การคูณสเกลาร์อิลลิปติกแบบเชื่อมตรงในระบบแทนจำนวนฐานสอง แบบมีเครื่องหมายน้ำหนักต่ำสุด

นายตะวัน ฉายกลิ่น

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2551

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

หัวข้อวิทยานิพนธ์	การคูณสเกลาร์อิลลิปติกแบบเชื่อมตรงในระบบแทนจำนวนฐานสองแบบมีเครื่องหมายน้ำหนักต่ำสุด
โดย	นายตะวัน ฉายกลิ่น
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร.อรรถสิทธิ์ สุรฤกษ์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์
(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(ศาสตราจารย์ ดร.ประภาส จงสถิตย์วัฒนา)

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

.....กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.พิษณุ คนองชัยยศ)

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

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

เนื่องจากการดำเนินการหลักของวิทยาการเข้ารหัสลับด้วยเส้นโค้งอิลลิปติกคือ การคำนวณค่า kP ซึ่งเรียกว่าการคูณสเกลาร์ โดยที่ค่า k คือจำนานเฉพาะที่มีค่ามาก และ P คือจุดซึ่งอยู่บนเส้นโค้งอิลลิปติก ความซับซ้อนของการคำนวณนั้นขึ้นอยู่กับค่าน้ำหนักของ k ในรูประบบจำนวนฐานสอง โดยการคำนวณนี้จะดำเนินการอย่างเป็นลำดับจากซ้ายไปขวา หรืออีกนัยหนึ่งคือจากบิตที่มีค่าความสำคัญมากสุดไปยังบิตที่มีค่าความสำคัญน้อยสุดด้วยวิธีการของชามีร์ ภายใต้ระบบจำนวนฐานสอง ดังนั้นเพื่อเป็นการเพิ่มประสิทธิภาพการคำนวณให้กับวิธีการของชามีร์ เราจึงได้เสนออัลกอริทึมการแปลงค่าตัวเลขฐานสองในรูปน้ำหนักต่ำสุดด้วยวิธีการเชื่อมตรง ซึ่งทำให้สามารถทำงานแบบสายท่อกับกระบวนการคูณสเกลาร์ของชามีร์ได้ทำให้เวลาในการทำงานโดยรวมลดลง

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต ตะวัน ฉายกลิ่น

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่ออาจารย์ที่ปรึกษา Athasit Surarerks

ปีการศึกษา 2551

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 Surarerks
Academic year: 2008

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างดียิ่งจาก 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 กรรมการสอบวิทยานิพนธ์ที่ได้กรุณาให้คำแนะนำในการแก้ไขวิทยานิพนธ์ให้มีคุณภาพยิ่งขึ้น และขอขอบพระคุณคณาจารย์ในภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่านที่ประสิทธิ์ประสาทความรู้อันมีค่ายิ่งแก่ผู้วิจัย

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

สุดท้ายนี้ ผู้วิจัยหวังเป็นอย่างยิ่งว่างานวิจัยนี้จะเป็นประโยชน์ต่อผู้ที่สนใจหรือผู้ที่เกี่ยวข้องทั่วไป และหากมีข้อผิดพลาดประการใด ผู้วิจัยขออภัยมา ณ ที่นี้ด้วย

สารบัญ

หน้า

บทที่ หน้า

สารบัญตาราง และอัลกอริทึม

ตารางที่ หน้า

อัลกอริทึมที่

สารบัญภาพ

ภาพที่ หน้า