UNIVERSITI PUTRA MALAYSIA

MULTI-BASE NUMBER REPRESENTATION IN APPLICATION TO SCALAR MULTIPLICATION AND PAIRING COMPUTATION

ABDULWAHED MOHAMMED ISMAIL

IPM 2011 18

MULTI-BASE NUMBER REPRESENTATION IN APPLICATION TO SCALAR MULTIPLICATION AND PAIRING COMPUTATION

By

ABDULWAHED MOHAMMED ISMAIL

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

May 2011

Dedication

Specially Dedicated to

My Parents,

My wife, Seween

And

My son Omar, My Daughters, Sara, Mariam and Sana

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

MULTI-BASE NUMBER REPRESENTATION IN APPLICATION TO SCALAR MULTIPLICATION AND PAIRING COMPUTATION

By

ABDULWAHED M. ISMAIL

May 2011

Chairman: Assoc. Prof. Mohamad Rushdan Md Said, PhD

Institute: Institute for Mathematical Research (INSPEM)

Elliptic curves scalar multiplication over finite fields has become a highly active research area. The efficiency of elliptic curves scalar multiplication is about keeping the memory and running time to be as low as possible. Providing new methods using chains beyond the binary chain will increase the efficiency and speed of elliptic based curve cryptosystems.

In this work, an extension of Greedy algorithm called xGreedy, is proposed. It finds the best approximated powers of each base to be used to convert large integers to new addition chains.

Then multi-bases number representation is applied to produce new elliptic curve single-scalar multiplication algorithm. Multi-base chains are provided with and without doubling operation. Due to the efficiency of point halving and its low costs,

for ordinary curves defined over binary finite fields, the results show fewer arithmetic operations.

The multi-bases number representation is also applied to construct another new elliptic curve joint-scalar multiplication algorithm, called the joint-multi base algorithm. This method computes two scalar multiplications simultaneously using multi bases in the chain. The joint-scalar is important in applications related to digital signature verification, such as elliptic curve digital signature algorithm and ElGamal signature scheme. The method is evaluated over different coordinate systems. The results show clear improvement compared to some previous methods proposed for the same purpose.

The efficiency of pairing-based cryptosystems depends on the elliptic curves scalar multiplication efficiency. Miller's algorithm for computing the Tate pairing, originally used the binary chains with corresponding point doubling operation in evaluating the rational function.

Multi-bases number representation is used to construct new versions of Miller's algorithm. These algorithms are formulated for computing Tate and ate pairing. The theoretical calculations and analyses are focused on the Tate pairing. The results show a speeding up. All the above developments are aimed at reducing the running cost of the pairing computation in pairing-based cryptosystems.

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

PERWAKILAN NOMBOR PELBAGAI ASAS DALAM PENGGUNAAN PENDARABAN SKALAR DAN PENGIRAAN PERPASANGAN

Oleh

ABDULWAHED M. ISMAIL

Mei 2011

Pengerusi: Assoc. Prof. Mohamad Rushdan Md Said, PhD

Institut : Institut Penyelidikan Matematik

Pendaraban skalar lengkung eliptik ke atas medan terhingga telah menjadi bidang penyelidikan yang sangat aktif. Kecekapan pendaraban skalar lengkung eliptik bertujuan menetapkan memori dan masa larian berada pada tahap serendah mungkin. Menyediakan kaedah baru menggunakan rantaian menjangkaui rantaian binari akan meningkatkan kecekapan dan kelajuan kriptografi berasaskan lengkung eliptik.

Dalam karya ini, satu perluasan dari algoritma Greedy disebut xGreedy, dicadangkan. Ia mencari penghampiran kuasa terbaik bagi setiap asas untuk digunakan bagi menukar integer besar kepada suatu rantai penambahan.

Seterusnya, perwakilan nombor multi-asas diterapkan untuk menghasilkan algoritma pendaraban skalar tunggal lengkung eliptik. Rantaian multi-asas disediakan dengan dan tanpa operasi ganda dua. Kerana kecekapan kaedah pengurangan separuh titik

dengan kos yang rendah, untuk lengkung biasa ditakrifkan pada medan binari terhingga, keputusan menunjukkan kurang operasi aritmetik.

Perwakilan nombor multi-asas juga digunakan untuk membina algoritma pendaraban skalar-bercantum lengkung eliptik baru yang dinamakan algoritma multi-asas-bercantum. Kaedah ini mengira dua pendaraban scalar secara serentak menggunakan multi-asas dalam rantaian. Skalar-bercantum adalah penting dalam aplikasi yang berkaitan dengan pengesahan tanda tangan digital, seperti algoritma tanda tangan digital lengkung eliptik dan skema tanda tangan ElGamal. Kaedah ini dinilai melalui sistem koordinat yang berbeza. Keputusan kajian menunjukkan peningkatan yang jelas berbanding dengan beberapa kaedah yang sebelumnya yang dicadangkan untuk tujuan yang sama.

Kecekapan sistem kriptografi berasaskan perpasangan bergantung pada kecekapan pendaraban skalar lengkung eliptik. Algoritma Miller untuk mengira perpasangan Tate pada awalnya menggunakan rantaian binari dengan operasi ganda dua yang sepadan dalam menilai fungsi nisbah.

Perwakilan nombor multi-asas digunakan untuk membina versi baru dari algoritma Miller. Algoritma ini diformulasikan untuk menghitung perpasangan Tate dan Ate. Perhitungan teori dan analisis difokuskan pada perpasangan Tate. Keputusan menunjukkan peningkatan kepada kelajuan. Semua perkembangan tersebut di atas, bertujuan untuk mengurangkan kos menjalankan pengiraan perpasangan dalam kriptosistem berasaskan perpasangan.

ACKNOWLEDGEMENTS

First of all, praise is for Allah Subhanahu Wa Taala for giving me the strength, guidance and patience to complete this thesis. May blessing and peace be upon Prophet Mohamed Sallalahu Alaihi Wasallam, who was sent as a mercy to the world. I am particularly grateful to Assoc. Prof. Dr. Mohamad Rushdan Md Said, chairman of the supervisory committee, for his excellent supervision, invaluable guidance, helpful discussions and continuous encouragement.

I am grateful for having the opportunity to work under his supervision. His invaluable assistance and comment in the preparation and completion of this thesis is also highly appreciated. I would like to thank the members of my supervisory committee, Prof. Dato Kamel Ariffin Mohd Atan, Dr. Isamiddin S. Rakhimov and Dr. Ramlan Mahmod, for their valuable discussions, comments and helps. I also wish to express my thanks to my close friends Dr. Hasan Eltayeb Gadain and Mustafa Munjit and all other friends and colleagues for their support during my study in University Putra Malaysia.

My deepest gratitude and love to my parents, brothers and all of my relatives, for their supports, encouragements, and prayers for my success.

Last but not least, I am especially grateful to my beloved wife, Seween Ali for her patience, love, and support, to my beloved son Omar, beloved daughters Sara, Mariam and Sana. My special thank to all of them for their patience during my study.

I certify that a Thesis Examination committee has met on 27th May 2011 to conduct the final examination of Abdulwahed M. Ismail on his thesis entitled "Multi-Base Number Representation in Application to Scalar Multiplication and Pairing Computation" in accordance with Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P. U. (A) 106] 15 March 1998. The committee recommends that the student be awarded the degree of Doctor of Philosophy.

Members of Thesis Examination Committee were as follows:

Mohd Rizam Abu Bakar, PhD
Associate Professor
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Adem Kilicman, PhD
Professor
Faculty of Science
Universiti Putra Malaysia
(Internal Examiner)

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

Fangguo Zhang, PhD
Professor
School of Information Science and Technology
San Yat-Sen University
Guangzhou, P. R. China
(External Examiner)

NORIFAH OMAR, PhD
Associate Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

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 the supervisory committee were as follows:

Mohamad Rushdan Md Said, PhD
Associate Professor
Institute For Mathematical Research (INSPEM)
Universiti Putra Malaysia
(Chairman)

Kamel Ariffin Mohd Atan, PhD
Professor
Institute For Mathematical Research (INSPEM)
Universiti Putra Malaysia
(Member)

Isamiddin S. Rakhimov, PhD
Associate Professor
Institute For Mathematical Research (INSPEM)
Universiti Putra Malaysia
(Member)

Ramlan Mahmod, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

HASANAH MOHD GHAZALI, PhD
Professor and Dean
School of Graduate Studies
University 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.

_____

ABDULWAHED M. ISMAIL

Date: 27th May 2011

TABLE OF CONTENTS