UNIVERSITI PUTRA MALAYSIA

ENHANCEMENT OF {0, 1, 3}-NAF RECODING ALGORITHM USING BLOCK METHOD TECHNIQUE FOR ELLIPTIC CURVE CRYPTOSYSTEM

MOHSEN BAFANDEHKAR

FSKTM 2015 8

ENHANCEMENT OF {0, 1, 3}-NAF RECODING ALGORITHM USING BLOCK METHOD TECHNIQUE FOR ELLIPTIC CURVE CRYPTOSYSTEM

By

MOHSEN BAFANDEHKAR

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirement for the Degree of Master of Science

July 2015

COPYRIGHT

DEDICATION

This thesis is especially dedicated to my parents.

Abstract of the thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the Degree of Master of Science

ENHANCEMENT OF {0, 1, 3}-NAF RECODING ALGORITHM USING BLOCK METHOD TECHNIQUE FOR ELLIPTIC CURVE CRYPTOSYSTEM

By

MOHSEN BAFANDEHKAR

July 2015

Chairman: Sharifah MD. Yasin, Ph.D.
Faculty: Computer Science and Information Technology

In mid 80s Neal Koblitz and Victor Miller independently proposed the use of elliptic curves in cryptography. Elliptic Curve Cryptosystem (ECC) is a type of public key cryptography (PKC) based on the algebraic structure of elliptic curve over finite fields. For a smaller key size, ECC is able to provide the same level of security with RSA. This feature made ECC one of the most popular PKC algorithms today. Scalar multiplication is known as the fundamental operation in ECC algorithm and protocols.

The efficiency of ECC critically depends on the efficiency of the scalar multiplication operation. Scalar multiplication involves three levels of computations: scalar arithmetic, point arithmetic and field arithmetic. Improving the first two levels will lead to significant increment in the efficiency of the scalar multiplication. Scalar arithmetic level can be improved by employing an enhanced scalar recoding algorithm that can reduce the Hamming weight or decrease the number of operations in the scalar representation process.

The objective of this research is to introduce an efficient implementation of {0, 1, 3}-NAF scalar recoding algorithm by implementing block method. With block method application on the based algorithm, a complex look up table is undesired. Instead a fix look up table is introduced with less computation required for recoding. The proposed look up table contains equivalent value for 256 binary number in {0, 1, 3}-NAF representation. Each binary number in table is 8 bits length. Therefore, the input binary must be partitioned in *n* blocks of 8 bits before being processed through look up table. The running time is used to measure the performance of the based and the proposed algorithm. The focus of this research is on the enhancement of the scalar arithmetic level by designing and analysing an inexpensive {0, 1, 3}-NAF scalar recoding algorithm in an

effort to maintain the Hamming weight for the based algorithm and reduce the algorithm complexity.

In order to clearly demonstrate the running time difference between the based and the proposed algorithm, both algorithms performance time are measured and compared. The environment is controlled and there is no effect from the test bed, the running process has been repeated 5, 10 and 20 times. To enhance the reliability of results the average of each run has been calculated and used. The result from the input data yielded the following results: The proposed algorithm has overall 86% speed up in comparison to the base algorithm. In the proposed algorithm, partitioning function takes up to 74% and look up table takes up to 29% of the total elapsed time.

Abstrak tesis ini dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk Ijazah Master Sains

PENINGKATAN REKOD ALGORITMA {0, 1, 3} -NAF MENGGUNAKAN TEKNIK KAEDAH BLOK DALAM KRIPTO SISTEM LENGKUNG ELIPTIK

Oleh

MOHSEN BAFANDEHKAR

Julai 2015

Pengerusi: Sharifah MD. Yasin, Ph.D.
Fakulti: Sains Komputer dan Teknologi Maklumat

Pada pertengahan 80-an Neal Koblitz dan Victor Miller secara berasingan mencadangkan penggunaan kriptografi lengkung eliptik. Kripto sistem Lengkung Eliptik (ECC) adalah berjenis kriptografi kunci awam (PKC) berdasarkan struktur algebra lengkung eliptik keatas medan terbatas. Untuk saiz kunci yang sama, ECC boleh memberikan tahap keselamatan yang sama dengan RSA. Ciri ini membuatkan ECC adalah salah satu algoritma PKC yang popular pada hari ini. Pendaraban skalar dikenali sebagai asas operasi di dalam algoritma dan protokol ECC.

Keberkesanan ECC adalah amat bergantung kepada keberkesanan operasi pendaraban skalar. Gandaan skalar melibatkan tiga peringkat pengiraan: aritmetik skalar, aritmetik titik dan aritmetik medan. Penambahbaikan dua paras yang pertama akan membawa kepada peningkatan ketara dalam pendaraban skalar. Tahap aritmetik skalar boleh ditingkatkan dengan menggunakan penambahbaikan algoritma rekod skalar yang boleh mengurangkan berat Hamming atau mengurangkan bilangan operasi dalam proses perwakilan skalar.

Objectif kajian ini adalah untuk memperkenalkan keberkesanan perlaksanaan {0, 1, 3}-NAF algoritma rekod skalar dengan melaksanakan kaedah blok. Dengan aplikasi kaedah block berasaskan algoritma asas, jadual carian yang kompleks adalah tidak diingini. Sebaliknya jadual carian tetap diperkenalkan dengan pengiraan yang kurang diperlukan untuk rekod. Jadual carian yang diperkenalkan mengandungi nilai yang sama untuk 256 nombor binari dalam perwakilan{0, 1, 3}-NAF. Setiap nombor binari didalam jadual adalah panjang 8-bit. Oleh itu, input binari mesti dibahagikan kepada n blok 8 bit sebelum diproses melalui jadual carian. Masa larian digunakan untuk mengukur prestasi berasaskan algoritma yang dicadangkan. Fokus kajian ini adalah terhadap peningkatan tahap aritmetik skalar dengan reka bentuk dan analisis yang murah

{0, 1, 3} -NAF algoritma kod semula dalam usaha untuk mengekalkan berat Hamming algoritma asas dan mengurangkan kerumitan algoritma.

Dalam usaha untuk menunjukkan dengan jelas perbezaan masa larian antara algoritma asas dan algoritma yang dicadangan, kedua-dua algoritma telah dijalankan dan masa prestasi mereka diukur. Kepada alam sekitar dikawal dan tidak ada apa-apa kesan dari katil ujian, proses berjalan dengan telah diulangi 5, 10 dan 20 kali dan purata telah dikira dan digunakan. Hasil daripada data input menghasilkan keputusan berikut: algoritma yang dicadangkan mempunyai keseluruhan kelajuan sehingga 86% berbanding dengan algoritma asas. Dalam algoritma yang dicadangkan, fungsi pembahagian mengambil masa sehingga 74% dan jadual carian mengambil masa sehingga 29% daripada jumlah masa yang telah berlalu.

ACKNOWLEDGEMENTS

First and foremost I offer my hearty and sincere gratitude to my resource person **"Dr. Sharifah MD Yasin"** who has supported me throughout my thesis with her patience and knowledge. Her attitude and priceless encouragements have given me a great opportunity to handle this project and grow as a researcher. Topics discussed with her would always remain in my mind. Besides my advisor, here I am to gratefully acknowledge the contribution and invaluable help of **"Prof. Dr. Ramlan Mahmod"**. Without his guidance I would not have been able to complete this project in such a wonderful fashion.

More my dedication would not finish without mentioning the devoted prayers of my Parents. So I heartily dedicate this project to them as well. This humble effort is dedicated to my honorable parents, who encouraged and guided me to get the aim of life with love and respect.

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

Sharifah MD. Yasin, Ph.D.
Senior Lecturer
Faculty of Computer Science & Information Technology
Universiti Putra Malaysia
(Chairman)

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

Zurina Mohd Hanapi, Ph.D.
Senior Lecturer
Faculty of Computer Science & Information Technology
Universiti Putra Malaysia
(Member)

BUJANG BIN KIM HUAT, 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
- the thesis has not been submitted previously or comcurrently 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 owned from supervisor and 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: Mohsen Bafandehkar GS34574

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: _____

Signature: _____
Name of
Member of
Supervisory
Committee: _____

Signature: _____
Name of
Member of
Supervisory
Committee: _____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

PKC	Public-Key Cryptography
SKC	Symmetric-Key Cryptography
ASKC	Asymmetric-Key Cryptography
PKI	Public-Key Infrastructure
IFP	Integer Factorization Problem
DLP	Discrete Logarithm Problem
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECC	Elliptic Curve Cryptosystem
RSA	Rivest-Shamir-Adleman
NAF	Non-Adjacent Form
PB	Polynomial Basis
XOR	Exclusive-OR
NB	Normal Basis
NIST	National Institute of Standards and Technology
FIPS 186-3	Federal Information Processing Standards Publication 186-3
ANSI	American National Standards Institute
NSA	National Security Administration
SECG	Standards for Efficient Cryptography Group
LSB	Least Significant Bit
RDTSC	Read Time Stamp Counter

CHAPTER 1

INTRODUCTION

1.1 Introduction

Over recent years, human lives have been massively computerized and depend not only on the usage of digital devices but reliability of technologies and trustworthy of the services they provide. The reality is, digital devices have become necessary tools of nowadays highly mobile lifestyle. These small, multi-purpose and fairly low-cost devices have several functionalities such as sending and receiving electronic mail and messages, storing documents and sensitive data, remotely accessing to servers and data. Although, these devices are giving us numerous benefits, they also raise new risks to organizations and individuals.

During these years digital communication has become a part of our daily lives. It has revolutionized in ways in which people remain connected. And as technology grows, the development of new features to digital devices has been on the increase, starting with the small phones and arriving to the generation of the smart phones which operates like a computer.

There is a trade-off between features and security of digital devices. The more feature available in digital devices the higher level of security is required. A digital environment would not be secure without implementing the security techniques such as encryption technique. Encrypting the sensitive data is one of the biggest defences to preserve their secrecy and confidentiality from unpermitted users. The concept of encryption has been around since the Ancient Babylonia, yet only recently has it been applied to the digital field.

1.2 Overview of Cryptography

Cryptography is the knowledge of creating and developing methods to securely conveying information. The main objective of cryptography is to only allow intended receivers to receive the data securely. Practically, cryptography is the act of restricting unintended viewers from viewing the actual content of a data. The cryptography terminology includes cryptosystem, plaintext, cipher text, encryption, and decryption.

- A **cryptosystem** is pair of algorithms that take a key and convert plaintext to cipher text and convert back from cipher text to plaintext (Desai *et al.*, 2014). Generally, the term cryptosystem is a short form of

cryptographic system. It is a computer system that involves cryptography. In the context of cryptography, a cryptosystem refer to a suite of algorithms needed to implement a particular form of encryption and decryption (Farlex, 2010). Typically, a cryptosystem consists of three important modules: key generation, encryption and decryption.

- **Plaintext** is referring to meaningful data which can be understood.
- **Cipher text** is meaningless data which cannot be understood.
- **Encryption** is the process of transforming meaningful data (plaintext) into meaningless data (cipher text) which cannot be understood.
- **Decryption** is the process of transforming scrambled data (cipher text) into meaningful data (plain text) which can be understood.

The key concept behind cryptography is to manipulate data in a way that can only be understood by the authorized user when the right key which acts as a password is applied to decrypt the data. Cryptography is an interdisciplinary science that concerns the knowledge of mathematics, information theory, computational complexity, statistics, combinatorial and number theory (Sandoval, 2008). It provides the following customary information security services to protect sensitive data (Medani *et al.*, 2011):

- **Confidentiality** is service to assure secrecy of data from all users whilst only available among authorized users.
- **Integrity** is a service used to verify that original form of data has not been altered into another context by unauthorized users.
- **Authentication** is a service to determine whether or not the user is authorized to access data.
- **Non-repudiation** is a service to ensure that both parties (sender and receiver) are obliged to acknowledge the authenticity of their signature on previous operations or commitments.

Generally there are two types of cryptographic algorithms available; Asymmetric-Key Cryptography (ASKC) and Symmetric-Key Cryptography (SKC). Asymmetric-Key Cryptography that uses public key and private key is also known as Public-Key Cryptography (PKC). The difference between the two cryptographic algorithms is in the key management (Sun *et al.*, 2012). SKC uses the same key to encrypt and decrypt data while PKC uses two different keys. Public key which is publicly available to everyone to encrypt the message, and a private key which is kept secret and available to only the recipient of the message to decrypt the message. SKC is highly efficient but it has drawbacks in key distribution, key management and in the provision of non-repudiation (Paryasto *et al.*, 2009).

With modern algorithms, the strength of protection depends solely on the length of the key if the algorithm itself is trusted (that is, it is believed not to contain a

mathematical shortcut). The more sensitive the data is, and the longer it needs to be kept secret, the longer key size must be used. There is a direct relationship between variable key lengths and level of security in asymmetric encryption algorithms. The bigger the key size, the more secure the algorithm it. But on the other hand, bigger key size requires more computational power and resources. And rationally these prerequisites will lower the algorithm's performance.

Therefore performance might be an issue that influences the choice of key length. And a good balance needs to be found between speed and protection strength, because PKC algorithms run slower with larger key sizes. This is challenging due to high performance and level of security demand whilst maintain user flexibility. PKC provides a method for exchange of secret keys if a Public-Key Infrastructure (PKI) is already in place. This enables the use of asymmetric algorithms to exchange or negotiate secret information, such as keys, to other encryption systems.

This procedure appears to be sound and easy to use, but an important assumption was made: that the first entity could reliably obtain the other's public key. This is not as easy as it seems, as there might be no secure way to obtain it over an untrusted network. To reduce the risk of key compromise, and to limit the damage an attacker can do by gaining access to a key, keys are often changed during communication. How frequently the keys are changed depends on key length and key usage.

In general, public-key algorithms have been designed based on few computationally hard problems. Three of them are well-known and each of them is based on modular arithmetic (Kumar, 2006):

a) Integer Factorization Problem (IFP)
b) Discrete Logarithm Problem (DLP)
c) Elliptic Curve Discrete Logarithm Problem (ECDLP)

Critical security factors such as confidentiality, authentication, data integrity and non-repudiation must be provided by any cryptosystem based on any of the above algorithms.

1.3 Motivation

By digitalization of human life and increasing the utilization of embedded and resource constrained devices, security of these devices is becoming a major concern. There is an inherent conflict between advantages and resource limitations of constrained device. Resource constrained devices have limited computation of resources such as CPU, memory and battery. As the chips and

microprocessors are becoming increasingly smaller, it is necessary to make cryptographic schemes both secure and uncostly.

According to recent study (Mishra *et al.*, 2014; Schmidt and Medwed, 2009; Shehzad *et al.*, 2014), Elliptic Curve Cryptosystem (ECC) can provide the same level of security with smaller size of key compared with the other similar algorithms such as Rivest-Shamir-Adleman (RSA). Bit size of the key determines space or memory demands. Smaller key size is more effective since it requires less hardware resources, low key transmission time, less memory for storage, low cost of arithmetic computation and low bandwidth. Therefore it is known as the most suitable cryptographic algorithms for constrained devices.

Thus, application of ECC is highly recommended to create more security and higher speed while computational load is not increased (Dabholkar and Yow, 2004). On the other hand chips are being designed with smaller size and extra limitations (i.e. computation power, memory and battery life). Also cryptographic scheme especially in resource constrained devices, need to be not only secure but also practical and uncostly.

The unique mathematical structure of ECC provides different point on the curve from addition of two other points (Paryasto *et al.*, 2009). Determination of primitive points is difficult. The two essential point operations in scalar multiplication operation are; point addition and point doubling. In order to add two different points addition operation is used. Doubling is used when the two points are the same.

Scalar multiplication operation is an iterative addition operation for given scalar k and point P:

$$Q = kP = P + P + \ldots + P \text{ (for } k \text{ times)} \quad (1.1)$$

In equation 1.1, P and Q are two distinct points on the elliptic curve and scalar k is the private key where $k \in Z$. To enhance the performance of ECC the scalar multiplication performance need to be optimized (Kodali *et al.*, 2013). Scalar multiplication involves with three levels of computations: scalar arithmetic, point arithmetic and field arithmetic (X. Huang *et al.*, 2010). To improve scalar representation in scalar arithmetic level, a scalar recoding algorithm that can greatly reduce the Hamming weight of the scalar is needed (Hankerson *et al.*, 2003). The Hamming weight is defined as the number of nonzero digits in a scalar representation. A fast scalar recoding algorithm can enhance the performance of ECC algorithm (Rezai and Keshavarzi, 2014).

1.4 Problem Statement

The fundamental operation in ECC algorithm and protocols is scalar multiplication. This operation is the most costly and time consuming operation in ECC (Li and Miri, 2011). Accordingly, efficiency of ECC critically depends on the efficiency of scalar multiplication operation (Kodali *et al.*, 2013). In addition, efficiency of the scalar multiplication operation is highly depended and can be optimized by improving the performance of scalar recoding (Rezai and Keshavarzi, 2014). Therefore according to literatures, optimization of recoding algorithm can result in the speed up of the whole ECC operations (Faz-Hernández *et al.*, 2014).

In this research, some of the traditional scalar recoding algorithms such as binary method and traditional NAF (non-adjacent form) method has been studied. Some of the available algorithms today include Modified Booth's algorithm (Villeger and Oklobdzija, 1993a), and {0, 1, 3}-NAF algorithm (Md Yasin, 2011) and NAF-Block Recoding Method (Pathak and Shanghi, 2010) and (Brar and Kaur, 2011) has been reviewed. Modified Booth's algorithm is a complicated method to compute the 2's complement and is less effective in improving scalar representation. This is due to the fact that operation of booth encoder is complex when compared to an AND array method in binary representation (Villeger and Oklobdzija, 1993a). While traditional NAF algorithm is more effective in reducing Hamming weight, but it is slightly more complex in the algorithm structure compared to booth method (Pathak and Sanghi, 2010). {0, 1, 3}-NAF performs more effective than the other two mentioned algorithms in terms of reducing hamming weight at average cases (Md Yasin, 2011) but used a lookup table which adds more to algorithm complexity. At average case, the number of digit 1 in the binary of k is half of its length l. Finally, NAF-Block Recoding Method which is using traditional NAF structure and by applying an innovative block method could manage to significantly and effectively reduce the number of iteration in traditional NAF algorithm and therefore enhance the running time of the algorithm (Brar and Kaur, 2011).

In {0, 1, 3}-NAF algorithm, if the hamming weight is h and the length of input binary is l the worst case of a binary expansion is when $h = l$. This algorithm has high hamming weight at worst case. In order to recode a binary input, this algorithm use a look up table which has conditions and special cases (Table 2.10). This conditions must be checked towards computation of the output. The look up with this conditions loads the algorithm complexity. This complexity defines the running time require to recode a binary input (Md Yasin, 2011). A relatively acceptable recoding algorithm is performance independent from the number of hamming weight, has fewer algorithm complexity, faster running time comparison with other algorithms.

1.5 Research Objective

The main objective of this research is to improve the {0, 1, 3}-NAF algorithm in terms of algorithm complexity and running time. These objectives can be achieved by designing a new {0, 1, 3}-NAF Block-Method algorithm which recodes binary bits in a real time operation. In particular, the sub objectives of this thesis are:

1. To propose a new technique to reduce the complexity of {0, 1, 3}- NAF recoding algorithm by implementing a new fix look-up table

2. To propose a new algorithm to speed up the running time for {0, 1, 3}- NAF recoding by applying Blocking method

1.6 Scope of the Research

The proposed recoding algorithm can be used for elliptic curve cryptosystem over binary field or prime field. Area of improvements particularly going to improve the scalar recoding technique at the scalar arithmetic level. The domain of this research is {0, 1, 3}-NAF base and the property of the base algorithm will be adopted in the new scalar algorithm. Thus, the performance comparison will be tested based on the two algorithms namely:

- {0, 1, 3}-NAF (Md Yasin, 2011) as base algorithm
- Proposed {0, 1, 3}-NAF Block method algorithm

This test will be carried out on a same machine. The algorithm efficiency (Big-*O* comparison) will be performed between base and proposed algorithm. To validate the proposed algorithm the performance time (μs) comparison will be performed between the two algorithms mentioned above. This comparison will help to evaluate the proposed method and the previous work.

1.7 Significant of the Research

This research intends to enhance the scalar arithmetic level by designing and analysing an inexpensive scalar recoding algorithm in an effort to maintain the minimum hamming weight of the {0, 1, 3}-NAF scalar representation. This

Joye, M. (2014, June 3) Exponentiation method resistant against side-channel and safe-error attacks. Google Patents.

Joye, M. and Yen, S.-M. (2000) Optimal left-to-right binary signed-digit recoding, *IEEE Transactions on Computers*, 49 (7), pp. 740–748.

Katti, R. (2002) Speeding up elliptic cryptosystems using a new signed binary representation for integers, in: *Digital System Design, 2002. Proceedings. Euromicro Symposium on*. IEEE, pp. 380–384.

Key Agreement and Key Transport Using Elliptic Curve Cryptography (1998) *X9.63 Public Key Cryptography for the Financial Services Industry:*. American National Standards Institute Std.

Khabbazian, M. (2004) Software Elliptic Curve Cryptography.

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

Klavžar, S., Milutinović, U. and Petr, C. (2007) Stern polynomials, *Advances in Applied Mathematics*, 39 (1), pp. 86–95.

Koblitz, N. (1987) Elliptic curve cryptosystems, *Mathematics of Computation*, 48 (177), pp. 203–209.

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 & Technology*, 9 (1).

Kristin Lauter (2004) The advantages of elliptic curve cryptography for wireless security, *IEEE Wireless Communications*, pp. 63.

Kumar, S. (2006) *Elliptic Curve Cryptography For Constrained Devices*. Rurh-University Bochum.

Li, M. and Miri, A. (2011) 1 Analysis of the Hamming Weight of the Extended wmbNAF.

Lochter, M. and Merkle, J. (2010) *Elliptic curve cryptography (ECC) brainpool standard curves and curve generation*. RFC 5639, March.

López, J. and Dahab, R. (1999) Fast multiplication on elliptic curves over GF (2m) without precomputation, in: *Cryptographic Hardware and Embedded Systems*. Springer, pp. 316–327.

Lvov, A., Lastras-Montaño, L. a., Trager, B., Paruthi, V., Shadowen, R. and El-Zein, A. (2014) Verification of Galois field based circuits by formal

Wang, B., Zhang, H. and Wang, Y. (2007) An efficient elliptic curves scalar multiplication for wireless network, in: *Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on*. IEEE, pp. 131–134.

Wang, B., Zhang, H., Wang, Z. and Wang, Y. (2007) Speeding Up Scalar Multiplication Using a New Signed Binary Representation for Integers, in: Sebe, N., Liu, Y., Zhuang, Y., and Huang, T. (eds.) *Multimedia Content Analysis and Mining SE - 35*. Springer Berlin Heidelberg,4577, pp. 277–285.

Wu, K., Li, D., Li, H., Chen, T. and Yu, F. (2009) Partitioned Computation to Accelerate Scalar Multiplication for Elliptic Curve Cryptosystems, in: *Parallel and Distributed Systems (ICPADS), 2009 15th International Conference on*. IEEE, pp. 551–555.