantially heterogeneous. The rapid progress of electronic commerce platforms, such as Lazada and Shopee, contributes to the widespread use of online banking transactions. Online transmission of information demands protection due to lurking cyber threats. One method that ascertains data security is secret writing or algorithm known as cryptography.

Cryptographic algorithms are high-performance and safe engines that require considerable design space. If countermeasures are included to thwart intrusion threats, the demands for space and memory further increase. Therefore, cryptographic algorithms have traditionally been incorporated into hardware, including smart cards and 8-bit chips as proprietary designs (Awaludin *et al.,* 2021; Seo *et al.,* 2015).

Practically, algorithms initiated by the crypto communities must meet the fundamental principles of security in terms of confidentiality, availability, integrity, authentication, and non-repudiation (Hankerson *et al.,* 2004; Jesus *et al.,* 2018; Menezes *et al.,* 1997). Cryptographic algorithms are composed of asymmetric and symmetric schemes (Zhang, 2021). The variance between these schemes lies in the key management during the encryption and decryption processes. The encryption process converts plaintext to ciphertext, while the decryption process recovers plaintext from ciphertext. Asymmetric cryptography, or public-key cryptography, uses two keys; one public key to encrypt and one private key to decrypt. Symmetric cryptography uses one single key for both encryption and decryption processes (Zhang, 2021).

Modern cryptosystems are designed mathematically based on several fundamental principle problems. For instance, the RSA cryptosystem (Rivest *et al.,* 1983) depends on integer factorization problem. Hasan *et al.* (2021) asserted that attack in cryptography is one way to solve an issue. The goal of an attack is to devise a quick solution to a problem that relies on an encryption algorithm (Xu *et al.,* 2020). This means; the difficulty of attacking RSA is based on the difficulty of identifying the prime factors of a composite number.

The ElGamal cryptosystem (ElGamal, 1985) is designed based on discrete logarithm problem (DLP). Let $x = g^n \bmod p$. The DLP refers to the problem used to determine the value of *n*. On the other hand, the ElGamal model works by integrating the discrete logarithm and integer factorization problems (Dijesh *et al.,* 2020). Elliptic curve cryptosystem (ECC) was introduced by Koblitz (1987) and Miller (1986b). The cryptosystem was developed based on elliptic curve discrete logarithm problem (ECDLP). Consider an elliptic curve *E* over a finite field F_q, a given point $P \in E(F_q)$ of order N_p and $Q \in E(F_q)$. A problem that is used to determine an integer *n* where $0 \le n \le N_p - 1$ such that $Q = nP$ is known as ECDLP (Adj *et al.,* 2018).

A well-known method of attacking an elliptic curve is DLP, whereby it works slowly for all curves and makes encryption practicable based on the problem (Zargar *et al.,* 2017). For any elliptic curve *E* over a prime field F_p, the base point in $E(F_p)$ must adhere to several properties so that the problem to solve ECDL turns difficult. A crucial property denotes that the elliptic curve group $E(F_p)$ must possess a large subgroup of prime order N_p and a bit length of ~ 160 or above with a small co-factor c_f. According to Scholl (2017), the next property is avoiding weak curves, such that the ECDLP can be solved within short time and the curve must have a large embedding degree to prevent Menezes, Okamoto, and Vanstone attack.

The ECC generates both public and private keys, apart from enabling two parties to communicate in a secure manner. Essentially, a 256-bit key in ECC enables approximately the same safety as a 3072-bit key with RSA (Keerthi & Surendiran, 2017; Wroński, 2016). Mahto and Yadav (2017) reported that in order to obtain 112 bits of security level, ECC only requires a key size of 224 bits and RSA needs 2048 bits of key size. Since ECC required shorter key length, then this attracted researchers to explore more on ECC field.

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the United States government to protect classified information. Table 1.1 lists the estimated, comparable, maximum-security strength for approved asymmetric-key algorithms and AES key lengths (Barker, 2020), where *L* is public key size, *N* is private key size, *k* is size of modulus *n*, *f* is size of N_p, and N_p is the order of base point.

Table 1.1: Comparable security strength of AES keys

AES Security Strength	Finite field	RSA (bits)	ECC (bits)
≤ 80	L = 1024 N_p = 160	$k = 1024$	$f = 160$ - 223
112	L = 2048 N_p = 224	$k = 2048$	$f = 224$ - 255
128	L = 3072 N_p = 256	$k = 3072$	$f = 256$ - 383
192	L = 7680 N_p = 384	$k = 7680$	$f = 384$ - 511
256	L = 15360 N_p = 512	$k = 15360$	$f = 512+$

Referring to Table 1.1, ECC requires a key length of more than 512 bits to be as strong as 256-bit AES. The performance of ECC relies on the efficiency of computing *nP* operation, which is also known as ECPM.

The compression techniques of elliptic curve representation have been patented by the United States National Security Agency held by Certicom (Brown, 2010a). As a provider of wireless security applications and services for information protection, Certicom keeps a patent on efficient multiplication over the binary field in normal representation. Several elliptic curves applied in ECC protocols can be classified to several standards and field sizes. The National Institute of Standard and Technology (NIST) (Standard curve database, 2020a), Brainpool, and Microsoft Nothing Up My Sleeve (NUMS) (Standard curve database, 2020b) are some ECC standards that are considered secure for cryptographic applications. In particular, the ECC domain parameters are given in the following:

q	Field size
G	Base point
b_1, b_2, b_6	Elliptic curve coefficients of type $y^2 + b_1xy = x^3 + b_2x^2 + b_6$
a, d	Elliptic curve coefficients of type $ax^2 + y^2 = 1 + dx^2y^2$
N_p	Order of base point
x, y	Coordinates of x and y for P

1.2 Problem Statement

Point multiplication (PM) is the most vital and expensive operation to implement ECC (Alkhudhayr *et al.,* 2021). Therefore, enhancing the performance of ECPM has always been the most important focus in cryptography. The ECPM is defined as follows:

Definition 1.1. ECPM refers to the operation of computing *n*-multiple of an element in a group of elliptic curves. The computational process is expressed as $Q = nP = \underbrace{P + P + \cdots + P}_{n \text{ times}}$, where *n* is a positive integer called scalar, while *P* and *Q* are points on the curve.

The conventional method to compute ECPM is the binary method (BM), which is based on chord and tangent or points addition and doubling. From Definition 1.1, the PM via BM works as a scalar *n* is decomposed to a binary number where 2*P* denotes DBL, and 2*P* + *P* refers to DBLADD process. According to Miller (1986b), ECPM can be calculated by using division polynomials in polynomial time. This method also known as elliptic net of rank one. Kanayama *et al.* (2014) had adapted this concept to yield the first ENPM on short Weierstrass curve over prime field to enhance PM. After that, the algorithm was improved by deploying the temporary variables method (Rao *et al.,* 2019). The first ENPM over binary field was proposed by Chen *et al.* (2017). The PM via elliptic net (EN) following Definition 1.1 but both DBL and DBLADD processes are based on EN. Given points *P* and *Q*, scalar *n* must be computationally difficult to calculate. Hence, reducing the number of operations in DBL and DBLADD methods can generate faster ENPM and consequently efficient ECC. In fact, many studies have looked into ways to speed up this operation over binary or prime fields (see AbdulRaheem *et al.,* 2019; Al-Saffar & Said, 2015; Bafandehkar *et al.,* 2016; Rao *et al.,* 2019).

Several cryptographic curves have been proposed to provide efficient points addition or doubling, such as Koblitz (Koblitz, 1991), Huff (Orhon & Hisil, 2018), Holm (Alberto, 2016), and Twisted Edwards curves (Bernstein *et al.,* 2008). As for ENPM, the non-supersingular Koblitz curve from the elliptic curve of $char(K) = 2$ and the recent elliptic curve of characteristic $char(K) \neq 2,3$ namely Twisted Edwards curves can be applied to compare these alternative curves. This is because; the division polynomials of the non-supersingular Koblitz and the Twisted Edwards curves satisfy the fundamental relations of EN values (Rao, 2016, 2017), and the curves contain change of variables from Weierstrass (Bernstein & Lange, 2011; Koblitz, 1991; Moloney & McGuire, 2009, 2011). More details on EN are discussed in Chapter 2 (see Section 2.8.2).

The ECPM can be operated in three levels of computation; scalar, point, and field arithmetics. All levels of computation were employed in this present study. At the first level, DBL and DBLADD methods are proposed with equivalent sequences in EN algorithm over binary and prime fields using eight and seven blocks, respectively. At the second level, point operations based on DBL and DBLADD processes in the new ENPM algorithms over binary and prime fields were enhanced. At the final level, field operations were improved by assessing the expected running time of the designed ENPM algorithms.

1.3 Research Objectives

The primary objective of this study is to improve the performance of PM using EN method. Thus, the research objectives are stated as follows:

Non-supersingular Koblitz curve over binary field

1. To propose DBL and DBLADD algorithms using Karatsuba method for non-supersingular Koblitz curve over binary field with equivalent sequences of $\widehat{W}(2)=1$.
2. To design the ENPM algorithm upon Koblitz curve using the proposed DBL and DBLADD in order to improve the computational efficiency of ECC over binary field.

Twisted Edwards curve over prime field

1. To propose DBL and DBLADD algorithms using Karatsuba method for Twisted Edwards curve over prime field with equivalent sequences of $\widehat{W}(2)=1$.
2. To design the ENPM algorithm upon Twisted Edwards curve using the proposed DBL and DBLADD in order to enhance the computational efficiency of ECC over prime field.

Essentially, this study attempt to answer the following research questions: (1) How do DBL and DBLADD via EN method confirm fast PM over binary and prime fields? and (2) Is the cost of PM via EN independent of the Hamming weight of scalar?

1.4 Research Contributions

The following lists the significant contributions of this study:

New DBL and DBLADD algorithms via EN over binary field

In the EN method over binary field, the first DBL and DBLADD algorithms were structured using eight terms block, together with equivalent sequences and the Karatsuba method. The cost of the proposed method was evaluated based on the number of DBL and DBLADD, and was later compared with the cost of DBL and DBLADD in Chen *et al.* (2017).

New DBL and DBLADD algorithms via EN over prime field

The DBL and DBLADD algorithms with equivalent sequences over prime field were formulated using the Karatsuba method based on seven blocks of EN. The second proposed method was evaluated based on the number of DBL and DBLADD, and was later benchmarked with Kanayama *et al.* (2014) and Rao *et al.* (2019).

New PM algorithm via EN over binary field

A new ENPM algorithm was designed for the non-supersingular Koblitz curve over binary field using the first proposed method. This algorithm applied the binary form to represent the scalar, as well as both DBL and DBLADD containing eight terms with equivalent sequences, along with the explicit formulae of the Karatsuba method and multiple points on non-supersingular Koblitz curve. Point operation, field operation, and running time of the proposed algorithms were evaluated for the new ENPM over binary field. The analysis was benchmarked for BM Koblitz and EN Chen.

New PM algorithm via EN over prime field

A new ENPM algorithm was constructed for the Twisted Edwards curve over prime field by using the new DBL and DBLDD formula via EN method. These algorithms represented the scalar in binary form, while DBL and DBLADD were used with equivalent sequences that had seven terms of EN block, explicit formulae of Karatsuba method, and multiple points on the Twisted Edwards curve. The designed algorithm over prime field was analysed based on field operation and running time. After that, the analysis was benchmarked with BM Twisted and EN Kanayama.

1.5 Scope and Thesis Organisation

The research scope and thesis organisation are stated in the following sections:

1.5.1 Scope of this Study

This study had focused on the ENPMs upon Koblitz curves over binary field and Twisted Edwards curves over prime field in the affine coordinate system. To implement the computation over binary field, three bases can be considered, namely polynomial, subfield, and normal bases. However, only polynomial base had been included for the computation of ENPM in this study. The ENPM algorithm over binary and prime fields had been computed by using properties of non-linear recurrence relations, while the experimental calculations were conducted in Python language using Sagemath via Intel Core i-7 8565 CPU 1.80 Ghz, 8 GB memory, and 64-bit operating system. In the computational analysis, only secure non-supersingular Koblitz curves over binary field namely sec283k1, sec409k1, and sec571k1 curves (Barker, 2020) and secure Twisted Edwards curve over prime field namely nums384t1 and nums512t1 (Bos *et al.,* 2016) are utilised. Some Sagemath references used in this study were Dulhare and Ahmad (2019), Finch (2011), and Zimmerman *et al.* (2018).

1.5.2 Thesis Organisation

The organisation of this thesis is stated in the following:

Chapter 1 begins with the introduction of this study and is followed by the overview, problem statement, research objectives, research contributions, and research scope.

Chapter 2 presents the group structure and finite fields. A comprehensive review of short Weierstrass, Koblitz, and Twisted Edwards curves are included. The review further looked into the division polynomial properties of the curves, multiple points, addition and doubling properties, as well as their affine coordinate systems. The review continues to describe PM via BM and EN.

Chapter 3 outlines the three phases of the research methodology which are problem identification, design, and implementation, and lastly the phase analysis and results. This chapter also explains computational analyses methods and the running environments that will be used during implementations.

Chapter 4 proposes new DBL and DBLADD using the Karatsuba method via eight blocks of EN over binary field. The explicit formulae of ENPM based on the non-supersingular Koblitz curve is introduced. An experimental calculation of ENPM using Koblitz's division polynomials in the polynomial base is depicted. Then, a new ENPM over binary field using proposed DBL and DBLADD is designed.

Chapter 5 highlights the new DBL and DBLADD using seven blocks of EN for Twisted Edwards curve over prime field. The explicit formulae of ENPM over prime field with equivalent sequences was obtained. The experimental calculation was provided starting from the EN initial values using Twisted Edwards division polynomial until the block centred at *n*-multiple points. Then, a new ENPM algorithm based on the Twisted Edwards curve over prime field is designed.

Chapter 6 presents the cost analysis of DBL and DBLADD, the costs of point and field operations, as well as the expected running time of the proposed ENPM algorithms over binary field. Additionally, the proposed ENPM algorithm was compared with BM and ENPM algorithm over binary field reported in the literature.

Chapter 7 outlines the computational analysis of DBL and DBLADD costs, point and field operations, as well as the timing of the proposed ENPM algorithm over prime field. The proposed ENPM algorithm over prime field was benchmarked with BM and ENPM algorithm reported in the literature.
Finally, Chapter 8 concludes this study and lists several suggestions for future research endeavour.

REFERENCES

Abarzúa, R., Valencia, C. & López, J. (2021). Survey on performance and security problems of countermeasures for passive side-channel attacks on ECC. *Journal of Cryptographic Engineering*, *11*, 71–102. https://doi.org/10.1007/s13389-021-00257-8

AbdulRaheem, W. K., Yasin, S. M., Udzir, N. I., & Ariffin, M. R. K. (2019). New quintupling point arithmetic 5P formulas for Lŏpez-Dahab coordinate over binary elliptic curve cryptography. *International Journal of Advanced Computer Science and Applications*, *10*(7), 397–401. https://dx.doi.org/10.14569/IJACSA.2019.0100754

Abel, N. H. (2013). *Oeuvres complètes de Niels Henrik Abel*. Cambridge University Press.

Abhishek, K., & Raj, E. G. D. P. (2021). Evaluation of computational approaches of short Weierstrass elliptic curves for cryptography. *Cybernetics and Information Technologies*, *21*(4), 105–118. https://doi.org/10.2478/cait-2021-0045

Adj, G., Canales-Martínez, I., Cruz-Cortés, N., Menezes, A., Oliveira, T., Rivera-Zamarripa, L., & Rodríguez-Henríquez, F. (2018). Computing discrete logarithms in cryptographically-interesting characteristic-three finite fields. *Advances in Mathematics of Communications*, *12*(4), 741–759. https://doi.org/10.3934/amc.2018044

Agievich, S. V. E., Poruchnik, S. V., & Semenov, V. I. (2022). Small scalar multiplication on Weierstrass curves using division polynomials. *Математические вопросы криптографии*, *13*(2), 17-35. https://doi.org/10.4213/mvk406

Al-Saffar, N. F. H., & Said, M. R. M. (2015). Speeding up the elliptic curve scalar multiplication using the window-w non adjacent form. *Journal of Discrete Mathematical Sciences and Cryptography*, *18*(6), 801–821. https://doi.org/10.1080/09720529.2015.1023538

Alberto, G. (2016). *The division polynomials for the Holm curve and their properties.* [Doctoral dissertation, Howard University]. ProQuest Dissertations and Theses Global.

Alimoradi, R., Arkian, H. R., Razavian, S. M. J., & Ramzi, A. (2020). Scalar multiplication in elliptic curve libraries. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(3), 657–666. https://doi.org/10.1080/09720529.2017.1378411

Alkhudhayr, F., Moulahi, T., & Alabdulatif, A. (2021). Evaluation study of Elliptic curve cryptography scalar multiplication on Raspberry Pie. *International Journal of Advanced Computer Science and Applications*, *12*(9), 472–479. https://doi.org/10.14569/IJACSA.2021.0120954

Araújo, J., Cameron, P. J., & Matucci, F. (2019). Integrals of groups. *Israel Journal of Mathematics*, *234*(1), 1–31. https://doi.org/10.48550/arXiv.1803.10179

Aung, T. M., & Hla, N. N. (2017). Implementation of elliptic curve arithmetic operations for prime field and binary field using Java BigInteger class. *International Journal of Engineering Research & Technology*, *6*(8), 454–459. https://dx.doi.org/10.2139/ssrn.3269703

Awaludin, A. M., Larasati, H. T., & Kim, H. (2021). High-speed and unified ecc processor for generic Weierstrass curves over GF(p) on Fpga. *Sensors*, *21*(1451), 1–20. https://doi.org/10.3390/s21041451

Bafandehkar, M., Yasin, S. M., & Mahmod, R. (2016). Optimizing (0, 1, 3)-NAF recoding algorithm using block-method technique in elliptic curve cryptosystem. *Journal of Computer Science*, *12*(11), 534–544. https://doi.org/10.3844/jcssp.2016.534.544

Barker, E. (2020). Recommendation for key management: Part 1 - General. *National Institute of Standards and Technology, U.S. Department of Commerce.* https://doi.org/10.6028/NIST.SP.800-57pt1r5

Bernstein, D. J., Birkner, P., Joye, M., Lange, T., & Peters, C. (2008). Twisted Edwards Curves. In S. Vaudenay (Ed.), *Progress in Cryptology – AFRICACRYPT 2008. AFRICACRYPT 2008. Lecture Notes in Computer Science* (Vol. 5023, pp. 389-405). Springer. https://doi.org/10.1007/978-3-540-68164-9_26

Bernstein, D. J., & Lange, T. (2007a). Analysis and optimization of elliptic-curve single-scalar multiplication. *Cryptology ePrint Archive*, *2007/455*. https://doi.org/10.1090/conm/461/08979

Bernstein, D. J., & Lange, T. (2007b). Faster addition and doubling on elliptic curves. In Kurosawa, K. (Ed.), *Advances in Cryptology – ASIACRYPT 2007. ASIACRYPT 2007. Lecture Notes in Computer Science* (Vol. 4833, pp. 29–50). Springer. https://doi.org/10.1007/978-3-540-76900-2_3

Bernstein, D. J., & Lange, T. (2011). A complete set of addition laws for incomplete Edwards curves. *Journal of Number Theory*, *131*(5), 858–872. https://doi.org/10.1016/j.jnt.2010.06.015

Blake, I., Seroussi, G., & Smart, N. (1999). *London Mathematical Society, Lecture Note Series 265: Elliptic curves in cryptography.* Cambridge University Press.

Bos, J. W., Costello, C., Longa, P., & Naehrig, M. (2016). Selecting elliptic curves for cryptography: an efficiency and security analysis. *Journal of Cryptographic Engineering*, *6*(4), 259–286. https://doi.org/10.1007/s13389-015-0097-y

Brown, D. R. L. (2010a). Standards for efficient cryptography 2 (SEC 2): Recommended elliptic curve domain parameters, ver. 2.0, Certicom Research, 2010. https://www.secg.org/sec2-v2.pdf

Brown, D. R. L. (2010b). Stange's elliptic nets and coxeter group F_4. *Cryptology ePrint Archive*, *2010/161.* https://ia.cr/2010/161

Chen, B., Hu, C., & Zhao, C. (2017). A note on scalar multiplication using division polynomials. *IET Information Security*, *11*(4), 195–198. https://doi.org/10.1049/iet-ifs.2015.0119

Cheon, J., & Hahn, S. (1998). Explicit valuations of division polynomials of an elliptic curve. *Manuscripta Mathematica*, *97*, 319–328. https://doi.org/10.1007/s002290050104

Chmielewski, Ł., Massolino, P. M. C., Vliegen, J., Batina, L., & Mentens, N. (2017). Completing the complete ECC formulae with countermeasures. *Journal of Low Power Electronics and Applications*, *7*(1), 1–13. https://doi.org/10.3390/jlpea7010003

Chu, D., Großschädl, J., Liu, Z., Müller, V., & Zhang, Y. (2013). Twisted Edwards-form elliptic curve cryptography for 8-bit AVR-based sensor nodes. *Proceedings of the First ACM Workshop on Asia Public-Key Cryptography*, (pp. 39-44). ACM Digital Library. https://doi.org/10.1145/2484389.2484398

Cuevas-Farfan, E., Morales-Sandoval, M., Morales-Reyes, A., Feregrino-Uribe, C., Algredo-Badillo, I., Kitsos, P., & Cumplido, R. (2013). Karatsuba-Ofman multiplier with integrated modular reduction for GF(2^m). *Advances in Electrical and Computer Engineering*, *13*(2), 3–10. https://doi.org/10.4316/AECE.2013.02001

Dijesh, P., Babu, S., & Vijayalakshmi, Y. (2020). Enhancement of e-commerce security through asymmetric key algorithm. *Computer Communications*, *153*, 125–134. https://doi.org/10.1016/j.comcom.2020.01.033

Dulhare, U. N., & Ahmad, K. (2019). Hands-on "SageMath". In Ahmad., K., Doja., M. N., Udzir, N. I. & Singh, M. P. (Eds.), *Emerging Security Algorithms and Techniques* (1st ed., pp. 293-308). CRC Press.

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

Eide, O. W. (2017). *Elliptic curve cryptography*. [Master's Thesis, University of Oslo]. University of Oslo Library.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, *31*(4), 469–472.

Elmegaard-Fessel, L. (2006). *Efficient scalar multiplication and security against power analysis in cryptosystems based on the NIST elliptic curves over prime fields.* [Master's Thesis, University of Copenhagen]. Cryptology ePrint Archive. https://ia.cr/2006/313

Emmart, N. (2018). *A study of high performance multiple precision arithmetic on graphics processing units*. [Doctoral dissertation, University of Massachusetts Amherst].Scholarworks@UMassAmherst. https://doi.org/10.7275/11399986.0

Finch, C. (2011). *Sage beginner's guide*. Packt Publishing Ltd.

Gezer, O. B. B. (2012). Cubes in elliptic divisibility sequences. *Math. Reports*, *14*(64), 21–29.

Ghosh, S., Mukhopadhyay, D., & Roychowdhury, D. (2011). Petrel: Power and timing attack resistant elliptic curve scalar multiplier based on programmable GF(p) arithmetic unit. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *58*(8), 1798–1812. https://doi.org/10.1109/TCSI.2010.2103190

Guo, C. & Gong, B. (2021). Efficient scalar multiplication of ECC using SMBR and fast septuple formula for IoT. *Journal on Wireless Communications and Networking*, *82*, 1–17. https://doi.org/10.1186/s13638-021-01967-7

Hadani, N. H., Yunos, F., Ariffin, M. R. K., Sapar, S. H., & Rahman, N. N. A. (2019). Alternative method to find the number of points on Koblitz curve. *Malaysian Journal of Mathematical Science*, *13*, 13–30.

Hankerson, D., Menezes, A. J., & Vanstone, S. (2004). *Guide to elliptic curve cryptography*. Springer.

Hanwa, A., & Fouotsa, E. (2021). Elliptic divisibility sequences over the Edwards model of elliptic curves. *Journal of Discrete Mathematical Sciences and Cryptography*. https://doi.org/10.1080/09720529.2020.1822042

Hasan, M. K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y. A., Nafi, N. S., & Vargas, D. E. (2021). Lightweight cryptographic algorithms for guessing attack protection in complex internet of things applications. *Complexity*, *2021*. https://doi.org/10.1155/2021/5540296

Hisil, H., Wong, K. K., Carter, G., & Dawson, E. (2008). Twisted Edwards Curves Revisited. In J. Pieprzyk (Ed.), *Advances in Cryptology - ASIACRYPT 2008. ASIACRYPT 2008. Lecture Notes in Computer Science* (Vol. 5350, pp. 326-343). Springer. https://doi.org/10.1007/978-3-540-89255-7_20

Hu, Y., Cui, Y. Y., & Li, T. (2010). An optimization base point choice algorithm of ECC on GF(p). *ICCMS 2010 - 2010 International Conference on Computer Modeling and Simulation* (pp. 103–105). IEEE. https://doi.org/10.1109/ICCMS.2010.128

Imran, M., Kashif, M., & Rashid, M. (2015). Hardware design and implementation of scalar multiplication in elliptic curve cryptography (ECC) over GF(2^{163}) on FPGA. *2015 International Conference on Information and Communication Technologies (ICICT)* (pp. 1-4). IEEE. https://doi.org/10.1109/ICICT.2015.7469484

Isa, M. A. M., Hashim, H., Adnan, S. F. S., Mohamed, N. N., & Alias, Y. F. (2018). Side-channel security on key exchange protocol: Timing and relay attacks. *Indonesian Journal of Electrical Engineering and Computer Science*, *11*(2), 688-695. https://doi.org/10.11591/ijeecs.v11.i2

Jacobson, M. J., Rad, M. R., & Scheidler, R. (2014). Comparison of scalar multiplication on real hyperelliptic curves. *Advances in Mathematics of Communications*, *8*(4), 389-406. https://doi.org/10.3934/amc.2014.8.389

Jao, D. (2010). Elliptic curve cryptography. In Stavroulakis, P. & Stamp, M. (Eds.), *Handbook of Information and Communication Security* (pp. 35–57). Springer.

Javeed, K., Wang, X., & Scott, M. (2017). High performance hardware support for elliptic curve cryptography over general prime field. *Microprocessors and Microsystems*, *51*, 331–342. https://doi.org/10.1016/j.micpro.2016.12.005

Jesus, E. F., Chicarino, V. R. L., De Albuquerque, C. V. N., & Rocha, A. A. D. A. (2018). A survey of how to use blockchain to secure internet of things and the stalker attack. *Security and Communication Networks*, *2018*, 1-27 https://doi.org/10.1155/2018/9675050

Jie, L. K., & Kamarulhaili, H. (2011). Comparison study on point counting algorithms of elliptic curves over prime field. *European Journal of Scientific Research*, *61*(4), 538–548.

Jin, J. (2013). Homogeneous division polynomials for Weierstrass elliptic curves. *ArXiv Preprint ArXiv:1303.4327*. https://arxiv.org/pdf/1503.08127.pdf

Judson, T. W. (2019). *Abstract Algebra: Theory and applications*. Orthogonal Publishing.

Kamarulhaili, H., & Jie, L. K. (2012). Elliptic curve cryptography and point counting algorithms. In J. Sen (Ed.), *Cryptography and Security in Computing*. IntechOpen. https://doi.org/10.5772/34042

Kanayama, N., Liu, Y., Okamoto, E., Saito, K., Teruya, T., & Uchiyama, S. (2014). Implementation of an elliptic curve scalar multiplication method using division polynomials. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *97*(1), 300–302. https://doi.org/10.1587/transfun.E97.A.300

Keerthi, K., & Surendiran, B. (2017). Elliptic Curve Cryptography for Secured Text Encryption. *2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT)* (pp. 1-5). IEEE. doi: 10.1109/ICCPCT.2017.8074210.

Khabbazian, M., Gulliver, T. A., & Bhargava, V. K. (2005). A new minimal average weight representation for left-to-right point multiplication methods. *IEEE Transactions on Computers*, *54*(11), 1454–1459. doi: 10.1109/TC.2005.173.

Khan, Z. U. A., & Benaissa, M. (2017). High-Speed and Low-Latency ECC Processor Implementation over GF(2^m) on FPGA. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *25*(1), 165–176. https://doi.org/10.1109/TVLSI.2016.2574620

Kim, S., Yoon, K., Kwon, J., Hong, S., & Park, Y.-H. (2018). Efficient isogeny computations on Twisted Edwards curves. *Security and Communication Networks*, *2018*, 1–11. https://doi.org/10.1155/2018/5747642

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, *48*(177), 203–209. https://doi.org/10.1090/S0025-5718-1987-0866109-5

Koblitz, N. (1991). Constructing elliptic curve cryptosystems in characteristic 2. In Menezes, A.J. & Vanstone, S.A. (Eds.), *Advances in Cryptology-CRYPT0' 90, Lecture Notes in Computer Science* (Vol. 537, pp. 156–167). Springer. https://doi.org/10.1007/3-540-38424-3_11

Koblitz, N. (1992). CM-curves with good cryptographic properties. In J. Feigenbaum (Ed.), *Advances in Cryptology-CRYPT0' 91, Lecture Notes in Computer Science* (Vol. 576, pp. 279–287). Springer. https://doi.org/10.1007/3-540-46766-1_22

Kodali, R. K., & Boppana, L. (2014). FPGA implementation of energy efficient multiplication over GF(2^m) for ECC. *Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2014*, (pp. 1815–1821). IEEE. https://doi.org/10.1109/ICACCI.2014.6968425

Kudithi, T., & Sakthivel, R. (2019). High-performance ECC processor architecture design for IoT security applications. *Journal of Supercomputing*, *75*(1), 447–474. https://doi.org/10.1007/s11227-018-02740-2

Kumar, M. (2014). *The signs in an elliptic net*. [Master's Thesis, University of Lethbridge]. ProQuest Dissertations Publishing.

Lee, C. Y., Fan, C.-C., Xie, J., & Yuan, S.-M. (2018). Efficient implementation of Karatsuba algorithm based three-operand multiplication over binary extension field. *IEEE Access*, *6*, 38234–38242.

Liu, S. G., An, S. J., & Du, Y. W. (2021). Efficient and secure elliptic curve scalar multiplication based on quadruple-and-add. *International Journal of Network Security*, *23*(5), 750–757. http://dx.doi.org/10.6633/IJNS.202109 23(5).02)

Liu, S., Heng, X., & Li, Y. M. (2020). Anti-SPA scalar multiplication algorithm on Twisted Edwards elliptic curve. *International Journal of Network Security*, *22*(6), 1015–1021. http://dx.doi.org/10.6633/IJNS.202011_22(6).16

Longa, P., & Gebotys, C. (2010). Efficient techniques for high-speed elliptic curve cryptography. In Mangard, S. & Standaert, F. X. (Eds.), *Cryptographic Hardware and Embedded Systems, CHES 2010. CHES 2010. Lecture Notes in Computer Science* (Vol. 6225). https://doi.org/10.1007/978-3-642-15031-9_6

López, J., & Dahab, R. (1999a). Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation. In Koç, C. K. & Paar, C. (Eds.), *Cryptographic Hardware and Embedded Systems. CHES 1999. Lecture Notes in Computer Science* (Vol. 1717, pp. 316-327). Springer. https://doi.org/10.1007/3-540-48059-5_27

López, J., & Dahab, R. (1999b). Improved algorithms for elliptic curve arithmetic in $GF(2^n)$. In Tavares, S. & Meijer, H. (Eds.), *Selected Areas in Cryptography. SAC 1998. Lecture Notes in Computer Science* (Vol. 1556, pp. 201-212). Springer. https://doi.org/10.1007/3-540-48892-8_16

Mahto, D., & Yadav, D. K. (2017). RSA and ECC: A comparative analysis. *International Journal of Applied Engineering Research*, *12*(19), 9053–9061.

Matteo, S. D., Baldanzi, L., Crocetti, L., Nannipieri, P., Fanucci, L. & Saponara, S. (2021). Secure elliptic curve crypto-processor for real-time IOT applications. *Energies*, *14*(15), 4676. https://doi.org/10.3390/en14154676

Menezes, A. J., Oorschot, P. C. V., & Vanstone, S. A. (1997). *Handbook of applied cryptography*. CRC Press.

Menezes, A. J., Vanstone, S. A., & Zuccherato, R. J. (1993). Counting points on elliptic curves over $F_2{}^m$. *Mathematics of Computation*, *60*(201), 407–420. https://doi.org/10.2307/2153177

Miller, V. S. (1986a). Short programs for functions on curves. [Unpublished Manuscript]. https://www.researchgate.net/profile/Victor-Miller-2/publication/2551688_Short_Programs_for_functions_on_Curves/links/0c96052e065ca0bdbf000000/Short-Programs-for-functions-on-Curves.pdf

Miller, V. S. (1986b). Use of elliptic curves in cryptography. In H. C. Williams (Ed.), *Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science* (Vol. 218, pp. 417–426). Springer. https://doi.org/10.1007/3-540-39799-X_31

Mohamed, M. A. (2011). *On the improvement of addition chain in applications to elliptic curve cryptosystem*. [Doctoral dissertation, Universiti Putra Malaysia]. Universiti Putra Malaysia.

Moloney, R., & McGuire, G. (2009). Two kinds of division polynomials for Twisted Edwards curves. *Applicable Algebra in Engineering, Communications and Computing*, *22*, 321–345. https://doi.org/10.1007/s00200-011-0153-5

Moloney, R., & McGuire, G. (2011). Division polynomials for Twisted Edward curves*. ArXiv Preprint ArXiv:0809.2182*. https://arxiv.org/pdf/0809.2182.pdf

Mordell, L. J. (1922). On the rational solutions of the indeterminate equations of the third and fourth degree. *Proc. Camb. Phil. Soc.*, *21*, 179–192.

Mrabet, A., El-Mrabet, N., Bouallegue, B., Mesnager, S., & MacHhout, M. (2017). An efficient and scalable modular inversion/division for public key cryptosystems. *International Conference on Engineering and MIS (ICEMIS)*, (pp. 1-6). IEEE. https://doi.org/10.1109/ICEMIS.2017.8272995.

Naccarato, F. (2021). Counting rational points on elliptic curves with a rational 2-torsion point. *Rendiconti Lincei*, *32*(3), 499-509. https://doi.org/10.48550/arXiv.2105.04032

Nagy, G. P., & Lanzone, V. (2015). Binary fields on limited systems. *Acta Scientiarum Mathematicarum*, *80*(3-4), 409-418. https://doi.org/10.14232/actasm-012-813-7

Orhon, N. G., & Hisil, H. (2018). Speeding up Huff form of elliptic curves. *Designs, Codes and Cryptography*, *86*, 2807–2823. https://doi.org/10.1007/s10623-018-0475-4

Rabah, K. (2005). Theory and implementation of elliptic curve cryptography. *Journal of Applied Sciences*, *5*(4), 604–633. https://dx.doi.org/10.3923/jas.2005.604.633

Rabah, K. (2006). Elliptic curve cryptography over binary field GF(2^m). *Information Technology Journal*, *5*(1), 204–229.

Rao, S. R. S., Hu, Z., & Zhao, C. A. (2019). Division polynomial-based elliptic curve scalar multiplication revisited. *IET Information Security*, *13*(6), 614–617. https://doi.org/10.1049/iet-ifs.2018.5361

Rao, S. R. S. (2016). An improved elliptic net algorithm for Tate pairing on Weierstrass' curves, faster point arithmetic and pairing on Selmer curves and a note on double scalar multiplication. In Batten, L. & Li, G. (Eds.), *Applications and Techniques in Information Security. ATIS 2016. Communications in Computer and Information Scienc*e (Vol. 651, pp. 93–105). Springer. https://doi.org/10.1007/978-981-10-2741-3_8

Rao, S. R. S. (2017). *Elliptic Curve Arithmetic for Cryptography*. [Doctoral dissertation, The Australian National University]. Australian National University Press.

Reynolds, J. (2012). Perfect powers in elliptic divisibility sequences. *Journal of Number Theory*, *132*(5), 998–1015. https://doi.org/10.1016/j.jnt.2011.09.013

Rivest, R. L., Shamir, A., & Adleman, L. (1983). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *26*(1), 96–99. https://doi.org/10.1145/357980.358017

Roy, M., Deb, N., & Kumar, A. J. (2014). Point generation and base point selection in ECC : An overview. *International Journal of Advanced Research in Computer and Communication Engineering*, *3*(5), 6711–6713.

Sadek, M., & El-Sissi, N. (2016). Edwards curves and gaussian hypergeometric series. *Journal de Theorie Des Nombres de Bordeaux*, *28*(1), 115–124. https://doi.org/10.5802/jtnb.931

Satoh, T. (2004). Generalized division polynomials. *Mathematica Scandinavica*, *94*(2), 161–184. https://doi.org/10.7146/math.scand.a-14436

Scholl, T. (2017). Isolated curves and the MOV attack. *Journal of Mathematical Cryptology*, *11*(3), 131–146. https://doi.org/10.1515/jmc-2016-0053

Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, *44*(170), 483–494. https://doi.org/10.2307/2007968

Schoof, R. (1995). Counting points on elliptic curves over finite fields. *Journal de Theorie Des Nombres de Bordeaux*, *7*(1), 219–254.

Seo, S. C., Kim, T., & Hong, S. (2015). Accelerating elliptic curve scalar multiplication over GF(2^m) on graphic hardwares. *Journal of Parallel and Distributed Computing*, *75*, 152–167.

Shipsey, R. (2000). *Elliptic divisibility sequences*. [Doctoral dissertation, University of London]. Goldsmiths Research Online.

Silverman, J. H. (2009). The arithmetic of elliptic curve. In S. Axler & K. A. Ribet, (Eds). *Graduate Text in Mathematics* (pp. 41-58). Springer.

Silverman, J. H. & Tate J. (1992). Rational points on elliptic curves. In Ewing, J. H., Gehring, F. W. & Halmos, P. R. (Eds). *Undergraduate Texts in Mathematics* (pp. 9-32). Springer-Verlag.

Silverman, J. H. (1994). *Advanced topics in the arithmetic of elliptic curves*. In P. Landweber, D. Rochrlich, (Eds). *Graduate Texts in Mathematics* (pp. 408-413). Springer-Verlag.

Somos, M. (1989). Problem 1470. *Crux Mathematicorum*, *15*(1989), 208.

Standard curve database. (2020a). *Standard curve database for NIST*. Retrieved June 10, 2022, from https://neuromancer.sk/std/nist

Standard curve database. (2020b). *Standard curve database for NUMS*. Retrieved June 10, 2022, from https://neuromancer.sk/std/nums

Stange, K. E. (2008). *Elliptic net and elliptic curve*. [Doctoral dissertation, Brown University]. Proquest.

Stange, K. E. (2012). *Formulary for elliptic divisibility sequences and elliptic nets* [UnpublishedManusript]. https://math.colorado.edu/~kstange/papers/edsformulary.pdf

Stange, K. E. (2016). Integral points on elliptic curves and explicit valuations of division polynomials. *Canadian Journal of Mathematics*, *68*(5), 1120–1158. https://doi.org/10.4153/CJM-2015-005-0

Sutherland, A. (2021). Stronger arithmetic equivalences. *Discrete Analysis*, 1-23. https://doi.org/10.19086/da.29452

Tall, A., & Sanghare, A. Y. (2013). Efficient computation of addition-subtraction chains using generalized continued fractions. *Cryptology ePrint Archive, 2013/466.* https://ia.cr/2013/466

Thangarasu, N. & Selvakumar, A. (2019). Improved elliptical curve cryptography and Abelian group theory to resolve linear system problem in sensor-cloud cluster computing. *Cluster Computing, 22*(6)*,* 13185–13194*.* https://doi.org/10.1007/s10586-017-1573-1

Trappe, W., & Washington, L. C. (2006). *Introduction to cryptography with coding theory*. Pearson Education India.

Ward, M. (1948). Memoir on elliptic divisibility sequences. *American Journal of Mathematics*, *70*(1), 31–74.

Wroński, M. (2016). Faster point scalar multiplication on short Weierstrass elliptic curves over Fp using Twisted Hessian curves over F_{p}^{2}. *Journal of Telecommunication and Information Technology*, 98–102.

Wu, H., & Zhao, C. (2011). Faster scalar multiplication on ordinary Weierstrass elliptic curves over fields of characteristic three. *Cryptology ePrint Archive*, *2011/468.* https://ia.cr/2011/468

Xu, J., Hu, L., & Sarkar, S. (2020). Cryptanalysis of elliptic curve hidden number problem from PKC 2017. *Designs, Codes, and Cryptography*, *88*, 341–361. https://doi.org/10.1007/s10623-019-00685-y

Yan, S. Y. (2002). *Number theory for computing*. Springer.

Yang, H. J., & Shin, K. W. (2021). A hardware implementation of point scalar multiplication on Edwards25519 curve. *2021 International Conference on Electronics, Information, and Communication, ICEIC 2021*, (pp. 1–3). IEEE. https://doi.org/10.1109/ICEIC51217.2021.9369815

Yasin, S. M. (2011). *New signed digit {0,1,3}-NAF scalar multiplication algorithm for elliptic curve over binary field*. [Doctoral dissertation, Universiti Putra Malaysia]. Universiti Putra Malaysia.

Yunos, F., Atan, K. A. M., Ariffin, M. R. K., & Said, M. R. M. (2015). Pseudo τ –adic non adjacent form for scalar multiplication on Koblitz curves. *Malaysian Journal of Mathematical Sciences*, *9*, 71–88.

Zargar, A. J., Manzoor, M., & Mukhtar, T. (2017). Encryption/Decryption using elliptical curve cryptography. *International Journal of Advanced Research in Computer Science*, *8*(7), 48–51. http://dx.doi.org/10.26483/ijarcs.v8i7.4208

Zhang, Q. (2021). An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption. *Proceedings - 2021 2nd International Conference on Computing and Data Science, CDS 2021*, (pp. 616–622). IEEE. https://doi.org/10.1109/CDS52072.2021.00111

Zimmerman, P., Casamayou, A., Cohen, N., Connan, G., Dumont T., Fousse, L. & Connan, G. (2018). *Computational mathematics with SageMath*. Society for Industrial and Applied Mathematics.