UNIVERSITI PUTRA MALAYSIA

DEVELOPMENT OF SOME FAST AND EFFICIENT METHODS FOR ELLIPTIC CURVE SCALAR MULTIPLICATION OVER PRIME FIELDS

NAJLAE FALAH HAMEED AL-SAFFAR

IPM 2015 19

DEVELOPMENT OF SOME FAST AND EFFICIENT METHODS FOR ELLIPTIC CURVE SCALAR MULTIPLICATION OVER PRIME FIELDS

By

NAJLAE FALAH HAMEED AL-SAFFAR

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

February 2015

To My

Parents, Brothers

And

Sisters

For Their Endless Love And Support,

For Continued Encouragement;

For Believing In Me.

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

DEVELOPMENT OF SOME FAST AND EFFICIENT METHODS FOR ELLIPTIC CURVE SCALAR MULTIPLICATION OVER PRIME FIELDS

By

NAJLAE FALAH HAMEED AL-SAFFAR

February 2015

Chairman: Mohamad Rushdan Md Said, Ph.D.
Faculty: Institute For Mathematical Research

Elliptic curve cryptosystem (ECC) is being used nowadays more than ever to fulfill the need for public key cryptosystem because of its ability to use shorter keys lengths and computationally more efficient algorithms than anther public key cryptosystems such as Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA) and $ElGamal$. The most time consuming operation in ECC is elliptic curve scalar multiplication ($ECSM$). Many research have been carried out to accelerate this operation. The structure of the $ECSM$ involves three mathematical levels: finite field arithmetic, point arithmetic and scalar arithmetic. The purpose of this work is to study different issues that arise in the efficient implementation of $ECSM$ over prime field, specifically targeting the point and scalar arithmetic levels over elliptic curve.

At the point arithmetic level, we introduce the $4-$ dimensional Jacobian coordinates system ($4 - DJC$), where a point (X, Y, Z, T) with $Z \neq 0$ and $T = Z^2$, corresponds to affine point $(X/T, Y/Z^3)$ and satisfying the elliptic curve equation over prime field. This is due to the expensive cost of the field multiplication inversion involves in both point doubling and point addition operation with the arithmetic of the a affine coordinates (x, y). This system has proven their efficiency in many contexts that is to reduce the number field operation for point doubling opera-

tion in comparison with point doubling operation using projective coordinates system and Jacobian coordinates system respectively, to reduce the number field operation for point addition operation in comparison with point addition operation using Jacobian coordinates system and to reduce the cost of computing point addition using mixed coordinates technique, also in comparison with using Jacobian coordinates in mixed coordinates technique.

At the scalar arithmetic level, we develop three new algorithms to accelerate the $ECSM$ using the non adjacent form (NAF), window $\omega-$ non adjacent form ($\omega - NAF$) and direct recoding method (DRM), by rewriting the scalar involved in $ECSM$. The proposed algorithm using NAF to represent the scalar in $ECSM$ reduced the cost of computation of the $ECSM$ by comparing with using the binary and NAF algorithm respectively. The second proposed algorithm which is using $\omega - NAF$ reduced the cost of computation of the $ECSM$ by comparing with using the binary, NAF and $\omega - NAF$ algorithm with $\omega = 3$ respectively. Finally, the proposed two algorithms using DRM to represent the scalar in $ECSM$ involve binary form and NAF. The computational complexity of this proposed methods have high performance when computing the $ECSM$ compared to the other methods. This is due to the number of operations required for execution is less comparing with using the mutual opposite form (MOF).

This thesis shows how we can serve the public key cryptosystems by speeding up the $ECSM$ operation by reducing operations in point and scalar arithmetic levels.

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

PEMBANGUNAN SUATU KAEDAH PENDARABAN SKALAR UNTUK KELUK ELIPTIK YANG PANTAS DAN CEKAP DALAM MEDAN PERDANA

Oleh

NAJLAE FALAH HAMEED AL-SAFFAR

Februari 2015

Pengerusi: Mohamad Rushdan Md Said, Ph.D.
Fakulti: Institut Penyelidikan Matematik

Sistem kripto Lengkungan eliptik (ECC) digunakan pada masa kini lebih daripada biasa untuk memenuhi keperluan untuk sistem kunci umum kerana keupayaannya untuk menggunakan kepanjangan kekunci lebih pendek dan algoritma pengiraannya lebih cekap daripada sistem kripto kunci awam seperti Rivest - Shamir - Adleman (RSA), Digital Algoritma Tandatangan (DSA) dan $ElGamal$. Yang paling memakan masa dalam operasi ECC adalah gandaan lengkungan eliptik skalar ($ECSM$). Banyak kajian telah dijalankan untuk mempercepatkan operasi ini. Struktur ini melibatkan tiga tahap matematik: aritmetik medan terbatas, titik aritmetik dan arimetik skalar. Tujuan kajian ini ialah untuk mengkaji isu-isu yang berbeza yang timbul dalam pelaksanaan kecekapan keatas medan- medan perdana, khususnya mensasarkan titik dan peringkat aritmetik skalar sepanjang lengkungan eliptik.

Di peringkat aritmetik titik, kami memperkenalkan sistem dimensi Koordinat Jakobian ($4-DJC$), di mana satu mata (X, Y, Z, T) dengan $Z \neq 0$ dan $T = Z^2$, sepadan dengan titik afin $(X/T, Y/Z^3)$ dan memuaskan persamaan lengkungan eliptik berbanding medan perdana. Ini adalah kerana kos yang mahal daripada penyongsangan medan melibatkan pengandaan dalam kedua-dua mata dua kali ganda dan titik operasi tambahan dengan satu aritmetik Koordinat afin (x, y). Sistem ini telah membuktikan kecekapan mereka dalam banyak konteks iaitu untuk mengurangkan operasi medan nombor untuk operasi mata dua kali ganda

berbanding dengan operasi mata dua kali ganda menggunakan masing-masing sistem Koordinat projektif dan Sistem Koordinat Jacoban, untuk mengurangkan operasi medan nombor untuk operasi tambahan mata berbanding dengan titik operasi Selain menggunakan sistem Koordinat Jacoban dan mengurangkan kos tambahan mata pengkomputeran menggunakan teknik campuran koordinat, turut membandingkan dengan menggunakan Koordinat Jacoban dalam teknik campuran koordinat.

Di peringkat aritmetik skalar, kami membangunkan tiga algoritma baru untuk mempercepatkan $ECSM$ menggunakan bentuk yang bukan bersebelahan (NAF), tingkap $\omega-$bentuk bukan bersebelahan ($\omega-NAF$) dan kaedah rekod secara langsung (DRM), dengan menulis kembali skalar yang terlibat dalam proses tersebut $ECSM$. Algoritma yang dicadangkan, NAF digunakan untuk mewakili skalar dalam $ECSM$ mengurangkan kos pengiraan $ESCM$ dengan membandingkan dengan menggunakan binari dan algoritma NAF masing-masing. Cadangan Algoritma kedua yang $\omega - NAF$ digunakan mengurangkan kos pengiraan dengan membandingkan penggunaan binari, NAF, algoritma $\omega - NAF$ dan $\omega = 3$ masing-masing. Akhir sekali, mencadangkan dua algoritma DRM yang digunakan untuk mewakili skalar $ESCM$ dalam melibatkan bentuk binari dan NAF. Kerumitan pengiraan bagi kaedah yang dicadangkan ini mempunyai prestasi yang tinggi apabila pengiraan $ECSM$ berbanding dengan kaedah lain. Ini disebabkan oleh bilangan operasi yang diperlukan untuk pelaksanaan adalah kurang berbanding dengan menggunakan bentuk bertentangan bersama (MOF).

Tesis ini menunjukkan bagaimana kita boleh memberi khidmat kepada cryptosystems umum utama dengan mempercepatkan $ECSM$ operasi dengan mengurangkan operasi di tempat dan tahap aritmetik skalar.

ACKNOWLEDGEMENTS

All praise and thanks be to Almighty Allah, the most Gracious, the most Merciful. I seize this opportunity to express that it is a great pleasure and honour for me to thank those who made this doctoral thesis possible.

First and foremost, my deepest appreciation, gratitude and respect to my supervisor, Associate Professor Dr. Mohamad Rushdan B Md Said for his patience and allowing me the space to develop my ideas. Without his tremendous help, I could not have completed this doctoral study.

I am thankful to the members of my thesis committee: Professor Dr. Isamiddin S. Rakhimov and Associate Professor Dr. Muhammad Rezal Bin Kamel Ariffin for their useful comments and discussions during my doctoral study.

The Institute For Mathematical Research provided a wonderful atmosphere during my doctoral studies. It was a pleasure being part of a group where students, faculty and staff have a number of occasions to get together and become better friends.

I also want to thank my country, Iraq and especially the Ministry of Higher Education and Scientific Research for giving me this opportunity to achieve this personal goal in life and reinforcing my commitment to contribute toward the development and progress of my country.

I owe a lot of thanks to my friends, for their support and friendship, especially in tough times, which means a lot to me.

Warm thanks to my father, brothers and sisters who have motivated me to do my best and have always been extraordinary examples for me.

Finally, I will always have the greatest love for my late mother and sister who gave me so much love, encouragement and intellectual motivation throughout the last few years to overcome my nostalgia and loneliness and enable me to complete this work as soon as possible. I deeply miss them.

I certify that a Thesis Examination Committee has met on 23/2/2015 to conduct the final examination of Najlae Falah Hameed Al-Saffar on her thesis entitled "Development of Some Fast and Efficient Methods for Elliptic Curve Scalar Multiplication over Prime Fields" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the degree of Doctor of Philosophy).

Members of the Thesis Examination Committee were as follows:

Mahendran Shitan, Ph.D.
Associate Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Chairperson)

Ibragimov Gafurjan, Ph.D.
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

Ramlan Mahmod, Ph.D.
Professor
Faculty of Computer Science & Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Tsuyoshi Takagi, Ph.D.
Professor
Institute of Mathematics for Industry
Kyushu University
Japan
(External Examiner)

_____

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 19 March 2015

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:

Mohamad Rushdan Md Said, Ph.D.
Associate Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Chairperson)

Isamiddin S. Rakhimov, Ph.D.
Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Member)

Muhammad Rezal Bin Kamel Ariffin, Ph.D.
Associate Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Member)

_____

BUJANG BIN KIM HUAT, Ph.D.
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by Graduate Student

I hereby confirm that:

- This thesis is my original work;
- Quotations, illustration and citations have been duly referenced;
- The thesis has not been submitted previously or concurrently for any other degree at any 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. : Najlae Falah Hameed Al-Saffar

Declaration by Members of Supervisory Committee

This is to confirm that:

- The research was 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: .....

Signature: .....
Name of
Member of
Supervisory
Committee: .....

Signature: .....
Name of
Member of
Supervisory
Committee: .....

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ALGORITHMS

LIST OF FIGURES

LIST OF ABBREVIATIONS

$DHKE$	Diffie Hellman Key Exchange
DSA	Digital Signature Algorithm
DRM	Direct Recoding Method
DLP	Discrete Logarithm Problem
$ElGamalECC$	ElGamal Elliptic Curve cryptosystem
ECC	Elliptic Curve Cryptosystem
$ECDHKE$	Elliptic Curve Diffie Hellman Key Exchange
$ECDSA$	Elliptic Curve Digital Signature Algorithm
$ECDLP$	Elliptic Curve Discrete Logarithm Problem
$ECSM$	Elliptic Curve Scalar Multiplication
IBM	International Business Machines
IFP	Integer Factorization Problem
MOF	Mutual Opposite Form
$NIST$	National Institute of Standards and Technology
NAF	Non Adjacent Form
RSA	Rivest Shamir Adleman
$\omega - NAF$	Window $\omega-$Non Adjacent Form
$4 - DJC$	4 Dimensional Jacobian Coordinates

CHAPTER 1

INTRODUCTION

1.1 Cryptography

Cryptography is the art and science of using mathematics to exchange massages parties authorized in a secret way to make it either impossible or computationally infeasible for unauthorized parties to do so (Yan, 2002; Mollin, 2010). The word cryptography is derived from Greek words: "kryptós", meaning hidden, and "graphein", meaning to write. The science of discovering weaknesses in methods used to exchange messages in secret is named cryptanalysis. This word also came from the Greek words also: "kryptós" and "analýein", meaning to loosen. Cryptography and cryptanalysis are subordinate to a more general term which is cryptology. That is, cryptology is the mathematical science of studying cryptography and cryptanalysis (Spillman, 2004; Oppliger, 2011). Cryptology also comes from the Greek words: "kryptós" and "lógos", meaning word, which is considered as the original intent on cryptology, in other words, it implies protecting the confidentiality of the data.

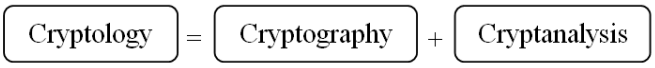

Figure 1.1: The Relationship Between Cryptology, Cryptography and Cryptanalysis

According to the literatures (Raphael and Sundaram, 2011; Poonia et al., 2013; Challita and Farhat, 2011), cryptography comprises steganography, which is a technique of hiding a file within another one, in way it cannot be seen. As an example would be invisible ink. The hidden file could be recovered by the attacker if he detect that steganography has been used (invisible ink) to be able to read the hidden file. While the objective of the cryptography is to make the message unreadable to anyone who does not have the key and know the correct algorithm.

The oldest evidence of using cryptography was found in a tomb of the nobleman Khnumhotep II in Egypt around 1900 B.C. (Damico, 2009; Gebbie, 2003). At that time the purpose was not to make the messages unreadable, but could also be to change its form in a way which would make it appear dignified. Modern cryptography is involved in ensuring secrecy of messages between military leaders, spies, and diplomat, so as to guarantee secure of exchange of confidential communication. In recent decades, people have employed cryptography for phone, fax, email communication, bank transactions, and credit card transactions on the web. It is also employed for a variety of information security issues including electronic signatures, which are used to prove who sent a message. In brief, cryptography has become a very common practice in internet based communications.

Cryptography plays an important role in providing security, by offering a high degree of security and flexibility. In addition to the fact that cryptography is a tool to protect the confidentiality of data, data integrity, authentication and non repudiation are other important goals of cryptography.

- In terms of confidentiality, the goal is to keep the content of information from all but those who are authorized to have it.
- In terms of data integrity, the goal is to be able to detect alteration of data.
- In terms of authentication, the goal is to be able to identify entities in communication.
- Finally, in terms of non repudiation, the goal is to prevent an entity from denying previous commitments or actions.

Three important issues are involved when dealing with the cryptography: encryption, decryption (usually defined by cryptographic systems

or cryptosystems) and the key. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Decryption is the process of decoding data that have been encrypted using encryption process. These two processes (encryption and decryption) would produce no useful result without a key. So, in encryption process, a key specifies the particular transformation of plaintext (that needs to be encrypted) into ciphertext (that has been encrypted), or vice versa during decryption process. The processes of encryption and decryption are shown in Figure 1.2 below.

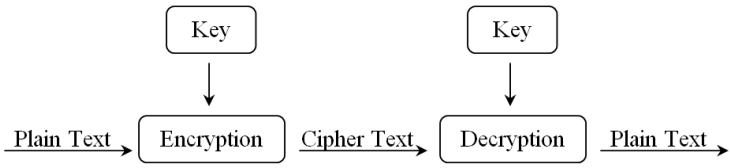

Figure 1.2: The Encryption and Decryption Process

There are two main different types of cryptosystems: private key cryptosystem and public key cryptosystem. In the private key system, the same key is used in the process of both encryption and decryption. This key must be kept as a secret by all parties involved in the communication. However, the disadvantage of this system is the risk of interception of the key by an attacker in the key exchange process. This problem has been dealt with by public key cryptosystem. The next two subsection cover these cryptographic systems in detail.

1.1.1 Private Key Cryptosystem

Conventional private key cryptosystem (also commonly known as a symmetric or secret key cryptosystem) is the type in which the same key is involved in the processing of encryption and decryption. That is, this key should be agreed to by the one who needs to encrypt and the one who needs to decrypt. The process of the encryption of the plain text to the cipher text is as follows:

The sender will define an invertible function f as

$$f : \mathcal{M} \xrightarrow{k} \mathcal{C}, \tag{1.1}$$

where $\mathcal{M}$ is the set of plain texts, and $\mathcal{C}$ is the set of cipher texts.

In order to produce the cipher text, compute

$$C = f_k(M), \qquad \text{for } M \in \mathcal{M} \text{ and } C \in \mathcal{C}, \tag{1.2}$$

The C will be transmitted over the public channel to the receiver, together with the key k but over a secure channel. When the receiver gets the cipher text C, he would be able to decrypt it as follows:

The receiver will use f^{-1} which is defined by

$$f^{-1} : \mathcal{C} \xrightarrow{k} \mathcal{M}, \tag{1.3}$$

to compute

$$\begin{aligned} f_k^{-1}(C) &= f_k^{-1}(f_k(M) \\ &= M \qquad \text{for } M \in \mathcal{M} \text{ and } C \in \mathcal{C}, \end{aligned} \tag{1.4}$$

Although the performance of the private key cryptosystem is very fast and it has been well tested, the key should be stored securely and exchanged within a secure channel. A stream cipher is one of the examples of a private key cryptosystem.

1.1.2 Public Key Cryptosystem

The idea and concept of a public key cryptosystem (also known as an asymmetric key cryptosystem) was introduced by Diffie and Hellman (1976), when they proposed the Diffie Hellman key exchange ($DHKE$) to exchange keys. In a public key cryptosystem, two different keys are involved for the processing of encryption and decryption. One key is considered as a public key and the second key will be kept secure.

Definition 1.1 : *A one way function is a function f such that for each x in the domain of f, it is easy to compute $f(x)$; but for essentially all y in the range of f, it is computationally infeasible to find any x such that $y = f(x)$*

Definition 1.2 : *A one way function $f : X \to Y$ is said to be a trapdoor one way function if there exist some information with which f can be efficiently inverted. This additional information is known as a trapdoor.*

Example 1.1 *The function $f_{k,n} : x \to x^k (mod\, n)$ is a trapdoor one way function, where $n = pq$ with p and q being two primes. As it is easy to compute since the modular exponentiation $x^k (mod\, n)$, then the computation of f is easy. But f^{-1} is difficult to compute. However, if k' the trapdoor is given, then f can be easily inverted, since $(x^k)^{k'} = x$*

Definition 1.3 : *A public key cryptosystem, comprises a family $f_k : \mathcal{M} \to \mathcal{C}$ of trapdoor one way functions.*

The process of encrypting the plain text to the cipher text is as follows: The sender will define an invertible function f as

$$f : \mathcal{M} \xrightarrow{e_k} \mathcal{C}, \qquad \text{where } e_k \text{ is the public key} \tag{1.5}$$

If he wants to produce the cipher text, he will compute

$$C = f_{e_k}(M), \qquad \text{for } M \in \mathcal{M} \text{ and } C \in \mathcal{C}, \tag{1.6}$$

The C will be transmitted over the public channel to the receiver. When the receiver gets the cipher text C, he would be able to decrypt it as follows:

The receiver will use his private key (d_k) and f^{-1} which is defined by

$$f^{-1} : \mathcal{C} \xrightarrow{d_k} \mathcal{M}, \tag{1.7}$$

to compute

$$\begin{aligned} f_{d_k}^{-1}(C) &= f_{d_k}^{-1}(f_{e_k}(M)) \\ &= M \qquad \text{for } M \in \mathcal{M}, \quad C \in \mathcal{C} \text{ and } e_k \neq d_k, \end{aligned} \tag{1.8}$$

The public key cryptosystem increases the security and convenience, where the two parties do not have any kind of previous communication. (For example, such as the communication which happens between members in a bank, if user wants to communicate with the specific user. This will cost only the application of the information in data bank.) That is, public key cryptosystems have some important advantages over private key cryptosystems in the distribution of the keys. However, it might be slow when a large amount of information needs to be exchanged securely.

A public key cryptosystem is based on the computational difficulty to derive the private key from the public key item. This comes from the difficulty of the underlying hard mathematical problem, such as integer factorization problem (IFP), discrete logarithm problem (DLP) (with best algorithms to solve them take subexponential time) and elliptic curve discrete logarithm problem ($ECDLP$) (with best algorithms to solve it take fully exponential time). The most popular systems of the public key cryptosystems are RSA (Rivest et al., 1978) which is based on the IFP, $ElGamal$ cryptosystem (ElGamal, 1985) which based on the DLP and elliptic curve cryptosystem (ECC) (Miller, 1986; Koblitz, 1987) which is based on the $ECDLP$. For more details of this systems, we will introduce a brief discussion of the RSA and $ElGamal$ cryptosystems.

Rivest et al. (1978) proposed the first practical public key cryptosystem, which is the RSA cryptosystem. This system is based on the difficulty of factoring a large number into two primes. Assuming that $Alice$ and Bob are two users who want to communicate using an RSA cryptosystem. The RSA processing is as follows:

$$\begin{aligned} C &\equiv M^e (mod\, N) \\ M &\equiv C^d (mod\, N) \end{aligned} \tag{1.9}$$

where

- M is the plain text.
- C is the cipher text.
- $N = pq$, with $p \neq q$ large primes.
- e and d are the public and private keys respectively, with $gcd(e, \phi(N)) = 1$ ($\phi(N)$ is the Euler's function).

The pair (N, e) will be the public item and d should be kept as a private key. Now, if $Alice$ wants to send a message M to Bob, she will use Bob's public key e and send C. Bob will use his own key d to decrypt C to the original message M. The proof of correctness of the RSA processing is as follows:

From assumption we have $gcd(e, \phi(N)) = 1$, then $de \equiv 1 (mod\, \phi(N))$. Then, there exists $t \in \mathbb{Z}$ such that $ed = t\phi(N) + 1$. Now,

$$C^d (mod\, N) \equiv (M^e)^d (mod\, N)$$

$$\equiv M^{t\phi(N)+1}(mod\, N)$$
$$\equiv (M^{\phi(N)})^t M(mod\, N)$$

Since $M < N$ and $N = pq$, then $gcd(M, N) = 1$. Now, using Euler's theorem (Yan, 2002) "If $gcd(a, n) = 1$ for any two positive numbers a and n, then $a^{\phi(n)} \equiv 1(mod\, n)$". As a result $C^d(mod\, N) \equiv M(mod\, N)$.

The underlying hard mathematical problem for security in the RSA cryptosystem is to find the factors p and q from N. Factoring a number of size 1024 bits is well beyond the capability of the best current factoring algorithms (Stinson, 2006).

ElGamal (1985) proposed $ElGamal$ public key cryptosystem, which is based on DLP. Assuming that $Alice$ and Bob are two users who want to communicate using an $ElGamal$ cryptosystem. The $ElGamal$ processing is simply as follows:

$$C_1 \equiv g^k(mod\, p) \tag{1.10}$$
$$C_2 \equiv Me^k(mod\, p) \tag{1.11}$$
$$M \equiv (C_1^d)^{-1}C_2(mod\, p) \tag{1.12}$$

where

- M is the plain text.
- C_1 and C_2 are the cipher texts.
- g is the primitive root of F_p.
- e is the public key.
- k and d are private keys.

$e \equiv g^d(mod\, p)$ is the public key and d should be kept as a private key. Now, if Bob wants to send a message M to $Alice$, he will use his chosen key k such that $1 \leqslant k \leqslant p-1$, and the public key e to send the pair C_1, C_2. $Alice$ will decrypt (C_1, C_2) to M by using her own key d. The proof of correctness of the $ElGamal$ processing is as follows:

$$M \equiv (C_1^d)^{-1}C_2(mod\, p)$$
$$\equiv ((g^k)^d)^{-1}Me^k(mod\, p)$$
$$\equiv (g^{dk})^{-1}M(g^d)^k(mod\, p)$$

$$\equiv M(mod\, p)$$

The underlying hard mathematical problem for security in the $ElGamal$ cryptosystem is to find the x such that $g^x \equiv h(modp)$ where g is the primitive root of F_p. The digital signature algorithm (DSA) (Locke and Gallagher, 2009) and $DHKE$ are other systems based on the difficulty of solving DLP.

In particular, DLP can be applied on the group of points on an elliptic curve over finite field, to be $ECDLP$. That is, to find the integer k, $1 \leqslant k \leqslant n-1$, given $Q = kP$, P a point on the elliptic curve over finite field, and P of order n. $ECDLP$ is the underlying hard mathematical problem for the security in the ECC (Koblitz et al., 2000). Since there is no known subexponential algorithm to solve the $ECDLP$ (Koblitz et al., 2000; Hankerson et al., 2004), then the ECC with smaller key size and less memory, offers the same level of security as the other public key cryptosystems.

In the mid 1980s, Miller (1986) and Koblitz (1987) opened the door for application of elliptic curve in cryptography. Nowadays, ECC is considered a good public key cryptosystem for low memory devices such as smart cards and phones since smaller bit sizes are used for operations. In Chapter 2, we will discuss the preliminaries of elliptic curve arithmetic. More specifically, we will introduce elliptic curve analogue of $DHKE$, $ElGamal$ and DSA systems.

1.2 Problem Statement

ECC has become widely accepted and standardized as the public key cryptosystem due to its ability to provide the same level of security as the other public key cryptosystems, while using far smaller key sizes. For example, ECC requirement for obtaining an acceptable security level is 163 bits, while it is 1024 bits for RSA (Xiao et al., 2011). Table 1.1 provides other examples of the superiority of the ECC over not only the RSA, but even the DSA in terms of security level (Sandeep and Shanavas, 2012; N.Thangarasu, 2014).

Table 1.1: Security Level of ECC

Time Braking in $MIPS$ Years	Key Size		Key Size Ratio
	RSA/DSA	ECC	
10^4	512	106	$5:1$
10^8	768	132	$6:1$
10^{11}	1024	163	$7:1$
10^{20}	2043	210	$10:1$
10^{78}	21000	600	$35:1$

The operation kP is involved in the $ECDLP$. Since ECC depends on the difficulty of solving the $ECDLP$, then the computational performance of ECC depends of the efficiency of the kP operation. kP is the elliptic curve scalar multiplication ($ECSM$) (also known as an elliptic curve point multiplication). $ECSM$ is the operation of computing an integer multiple of an element in the group of elliptic curve. In other words, this operation is exactly the processing of computing Q as follows:

$$Q = kP = \underbrace{P + P + ... + P}_{k \text{ times}} \tag{1.13}$$

where k is a positive integer called scalar and P, Q are elliptic curve points. P and Q are considered as public keys, while the scalar k is considered as a private key. As mentioned earlier, given P and Q, it is computationally hard to calculate the scalar k. Therefore, reducing the number of these additions ($k\ times$) will make the $ECSM$ faster, and then it will make ECC more efficient. Another reason for considering the $ECSM$ as the most important part of ECC is the involvement of this operation in the key generation, key exchange, encryption, and decryption processing and even in the elliptic curve digital signature algorithm ($ECDSA$) (Johnson et al., 2001). There are multiple investigations on how to make this operation over prime or binary fields faster as much as possible.

The structure of the $ECSM$ operation involves three computational levels: field arithmetic, point arithmetic and scalar arithmetic (Hankerson et al., 2004). In this work, the focus is on developments at the elliptic

curve point arithmetic and scalar arithmetic levels of elliptic curves over prime field.

The computation of the elliptic curve point arithmetic involves the effective implementation of point doubling and point addition operations. An elliptic curve can be represented using several coordinates systems. For each such system, the speed of point doubling and point addition operations is different. This means a good choice of coordinates system is an important factor for speeding up the $ECSM$.

In the scalar arithmetic level, efforts have been mainly focused on developing efficient algorithms for representation of the scalar k that reduces the number of operations required for the computation of the $ECSM$. The basic technique to compute the $ECSM$ kP is based on the binary form of the scalar k which is called the binary method (Knuth, 1997), the non adjacent form (NAF) (Booth, 1951) and window $\omega-$non adjacent ($\omega - NAF$) (Cohen et al., 2010) are efficient methods to compute kP.

1.3 Objectives

The objective of this study is to improve the performance of the $ECSM$ operation for elliptic curve over prime field. The structure of the $ECSM$ operation involves three computational levels: field arithmetic, point arithmetic and scalar arithmetic. In this work, the focus is on developments at the elliptic curve point arithmetic and scalar arithmetic levels of elliptic curves over prime field. The intention is to achieve this objective by accomplishing the following items:

1. To look for efficient point doubling and point addition operations using minimum cost and less complexity. To achieve this objective, methods employed to compute the elliptic curve scalar multiplication by introducing a new coordinate system in 4 dimension.
2. To look for scalar representation with minimal hamming weight or shorter bit length, To achieve this objective, it is proposed to use methods to compute the elliptic curve scalar multiplication operation by reducing the number of operations in the scalar. This will be by employing the NAF and $w - NAF$ to represent the scalar by using the addition operation.
3. To look for scalar representation with minimal hamming weight or shorter bit length. To achieve this objective, it is proposed to use

methods based on DRM algorithm.

1.4 Thesis Organization

This thesis a study of the $ECSM$ operation and discusses theoretical and practical aspects of this operation. It is organized as follows:

- In this Chapter 1 we have provided a background on cryptology and explained the original of the verious related crytology terms used in this study, followed by the Problem Statement. The Private and Public Key Cryptosystems are then discussed., followed by the Study Objectives which are defined.

- Chapter 2 introduces the basic concepts of the mathematical background needed to understand computational aspects of elliptic curves relevant to their use in cryptography. Starting from the abstract algebra of groups and finite fields to the arithmetic concepts that form the computation of the $ECSM$, this is followed by the underlying hard problem for security in the ECC, and the examples for ECC such as curve analogue of $DHKE$, $ElGamal$ and DSA systems.

- In Chapter 3, this thesis briefly surveys the algorithms known for computing the $ECSM$ operation with a discussion of how we can develop. All methods mentioned (except the binary method) will form the basis for speeding up the $ECSM$ operation in Chapters Five and Six. It starts with an introduction on $ECSM$ describing the mathematical levels involved in its structure. And then, some basic definitions are listed when the cost of computing the $ECSM$ operation is discussed.

- Chapter 4 introduces a modification on Jacobian coordinates, which give faster $ECDBL$ and $ECADD$ operations than affine, projective, and Jacobian coordinates systems. Each point on the elliptic curve over prime field is present by the $4-$ dimensional coordinates $(X = xT, Y = yZ^3, Z, T = Z^2)$ corresponding to the affine point on the same curve $y^2 = x^3 + ax + b$ over F_p. The basis of this technique is to rewrite the $ECDBL$ and $ECADD$ operations with less costly field multiplication inversion, multiplication and squaring operation.

- Chapter 5 comprised the introduction of two methods to enhance the computation of the $ECSM$ operation:

    - First proposed method is to compute the $ECSM$ operation. This algorithm will give a guarantee that it is one of the methods that accelerate the $ECSM$ operation on ECC. The NAF is used to represent the scalar in $ECSM$, which will reduce the cost of computation of the $ECSM$ operation.

    - The second proposed method is to compute the $ECSM$ operation. This algorithm will guarantee that it is one of the methods that accelerate this operation on ECC. The $\omega - NAF$ will be used to represent the scalar in $ECSM$, which will reduce the cost of computation of the $ECSM$ operation. Furthermore, it will be proven that the form coming in this proposed method with its condition exists.

- In Chapter 6, we will introduce other algorithms (third and fourth) to compute the $ECSM$ (kP) operation using the DRM technique but with the lowest number of non zero bits of the scalar k compared with existing algorithms to compute $ECSM$ operation.

    - The third proposed method will be based on the DRM technique and binary form for the scalar k.

    - The fourth proposed method will be based on the DRM technique and NAF for the scalar k.

- Chapter 7 will provide a conclusion and recommendations for related future research.

- Finally, in Appendix A we will list all programs which used the computations of this study. All these programs are written in $Intel(R)Core(Tm)2Duo$ with processor $2.99GHz$ and $3.00GB$ of memory using $MATLAB$ version $7.10.0.499$ ($R2010a$).

BIBLIOGRAPHY

Agnew, G. B., Mullin, R. C. and Vanstone, S. A. 1993. An Implementation of Elliptic Curve Cryptosystems over $F_{2^{155}}$. *IEEE Journal on Selected Areas in Communications* 11 (5): 804–813.

Al-Daoud, E., Mahmod, R., Rushdan, M. and Kilicman, A. 2002. A New Addition Formula for Elliptic Curves Over $GF(2^n)$. *IEEE Transactions on Computers* 51 (8): 972–975.

Avanzi, R. M. 2002. On Multi-Exponentiation in Cryptography. *IACR Cryptology ePrint Archive, Report 2002/154, Available at: http://eprint.iacr.org/2002/154.pdf, September 2014.* .

Avoine, G., Monnerat, J. and Peyrin, T. 2004. Advances in Alternative Non-Adjacent Form Representations. In *Progress in INDOCRYPT 2004, LNCS 3348*, 260–274. Springer-Verlag.

Bahig, H. M. 2008. On a Aeneralization of Addition Chains: Addition-Multiplication Chains. *Discrete Mathematics* 308 (4): 611–616.

Balasubramaniam, P. and Karthikeyan, E. 2007a. Elliptic Curve Scalar Multiplication Algorithm Using Complementary Recoding. *Applied Mathematics and Computation* 190 (1): 51–56.

Balasubramaniam, P. and Karthikeyan, E. 2007b. Fast Simultaneous Scalar Multiplication. *Applied Mathematics and Computation* 192 (2): 399–404.

Bernstein, D. J. and Lange, T. 2015. Explicit-Formulas Database. Available at: http://http://www.hyperelliptic.org/EFD/g1p .

Blake, I. F., Seroussi, G. and Smart, N. 1999. *Elliptic Curves in Cryptography. London Mathematical Society Lecture Note Series 265*. Cambridge: Cambridge University Press.

Blake Ian F., Seroussi Gadiel, P. S. N. 2005. *Advances in Elliptic Curve Cryptography*. Cambridge: Cambridge University Press.

Booth, A. D. 1951. A Signed Binary Multiplication Technique. *The Quarterly Journal of Mechanics and Applied Mathematics* 4 (2): 236–240.

Bos, J. and Coster, M. 1990. Addition Chain Heuristics. In *Advances in Cryptology-CRYPTO'89, LNCS 435*, 400–407. Springer-Verlag.

Bos, J. W., Costello, C., Longa, P. and Naehrig, M. 2014. Selecting Elliptic Curves for Cryptography: An Efficiency and Security Analysis. *IACR Cryptology ePrint Archive, Report 2014/130, Available at: http://eprint.iacr.org/2014/130.pdf, September 2014.* .

Bosma, W. 2001. Signed Bits and Fast Exponentiation. *Journal de theorie des nombres de Bordeaux* 13 (1): 27–41.

Brier, E. and Joye, M. 2003. Fast Point Multiplication on Elliptic Curves Through Isogenies. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* 2643: 43–50.

Burton, D. M. 1980. *Elementary Number Theory*. Revised printing edn. Boston: Allyn & Bacon.

Challita, K. and Farhat, H. 2011. Combining Steganography and Cryptography: New Directions. *International Journal of New Computer Architectures and their Applications* 1 (1): 199–208.

Chris, S. 2002. *The Discrete Log Problem. PhD's Thesis*. Toronto: University of Toronto.

Chudnovsky, D. V. and Chudnovsky, G. V. 1986. Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests. *Advances in Applied Mathematics* 7 (4): 385–434.

Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K. and Vercauteren, F. 2010. *Handbook of Elliptic and Hyperelliptic Curve Cryptography. Series on Discrete Mathematics and Its Applications*. Boca Raton: Chapman & Hall/CRC.

Cohen, H., Miyaji, A. and Ono, T. 1998. Efficient Elliptic Curve Exponentiation Using Mixed Coordinates. In *Advances in Cryptology-ASIACRYPTO'98, LNCS 1514*, 51–65. Springer-Verlag.

Damico, T. M. 2009. A Brief History Of Cryptography. *Student Pulse* 1 (11).

Daswani, N. and Boneh, D. 1999. Experimenting With Electronic Commerce on the PalmPilot. In *Proc. Financial Cryptography, LNCS 1648*, 1–16. Springer-Verlag.

Diffie, W. and Hellman, M. E. 1976. New Directions in Cryptography. *IEEE Transactions on Information Theory* IT-22 (6): 644–654.

Doche, C. and Sutantyo, D. 2014. Faster Repeated Doublings on Binary Elliptic Curves. In *Selected Areas in Cryptography-SAC 2013, LNCS 8282*, 456–470. Springer-Verlag.

Ebeid, N. and Hasan, M. A. 2007. On Binary Signed Digit Representations of Integers. *Designs, Codes and Cryptography* 42 (1): 43–65.

ElGamal, T. 1985. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory* IT-31 (4): 469–472.

Elias, Y. and McKenzie, P. 2014. On Generalized Addition Chains. *Electronic Journal of Combinatorial Number Theory* 14 (A16).

Farashahi, R. R., Wu, H. and Zhao, C. A. 2013. Efficient Arithmetic on Elliptic Curves over Fields of Characteristic Three. In *Selected Areas in Cryptography-SAC2012, LNCS 7707*, 135–148. Springer-Verlag.

Faz-Hernandez, A., Longa, P. and Sanchez, A. H. 2014. Efficient and Secure aAlgorithms for GLV-Based Scalar Multiplication and Their Implementation on $GLV - GLS$ Curves. In *Topics in Cryptology-CT-RSA 2014, LNCS 8366*, 1–27. Springer International Publishing Switzerland.

Fessel, L. E. 2006. *Efficient Scalar Multiplication and Security against Power Analysis in Cryptosystems based on the $NIST$ Elliptic Curves Over Prime Fields. Master's Thesis*. Denmark: University of Copenhagen.

Fong, K., Hankerson, D., Lopez, J. and Menezes, A. 2004. Field Inversion and Point halving Revisited. *IEEE Transactions on Computers* 53 (8): 1047–1059.

Gallant, R. P., Lambert, R. J. and Vanstone, S. A. 2001. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. In *Advances in Cryptology-CRYPTO 2001, LNCS 2139*, 190–200. Springer-Verlag.

Gebbie, S. 2003. *A survey of the Mathematics of Cryptology. Master's thesis*. Johanesburg: University of the Witwatersrand.

Gordon, D. M. 1998. A Survey of Fast Exponentiation Methods. *Journal of Algorithms* 27 (1): 129–146.

Han, D. G., Yi, O. and Takagi, T. 2013. Some Explicit Formulae of NAF and its Left-to-Right Analogue Based on Booth Encoding. *International Journal of Security and Its Applications* 7 (6): 269–274.

Hankerson, D., Menezes, A. J. and Vanstone, S. 2004. *Guide to Elliptic Curve Cryptography*. New York: Springer-Verlag.

Henriquez, F. R., Saqib, N. A., Perez, A. D. and Koc, C. K. 2007. *Cryptographic Algorithms on Reconfigurable Hardware*. USA: Springer-Verlag.

Herbaut, F. and Veron, P. 2010. A Public Key Cryptosystem Based upon Euclidean Addition Chains. In *Sequences and Their Applications-SETA 2010, LNCS 6338*, 284–297. Springer-Verlag.

Heuberger, C. and Krenn, D. 2013. Analysis of Width-ω Non-Adjacent Forms to Imaginary Quadratic Bases. *Journal of Number Theory* 133 (5): 1752–1808.

Heuberger, C. and Mazzoli, M. 2013. Symmetric Digit Sets for Elliptic Curve Scalar Multiplication without Precomputation. *IACR Cryptology ePrint Archive, Report 2013/705, Available at: http://eprint.iacr.org/2013/705.pdf, September 2014.* .

IEEE. 2000. IEEE Standard Specifications for Public-Key Cryptography. 1363^{TM}. *The Institute of Electrical and Electronics Engineers* .

Isidro, S. D. and Montes, E. M. 2011. An Evolutionary Programming Algorithm to Find Minimal Addition Chains. In *I Congreso Internacional de Ingenieria Electronica, Instrumentacion y Computacion. Available at: http://www.lania.mx/ emezura/util/files/A033.pdf, September 2014.*.

Jacobson, M., Menezes, A. and Stein, A. 2001. Solving Elliptic Curve Discrete Logarithm Problems Using Weil Descent. *Journal of the Ramanujan Mathematical Society* 16: 231–260.

Jedwab, J. and Mitchell, C. J. 1989. Minimum Weight Modified Signed-Digit Representations and Fast Exponentiation. *Electronics Letters* 25 (17): 1171–1172.

Johnson, D., Menezes, A. and Vanstone, S. 2001. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security* 1 (1): 36–63.

Joye, M. and Tymen, C. 2001. Compact Encoding of Non-Adjacent Forms with Applications to Elliptic Curve Cryptography. In *Public Key Cryptography, K. Kim, Ed. of Lecture Notes in Computer Science*, 353–364. Springer-Verlag.

Joye, M. and Yen, S. M. 2000. Optimal Left-to-Right Binary Signed-Digit Recoding. *IEEE Transactions on Computers* 49 (7): 740–748.

Joye, M. and Yen, S. M. 2002. New Minimal Modified Radix-r Representation with Applications to Smart Cards. In *Public Key Cryptography - 5th International Workshop on Practice and Theory in Public Key Cryptosystems*, 375–383. Springer-Verlag.

Judson, T. W. 2013. *Abstract Algebra: Theory and Applications*. Boston: MA: PWS Publishing Company.

Jurisic, A. and Menezes, A. 1997. Elliptic Curves and Cryptography. *Dr.Dobb's Journal* 26–36.

Kim, K. H. and Kim, S. I. 2007. A New Method for Speeding Up Arithmetic on Elliptic Curves over Binary Fields. *IACR Cryptology ePrint Archive, Report 2007/181, Available at: http://eprint.iacr.org/2007/181.pdf, September 2014.* .

Kim, K. H., Kim, S. I. and Choe, J. S. 2007. New Fast Algorithms for Arithmetic on Elliptic Curves Over Finite Fields of Characteristic Three. *IACR Cryptology ePrint Archive, Report 2007/179, Available at: http://eprint.iacr.org/2007/179.pdf, September 2014.* .

Knuth, D. E. 1997. *The Art of Computer Programming: Seminumerical Algorithms*. 3rd edn. Canada: Addison Wesley Longman.

Koblitz, N. 1987. Elliptic Curve Cryptosystems. *Mathematics of Computation* 48 (177): 203–209.

Koblitz, N. 1993. *Introduction to Elliptic Curves and Modular Forms. Graduate Texts in Mathematics*. 2nd edn. New York: Springer-Verlag.

Koblitz, N., Menezes, A. and Vanstone, S. 2000. The State of Elliptic Curve Cryptography. *Designs, Codes and Cryptography* 19: 173–193.

Kodali, R. K., Patel, K. H. and Sarma, N. 2013. Implementation of Energy Efficient Scalar Point Multiplication Techniques for ECC. *International Journal on Recent Trends in Engineering and Technology* 9 (14-19).

Koyama, K. and Tsuruoka, Y. 1993. Speeding up Elliptic Cryptosystems by Using a Signed Binary Window Method. In *Advances in cryptology-CRYPTO'92*, 345–357. Springer-Verlag.

Lange, T. 2006. A Note on López-Dahab Coordinates. *Tatra Mt. Math. Publ* 33: 75–81.

Lehmann, F., Maurer, M., Muller, V. and Shoup, V. 1994. Counting the Number of Points on Elliptic Curves over Finite Fields of Characteristic Greater than Three. In *Proc. 1st Algorithmic Number Theory Symposium*, 60–70. Springer-Verlag.

Lercier, R. and Morain, F. 1995. Counting the Number of Points on Elliptic Curves over Finite Fields: Strategies and Performances. In *Advances in Cryptology-EUROCRYPT'95, LNCS 921*, 79–94. Springer-Verlag.

Lim, C. H. and Hwang, H. S. 2000. Speeding up Elliptic Scalar Multiplication with Precomputation. In *Information Security and Cryptology-ICISC'99, LNCS 1787*, 102–119. Springer-Verlag.

Locke, G. and Gallagher, P. 2009. FIPS PUB 186-3: Digital Signature Standard (DSS). Federal Information Processing Standards Publication. *National Institute of Standards and Technology* .

Longa, P. 2007. *Accelerating the Scalar Multiplication on Elliptic Curve Cryptosystems over Prime Fields. PhD's Thesis*. Canada: University of Ottawa.

Longa, P. and Miri, A. 2008. New Multibase Non-Adjacent Form Scalar Multiplication and its Application to Elliptic Curve Cryptosystems (Extended Version). *IACR Cryptology ePrint Archive, Report 2008/052, Available at: http://eprint.iacr.org/2008/052.pdf.pdf, September 2014.* .

Lopez, J. and Dahab, R. 1999. Improved Algorithms for Elliptic Curve Arithmetic in $GF(2^n)$. In *Selected Areas in Cryptography in Cryptography-SAC'98, LNCS 1556*, 201–212. Springer-Verlag.

Lu, C. Y., Jen, S. M. and Laih, C. S. 2013. A General Framework of Side-Channel Atomicity for Elliptic Curve Scalar Multiplication. *IEEE Transactions on Computers* 62 (3): 428–438.

Mahe, E. and Chauvet, J.-M. 2014. Fast $GPGPU$-Based Elliptic Curve Scalar Multiplication. *IACR Cryptology ePrint Archive, Report 2014/198, Available at: http://eprint.iacr.org/2014/198.pdf, September 2014.* .

Mignotte, M. and Tall, A. 2011. A Note on Addition Chains. *International Journal of Algebra* 5 (6): 269–274.

Mihailescu, P. and Rassias, M. T. 2014. *Computational Number Theory and Cryptography*, *Applications of Mathematics and Informatics in Science and Engineering, Springer Optimization and Its Applications*, vol. 91, 349–373.

Miller, V. S. 1986. Use of Elliptic Curves in Cryptography. In *Advances in Cryptology-CRYPTO'85 Proceedings (Santa Barbara, Calif., 1985)*, 417–426. Springer-Verlag.

Mishra, A. M. 2014. A Digital Signature Scheme Based on Pell Equation. *International Journal of Innovative Research in Science, Engineering and Technology* 3 (1): 8596–8600.

Miyaji, A., Ono, T. and Cohen, H. 1997. Efficient Elliptic Curve Exponentiation. In *Advances in Cryptology Proceedings of ICICS'97*, 282–290. Springer-Verlag.

Mohamed, M. A. 2011. On the Improvement of Addition Chain in Applications to Elliptic Curve Cryptosystem. PhD's Thesis .

Mollin, R. A. 2010. *An introduction to cryptography*. 2nd edn. New York: Chapman & Hall/CRC.

Morain, F. and Olivos, J. 1990. Speeding Up the Computations on an Elliptic Curve Using Addition-Subtraction Chains. *Theoretical Informatics and Applications* 24: 531–543.

Muir, J. 2004. *Efficient Integer Representations for Cryptographic Operations. PhD's Thesis*. Canada: University of Waterloo.

Muir, J. A. and Stinson, D. R. 2006. Minimality and Other Properties of the Width-ω Nonadjacent Form. *Mathematics of Computation* 75 (253): 369–384.

Musiker, G. 2005. Schoo's Algorithm for Counting Points on $E(F_q)$. *Available at: http://www.math.umn.edu/ musiker/schoof.pdf, September 2014.* .

N.Thangarasu. 2014. Implementation Secure Authentication Using Elliptic Curve Cryptography 1 (1): 41–44.

Okeya, K., Schmidt-Samoa, K., Spahn, C. and Takagi, T. 2004. Signed Binary Representations Revisited. In *Advances in Cryptology-CRYPTO2004, LNCS 3152*, 123–139. Springer-Verlag.

Okeya, K. and Takagi, T. 2003a. A More Flexible Countermeasure Against Side Channel Attacks Using Window Method. In *Cryptographic Hardware and Embedded Systems, LNCS 2779*, 397–410. Springer-Verlag.

Okeya, K. and Takagi, T. 2003b. The Width-ω NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure Against Side Channel Attacks. In *CT-RSA2003, Lecture Notes in Computer Science*, 328–343. Springer-Verlag.

Oppliger, R. 2011. *Contemporary Cryptography*. 2nd edn. Norwood: Artech House.

Oswald, E. 2002. Introduction to Elliptic Curve Cryptography. *Available at: http://vanilla47.com/PDFs/Cryptography/Miscellenea/ElipticSeptember 2014.* .

Pathak, H. K. and Sanghi, M. 2010. Speeding up Computation of Scalar Multiplication in Elliptic Curve Cryptosystem. *International Journal on Computer Science and Engineering* 2 (4): 1024–1028.

Poonia, S., Nokhwal, M. and Shankar, A. 2013. A Secured Image based Steganography and Cryptography with Watermarking. *International Journal of Engineering Science and Engineering* 1 (8): 66–70.

Raphael, A. J. and Sundaram, V. 2011. Cryptography and Steganography- A Survey. *International Journal of Computer Technology and Applications* 2 (3): 626–630.

Reitwiesner, G. W. 1960. Binary Arithmetic. *Advances in Computers* 1: 231–308.

Rivain, M. 2011. Fast and Regular Algorithms for Scalar Multiplication over Elliptic Curves. *IACR Cryptology ePrint Archive* 2011/338.

Rivest, R. L., Shamir, A. and Adleman, L. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM* 21 (2): 120–126.

Robert, J.-M. 2014. Software Implementation of Parallelized $ECSM$ over Binary and Prime Fields. *Hal. Archives, Available at: https://hal.archives-ouvertes.fr/file/index/docid/998277/filename/paper.pdf, September 2014.* .

Rosen, K. H. 1993. *Elementary Number Theory and Its Applications*. 3rd edn. Canada: Addison Wesley Publishing Company.

Roy, D. B., Mukhopadhyay, D., Izumi, M. and Takahashi, J. 2014. Tile Before Multiplication: An Efficient Strategy to Optimize DSP Multiplier for Accelerating Prime Field ECC for $NIST$ Curves. In *Proceedings of the The 51st Annual Design Automation Conference on Design Automation Conference-DAC'14*, 1–6. ACM.

Sandeep, S. and Shanavas, H. 2012. Hardware Implementation of Elliptic Curve Cryptography over Binary Field. *International Journal of Computer Network and Information Security* 4 (2): 1–7.

Schmidt-Samoa, K., Semay, O. and Takagi, T. 2006. Analysis of Fractional Window Recoding Methods and Their Application to Elliptic Curve Cryptosystems. *IEEE Transactions on Computers* 55 (1): 48–57.

Schonhage, A. 1975. A Lower Bound for the Length of Addition Chains. *Theoretical Computer Science* 1 (1): 1–12.

Schoof, P. R. E. 1995. Counting Points on Elliptic Curves over Finite Fields. *Theorie Nombres Bordeaux Journal* 7 (1): 219âĂŞ254.

Schoof, R. 1985. Elliptic Curves Over Finite Fields and the Computation of Square Roots $modp$. *Mathematics of Computation* 44 (170): 483–494.

Silverman, J. H. 2009. *The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 106*. 2nd edn. New York: Springer.

Solinas, J. A. 1997. An Improved Algorithm for Arithmetic on a Family of Elliptic Curves. In *Advances in Cryptology-CRYPTO'97, LNCS 1294*, 357–371. Springer-Verlag.

Solinas, J. A. 2000. Efficient Arithmetic on Koblitz Curves. *Designs, Codes and Cryptography* 19 (2-3): 195–249.

Spillman, R. J. 2004. *Classical and Contemporary Cryptology*. USA: Prentice-Hall.

Stinson, D. R. 2006. *Cryptography: Theory and Practice. Series on Discrete Mathematics and Its Applications*. 3rd edn. Boca Raton: Chapman & Hall/CRC.

Thilagavathi, K. and Rajeswari, P. 2012. Efficiency and Effectiveness Analysis over ECC-Based Direct and Indirect Authentication Protocols: An Extensive Comparative Study. *Journal on Communication Technology* 3 (1): 515–524.

Thurber, E. G. 1999. Efficient Generation of Minimal Length Addition Chains. *SIAM Journal on Computing* 28 (4): 1247–1263.

Tsaur, W. J. and Chou, C. H. 2005. Efficient Algorithms for Speeding up the Computations of Elliptic Curve Cryptosystems. *Applied Mathematics and Computation* 168 (2): 1045–1064.

Ugus, O., Westhoff, D., Laue, R., Shoufan, A. and Huss, S. A. 2009. Optimized Implementation of Elliptic Curve Based Additive Homomorphic Encryption for Wireless Sensor Networks. *CoRR journal* abs/0903.3900.

Vijayakumar, P., Vijayalakshmi, V. and Zayaraz, G. 2013. Enhanced Level of Security using DNA Computing Technique with Hyperelliptic Curve Cryptography. *International Journal of Network Security* 4 (1).

Washington, L. C. 2008. *Elliptic Curves Number Theory and Cryptography. Series on Discrete Mathematics and Its Applications*. 2nd edn. Boca Raton: Chapman & Hall/CRC.

Wiener, M. J. and Zuccherato, R. J. 1999. Faster Attacks on Elliptic Curve Cryptosystems. In *Selected Areas in Cryptography in Cryptography-SAC'98, LNCS 1556*, 190–200. Springer-Verlag.

Xiao, Y., Li, F. H. and Chen, H. 2011. *Handbook of Security and Networks*. Singapore: World Scientific Publishing Co. Pte. Ltd.

Yan, S. Y. 2002. *Number Theory for computing*. 2nd edn. Berlin: Springer-Verlag.

Yasin, S. M. 2011. *New Signed-Digit* $\{0, 1, 3\} - NAF$ *Scalar Multiplication Algorithm for Elliptic Curve over Binary Field. PhD's Thesis*. Malaysia: University Putra Malaysia.

Yasin, S. M., Mahmod, R. and Nor, R. N. H. 2015. Performance Analysis of Signed- Digit $\{0, 1, 3\} - NAF$ Scalar Multiplication Algorithm in Lopez- Dahab Model. *Research Journal of Information Technology. Available at: http://ftp.ansijournals.com/fulltext/?doi=rjit.0000.66252.66252&org=10, February 2015.* .

Zhang, J. and Wang, P. 2010. Non-Adjacent Form Recursive Algorithm on Elliptic Curves Cryptograph. In *International Conference on Computational Intelligence and Security*, 394–397. IEEE.

Zhang, N., Chen, Z. and Xiao, G. 2007. Efficient Elliptic Curve Scalar Multiplication Algorithms Resistant to Power Analysis. *Information Sciences* 177 (10): 2119–2129.

Zhang, Y., Tanaka, Y. and Wei, S. 2013. Recoding Algorithms for Minimal Signed-Digit Numbers in Residue Number System. In *Conference TENCON 2013 IEEE Region*.