
**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*time$^2$ ($AT^2$) 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 menmenuhi 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 apaila 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*masa$^2$ ($AT^2$). 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 dipersembhakan. Rekabentuk yang dicadangkan juga diimplimentasikan menggunakan VHDL, dan kemudian aplikasi Xilinx digunakan untuk mensintesiskan 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 menunjukan 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 penyelesain 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. Riyad 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**