

การคูณสเกลาร์อีลิปติกแบบเชื่อมตรงในระบบแทนจำนวนฐานสอง
แบบมีเครื่องหมายน้ำหนักต่ำสุด

นายตะวัน ฉายกลิ่น

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2551
ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

ON-LINE ELLIPTIC SCALAR MULTIPLICATION IN MINIMUM WEIGHT
SIGNED-BINARY NUMBER REPRESENTATION SYSTEM

Mr.Tawan Chaiklin

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Chulalongkorn University

Academic Year 2008

Copyright of Chulalongkorn University

511916

หัวข้อวิทยานิพนธ์

การคูณสเกลาร์อีลลิปติกแบบเชื่อมโยงตรงในระบบแทน
จำนวนฐานสองแบบมีเครื่องหมายน้ำหนักต่ำสุด

โดย

นายตะวัน ฉายกลิ่น

สาขาวิชา

วิทยาศาสตร์คอมพิวเตอร์

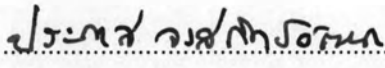
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

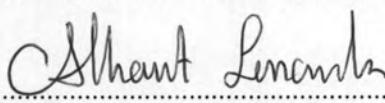
ผู้ช่วยศาสตราจารย์ ดร.อรรถสิทธิ์ สุรฤกษ์

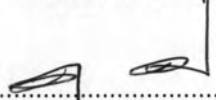
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้รับวิทยานิพนธ์ฉบับนี้
เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต



.....คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศธีรวงวงศ์)

คณะกรรมการสอบวิทยานิพนธ์


.....ประธานกรรมการ
(ศาสตราจารย์ ดร.ประภาส จงสิตย์วัฒนา)


.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ ดร.อรรถสิทธิ์ สุรฤกษ์)


.....กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.พิเชษฐ คงชัยยศ)


.....กรรมการภายนอกมหาวิทยาลัย
(ผู้ช่วยศาสตราจารย์ ดร.อานนท์ รุ่งสว่าง)

ตะวัน ฉายกลิ่น : การคูณสเกลาร์อีลิปติกแบบเชื่อมตรงในระบบแทนจำนวนฐานสองแบบมีเครื่องหมายน้ำหนักต่ำสุด (ON-LINE ELLIPTIC SCALAR MULTIPLICATION IN MINIMUM WEIGHT SIGNED-BINARY NUMBER REPRESENTATION SYSTEM) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ.ดร.อรรถสิทธิ์ สุรฤกษ์, 32 หน้า

เนื่องจากการดำเนินการหลักของวิทยาการเข้ารหัสลับด้วยเส้นโค้งอีลิปติกคือ การคำนวณค่า kP ซึ่งเรียกว่าการคูณสเกลาร์ โดยที่ค่า k คือจำนวนเฉพาะที่มีค่ามาก และ P คือจุดซึ่งอยู่บนเส้นโค้งอีลิปติก ความซับซ้อนของการคำนวณนั้นขึ้นอยู่กับค่าน้ำหนักของ k ในรูประบบจำนวนฐานสอง โดยการคำนวณนี้จะดำเนินการอย่างเป็นลำดับจากซ้ายไปขวา หรืออีกนัยหนึ่งคือจากบิตที่มีค่าความสำคัญมากที่สุดไปยังบิตที่มีค่าความสำคัญน้อยสุดด้วยวิธีการของชาเมียร์ ภายใต้ระบบจำนวนฐานสอง ดังนั้นเพื่อเป็นการเพิ่มประสิทธิภาพการคำนวณให้กับวิธีการของชาเมียร์ เราจึงได้เสนออัลกอริทึมการแปลงค่าตัวเลขฐานสองในรูปน้ำหนักต่ำสุดด้วยวิธีการเชื่อมตรง ซึ่งทำให้สามารถทำงานแบบสายต่อกับกระบวนการคูณสเกลาร์ของชาเมียร์ได้ ทำให้เวลาในการทำงานโดยรวมลดลง

ภาควิชาวิศวกรรมคอมพิวเตอร์.....
สาขาวิชา.....วิทยาศาสตร์คอมพิวเตอร์.....
ปีการศึกษา2551.....

ลายมือชื่อนิสิตตะวัน ฉายกลิ่น.....
ลายมือชื่ออาจารย์ที่ปรึกษา*Amnat Luenwih*.....

4870301221: MAJOR COMPUTER SCIENCE

KEY WORD: SCALAR MULTIPLICATION / SIGNED-BINARY NUMBER / ON-LINE ARCHITECTURE

TAWAN CHAIKLIN: ON-LINE ELLIPTIC SCALAR MULTIPLICATION IN MINIMUM WEIGHT SIGNED-BINARY NUMBER REPRESENTATION SYSTEM. THESIS PRINCIPAL ADVISOR: ASST. PROF. ATHASIT SURARERKS, Ph.D., 32 pp.

Since the main operation of elliptic curve cryptography is the computation of product kP , also known as scalar multiplication, where k is a large prime number and P is a point on the elliptic curve. The computational complexity depends on the weight of the binary expansion of k . This operation sequentially operates from left (the most significant bit) to right (the least significant bit) with Shamir's method based on binary expansions. So to extend Shamir's method, we present a minimum weight on-line binary digit conversion algorithm that allows the pipeline architecture compatible with the scalar multiplication process by Shamir's method to reduce the operation time.

Department: Computer Engineering Student's signature: *Tawan Chaiklin*
 Field of study: Computer Science Principal Advisor's signature: *Athasit Surarerk*
 Academic year: 2008

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างยิ่งจาก ผศ.ดร.อรรถสิทธิ์ สุรฤกษ์ อาจารย์ที่ปรึกษา ซึ่งเป็นผู้ให้คำปรึกษา ให้ข้อเสนอแนะที่เป็นประโยชน์อย่างยิ่งต่อการวิจัย และช่วยตรวจแก้ไขในส่วนที่บกพร่องต่างๆ จนกระทั่งบรรลุผลสำเร็จเป็นอย่างดี โดยเฉพาะอย่างยิ่งขอขอบพระคุณ ผศ.ดร.อรรถสิทธิ์ สุรฤกษ์ เป็นอย่างสูงที่ช่วยติดตามดูแลงานวิจัยอย่างใกล้ชิดมาโดยตลอด

ขอขอบพระคุณในความเอื้อเฟื้อของ ศ.ดร.ประภาส จงสถิตย์วัฒนา ประธานกรรมการ ผศ.ดร.พิษณุ คนองชัยยศ และ ผศ.ดร.อานนท์ รุ่งสว่าง กรรมการสอบวิทยานิพนธ์ ที่ได้กรุณาให้คำแนะนำในการแก้ไขวิทยานิพนธ์ให้มีคุณภาพยิ่งขึ้น และขอขอบพระคุณคณาจารย์ในภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่านที่ประสิทธิ์ประสาทความรู้อันมีค่าให้แก่ผู้วิจัย

กราบขอบพระคุณ บิดา มารดา ที่มีความเมตตา กรุณา และเป็นผู้คอยให้กำลังใจตลอดมา ขอขอบคุณ พี่ๆ เพื่อนๆ และน้องๆ ทุกคน โดยเฉพาะสมาชิกห้องปฏิบัติการ ELITE ที่ได้ให้ความช่วยเหลือและแก้ไขเอกสาร จนกระทั่งวิทยานิพนธ์สำเร็จเป็นรูปเล่ม และขอขอบคุณแรงสนับสนุนและกำลังใจทุกท่านที่ได้กล่าวนามไว้ ณ ที่นี้

สุดท้ายนี้ ผู้วิจัยหวังเป็นอย่างยิ่งว่างานวิจัยนี้จะเป็นประโยชน์ต่อผู้ที่สนใจหรือผู้ที่เกี่ยวข้องทั่วไป และหากมีข้อผิดพลาดประการใด ผู้วิจัยขออภัยมา ณ ที่นี้ด้วย

สารบัญ

| | หน้า |
|--|------|
| บทคัดย่อภาษาไทย | ง |
| บทคัดย่อภาษาอังกฤษ | จ |
| กิตติกรรมประกาศ | ฉ |
| สารบัญ | ช |
| สารบัญตาราง และอัลกอริทึม | ฅ |
| สารบัญภาพ | ญ |
| | |
| บทที่ | |
| 1 บทนำ | 1 |
| 1.1 ความเป็นมาและความสำคัญของปัญหา | 1 |
| 1.2 วัตถุประสงค์ของการวิจัย | 2 |
| 1.3 ขอบเขตของการวิจัย | 2 |
| 1.4 ขั้นตอนและวิธีดำเนินการวิจัย | 2 |
| 1.5 ประโยชน์ที่คาดว่าจะได้รับการวิจัย | 2 |
| 1.6 ผลงานที่ตีพิมพ์จากวิทยานิพนธ์ | 3 |
| | |
| 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง | 4 |
| 2.1 กลุ่มเส้นโค้งอิลลิปติกบนขอบเขตจำกัด | 4 |
| 2.2 การคูณจุดหรือสเกลาร์ | 5 |
| 2.3 การดำเนินการเลขคณิตในการคูณสเกลาร์ | 6 |
| 2.3.1 การบวกจำเพาะระหว่างจุด P และ G | 6 |
| 2.3.2 การเพิ่มทวีของจุด P | 6 |
| 2.4 ปัญหาดิสครีทลอการิทึมของเส้นโค้งอิลลิปติก | 7 |
| 2.5 วิธีการของชาเมียร์ | 7 |
| 2.6 ระบบจำนวน | 8 |
| 2.7 การแปลงแบบเชื่อมตรง | 9 |
| 2.8 การแทนฐานสองแบบมีเครื่องหมายในรูประหว่างกลาง | 10 |
| 2.9 การแลกเปลี่ยนกุญแจด้วยอีซีซี | 10 |

| บทที่ | หน้า |
|--|------|
| 3 การแปลงจำนวนให้อยู่ในรูปน้ำหนักต่ำสุดด้วยวิธีการเชื่อมตรง..... | 12 |
| 3.1 การแปลงจำนวนให้อยู่ในรูปไอเอสบีภายใต้เซตตัวเลข $\{1,0,1\}$ | 12 |
| 3.2 การแปลงจำนวนให้อยู่ในรูปน้ำหนักต่ำสุดภายใต้เซตตัวเลข $\{3,1,0,1\}$ | 14 |
| 3.3 การคูณสเกลาร์ด้วยวิธีการของซามิร์ภายใต้เซตตัวเลข $\{3,1,0,1\}$ | 19 |
| 3.4 สรุป..... | 21 |
| 4 รูปแบบทั่วไปของการแปลงให้อยู่ในรูปน้ำหนักต่ำสุดแบบเชื่อมตรง | 22 |
| 4.1 การแปลงให้อยู่ในรูปน้ำหนักต่ำสุดภายใต้ระบบจำนวนฐาน β | 22 |
| 4.2 การคูณสเกลาร์ด้วยวิธีการของซามิร์ภายใต้ระบบจำนวนฐาน β | 25 |
| 4.3 สรุป..... | 27 |
| 5 สรุปผลการวิจัยและข้อเสนอแนะ | 28 |
| 5.1 สรุปผลการวิจัย..... | 28 |
| 5.2 ข้อเสนอแนะ | 29 |
| อภิธานศัพท์ | 30 |
| รายการอ้างอิง | 31 |
| ประวัติผู้เขียนวิทยานิพนธ์ | 32 |

สารบัญตาราง และอัลกอริทึม

| ตารางที่ | หน้า |
|--|------|
| 2.1 การคำนวณ $61P$ ด้วยวิธีการของซามิรีใช้เซตตัวเลข $\{0,1\}$ | 8 |
| 2.2 ขั้นตอนการสร้างกุญแจด้วยอีซีซี | 10 |
| 3.1 การคำนวณ $61P$ ด้วยวิธีการของซามิรีใช้เซตตัวเลข $\{\bar{1},0,1\}$ | 14 |
| 3.2 ตารางสถานะของกระบวนการในอัลกอริทึมที่ 3.2 | 17 |
| 3.3 การคำนวณ $61P$ ด้วยวิธีการของซามิรีใช้เซตตัวเลข $\{3,\bar{1},0,1\}$ | 18 |
| 3.4 ตารางการเรียกใช้ตัวนำเนนการเพื่อคำนวณ $103P$ ด้วยวิธีการของซามิรี | 20 |
| 4.1 ตารางการแปลง $k = 293$ ด้วยอัลกอริทึมที่ 4.1 | 24 |
| 4.2 ตารางทั่วไปในการคูณสเกลาร์สำหรับระบบจำนวนฐาน β | 25 |
| 4.3 การคูณสเกลาร์ภายใต้ระบบจำนวนฐานสามเพื่อหา $293P$ | 26 |
| | |
| อัลกอริทึมที่ | |
| 2.1 อัลกอริทึมการเพิ่มทวีคูณ | 6 |
| 3.1 อัลกอริทึมการแปลงจำนวนเป็นไอเอสบี | 12 |
| 3.2 อัลกอริทึมการแปลงจำนวนให้อยู่ในระบบจำนวนฐานสองที่มีน้ำหนักต่ำสุด | 15 |
| 3.3 อัลกอริทึมการคูณสเกลาร์ภายใต้เซตตัวเลข $\{3,\bar{1},0,1\}$ ฐานสอง | 19 |
| 4.1 อัลกอริทึมการแปลงจำนวนให้อยู่ในระบบจำนวนฐาน β ที่มีน้ำหนักต่ำสุด | 23 |
| 4.2 อัลกอริทึมการคูณสเกลาร์ภายใต้เซตตัวเลข $\{(\bar{\beta}+1),\bar{1},0,\dots,(\beta-1)\}$ ฐาน β | 25 |

สารบัญภาพ

| ภาพที่ | หน้า |
|--|------|
| 2.1 รูปกราฟของสมการ $y^2 = x^3 - 6x - 6$ | 4 |
| 2.2 รูปกราฟของสมการ $y^2 = x^3 - x$ บนขอบเขตจำกัด F_{23} | 5 |