UNIVERSITI PUTRA MALAYSIA

ON THE IMPROVEMENT OF ADDITION CHAIN IN APPLICATIONS TO ELLIPTIC CURVE CRYPTOSYSTEM

MOHAMAD AFENDEE MOHAMED

IPM 2011 9

ON THE IMPROVEMENT OF ADDITION CHAIN IN APPLICATIONS TO ELLIPTIC CURVE CRYPTOSYSTEM

By

MOHAMAD AFENDEE MOHAMED

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

November 2011

DEDICATION

My

MADRE and *PADRE* Whom without there'll be no I

FAMILIA Whom for I have my blood flowing

MUJER Whom with I spend my ups and downs

NICKO and *NICKY* Whom with I grew my childhood

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

ON THE IMPROVEMENT OF ADDITION CHAIN IN APPLICATIONS TO ELLIPTIC CURVE CRYPTOSYSTEM

By

MOHAMAD AFENDEE MOHAMED

November 2011

Chair: Mohamad Rushdan Md Said, PhD

Faculty: Institute for Mathematical Research

A hard problem most of the time can be broken into a sequence of simple tasks from which a solution to the original problem is obtainable. Originally, elliptic curve cryptography is based on a non-singular algebraic curve of genus 1. The process of encrypting message involves modular operation of huge integer n acting on points on elliptic curve. This operation namely scalar multiplication is formularized as $Q = nP$. By restricting to only addition and doubling operations of two previous terms, it can be transformed into an equivalent iteration of $Q = (2 \ldots (2(2(P) + b_{r-1}P) + b_{r-2}P) + \ldots) + b_0P)$. The resulting ascending sequence is called an addition chain. Finding an optimal chain was proven to be an NP-complete problem. Notwithstanding, this gives way to the emergence of many heuristics methods offering near optimal solution. All in all, the study of efficient point arithmetic on elliptic curves can be reduced to the study of optimizing an addition chain.

This thesis centers around an investigation into a new method to improve scalar multiplication operation. Ultimately, the objective is to minimize the execution time of EC point arithmetic. One of the ways to achieve this is through shorter addition chain. The proposed method will be developed from scratch, and are subjected to some theoretical analysis. For the purpose of empirical test, some parameters are defined in the course to validating the findings.

Existing methods exploit the binary(m-ary) representation of an integer n, whilst the new method to be proposed opens up a new window of research into the problem. An integer n is decomposed into its prime factor $p_1^{e_1}p_2^{e_2}\dots p_s^{e_s}$. A classical one-layered approach is transformed into a two-layered approach. Efficiency can be improved at prime p_i layer, prime power $p_i^{e_i}$ layer and the combination of prime power layer that make up an n.

Initially, a Decomposition Method (DM) is developed based on prime power factorization of an integer n. Each factor p_i is assigned a unique rule from which an addition chain will be generated. An e_i multiple of each rule p_i generates an addition chain for $p_i^{e_i}$ of which be further combined altogether to build up n. Mathematical analysis shows that the chain generated by this method is confined to the similar boundary as that of an optimal chain studied by A. Brauer. Experiment shows a significant advantage over existing methods under appropriate working conditions. An improved version, Signed Decomposition Method (SDM) introduces a subtraction operation into the sequence to generate an addition subtraction chain. P. Erdos stated that addition subtraction chain is always at most as lengthy as an addition chain. It follows that SDM

outperforms its predecessor by 8 percents. Moreover, the generated chains are shown to outclass existing methods with significant improvement.

Additionally, we developed a Composition Method (CM) which bears the idea of computing addition chain directly from the respective rule for n. Unlike decomposition based methods, CM brings back the approach to one-layered with most of its properties are inherited from DM at prime layer. An improved version called Signed Composition Method (SCM) is also proposed as an implication of introducing a subtraction operation into CM. The generated chain by SCM has recorded an improvement of 10 percent over its predecessor. Furthermore, SCM has shown an advantage over existing methods for selected integers.

Earlier comparison between DM and CM favours DM for most n. However, experimental result for SDM against SCM shows that for small integers SDM is in favour over SCM, but as n grows, SCM gradually start to outperform SDM.

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

TENTANG PENAMBAHBAIKAN RANTAIAN PENAMBAHAN DALAM APLIKASI KRIPTOGRAFI KELUK ELIPTIK

Oleh

MOHAMAD AFENDEE MOHAMED

November 2011

Pengerusi: Mohamad Rushdan Md Said, PhD

Fakulti: Institut Penyelidikan Matematik

Kebiasaanya, sesuatu permasalahan yang genting dapat dijelma menjadi satu siri permasalahan yang sederhana kesukarannya di mana penyelesaian kepada masalah asal mudah didapati. Pada awalnya, kriptografi keluk eliptik didasarkan pada keluk aljabar tak-tunggal dengan kerabat 1. Proses pengkriptanan mesej melibatkan operasi nombor bulat besar modulo n yang bertindak ke atas titik-titik di atas keluk eliptik. Operasi yang dinamakan hasil darab skala ini boleh dirumuskan sebagai $Q = nP$. Dengan membataskan operasi hanya kepada hasil tambah dan ganda-dua oleh dua sebutan terdahulu, ianya boleh ditransformasikan menjadi iterasi setara $Q = (2 \ldots (2(2(P) + b_{r-1}P) + b_{r-2}P) + \ldots) + b_0P)$. Turutan menaik yang dihasilkan dikenali sebagai rantaian tambahan. Menemukan sesuatu rantai optimum telah terbukti menjadi permasalahan NP-lengkap. Perihal ini memberi ruang kepada kemunculan kaedah-kaedah heuristik yang menyediakan penyelesaian hampir optimum. Dengan

ini, kajian tentang aritmetik titik yang cekap pada keluk eliptik boleh dipermudahkan menjadi kajian cara pengoptimuman rantaian tambahan.

Tesis ini berkisar tentang penyelidikan suatu kaedah baru untuk mempercekapkan hasil darab skala. Ianya bertujuan untuk meningkatkan kelajuan pelaksanaan aritmetik titik EC. Hal ini boleh dicapai melalui pemendekan rantaian tambahan. Kaedah baru ini akan dibangunkan dari awal, dan dianalisis secara matematik. Untuk tujuan ujian makmal, beberapa pembolehubah akan digunakan untuk mengesahkan penemuan-penemuan ini.

Kaedah-kaedah sedia ada mengeksploitasi perwakilan dedua(de-m) untuk sesuatu nombor bulat n, sementara kaedah baru yang akan dicadangkan pula membuka lembaran baru untuk mengkaji permasalahan ini. Nombor bulat n dileraikan kepada hasil darab unsur perdana berbentuk $p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$. Pendekatan klasik satu-lapisan digubah menjadi pendekatan dua-lapisan. Kecekapan boleh dipertingkatkan di lapisan perdana p_i, lapisan kuasa perdana $p_i^{e_i}$ dan juga lapisan penggabungan sesama kuasa perdana dalam membentuk sesuatu n.

Pada awalnya, Kaedah Terurai (DM) telah dibangunkan berasaskan kepada peleraian kuasa perdana dari sesuatu nombor bulat n. Setiap perdana p_i, diberikan satu peraturan yang unik bagi menghasilkan rantaian tambahan. Suatu e_i penggandaan setiap peraturan p_i menghasilkan rantaian tambahan untuk $p_i^{e_i}$ yang jika digabungkan sesama sendiri akan menghasilkan n. Analisis bermatematik menunjukkan bahawa rantaian yang dihasilkan oleh kaedah ini terbatas pada lingkungan rantai optimum yang dikaji oleh A. Brauer. Ujian menunjukkan penambahbaikan yang besar telah terhasil melalui kaedah ini

berbanding dengan kaedah-kaedah yang terdahulu. Suatu versi yang lebih baik dinamakan Kaedah Terurai Bertanda (SDM), memperkenalkan operasi pengurangan ke dalam turutan bagi menghasilkan rantaian tambahan kurangan. P. Erdos menyatakan bahawa paling panjang rantaian tambahan kurangan adalah sepanjang rantaian tambahan. Hasilnya, SDM berjaya menambahbaik DM sebanyak 8 peratus. Lebih lagi, ia berjaya mengatasi kebolehan kaedah-kaedah yang sebelumnya dengan penambahbaikan yang besar dan sejajar.

Sebagai tambahan, kami telah bangunkan Kaedah Komposisi (CM) yang berasaskan pengiraan rantaian tambahan secara langsung dari peraturan bagi n. Berbeza dari kaedah penguraian, CM kembali kepada pendekatan satu lapisan dengan kebanyakan sifatnya diwarisi dari DM pada lapisan perdana. Suatu versi penambahbaikan yang dinamakan Kaedah Komposisi Bertanda (SCM) juga dicadangkan sebagai implikasi memperkenalkan operasi pengurangan ke dalam CM. Rantaian yang dihasilkan oleh SCM telah mencatatkan peningkatan sebanyak 10 peratus berbanding dengan CM. Tambahan pula, SCM telah menunjukkan kelebihan berbanding kaedah sedia ada bagi kebanyakan n.

Perbandingan awal antara DM dan CM memihak ke arah DM untuk semua n. Walau bagaimanapun, uji kaji antara SDM dan SCM menunjukkan bahawa untuk n yang kecil, SDM adalah lebih baik dari SCM, tetapi untuk n yang besar, SCM sebaliknya mengatasi SDM.

ACKNOWLEDGEMENTS

This thesis describes the months of research works I conducted during my PhD candidature at INSPEM, Universiti Putra Malaysia. The studies centered on elliptic curve cryptography. This thesis shows the result of contribution of many people whom expressed their ideas, experiences, knowledge and competence and like. For this reason, here is my short but sole and sincere appreciation.

First and foremost, all praise to the Almighty Allah for His blessings and mercifuls that enable me to learn.

I am priviledged to have known Dr. Rushdan who had offered progressive support, ingeneous critics and brilliant suggestions throughout the tenure. I am deeply indebted to Prof. Kamel for his invaluable insights and thorough inductiveness on theoretical foundation of my studies. I am grateful to Dr. Zuriati for her encouragement and continous support from the first day of my PhD.

My sincere appreciation to Prof. Kamel for his lectures on number theory and algebraic number theory and for being with so much patient with my overtimely manner questions, Dr Isamiddin for his lectures on abstract algebra and for being able to answer if not all, most of my non-stopped questions, and Dr. Ali for his lectures on computational algorithm, of which altogether, they have had (almost) completed the foundation I need to conduct this research.

My special thanks to INSPEM secretaries for the documentation and administrative issues, anonymous reviewers for which have contributed to the improvement of the quality of my articles, thesis examiners for their reviews, constructive feedbacks and corrections which have put up my thesis for the better.

Last but never least, my everything, my mother for her unlimited love, my wife and my family for whom I am inspired to do this study.

I certify that a Thesis Examination Committee has met on 15 November 2011 to conduct the final examination of Mohamad Afendee Mohamed on his thesis entitled "On the Improvement of Addition Chain in Applications to Elliptic Curve Cryptosystem" 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 Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Hishamuddin Zainuddin, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Azmi Jaafar, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Siti Hasana Sapar, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

Raphael Phan, PhD
Lecturer
Loughborough University
England
(External Examiner)

SEOW HENG FONG, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 20 December 2011

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

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

Kamel Ariffin Mohd Atan, PhD
Professor
Faculty of Science
Universiti Putra Malaysia
(Member)

Zuriati Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

BUJANG KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

MOHAMAD AFENDEE MOHAMED

Date: 15 November 2011

TABLE OF CONTENTS