UNIVERSITI PUTRA MALAYSIA

A LIGHTWEIGHT AND SECURE ALGORITHM OF ELLIPTIC CURVE CRYPTOGRAPHY SCALAR MULTIPLICATION USING Q-NAF METHOD IN LOPEZ-DAHAB COORDINATE

WALEED KHALID AMIN ABDULRAHEEM

FSKTM 2019 1

A LIGHTWEIGHT AND SECURE ALGORITHM OF ELLIPTIC CURVE CRYPTOGRAPHY SCALAR MULTIPLICATION USING Q-NAF METHOD IN LOPEZ-DAHAB COORDINATE

By

WALEED KHALID AMIN ABDULRAHEEM

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

April 2019

DEDICATION

To my beloved.

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

A LIGHTWEIGHT AND SECURE ALGORITHM OF ELLIPTIC CURVE CRYPTOGRAPHY SCALAR MULTIPLICATION USING Q-NAF METHOD IN LOPEZ-DAHAB COORDINATE

By

WALEED KHALID AMIN ABDULRAHEEM

April 2019

Chairman : Sharifah Bte Md Yasin, PhD
Faculty : Computer Science and Information Technology

Elliptic curve cryptography (ECC) is gaining increasing popularity and acceptance within the research community. This is because it uses shorter keys to achieve security level equivalent to other public-key cryptosystems. Over the years, special attention has been given to improving the scalar recoding algorithm, since it is the most computationally intensive operation of ECC.

The general research objective of this thesis is to improve the efficiency of the scalar multiplication algorithm of ECC in Lopez Dahab coordinate for elliptic curve over binary field. This is targeted at constrained-resource devices for the internet of things (IoT) such as field programmable gate array (FPGA), radio frequency identifications (RFID) and smart cards.

In literature, window w-NAF method is considered one of the best and most widely used methods for scalar recoding. However, this method does not stand against the recent side channel attack (SCA). The first objective of this thesis is to introduce a new scalar recoding algorithm to achieve better efficiency in terms of security and performance for constrained-resource devices. A new Q-NAF scalar recoding algorithm is proposed to improve the scalar recoding efficiency criteria. Specifically, these criteria includes, hamming weight HW (numbers of non-zeroes), security, and its performance in terms of execution time and memory consumption. To conform to the application requirements of the IoT, the new algorithm improves w-NAF, where w=4. The proposed scalar recoding converts the binary scalar into {-1, 0, 1, 3, 5}-NAF using Q-NAF scalar recoding lookup table or a Q-NAF scalar recoding mathematical formula. Markov chain is used to calculate the HW of the lookup table. Q-NAF reduces the HW of the scalar by 81% on average for n-bit scalar rather than the 80%

HW for w-NAF. By coding the two algorithms, the proposed algorithm improves the execution time and memory consumption with a percentage of about 58% and 93% respectively. Theoretically, Q-NAF scalar recoding is proven to be secure against SCA in terms of timing and simple power attacks.

Since the scalar recoding contains the digit 5 in the representation digits, using quintupling point 5P will increase the efficiency of the scalar multiplication. However, 5P over Lopez-Dahab coordinate in the binary curve has not been considered in literature despite its potential to increase the scalar multiplication performance. A new valid quintupling point 5P arithmetic formula is thus proposed to improve the cost of elliptic curve scalar multiplication method on binary curve over Lopez-Dahab coordinate. The proposed point is formulated as (2(2P) + P) using Al-Daoud for doubling and mix addition. The cost of the proposed point is 17M+12S.

By combining the proposed scalar arithmetic and the new point arithmetic 5P, a new scalar multiplication algorithm was developed. This scalar multiplication algorithm is named Q-NAF scalar multiplication for binary curve over Lopez-Dahab coordinates. The proposed scalar multiplication is more efficient in term of performance than w-NAF scalar multiplication. This is because Q-NAF method reduces the HW without the need to use the digit 7, which it is highly cost during point arithmetic. So, the proposed cryptosystem is more efficient than w-NAF while scalar recoding cost of points to recode and during the scalar multiplication.

Finally, a new look-up table is proposed to optimize the formula {0, 1, 3}-NAF lookup table. The new lookup table reduces the size of the {0, 1, 3}-NAF lookup table from 15X6 into 4X5. This is achieved by scanning two digits to produce one digit instead of three digits, which significantly reduces the time and memory with percentage of about 60% and 75% respectively.

In the first three contributions, a new Q-NAF scalar multiplication method is proposed for the three scalar levels, such that scalar recoding, point arithmetic and scalar multiplication. Compare to 4-NAF, Q-NAF scalar recoding gives better results in terms of HW, time, memory and security, Q-NAF proposed a new point quintupling which used in the scalar recoding. While 4-NAF used more digits in the first two contributions, Q-NAF scalar multiplication is better than 4-NAF scalar multiplication in terms of precomputed points, security, HW and performance. While for the fourth contribution, a modified lookup table is proposed to improve the original method in terms of time, memory and security.

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

ALGORITMA RINGAN DAN SELAMAT BAGI PENDARABAN SKALAR LENGKUNGAN ELLIPTIK KRIPTOGRAFI MENGGUNAKAN KAEDAH Q-NAF DALAM KOORDINAT LOPEZ-DAHAB

Oleh

WALEED KHALID AMIN ABDULRAHEEM

April 2019

Pengerusi : Sharifah Bte Md Yasin, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Populariti dan penerimaan kriptografi lengkung eliptik (ECC) dalam komuniti penyelidikan semakin meningkat. Ini kerana ia menggunakan kekunci yang lebih pendek untuk mencapai tahap keselamatan yang sepadan dengan kriptosistem utama awam yang lain. Selama bertahun, perhatian khas diberikan bagi meningkatkan algoritma pengekodan skalar, kerana perkara ini merupakan operasi yang paling intensif dalam komputasi ECC.

Objektif penyelidikan umum tesis ini adalah untuk meningkatkan kecekapan algoritma pendaraban skalar ECC melalui Lopez Dahab bagi menyelaras lengkung elips ke atas bidang binari. Ini telah disasarkan pada peranti sumber daya terkurung untuk ‘perkara dalam internet’ (IoT) seperti jajaran pintu masuk boleh diprogram (FPGA), pengenalan frekuensi radio (RFID) dan kad pintar.

Dalam literatur, kaedah tertingkap w-NAF dianggap salah satu kaedah terbaik dan paling banyak digunakan untuk pengekalan skalar. Walau bagaimanapun, baru-baru ini kaedah ini tidak menentang serangan saluran sampingan (SCA). Objektif pertama tesis ini adalah untuk memperkenalkan algoritma pengekalan skalar baru untuk mencapai kecekapan yang lebih baik dari segi keselamatan dan prestasi untuk peranti sumber daya terkurung. Algoritma pengekodan skalar Q-NAF telah dicadang untuk meningkatkan kriteria kecekapan pengimbasan skalar. Khususnya, kriteria ini termasuk, ‘berat hamming’ HW (bukan nombor sifar), keselamatan, dan prestasinya dari segi masa pelaksanaan dan penggunaan memori. Untuk mematuhi kehendak aplikasi IoT, algoritma baru meningkatkan w-NAF, di mana w = 4. Pengekalan skalar yang dicadang bagi menukar skalar binari menjadi {-1, 0, 1, 3, 5} -NAF menggunakan jadual carian pengimbasan skalar Q-NAF atau formula matematik berskalar yang

dikod Q-NAF. Rantaian Markov digunakan untuk mengira HW jadual carian. Q-NAF mengurangkan scalar HW sebanyak 81% secara purata untuk skalar n-bit, bukannya 80% HW untuk w-NAF. Dengan pengekodan kedua algoritma, algoritma yang dicadangkan dapat memperbaiki masa pelaksanaan dan penggunaan memori dengan peratusan masing-masing sekitar 58% dan 93%. Secara teori, pengekalan skalar Q-NAF terbukti selamat terhadap SCA dari segi masa dan serangan mudah kuasa.

Oleh kerana skalar yang dikod mengandungi angka 5 dalam digit perwakilan, dengan menggunakan titik *quintupling* 5P akan meningkatkan kecekapan pendaraban skalar. Walau bagaimanapun, 5P di atas koordinat Lopez-Dahab dalam lengkung binari tidak dipertimbangkan dalam literatur, walaupun berpotensi dalam meningkatkan prestasi pendaraban skalar. Oleh itu, formula aritmetik 5P titik kuantiti yang sah adalah dicadangkan untuk menambah baik kos kaedah pendaraban skalar lengkung elips pada lengkung binari ke atas koordinat Lopez-Dahab. Titik yang dicadangkan formulanya sebagai (2 (2P) + P) dengan menggunakan Al-Daoud untuk menggandakan dan penambahan tambahan. Kos titik yang dicadangkan ialah 17M + 12S.

Dengan menggabungkan aritmetik skalar yang dicadangkan dan aritmetik titik 5P baru, algoritma pendaraban skalar baru telah dibangunkan. Algoritma pendaraban skalar ini dinamakan multiplikasi skalar Q-NAF untuk lengkung binari berbanding koordinat Lopez-Dahab. Pendaraban skalar yang dicadangkan lebih berkesan dari segi prestasi berbanding pendaraban skalar w-NAF. Ini kerana kaedah Q-NAF mengurangkan HW tanpa perlu menggunakan angka 7, yang sangat tinggi semasa aritmetik titik. Oleh itu, kriptosistem yang dicadangkan adalah lebih cekap daripada w-NAF melalui kos pengiraan skalar untuk dikod serta semasa pendaraban skalar.

Akhir sekali, jadual paparan baru dicadangkan untuk mengoptimumkan jadual carian {0, 1, 3} -NAF. Jadual carian baru mengurangkan saiz jadual carian {0, 1, 3} -NAF dari 15X6 ke 4X5. Ini dapat dilaksanakan dengan mengimbas dua digit untuk menghasilkan satu digit dan bukannya tiga digit, secara signifikan dapat mengurangkan masa dan memori dengan peratusan masing-masing sekitar 60% dan 75%.

Dalam tiga sumbangan pertama, kaedah pendaraban skalar Q-NAF baru dicadangkan untuk tiga tahap skalar, seperti pengekalan skalar, aritmetik titik dan pendaraban skalar. Perbandingan antara 4-NAF dan Q-NAF, pengimbasan skalar Q-NAF memberi hasil yang lebih baik dari segi HW, masa, memori dan keselamatan, Q-NAF mencadangkan titik mata baru yang digunakan untuk pengimbasan skalar. Sementara 4-NAF menggunakan lebih banyak digit dalam dua sumbangan pertama, pendaraban skalar Q-NAF pula adalah lebih baik daripada pendaraban skalar antara 4-NAF dari segi titik, keselamatan, HW dan prestasi. Walaubagaimanapun, untuk sumbangan keempat, jadual carian yang telah diubahsuai pula dicadangkan untuk memperbaiki kaedah asal dari segi masa, memori dan keselamatan.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank ALLAH Subhanahu Wataala, who has strengthened me through the best and toughest years of my life, and without his blessings, this achievement would not be possible. I'm asking Him to accept this work.

I'm particularly grateful to Dr. Sharifah Bte Md Yasin for the supervising, encouraging and support given towards the execution this research, and to my committee Dr. Muhammad Rezal Bin Dato' Kamel Ariffin and Dr. Nur Izura Binti Udzir for their support. I'm also appreciating the efforts of Sis.Miza Mumtaz, I learnt a lot from her.

I would like to thank my parent, sisters, brothers and friends.

For the past four years, my son Yousef and two daughters Nada and Hala kept on reminding me to go to study and complete this research! I'm very grateful to them.

Finally, and most importantly, I owe more than thanks to the light of my life, my wife, Bushra Hussein AbuHaq. Her support, encouragement, quiet patience and unwavering love. Many thanks also to her family.

Thank You All.

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

Sharifah Bte Md Yasin, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Muhammad Rezal Bin Dato' Kamel Ariffin, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

Nur Izura Binti Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
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, illustrations and citations have been duly referenced;
- this 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.: Waleed Khalid Amin Abdulraheem, (GS43330)

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) were adhered to.

Signature: ______________________

Name of Chairman of Supervisory Committee: Dr. Sharifah Bte Md Yasin

Signature: ______________________

Name of Member of Supervisory Committee: Associate Professor Dr. Muhammad Rezal Bin Dato' Kamel Ariffin

Signature: ______________________

Name of Member of Supervisory Committee: Associate Professor Dr. Nur Izura Binti Udzir

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	Advance encryption standard
DBNS	Double Base Number System
DES	Data Encryption Standard
DLP	Discrete logarithm problem
DSA	Digital signature algorithm
EC	Elliptic curve
ECC	Elliptic curve cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDLP	Elliptic curve discrete logarithm problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECE	Elliptic Curve ElGamal
FPGA	Field programmable gate array
GF	Galois field
HW	Hamming weight
IFP	Integer factoring problem
IoT	Internet of Things
L2R	Left-to-right
LD	Lŏpez-Dahab
LSB	Least significant bit
MSB	Most significant bit
NAF	Non-adjacent form
NIST	National institute of standards and technology

PDA	Personal digital assistants
PKC	public key cryptography
Q-NAF	Quintupling Non-adjacent form
R2L	Right-to-left
RFID	Radio frequency identifications
SCA	side channel attack
WSN	Wireless sensor network
w-NAF	Width Non-Adjacent Form
wmbNAF	Window Multi-base Non-Adjacent Form

CHAPTER 1

INTRODUCTION

1.1 Introduction

Technological advances made in the development of smart devices and e-communication has affected almost all facets of life. By 2020, more than 30 billion devices are expected to be connected to the internet in what is called Internet of Things (IoT). This unprecedented number of devices, along with their expected fast increase, puts two principal concerns, i.e. security and power consumption on the spot light. Constrained-resource devices are a major component of this recent technology, where memory and power are limited, while secure communication channel is crucial. These constrained-resource devices access and connection flexibility that recent technology makes occur with various threats and introduces the need for computational and performance-demanding security mechanisms (Suárez-Albela, Fraga-Lamas, & Fernández-Caramés, 2019).

Constrained-resource devices like RFID and sensors are applied in diverse areas to sense, transmit and store sensitive information. The most appropriate technique to ensure privacy and confidentially of the sensitive information is cryptography. Usually, digital signature and encryption are used to secure documents during storage and transmission. Due to the device limited computational strength, capability of the device resources such as time, memory, energy and security by encryption schemes must be minimized. This way, constrained-resource devices can also participate in secure communication channel (Aditia, 2019).

Lightweight cryptography scheme is a branch of cryptography supported by the National Institute of Standards and Technology (NIST). Lightweight cryptography consumes minimal execution time, memory consumption, energy and bandwidth. Devices such as embedded frameworks, RFID, wireless sensor network (WSN) and field programmable gate array (FPGA) are on the lower end of the constrained-resource devices range (Shah & Engineer, 2019).

To secure digital information on constrained-resource devices from attackers, different cryptosystem algorithms are implemented at the core of the cryptographic protocol to encrypt and decrypt the data. Two main subsets of the method are symmetric and asymmetric cryptography (Baccarini & Hayajneh, 2019).

1.1.1 Cryptography

Cryptography is mainly concerned with establishing the secrecy between the communication entities. The term cryptography expresses the art of writing or solving the codes in this world either everything is private, or everything is public to all for free access. Cryptography rises from the old Greeks; it means encoding message to be shared with other people. This encoded message is transferred through the public communication way so that no eavesdropper can understand the plain message even he carries that cipher message (Ajith, Balaji Ganesh Kumar, Latha, Samiappan, & Muthu, 2018).

Recently, cryptosystem protocols are being designed to improve the strength of security algorithms with information transmission. Different branches of knowledge are involved in these cases. These include using number theory, mathematics, information theory, statistics and computational complexity. For the purpose of data transmission and data storage, these areas of knowledge applied to cryptography aims to provide four cryptographic services which are confidentiality, integrity, authentication and non-repudiation. Confidentially service ensures information remains secret, and integrity service ensure that the information has not been changed, authentication service ensures the origin of the message is correctly identified, whereas non-repudiation service ensures that both sender and receiver will not deny the transmission commitment (Bhat & Kapoor, 2019).

1.1.2 Public-Key Cryptosystem

Generally, cryptology has two major types, i.e., private key and public key cryptography. The term private key or symmetric key cryptography refers to any system that utilizes one key for both encryption and decryption of the plain text for communicating parties involved. On the other hand, the public key cryptography refers to any system that utilizes a pair of keys, one is used for data encryption (the public key), while the other is used for data decryption (the private key). Although private key cryptography (symmetric) is achieving highly efficient, it has drawbacks with key management, non-repudiation service and efficient secure key distribution through a communication channel (Hodgson, 2019).

Examples of symmetric cryptosystem Data Encryption Standard (DES), Advance Encryption Standard (AES), Carlisle Adams and Stafford Tavares (CAST), Blowfish, Two fish, International Data Encryption Algorithm (IDEA), and secure and fast encryption routine (SAFER) algorithms. Other cryptographic algorithms such as Rivest, Shamir and Adleman (RSA), digital signature algorithm (DSA), Elgamal, and elliptic curve cryptography (ECC) are examples of asymmetric cryptosystem algorithm. Asides the aforementioned categories, there is hash function, which uses a mathematical transformation to iterate a compression function on the input message, such as message digest (MD) and SHA family. These categories of cryptography algorithms are as illustrated in Figure 1.1 (Dixit, Gupta, & Trivedi, 2018) .

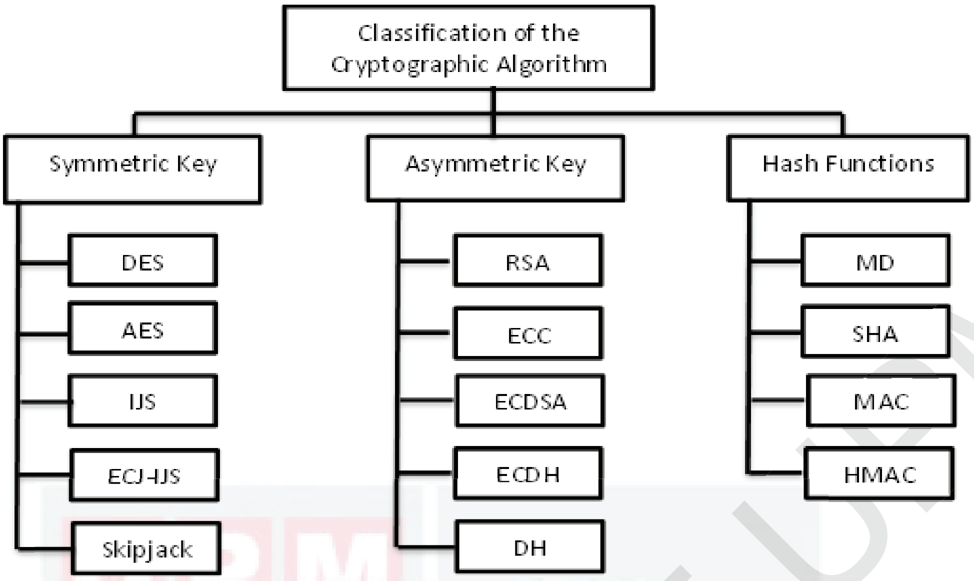

Figure 1.1 : Classification of the cryptographic algorithm

Public key cryptography simplifies the mechanism of key distribution, and ensures information can be made confidential by encrypted with public key (Baek et al., 2019). If using asymmetric cryptosystem offers a better key distribution solution, however, performance is slower than symmetric cryptosystem (Baccarini & Hayajneh, 2019). The security of modern asymmetric cryptosystem depends on the hardness of mathematical problems, such as integer factoring problem (IFP), discrete logarithm problem (DLP), elliptic curve discrete logarithm problem (ECDLP) and others (Liu, Choo, & Grossschadl, 2018).

1.2 Problem Statement

Working on the security of constrained-resource devices is essential. Cryptography is one of the significant ways to ensure privacy and to protect information from unauthorized personel. In ECC applications and protocols, the scalar multiplication algorithm is considered as a major operation (Thangarasu & Selvakumar, 2018). The elliptic curve scalar multiplication computational process is the most time and resource consuming operation.

Implementation of ECC is a challenge for constrained-resource devices such as mobile technology devices, personal digital assistants (PDA's), embedded systems, sensors and smart cards (Bafandehkar, Yasin, Mahmod, & Hanapi, 2013). These devices have constraints in memory, CPU, energy consumptions and battery, while the performance like timing and speed are highly required with privacy (security) usage.

The width non-adjacent form (w-NAF) method was proposed by (Okeya & Takagi, 2003a). The main objective of this method is to provide fast scalar multiplication using small memory, and to be secure against side channel attack (SCA). Recently, w-NAF method has been still widely used to reduce the computational cost in ECC and it is considered as one of the best methods known so far (Dou, Weng, Ma, & Wei, 2017). However, w-NAF, double-and-add algorithm and width-4 NAF methods are prone to and not more secure against SCA, (Abdulrahman & Reyhani-Masoleh, 2015) & (Järvinen & Balasch, 2017). The algorithm representation of the key in w-NAF is vulnerable to several SCA attacks, such as cache-timing attacks. This is due to its non-constant time execution which targeted previously using cache-timing techniques (Tuveri, Hassan, Garcia, & Brumley, 2018), this prove that the algorithm of w-NAF needs to be improved in term of security. The suitable width for w-NAF to be used in constrained-resource devices is $w = 4$ for its number operation required (M. F. De Oliveira & Henriques, 2015), since 4-NAF requires only 3P, 5P and 7P precomputed points. Related literature on w-NAF attempted to reduce its HW such as multi-base mb-NAF method (Longa & Gebotys, 2010) and $frac\, w$-NAF method (Méloni & Hasan, 2016). Reducing the HW will increase the performance of scalar multiplication (Musa & Xu, 2017). However, the high precomputed point also is costly in terms of time, memory, CPU and battery power for constrained-resource devices (Bafandehkar et al., 2013). Selecting less precomputing points such as 3P and 5P only in the scalar recoding with the same HW of 4-NAF scalar recoding will increase the efficiency of scalar multiplication, without losing its security characters.

The scalar multiplication performance depends on the performance of the elliptic curve point operations. Point multiplication is important and dominates the execution time of the elliptic curve (Rashidi, 2017). Basically in the operation, there is $Q = kP = P + P + P + \ldots + P$ (k times), where k the secret (private) key is a positive integer, P and Q are two points on a curve. Binary curve according to NIST requires a smaller key size to be secure than the prime curve (NIST, 2013). Over binary curve, Lopez-Dahab (LD) coordinate gives the best performance for elliptic curve over the binary field (S. Yasin & Muda, 2015) (Rashidi, 2017) and it is the most studied coordinate system for binary elliptic curves (T. Oliveira, López, Aranha, & Rodríguez-Henríquez, 2014). According to (Musa & Xu, 2017), the point quintupling 5P using LD is not available in the literature. Since scalar multiplication can be improved by using efficient point operations (S. Yasin & Muda, 2015), introducing point quintupling 5P will be efficient for scalar multiplication

Introducing a new scalar recoding and point arithmetic should be accomplished with scalar multiplication algorithm. Different scalar multiplication methods have been proposed, however, double-and-add method has remained the most straightforward form to compute scalar multiplication (Mostafa, 2018). Double-and-add method entails doubling all scalar digits while adding the nonzero digits only (Allan, Brumley, & Falkner, 2016).

{0, 1, 3}-NAF scalar recoding method is introduced by (S. M. Yasin, 2011). The method uses lookup table of size 15 rows and 6 columns. During the recoding process, the proposed lookup table scans three consecutive digits to produce one. The original lookup table contains two special cases during recoding execution, which require more time than other, non-constant time execution of these two special cases according to other cases make the lookup table vulnerable to SCA. Improving a lookup table which reduces the scanning digits from three into two and contains no special cases will be more efficient and secure.

1.3 Research Objectives

In general, working on ECC scalar multiplication contains three levels of computation (Rezai & Keshavarzi, 2011) and (Bafandehkar, Yasin, & Mahmod, 2016) as shown in Figure 1.2. For an efficient scalar multiplication algorithm, it is necessary to accomplish the three levels of arithmetic operation.

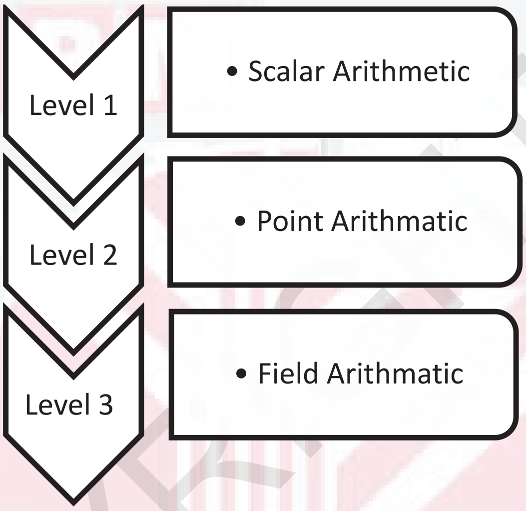

Figure 1.2 : Computational levels in the scalar multiplication

The principal objective of this thesis is to propose a scalar multiplication algorithm with a simple form and less cost for elliptic curve over binary field. A number of other objectives must be accomplished. These objectives are discussed in what follows:

Propose New Scalar Recoding Algorithm

Hamming weight (HW) is the number of nonzero digit in the binary number. The efficiency of the scalar multiplication kP depends on the number of hamming weight in the scalar k. The proposed Q-NAF scalar recoding algorithm converts the binary number of k into {-1, 0, 1, 3, 5} digits since it is the only digits use in 3 bits lookup table. The Q-NAF scalar recoding has the non-adjacent form (NAF) property. Q-NAF scalar recoding algorithm can be represented either in form of lookup table or mathematical formula. In order to cater for the application requirement of resource constrained devices The new algorithm makes a trade-off between the performances of the recoding algorithm with respect to hamming weight, security, time, and memory consumption, so as to be suitable for constrained-resource devices. Binary field is chosen since its secured key size is smaller than prime key size, which is more suitable for constrained-resource devices.

Propose a New Point Quintupling (5P) for General Binary Curve Using Lopez-Dahab Coordinate

To achieve an efficient elliptic curve scalar multiplication performance, precomputed points help to realize a faster computation (T. Oliveira et al., 2014) which takes away the need to repeat the addition process every time. Mixed addition in Affine and Lŏpez-Dahab is used for point formula since the mixed addition computation cost is better than the traditional addition in Lopez-Dahab coordinates (S. Yasin & Muda, 2015). While using digit 5 in the scalar recoding, new point arithmetic namely Quintupling (5P) is proposed for the general binary curve for implementation in scalar multiplication. To save the quintupling (5P) cost, it is computed as (2(2P) + P) where two doubling and one mixed addition is required. The quintupling cost is measured by calculating the number of field operation in the computation.

Propose New Scalar Multiplication Algorithm

Scalar multiplication algorithm is the main computation in the ECC. Thus, after introducing a new scalar recoding arithmetic and a new point arithmetic, there is a need to have a new Q-NAF scalar multiplication algorithm to integrate the scalar recoding and the new point quintupling. The complexity of Q-NAF is measured by counting the number of point operations per scalar during its execution.

Improve the lookup table of {0, 1, 3}-NAF method

The $\{0,1,3\}-$NAF was introduced as an efficient and lightweight method used to recode the scalar with NAF property. The original method uses lookup table which is of size 15x6, contains special cases and scan three digits to produce one through scalar recoding process. For more efficiency, this study aims to propose a modified lookup table smaller in size than the original, scanning two digits instead of three digits and contains no special case while recoding to be secure against SCA. The proposed lookup table aims to be more efficient in terms of time, memory and security.

1.4 Research Contributions

This research contains four contributions at different ECC computational levels as in Figure 1.1 above. These contributions are highlighted as following:

1.4.1 Q-NAF Scalar Recoding Algorithm

Q-NAF scalar recoding method is proposed as an improvement to the w-NAF method where $w = 4$ for specifically caters for constrained-resource devices. The proposed method recodes the scalar from binary into {-1, 0, 1, 3, 5}-NAF. Q-NAF can be executed using either lookup table or its associated mathematical formula. HW of Q-NAF is $\frac{2}{11}n$ (where n is scalar size). Q-NAF is more efficient compared with 4-NAF in terms of time, memory and security.

1.4.2 New Quintupling Formula for Point Arithmetic

A new 5P point arithmetic formula for Lopez-Dahab coordinate system is proposed over the binary curve. The new quintupling point (5P) is introduced using the formula 5P = 4P + P = 2(2P) + P using Al-Daoud formula (Al-Daoud, Mahmod, Rushdan, & Kilicman, 2002) for doubling and mix addition with cost 17M+12S.

1.4.3 Q-NAF Scalar Multiplication Algorithm

The Q-NAF scalar recording and the new quintupling point 5P arithmetic formula are integrated into the design of Q-NAF Scalar Multiplication for Lopez-Dahab coordinate over the binary curve using the double-and-add method.

1.4.4 Improving the Lookup Table of {0, 1, 3}-NAF Method

A new Lookup table is proposed to improve the {0, 1, 3}-NAF lookup table. The new lookup table reduces table size from 15x6 into 6x5 without special cases and with constant time during execution for all rows. The improved table scans two digits only, which improved execution time and memory consumption.

1.5 Research Scope

This work concentrates on the first two levels of scalar multiplication, the scalar recoding and point arithmetic. It includes proposing, enhancement, and analysis of the scalar multiplication for an elliptic curve using LD in the binary field. For the improvement on scalar arithmetic, w-NAF is chosen to compare where $w = 4$.

1.6 Thesis Outline

This thesis is organised as follows:

Chapter 2 introduces the related literature in general to this work and the associated background information on cryptography and the elliptic curve cryptography. It gives an introduction to each level in the computational scalar multiplication. In Chapter 3, the methodology of this research is proposed by introducing a general scheme which contains four phases related to problem identification, suggested solution, analysis and performance evaluation and expected results phase. Chapters 4, 5, 6 and 7 discuss the proposed contributions 1, 2, 3 and 4 respectively and their associated results. Diverse techniques used for deriving and substantiating these results such as algorithms, lemmas, mathematical proofs and coding are also detailed in these chapters. Chapter 8 concludes this thesis with an overall summary of these contributions and makes suggestions for future research.

1.7 Summary

Thesis implication is summarized as in Table 1.1 below.

Table 1.1 : Summary of Research Plan

Current Technique	Research Problem	Research Objective	Proposed Solution	Analysis Methods	Findings
1. w-NAF technique is still widely used for scalar recoding. 2. $w = 4$ is suitable for constrained-resource devices	1. w-NAF insecure against SCA. 2. Need to improve in terms of performance.	Objective 1: 1. Improve HW, time and memory. 2. Secure against SCA.	Contribution 1: Q-NAF method using lookup table or mathematical formula with a special case where $w = 4$ using the digits {-1,0,1,3,5}.	1. Markov chain for HW. 2. Java code: timing and RAM. 3. Mathematical proofs: Efficiency. 4. Security analysis: SCA.	1. HW=81%, 2. Reduce memory: 80-90% and reduce time 10-60%. 3. Secure against SCA. 4. Suitable for constrained-resource devices.
1. Binary curve requires small secure key. 2. Lopez-Dahab best coordinate over binary curve. 3. Mixed addition minimize cost	1. While using the digit 5 in the scalar recoding, point quintupling 5P need to be implemented using proper curve and coordinate.	Objective 2: Propose a new point quintupling 5P over binary curve using LD coordinate	Contribution 2: Formulate new 5P point quintupling with forms using LD coordinate and mixed addition operation of forms 5P=3P+2P and 2. 5P=2(2P)+P	1. The two forms are proven as a valid using affine coordinate method equation over the mixed addition and LD coordinate. 2. Calculating the cost.	1. The form of 5P=3P+2P cost is 23M+13S with 2D+2A 2. The form 5P=2(2P)+P cost is 17M+12S with 2D+1A
Double-and-add still the most straightforward form to compute scalar multiplication.	1. w-NAF scalar multiplication recodes the digits $\{0, \mp1, \mp3, \mp5, \mp7\}$. 2. Q-NAF recodes digits {-1, 0, 1, 3, 5}-NAF, a new scalar multiplication algorithm should be implemented.	Objective 3: Propose a new scalar that comprises Q-NAF scalar recoding digits and the proposed 5P	Contribution 3: Q-NAF scalar multiplication algorithm is proposed considers the recoding digits and the new point 5P using double-and-add algorithm since it is the most straightforward method.	1. The scalar multiplication algorithm using the proposed lookup table and the point quintupling and the multiplication algorithm. Evaluate the omit 7P in w-NAF with HW and multiplication cost.	Theoretically, Q-NAF is better than 4-NAF in terms of: 1. HW with 1% while 7P is highly cost in w-NAF. 2. Time and memory 3.Q-NAF multiplication is secure only by adding additional anti-SCA software and hardware
1. {0, 1, 3}-NAF method proved as efficient for scalar recoding using lookup table and mathematical formula.	1. The lookup table is of size 15x6. 2. Not secured against SCA. 3. The lookup table scans three digits.	Objective 3: 1. To improve the {0, 1, 3}-NAF lookup table with smaller size, and the same HW. 2. Secure against SCA. 3. Scan two digits only.	Contribution 4: 1. Modified {0, 1, 3}-NAF lookup table of size 6x5 and its mathematical formula are proposed. 3. Scans two digits only. 3. Lookup table contain no special case while execution with no special case.	1. Java code used to compare time and memory consumed to recode different scalar size. 2. Security analysis for SCA.	1. Execution time reduced by 50-60%, memory consumed reduced by 60-75% with same HW. 2. Secure against SCA.

REFERENCES

Abarzúa, R., Martínez, S., Mendoza, V., & Valera, J. (2018). Avoiding Side-Channel Attacks by Computing Isogenous and Isomorphic Elliptic Curves. Mathematics in Computer Science, 12(3), 295–307.

Abdulrahman, E. A. H., & Reyhani-Masoleh, A. (2015). New Regular Radix-8 Scheme for Elliptic Curve Scalar Multiplication without Pre-Computation. IEEE Transactions on Computers, 64(2), 438–451.

Aditia, M. K. (2019). Optimized CL-PKE with Lightweight Encryption for Resource Constrained Devices. In Proceedings of the 20th International Conference on Distributed Computing and Networking (pp. 427-432). ACM. (pp. 427–432).

Agrawal, R., & Vemuri, R. (2018). On State Encoding Against Power Analysis Attacks for Finite State Controllers. In 2018 IEEE International Symposium on Hardware Oriented Security and Trust (pp. 181–186). IEEE.

Ahmad, M. M., Yasin, S. M., Mahmod, R., & Mohamed, M. A. (2015). X-Tract Recoding Algorithm for Minimal Hamming Weight Digit Set Conversion. Journal of Theoretical and Applied Information Technology, 75(1), 109–114.

Ajeena, R. K. K., & Kamarulhaili, H. (2015). Accelerating Integer Sub-Decomposition for Elliptic Scalar Multiplication using the Generalized w. Malaysian Journal of Mathematical Sciences, 9, 115–137.

Ajith, S., Balaji Ganesh Kumar, M., Latha, S., Samiappan, D., & Muthu, P. (2018). Iris Cryptography for Security Purpose. Journal of Physics: In Series, 1000(1).

Al-Daoud, E., Mahmod, R., Rushdan, M., & Kilicman, A. (2002). A new addition formula for elliptic curves over GF(2n). IEEE Transactions on Computers, 51(8), 972–975. https://doi.org/10.1109/TC.2002.1024743

Allan, T., Brumley, B. B., & Falkner, K. (2016). Amplifying Side Channels Through Performance Degradation. In Proceedings of the 32nd Annual Conference on Computer Security Applications, ACM (pp. 422–435).

Araújo, J., Cameron, P. J., & Matucci, F. (2018). An Invitation to Inverse Group Theory. ArXiv Preprint ArXiv:1803.10179, 1–33.

Atiyah, M. (2018). Introduction to commutative algebra. CRC Press, (c), 1–4.

Baccarini, A. N., & Hayajneh, T. (2019). Evolution of Format Preserving Encryption on IoT Devices : FF1 +. In Proceedings of the 52nd Hawaii International Conference on System Sciences (Vol. 6, pp. 1628–1637).

Baek, J., Susilo, W., Salah, K., Ha, J. S., Damiani, E., & You, I. (2019). Stateful Public-Key Encryption: A Security Solution for Resource-Constrained Environment. In In Advances in Cyber Security: Principles, Techniques, and

Applications (pp. 1–22). Springer Singapore.

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.

Bafandehkar, M., Yasin, S. M., Mahmod, R., & Hanapi, Z. M. (2013). Comparison of ECC and RSA algorithm in resource constrained devices. 2013 International Conference on IT Convergence and Security, ICITCS 2013, 0–2.

Barreto, P. S. L. M., & Naehrig, M. (2006). Pairing-friendly elliptic curves of prime order. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3897 LNCS, 319–331.

Bellemou, A., Benblidia, N., Anane, M., & Issad, M. (2018). MicroBlaze-Based Multiprocessor embedded cryptosystem on FPGA for Elliptic Curve Scalar Multiplication over Fp. Journal of Circuits, Systems, and Computers.

Bernstein, D. J. (2006). Curve25519: new Diffie-Hellman speed records. International Workshop on Public Key Cryptography, 25519, 207–228.

Bharathi, C. R. (2018). Improved ELGAMAL Encryption for Elliptic Curve Cryptography. International Journal of Pure and Applied Mathematics, 118(17), 341–353.

Bhat, S., & Kapoor, V. (2019). Secure and Efficient Data Privacy, Authentication and Integrity Schemes Using Hybrid Cryptography. In International Conference on Advanced Computing Networking and Informatics (Vol. 2, pp. 279–285).

Boruah, D., & Saikia, M. (2015). Implementation of ElGamal Elliptic Curve Cryptography Over Prime Field Using C. Information Communication and Embedded Systems (ICICES, (May), 1–7.

Chabrier, T., Pamula, D., Tisserand, A., Chabrier, T., Pamula, D., Tisserand, A., … Bretagne, R. (2011). Hardware implementation of DBNS recoding for ECC processor Processor. In Signals, Systems and Computers (ASILOMAR), 2010 Conference Record of the Forty Fourth Asilomar Conference on. IEEE (pp. 1129–1133).

Chande, M. K., Lee, C.-C., & Li, C.-T. (2018). Cryptanalysis and improvement of a ECDLP based proxy blind signature scheme. Journal of Discrete Mathematical Sciences and Cryptography, 21(1), 23–34.

Chang, C., Kuo, Y., & Lin, C. (2003). Fast algorithms for common-multiplicand multiplication and exponentiation by performing complements. In Advanced Information Networking and Applications, 2003. AINA 2003. 17th International Conference on (pp. 1–5).

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

Ciet, M., Joye, M., Lauter, K., & Montgomery, P. L. (2006). Trading inversions for multiplications in elliptic curve cryptography. Designs, Codes, and Cryptography, 39(2), 189–206.

Cohen, H., Frey, G., & Avanzi, R. (2006). Handbook of Elliptic and Hyperelliptic Curve Cryptography. Taylor & Francis Group.

Corrigan-Gibbs, H., & Kogan, D. (2018). The Discrete-Logarithm Problem with Preprocessing. In In Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham. (p. (pp. 415-447)).

De Oliveira, M. F., & Henriques, M. A. A. (2015). A secure and efficient method for scalar multiplication on supersingular elliptic curves over binary fields. Information Security, 407–416.

Dimitrov, V., Imbert, L., & Mishra, P. K. (2008). The double-base number system and its application to elliptic curve cryptography. Mathematics of Computation, 77(262), 1075–1104.

Dimitrov, V. S., Jullien, G. A., & Miller, W. C. (1999). Theory and applications of the double-base number system. IEEE Transactions on Computers, 48(10), 1098–1106.

Dixit, P., Gupta, A. K., & Trivedi, M. C. (2018). Traditional and Hybrid Encryption Techniques: A Survey. In Networking Communication and Data Knowledge Engineering (Vol. 3, pp. 239–248).

Doche, C., Icart, T., & Kohel, D. R. (2006). by Isogeny Decompositions. In Annual Cryptology Conference . Springer, Berlin, Heidelberg.

Dou, Y., Weng, J., Ma, C., & Wei, F. (2017). Secure and efficient ECC speeding up algorithms for wireless sensor networks. Soft Computing, 21(19), 5665–5673.

Dubal, M., & Deshmukh, A. (2013). On Pseudo-random Number Generation. In International Symposium on Security in Computing and Communication (pp.77-89). Springer, Berlin, Heidelberg.

Dzurenda, P., Ricci, S., Hajny, J., & Malina, L. (2017). Performance Analysis and Comparison of Different Elliptic Curves on Smart Cards. In International Conference on Privacy, Security and Trust ., 1–10.

Eğecioğlu, Ö., & Koç, Ç. K. (1994). Exponentiation using canonical recoding. Theoretical Computer Science, Elsevier, 129(2), 407–417.

Fan, J., & Verbauwhede, I. (2012). An updated survey on secure ECC implementations: Attacks, countermeasures and cost. Lecture Notes in Computer

Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6805 LNCS, 265–282.

Fong, K., Hankerson, D., López, J., & Menezes, A. (2004). Field inversion and point halving revisited. IEEE Transactions on Computers, 53(8), 1047–1059.

Forouzan, B. A. (2007). Cryptography and Network Security. McGraw-Hill, Inc. New York, NY, USA.

Gagniuc, P. A. (2017). Markov chains : from theory to implementation and experimentation. John Wiley & Sons.

Ge, Q., Yarom, Y., Cock, D., & Heiser, G. (2018). A Survey of Microarchitectural Timing Attacks and Countermeasures on Contemporary Hardware. Journal of Cryptographic Engineering, 8(1), 1–27.

Grinstead, C. M., & Snell, J. L. (2012). Markov Chains (Chapter 11). In Introduction to Probability (pp. 405–470). John Wiley & Sons.

Guerrini, E., Imbert, L., & Winterhalter, T. (2018). Randomized Mixed-Radix Scalar Multiplication. IEEE Transactions on Computers, 67(3), 418–431.

Hamburg, M. (2015). Decaf: Eliminating cofactors through point compression. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9215, 705–723.

Hankerson, D. (2004). Guide to Elliptic Curve Cryptography. Springer.

Harvey, D., Hoeven, J. Van Der, & Lecerf, G. (2014). Faster polynomial multiplication over finite fields. ArXiv Preprint ArXiv:1407.3361, 2052, 1–23.

Higuchi, A., & Takagi, N. (2000). Fast addition algorithm for elliptic curve arithmetic in GF(2n) using projective coordinates. Information Processing Letters, 76(3), 101–103.

Hodgson, R. (2019). Solving the security challenges of IoT with public key cryptography. Network Security, 2019(1), 17–19.

Järvinen, K., & Balasch, J. (2017). Single-trace side-channel attacks on scalar multiplications with precomputations. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10146 LNCS, 137–155.

Järvinen, K., Sinha, S., & Ingrid, R. (2018). Arithmetic of τ -adic expansions for lightweight Koblitz curve cryptography. Journal of Cryptographic Engineering, 1–16.

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.

Joye, M. (2007). Highly regular right-to-left algorithms for scalar multiplication. In In International Workshop on Cryptographic Hardware and Embedded Systems, Springer, Berlin, Heidelberg (pp. 135–147).

Joye, M., & Quisquater, J.-J. (2001). Hessian Elliptic Curves and Side-Channel Attacks. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 402-410). Springer, Berlin, Heidelberg.

Joye, M., & Yen, S. (2000). Optimal Left-to-right Binary Signed-Digit Recoding. IEEE Transactions on Computers, 49(7), 1–8.

Kak, A. (2015). Lecture 12 : Public-Key Cryptography and the RSA Algorithm Lecture Notes on " Computer and Network Security ." Avinash Kak, Purdue University, 1–94.

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.

Khandaker, A., & Nogami, Y. (2016). Isomorphic Mapping for Ate-based Pairing over KSS Curve of Embedding Degree 18. In 2016 Fourth International Symposium on Computing and Networking (CANDAR) (pp. 629-634). IEEE.

King, B. (2008). wNAF*, an efficient left-to-right signed digit recoding algorithm. In International Conference on Applied Cryptography and Network Security, Springer, Berlin, Heidelberg. (pp. 429–445).

Kodali, R. K., Budwal, H. S., Patel, K., & Sarma, N. (2013). High Performance Scalar Multiplication for ECC. IEEE 2013 Tencon - Spring, TENCONSpring 2013 - Conference Proceedings, (April 2013), 352–356.

Kong, F., & Li, D. (2005). A Note on Signed Binary Window Algorithm for Elliptic Curve Cryptosystems. In In International Conference on Cryptology and Network Security. Springer, Berlin, Heidelberg. (pp. 223–235).

Lalonde, D. R. (2017). Private and Public-Key Side-Channel Threats Against Hardware Accelerated Cryptosystems.

Lange, T. (2004). A note on L´opez-Dahab coordinates. Tatra Mountains Mathematical Publications, 33, 75-81.

Lee, E. A. (2015). The past, present and future of cyber-physical systems: A focus on models. Sensors (Switzerland), 15(3), 4837–4869.

Li, M., Miri, A., & Zhu, D. (2011). Analysis of the Hamming Weight of the Extended wmbNAF. IACR Cryptology ePrint Archive.

Liardet, P.-Y., & Smart, N. P. (2001). Preventing SPA/DPA in ECC Systems Using the Jacobi Form. In In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 391–401).

Liu, Z., Choo, K. K. R., & Grossschadl, J. (2018). Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography. IEEE Communications Magazine, 56(2), 158–162.

Liu, Z., Longa, P., Pereira, G. C. C. F., Reparaz, O., & Seo, H. (2018). Four$\mathbb{Q}$ on embedded devices with strong countermeasures against side-channel attacks. IEEE Transactions on Dependable and Secure Computing., 529(10), 665–686.

Longa, P. (2011). High-Speed Elliptic Curve and Pairing-Based Cryptography. University of Waterloo,Canada.

Longa, P., & Gebotys, C. H. (2008). Setting Speed Records with the (Fractional) Multibase Non-Adjacent Form Method for Efficient Elliptic Curve Scalar Multiplication. IACR Cryptology EPrint Archive, 2008, 118.

Longa, P., & Gebotys, C. H. (2010). Efficient techniques for high-speed elliptic curve cryptography. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 80-94). Springer, Berlin, Heidelberg.

Longa, P., & Miri, A. (2016). New Multibase Non-Adjacent Form Scalar Multiplication and its Application to Elliptic Curve Cryptosystems (extended version). IACR Cryptology EPrint Archive, 1(1), 52.

López, J., & Dahab, R. (1999). Improved Algorithms for Elliptic Curve Arithmetic in GF (2 n). Springer-Verlag Berlin Heidelberg, 97(107), 201–212.

Marouf, I., Asad, M. M., & Al-haija, Q. A. (2017). Comparative Study of Efficient Modular Exponentiation Algorithms. An International Journal of Advanced Computer Technology, 8(6).

McKenzie, R. N., McNulty, G. F., & Taylor, W. F. (2018). Algebras, lattices, varieties. American Mathematical Soc, 383(204).

Méloni, N., & Hasan, M. A. (2016). Random Digit Representation of Integers. ARITH, San Francisco, United States., pp 1-9.

Montgomery, P. L. (1987). Speeding the Pollard and elliptic curve methods of factorization. Mathematics of Computation, 48(177), 243–243.

Moon, J., Jung, I. Y., & Park, J. H. (2018). IoT application protection against power analysis attack. Computers and Electrical Engineering, 67, 566–578.

Moon, S. (2006). A binary redundant scalar point multiplication in secure elliptic curve cryptosystems. International Journal of Network Security, 3(2), 132–137.

Mostafa, M. (2018). Using Random Digit Representation for Elliptic Curve Scalar Multiplication.

Muir, J. A., & Stinson, D. R. (2006). Minimality and other properties of the width-w nonadjacent form. Mathematics of Computation, 75(253), 369–384.

Murdica, C., & Guilley, S. (2017). Countermeasure method for an electronic component implementing an elliptic curve cryptography algorithm.

Musa, S. Al, & Xu, G. (2017). Fast Scalar Multiplication for Elliptic Curves over Binary Fields by Efficiently Computable Formulas. In International Conference in Cryptology in India, Springer, Cham (pp. 206–226).

Najlae, F. H., & Rushdan, M. (2015). Speeding up the Elliptic Curve Scalar Multiplication Using Non Adjacent Form. Journal of Discrete Mathematical Sciences and Cryptography, 18(6), 801–821.

Ngyen, P., & Igor. (2003). The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces. Designs, Codes and Cryptography, 55(30,), 201–217.

Nicolas, M., & Hasan, M. A. (2009). Exponentiation Using a Large-Digit Representation and ECC Applications. Univ. Waterloo, 1–15.

NIST. (2013). Digital Signature Standard (DSS). (No. Federal Inf. Process. Stds.(NIST FIPS)-186-4).

Nofriansyah, D., Defit, S., Nurcahyo, G. W., Ganefri, G., Ridwan, R., Ahmar, A. S., & Rahim, R. (2018). A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm. Journal of Physics: Conference Series, 954(1), 1–7.

Okeya, K., & Schmidt-samoa, K. (2004). LNCS 3152 - Signed Binary Representations Revisited. In Annual International Cryptology Conference . Springer, Berlin, Heidelberg. (pp. 123–139).

Okeya, K., & Takagi, T. (2003a). The Width- w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications, CT-RSA 2003, 328–343.

Okeya, K., & Takagi, T. (2003b). The Width-w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks. Topics in Cryptology — CT-RSA 2003 SE - 23, 2612, 328–343.

Oliveira, Thomaz, Julio López, and F. R.-H. (2017). The Montgomery ladder on binary elliptic curves. Journal of Cryptographic Engineering, 8(3), 1–18.

Oliveira, T., López, J., Aranha, D. F., & Rodríguez-Henríquez, F. (2014). Two is the fastest prime: Lambda coordinates for binary elliptic curves. Journal of Cryptographic Engineering, 4(1), 3–17.

Olyan, R., & Malik, S. (2015). Complexity Analysis Of Improved ECC Algorithm. International Journal of Scientific Engineering and Applied Science (IJSEAS), 2(5), 113–118.

Patil, J., Bansod, G., & Kant, K. S. (2019). DoT: A New Ultra-lightweight SP Network Encryption Design for Resource-Constrained Environment. In Data Engineering and Communication Technology, Advances in Intelligent Systems and Computing 828, (Vol. 828, pp. 249–257). Springer Singapore.

Pohlig, S. C., & Hellman, M. E. (1978). An improved algorithm for computing logarithms over GF (p) and its cryptographic significance. IEEE Transactions on Information Theory, 24(1), 106–110.

Pollard, J. M. (1978). Monte Carlo methods for index computation mod p. Mathematics of Computation, 32(143), 918–918.

Qin, B., Li, M., Kong, F., & Li, D. (2009). New left-to-right minimal weight signed-digit radix-r representation. Computers and Electrical Engineering, 35(1),

150–158.

Rahaman, O. (2017). Data and Information Security in Modern World. Computer Science and Engineering, 7(1), 12–21.

Rao, S. (2017). Elliptic Curve Arithmetic for Cryptography. The Australian National University, Australia.

Rashidi, B. (2017). A Survey on Hardware Implementations of Elliptic Curve Cryptosystems. ArXiv Preprint ArXiv:1710.08336., (December), 1–61.

Realpe-Muñoz, P., Trujillo-Olaya, V., & Velasco-Medina, J. (2014). Design of elliptic curve cryptoprocessors over GF(2163) on Koblitz curves. In 2014 IEEE 5th Latin American Symposium on Circuits and Systems, LASCAS 2014 - Conference Proceedings (pp. 14–17).

Reyes, A. C., Castillo, A. K. V., Morales-Sandoval, M., & Diaz-Perez, A. (2013). A performance comparison of elliptic curve scalar multiplication algorithms on smartphones. In 23rd International Conference on Electronics, Communications and Computing, CONIELECOMP 2013 (pp. 114–119).

Rezai, A., & Keshavarzi, P. (2011). High-performance implementation approach of elliptic curve cryptosystem for wireless network applications. 2011 International Conference on Consumer Electronics, Communications and Networks, CECNet 2011 - Proceedings, 1323–1327.

Rezai, A., & Keshavarzi, P. (2015). A New Left-to-Right Scalar Multiplication Algorithm Using a New Recoding A New Left-to-Right Scalar Multiplication Algorithm Using a New Recoding Technique. International Journal of Security and Its Applications, 8(3), 31–38.

Rezai, A., & Keshavarzi, P. (2016). CCS Representation : A new non-adjacent form and its application in ECC. Journal of Basic and Applied Scientific Research, 2(5), 4577–4586.

Rozanov, Y. A. (2012). Introduction to Random Processes. Springer Science & Business Media.

Sasdrich, P., & Güneysu, T. (2015). Implementing Curve25519 for Side-Channel--Protected Elliptic Curve Cryptography. ACM Transactions on Reconfigurable Technology and Systems, 9(1), 1–15.

Setiadi, I., Kistijantoro, A. I., & Miyaji, A. (2015). Elliptic curve cryptography: Algorithms and implementation analysis over coordinate systems. In 2nd International Conference on Advanced Informatics: Concepts, Theory and Applications (ICAICTA), 2015 (pp. 1–12).

Shah, A., & Engineer, M. (2019). Advances in Computer Communication and Computational Sciences (Vol. 759). Springer Singapore.

Smart, N. P. (2001). The Hessian Form of an Elliptic Curve. Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings, 2162, 118–125.

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

Spreitzer, R., Moonsamy, V., Korak, T., & Mangard, S. (2018). Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. IEEE Communications Surveys and Tutorials, 20(1), 465–488.

Suárez-Albela, M., Fraga-Lamas, P., & Fernández-Caramés, T. (2019). A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices. Sensors, 18(11), 3868.

Sullivan, N. T. (2008). Fast Algorithms for Arithmetic on Elliptic Curves Over Prime Fields. IACR Cryptology EPrint Archive, 2008, 60.

Thangarasu, N., & Selvakumar, A. A. L. (2018). Improved elliptical curve cryptography and Abelian group theory to resolve linear system problem in sensor-cloud cluster computing. Cluster Computing, 1–10.

Tun Myat Aung, & Ni Ni Hla. (2017). A Study of General Attacks on Elliptic Curve Discrete Logarithm Problem over Prime Field and Binary Field. World Academy of Science, Engineering and Technology, 11(11), 1153–1160.

Tuveri, N., Hassan, S. ul, Garcia, C. P., & Brumley, B. B. (2018). Side-Channel Analysis of SM2: A Late-Stage Featurization Case Study. In Proceedings of the 34th Annual Computer Security Applications Conference on - ACSAC '18 (pp. 147–160).

Wang, J., Li, J., Wang, H., Zhang, L. Y., Cheng, L.-M., & Lin, Q. (2018). Dynamic Scalable Elliptic Curve Cryptographic Scheme and Its Application to In-Vehicle Security. IEEE Internet of Things Journal, PP(c), 1–10.

Wenger, E., & Hutter, M. (2012). Exploring the design space of prime field vs. binary field ECC-hardware implementations. Springer Science & Business Media, 7161 LNCS, 256–271.

Yasin, S.M., Mahmod, R. and Nor, R. N. . (2015). performance analysis of signned-digit {0,1,3}-NAF scalar multiplication algorithm in Lopez-Dahab model. Research Journal of Information Technology, 7(7), .80-100.

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

Yasin, S., & Muda, Z. (2015). Tripling formulae of elliptic curve over binary field in Lopez-Dahab model. Journal of Theoretical and Applied Information Technology, 75(2), 212–216.

Yi, J. H., Kim, E., & Cheon, J. H. (2012). US 8,255,691 B2.

Yi, J.H., Cheon, J.H., Kwon, T., Lee, M.K. and Kim, E., S. E. C. L. (2012). US 8,160,256 B2.

Yu, W., Wang, K., Li, B., & Tian, S. (2013). On the Expansion Length Of Triple-Base Number Systems. In International Conference on Cryptology in Africa (pp. 424–432).

BIODATA OF STUDENT

Waleed Khalid Amin Abdulraheem was born on October 15, 1977 in Kuwait, Jordanian nationality. He has studied a bachelor degree in Computer science in 2012, and he received in 2014 his master's degree in computer science. Currently, he is working towards the PhD degree in Universiti Putra Malaysia (UPM). He worked in a business in the past years.

LIST OF PUBLICATIONS

Waleed K AbdulRaheem, Sharifah Bte Md Yasin, Nur Izura Binti Udzir and Muhammad Rezal bin Kamel Ariffin, "Improving the Performance of {0,1,3}-NAF Recoding Algorithm for Elliptic Curve Scalar Multiplication" *International Journal of Advanced Computer Science and Applications (IJACSA),* 10(4), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100432.

AbdulRaheem, Waleed and Yasin, Sharifah. (2019). "New Quintupling Point Arithmetic 5P Formulas for Lŏpez-Dahab Coordinate Over Binary Elliptic Curve Cryptography" *International Journal of Advanced Computer Science and Applications (IJACSA)*. Manuscript number IJACSA_2019_10_6. Submitted on 13 May 2019

UNIVERSITI PUTRA MALAYSIA

STATUS CONFIRMATION FOR THESIS / PROJECT REPORT AND COPYRIGHT

ACADEMIC SESSION : ____________________

TITLE OF THESIS / PROJECT REPORT :

A LIGHTWEIGHT AND SECURE ALGORITHM OF ELLIPTIC CURVE CRYPTOGRAPHY SCALAR MULTIPLICATION USING Q-NAF METHOD IN LOPEZ-DAHAB COORDINATE

NAME OF STUDENT: WALEED KHALID AMIN ABDULRAHEEM

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as :

*Please tick (√)

☐ **CONFIDENTIAL** (Contain confidential information under Official Secret Act 1972).

☐ **RESTRICTED** (Contains restricted information as specified by the organization/institution where research was done).

☐ **OPEN ACCESS** I agree that my thesis/project report to be published as hard copy or online open access.

This thesis is submitted for :

☐ **PATENT** Embargo from ______________ (date) until ______________ (date)

Approved by:

(Signature of Student)
New IC No/ Passport No.:

Date :

(Signature of Chairman of Supervisory Committee)
Name:

Date :

[Note : If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]