



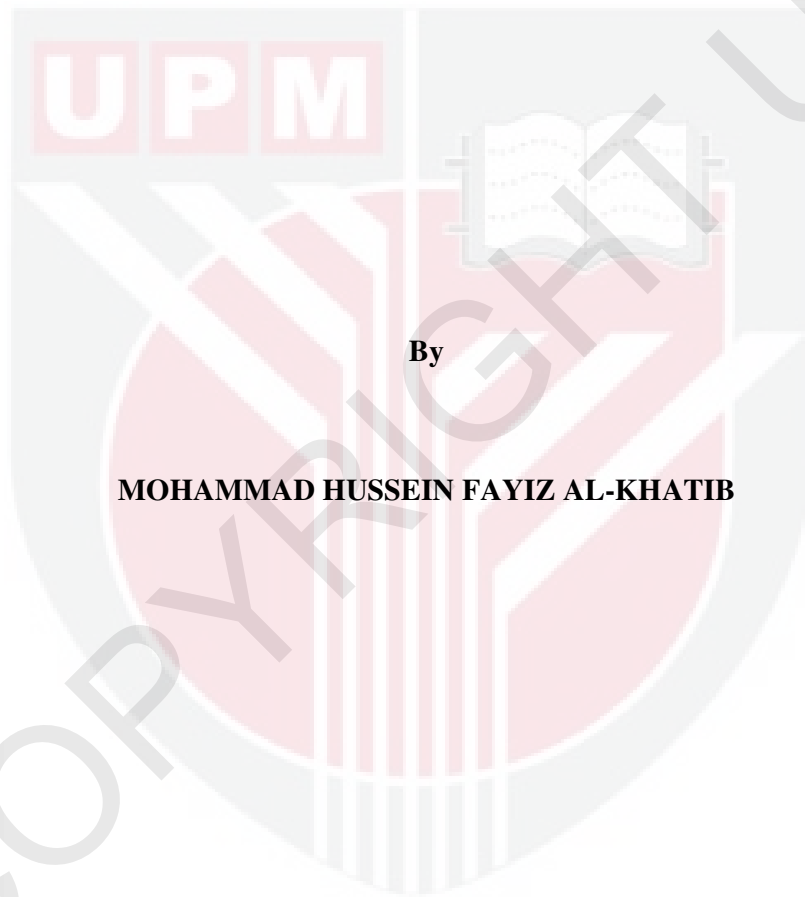
UNIVERSITI PUTRA MALAYSIA

***DESIGN AND PERFORMANCE EVALUATION OF PARALLEL ELLIPTIC
CURVE CRYPTOSYSTEM WITH $GF(P)$ PROJECTIVE COORDINATES***

MOHAMMAD HUSSEIN FAYIZ AL-KHATIB

FSKTM 2012 25

**DESIGN AND PERFORMANCE EVALUATION OF PARALLEL ELLIPTIC
CURVE CRYPTOSYSTEM WITH GF(P) PROJECTIVE COORDINATES**



By

MOHAMMAD HUSSEIN FAYIZ AL-KHATIB

**Thesis submitted to the School of Graduate Studies, Universiti Putra Malaysia,
in fulfillment of the Requirements for the Degree of Doctor of Philosophy
July 2012**

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

DESIGN AND PERFORMANCE EVALUATION OF PARALLEL ELLIPTIC CURVE CRYPTOSYSTEM WITH GF(P) PROJECTIVE COORDINATES

By

MOHAMMAD HUSSEIN FAYIZ AL-KHATIB

July 2012

Chairman: Associate Prof. Azmi Jaafar, PhD

Faculty: Computer Science and Information Technology

Elliptic Curves Cryptosystem (ECC) has been introduced as a secure and efficient public key algorithm. A number of elliptic curves representations have been presented, such as Standard (Weierstrass), Edwards, Binary Edwards, Montgomery curves, and others. ECC's computations suffer the long time inversion operation when applied using the usual affine coordinates, the use of serial design also increases the time delay, which affects the performance of ECC. The efficient selection of appropriate coordinates system to be applied with particular curve is one of the main concerns when designing efficient and high-speed ECC architecture. Moreover, other factors that play a crucial role in designing efficient ECC for different applications have not been intensively addressed in the majority of present ECC designs. These factors include area, system utilization, resources consumption,

area*time (AT), and area*time² (AT²) cost factors. The variation in elliptic curves and security applications in recent years, calls for finding several design solutions (choices) of ECC that fit the different security applications according to the requirements of particular application and the available resources. It is worth mentioning that relatively few research works were conducted on the prime field (GF (p)).

The approach adopted in this thesis uses several projective coordinates to apply ECC computations over GF (p), in order to eliminate inversion operation. In addition to the current projective coordinates, projection form $(X/Z^2, Y/Z^2)$ was proposed to be used for Edwards ECC. To improve performance even further, this work proposed using parallel hardware designs by utilizing the inherent parallelism in ECC computations.

Our proposed designs were supported by mathematical analytical study and solutions for different ECCs presented. The proposed designs were also implemented using VHDL, and then the Xilinx tool was used to synthesize the designs. A number of comparisons were conducted to highlight enhancements achieved using presented ECC designs.

The designs proposed improved the performance of the Binary Edwards ECC considerably. The best performance level was achieved using homogeneous coordinates. This projection also showed the highest performance for both Montgomery and Standard curves when applied using four and five parallel multipliers (PM) respectively. Furthermore, the performance of Edwards ECC using projection $(X/Z^2, Y/Z^2)$ overcame other known projective coordinates systems.

This thesis proposed several design solutions for the aforementioned curves by varying the degree of parallelism for ECC designs. The proposed designs provided an attractive trade-off between mentioned factors, which improved these factors. Furthermore, this research determined the most efficient coordinates to be applied with particular parallelization level for ECC. Such findings and others presented in this work lead to the building of efficient ECCs that satisfies different applications.



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

**REKAAN DAN PENILAIAN PRESTASI BAGI SISTEMKRIPTO
LENGKUNGAN ELIPTIK SELARI DENGAN KOORDINAT UNJURAN
GF(P)**

Oleh
MOHAMMAD HUSSEIN FAYIZ AL-KHATIB

Julai 2012

Pengerusi: Prof. Madya Azmi Jaafar, PhD

Fakulti: Sains Komputer dan Teknologi Maklumat

Sistemkripto Lengkungan Eliptik (ECC) telah diperkenalkan sebagai satu algoritma kunci awam yang selamat dan efisien. Beberapa perwakilan lengkungan eliptik telah diketengahkan, seperti, Lengkungan Standard (Weierstrass), Edwards, Binary Edwards, Montgomery dan sebagainya. Pengkomputan ECC memakan masa yang lama bagi operasi sonsangan apabila menggunakan koordinat “*affine*”, penggunaan reka bentuk bersiri juga membuatnya jadi lambat, yang memberi kesan terhadap prestasi ECC. Pemilihan sistem koordinat yang berkesan bagi digunakan dengan lengkungan tertentu adalah isu utama apabila mereka bentuk seni bina ECC yang efisien dan laju. Tambahan lagi, faktor lain yang memainkan peranan yang penting dalam mereka bentuk ECC yang efisien bagi penggunaan yang berlainan tidak difikirkan secara intensif dalam kebanyakan reka bentuk ECC sedia ada. Faktor-faktor tersebut ialah luas, penggunaan sistem, penggunaan-sumber, luas*masa(AT) dan luas*masa² (AT²). Kepelbagaian lengkungan eliptik dan aplikasi keselamatan dalam beberapa tahun kebelakangan ini, mengundang penerokaan reka bentuk ECC

yang boleh menepati pelbagai aplikasi keselamatan, berpadanan dengan keperluan aplikasi yang berkenaan dan sumber tersedia. Adalah berbaloi untuk menyatakan bahawa secara relatifnya amat sedikit penyelidikan dilaksanakan ke atas medan perdana ($GF(p)$).

Pendekatan dalam tesis ini ialah menggunakan beberapa koordinat unjuran bagi mengaplikasikan ECC ke atas medan $GF(p)$, untuk menghapuskan operasi sonsangan. Sebagai tambahan kepada koordinat unjuran semasa, bentuk unjuran $(X/Z^2, Y/Z^2)$ dicadangkan untuk digunakan bagi Lengkungan Eliptik Edward. Bagi mempertingkatkan prestasi seterusnya, tesis ini mencadangkan rekabentuk perkakasan selari dengan menggunakan keselarian yang sedia wujud dalam pengkomputan ECC.

Rekabentuk yang dicadangkan disokong dengan kajian analitik dan penyelesaian bagi beberapa ECC dipersembahkan. Rekabentuk yang dicadangkan juga diimplimentasikan menggunakan VHDL, dan kemudian aplikasi Xilinx digunakan untuk mensintesis rekabentuk tersebut. Beberapa perbandingan dilaksanakan untuk member nilai tambah kepada rekebrntuk ECC yang dipersembahkan.

Reka bentuk yang dicadangkan menambahbaik prestasi ECC Binary Edwards sekadarnya. Prestasi terbaik dicapai dengan menggunakan kordinat homogen. Unjuran ini menunjukkan prestasi tertinggi bagi kedua-dua lengkungan Montgomery dan Standard apabila masing-masing menggunakan empat dan lima pekali selari (PM). Tambahan pula, prestasi ECC Edwards menggunakan unjuran $(X/Z^2, Y/Z^2)$ mengatasi sistem koordinat sedia ada.

Tesis ini mencadangkan beberapa penyelesaian reka bentuk bagi lengkungan tersebut di atas dengan mempelbagaikan darjah selari rekabentuk ECC. Reka bentuk yang

dicadangkan menyediakan timbal-balik yang menarik diantara faktor-faktor tersebut, iaitu yang menambahbaik faktor-faktor tersebut. Tambahan pula, penyelidikan ini telah menentukan koordinat yang paling efisien untuk diaplikasikan kepada aras keselarian ECC yang tertentu. Penemuan-penemuan ini dan lain-lain yang dicadangkan dalam tesis ini membuka halatuju ke arah pembinaan ECC yang efisien yang memenuhi pelbagai aplikasi.



DEDICATION

This thesis is dedicated to my parents who have never failed in their support of my endeavors, and who taught me the very important lesson that even the most challenging task can be accomplished if it is done one step at a time.



ACKNOWLEDGEMENTS

I am grateful to my supervisor, Assoc. Prof. Azmi Jaafar for his reviews, help, guidance and encouragement in conducting this research and producing the papers that formed the basis for this thesis. I also thank the supervisory committee members, Assoc. Prof. Mohammad Rushdan, and Dr. Zutiati Ahmad for their assistance and direction in the completion of this thesis.

An efficient research environment, infrastructure, and facilities were required to conduct this research. In this regard I am thankful to the Faculty of Computer Science and Information Technology of Universiti Putra Malaysia (UPM).

Finally, I owe a debt of gratitude for the best parts of my life to my loving parents, and my wonderful family, without whose patience and understanding this project could not have been done.



APPROVAL

I certify that a Thesis Examination Committee has met on 20/7/2012 to conduct the final examination of Mohammad Hussein Fayiz Al-khatib on his thesis entitled “Design and Performance Evaluation of Parallel Elliptic Curve Cryptosystem with GF(p) Projective Coordinates” in accordance with the Universities and University Colleges Act 1971 and the Constitution of 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:

Dr. Hamidah Ibrahim, PhD

Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Chairman)

Dr. Muhammad Rezal Kamel Ariffin, PhD

Faculty of Science

Universiti Putra Malaysia

(Internal Examiner)

Dr. Khairulmizam Bin Samsudin, PhD

Faculty of Engineering

Universiti Putra Malaysia

(Internal Examiner)

Dr. Riyadh Al-shalabi, PhD

Professor

Faculty of Computer Sciences and Informatics

Amman Arab University

Jordan

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

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

Azmi Jaafar, PhD

Associate Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Chairman)

Zuriati Zukarnain Ahmad, PhD

Associate Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Member)

Mohammad Rushdan, PhD

Associate Professor

Faculty of Science

Universiti Putra Malaysia

(Member)

BUJANG BIB KIM HUAT, PhD

Professor and Dean

School of Graduate Studies

Universiti Putra Malaysia

Date: 27 September 2012

DECLARATION

I declare that the thesis is my original work except from 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.

MOHAMMAD HUSSEIN FAYIZ AL-KHATIB

Date: 20 July 2012

TABLE OF CONTENTS

	Page
ABSTRACT	ii
ABSTRAK	v
ACKNOWLEDGEMENTS	ix
APPROVALS	x
ABBREVIATIONS	xvi
CHAPTER	
1. INTRODUCTION	
1.1. Problem Statement	8
1.2. Research Objective	9
1.3. Thesis Motivation	10
1.4. Thesis Scope	11
1.5. Thesis Organization	12
1.6. Contributions and Publications	13
2. LITERATURE REVIEW	
2.1. Mathematical Background for Elliptic Curve Cryptography	17
2.1.1. Elliptic Curve Scalar Multiplication Algorithms	17
2.1.2. Fields Arithmetic	20
2.1.3. Elliptic Curves Arithmetic over GF (p)	20
2.1.4. Elliptic Curve Representations over GF (p)	22
2.1.5. Elliptic Curve Point Operations over GF (p)	23
2.1.6. Elliptic Curve Arithmetic over GF (2^m)	25
2.1.7. Elliptic Curve Point Operations over GF (2^m)	26
2.2. Comparison Between GF (p) and GF (2^m)	26
2.3. Fundamental Elliptic Curve on Regular and Projective Coordinates	27
2.3.1. Affine Coordinates	28
2.3.2. Projective Coordinates	30
2.4. Comparison Between Ratios of Time Cost for both Multiplication and Inversion Operations	32
2.5. Encryption and Decryption in Elliptic Curve Cryptography	34
2.6. Related Work	35
3. METHODOLOGY	44
4. Article 1: "Choices on Designing GF (p) Elliptic Curve Coprocessor Benefiting from Mapping Homogeneous	

	Curves in Parallel Multiplications"	51
	Acceptance Letter	72
5.	Article 2: "Hardware Architectures & Designs for Projective Elliptic Curves Point Addition Operation Using Variable Levels of Parallelism"	73
	Acceptance Letter	99
6.	Article 3: "Performance Evaluation of Projective Binary Edwards Elliptic Curve Computations with Parallel Architectures"	100
	Permission/Acceptance Letter	116
7.	Article 4: "On the Design of Projective Binary Edwards Elliptic Curves over GF (p) Benefiting from Mapping Elliptic Curves Computations to Variable Degree of Parallel Design"	117
	Permission/Acceptance Letter	145
8.	Article 5: "Parallel Designs for Edwards Elliptic Curves CryptoSystem Point Doubling Operation over GF (p) Using New Projective Coordinates Benefiting from Varying the Degree of Parallelism for Elliptic Curves Computation"	146
	Acceptance Letter	161
9.	Article 6: "Trade-off between Area and Speed for Projective Edwards Elliptic Curves CryptoSystem over GF (p) Using Parallel Hardware Designs and Architectures"	162
	Acceptance Letter	190
10.	Article 7: "Hardware Designs and Architectures for Projective Montgomery ECC over GF (p) Benefiting from Mapping Elliptic Curve Computations to Different Degrees of Parallelism"	191
	Acceptance Letter	221
11.	RESULTS AND CONCLUSION	222
11.1.	Simulation and Synthesizing	224
11.2.	Performance Results and Comparisons	225
	11.2.1. Binary Edwards ECC	227
	11.2.2. Edwards ECC	229
	11.2.3. Standard (Weierstrass) ECC	232
	11.2.4. Montgomery ECC	235
	11.2.5. Comparison Between Parallel and Serial Design Implementations	236
11.3.	Area Comparison Between Parallel and Serial Designs	241
11.4.	Performance Comparison with Previous Designs	245
11.5.	Comparison between Area and Time for Different Parallelization Levels for ECCs	249
11.6.	Conclusion and Future Work	253

REFERENCES	257
APPENDICES	266
A. List of Publications	266
B. The Computations of Scalar Multiplication Operations	268
BIODATA OF STUDENT	269

