บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

วิทยาการเข้ารหัสลับด้วยเส้นโค้งอิลลิปติก หรืออีซีซี (elliptic curve cryptography: ECC) ซึ่งถูกคิดค้นในปี ค.ศ.1985 โดย มิลเลอร์ และ โคบลิส (Miller and Koblitz) [1-3] เป็นวิธีการหนึ่งที่มีประสิทธิมากในการเข้ารหัสข้อมูล เนื่องด้วยความซับซ้อนของรูปแบบการเข้ารหัสที่เรียกว่า ปัญหาดิสครีทลอการิทึมของเส้นโค้งอิลลิปติก หรืออีซีดีแอลพี (elliptic curve discrete logarithm problem: ECDLP) [4] ทำให้เป็นการยากในการถอดรหัสกลับ และในระดับความปลอดภัยเดียวกันเมื่อเปรียบเทียบกับวิธีการอื่นๆ อีซีซีมีขนาดของกุญแจ (key) ที่ใช้ในการเข้ารหัสเล็กกว่ามาก ทำให้ตัวดำเนินการในการเข้ารหัส (cryptographic operation) สามารถถูกเก็บลงในฮาร์ดแวร์ขนาดเล็ก มีโปรเซสการทำงานน้อยลงทำให้ประมวลผลได้รวดเร็ว นั่นหมายถึงการใช้ทรัพยากรลดน้อยลง และเกิดความร้อนต่ำ โดยการเพิ่มประสิทธิภาพการทำงานให้กับการเข้ารหัสนั้น จะต้องลดการทำงานของตัวดำเนินการ (operator) ให้มีการถูกเรียกใช้งานน้อยลง แต่ยังสามารถรักษาประสิทธิภาพการทำงานให้คงเดิม ซึ่งอาจปรับปรุงในส่วนของขั้นตอนการทำงาน ทั้งในส่วนของเป็นอัลกอริทึมการทำงานหลัก หรือในส่วนของการดำเนินการทางด้านเลขคณิต โดยพิจารณาถึงสถาปัตยกรรมทำงานที่สามารถปรับการทำงานโดยรวมให้เร็วขึ้น และสามารถทำงานไปด้วยกันในแต่ละการดำเนินการได้

อีซีซีได้ถูกในไปใช้ในหลายกระบวนการเข้ารหัสลับดังนี้ การเข้ารหัสลับ (encryption) การสร้างลายเซ็นดิจิทัล (digital signatures) และการตกลงกุญแจ (key agreement) โดยในงานวิจัยชิ้นนี้จะสนใจในส่วนของการตกลงกุญแจ ซึ่งมีการดำเนินการหลักคือการคำนวณผลิตผลของ kP โดยที่ P คือจุดบนเส้นโค้งอิลลิปติก และ k เป็นจำนวนเฉพาะ (prime number) โดยเรียกการดำเนินการดังกล่าวว่า การคูณสเกลาร์อิลลิปติก (elliptic scalar multiplication) [5] ซึ่งจะใช้วิธีการของ ชามีร์ (Shamir's method) [6] ในการดำเนินการ โดยความซับซ้อนของวิธีการนี้ขึ้นอยู่กับน้ำหนัก (weight) ซึ่งก็คือจำนวนของบิตที่ไม่ใช่ศูนย์ (non-zero bit) ของ k ที่ถูกแสดงด้วยระบบจำนวนฐานสอง (binary number system) กล่าวคือ การคูณสเกลาร์อิลลิปติกด้วยวิธีการของชามีร์ จะดำเนินการได้รวดเร็วเมื่อ การแทนรูปของ k ในระบบจำนวนฐานสองมีค่าน้ำหนักต่ำ ดังนั้นงานวิจัยชิ้นนี้จึงมุ่งเสนออัลกอริทึมการแปลงจำนวน k ให้มีค่าน้ำหนักต่ำสุด สำหรับใช้ในการคูณด้วยสเกลาร์อิลลิปติก เพื่อคำนวณผลิตผลของ kP ด้วยวิธีการของชามีร์ โดยแปลงจำนวน k ให้อยู่ในเซตตัวเลขที่สามารถให้ค่าน้ำหนักที่ต่ำสุดภายใต้ระบบจำนวนฐาน (base) และความหน่วง (delay) ที่กำหนดไว้ ซึ่งตัวดำเนินการในการคูณสเกลาร์ก็จะถูกปรับเปลี่ยนไปตามระบบจำนวนฐาน และเซตตัวเลขที่ใช้แทนรูปเช่นกัน

1.2 วัตถุประสงค์ของการวิจัย

ออกแบบอัลกอริทึมสำหรับใช้แปลงจำนวนเต็มบวก k ให้มีค่าน้ำหนักต่ำสุด สำหรับใช้ในการคูณสเกลาร์อิลลิปติกพร้อมคำนวณผลิตผลของ kP ด้วยวิธีการของชามีร์ พร้อมทั้งสร้างเครื่องแปลงสัญญาณ (transducer) ในรูปของตารางสถานะ (state table) เพื่อใช้อธิบายลำดับการแปลงจำนวน

1.3 ขอบเขตของการวิจัย

1.3.1 เสนออัลกอริทึมสำหรับใช้แปลงจำนวนเต็มบวก k ให้มีค่าน้ำหนักต่ำสุด สำหรับใช้ในการคูณสเกลาร์อิลลิปติกพร้อมคำนวณผลิตผลของ kP ด้วยวิธีการของชามีร์

1.3.2 ปรับการคูณสเกลาร์อิลลิปติกตามวิธีการของชามีร์ให้อยู่ในรูปแบบเชื่อมตรงตามอัลกอริทึมที่ได้ในข้อ 1.3.1

1.3.3 ออกแบบเครื่องแปลงสัญญาณในรูปของตารางสถานะ เพื่อใช้อธิบายลำดับการแปลงจำนวนเต็มบวก k ในระบบจำนวนฐานสองที่ให้ค่าน้ำหนักต่ำสุด

1.4 ขั้นตอนและวิธีดำเนินการวิจัย

1.4.1 ศึกษาคุณลักษณะและคุณสมบัติของกลุ่มเส้นโค้งอิลลิปติกบนขอบเขตจำกัด

1.4.2 ศึกษาและวิจัย การทำงานของวิธีการของชามีร์

1.4.3 ศึกษารูปแบบการแทนจำนวนในระบบจำนวนฐานสอง และคุณสมบัติของจำนวน

1.4.4 เสนออัลกอริทึมสำหรับใช้แปลงจำนวนเต็มบวก k ให้มีค่าน้ำหนักต่ำสุด สำหรับใช้ในการคูณสเกลาร์อิลลิปติกพร้อมคำนวณผลิตผลของ kP ด้วยวิธีการของชามีร์

1.4.5 วัดประสิทธิภาพของอัลกอริทึมด้วยการพิสูจน์

1.4.6 ปรับการคูณสเกลาร์อิลลิปติกตามวิธีการของชามีร์ให้อยู่ในรูปแบบเชื่อมตรง

1.4.7 ออกแบบเครื่องแปลงสัญญาณในรูปของตารางสถานะ เพื่อใช้อธิบายลำดับการแทนรูปของ k ในระบบจำนวนฐานสองที่ให้ค่าน้ำหนักต่ำสุด

1.4.8 ปรับปรุงและแก้ไข

1.4.9 วิเคราะห์ สรุปผล และจัดทำวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1.5.1 ได้อัลกอริทึมสำหรับใช้แปลงจำนวนเต็มบวก k ให้มีค่าน้ำหนักต่ำสุด เพื่อเพิ่มประสิทธิภาพในการคำนวณ สำหรับใช้ในการคูณสเกลาร์อิลลิปติกพร้อมคำนวณผลิตผลของ kP ด้วยวิธีการของชามีร์แบบเชื่อมตรง

1.5.2 ได้เครื่องแปลงสัญญาณในรูปของตารางสถานะสำหรับใช้อธิบายลำดับการแปลงจำนวนเต็มบวก k ในระบบจำนวนฐานสองที่ให้ค่าน้ำหนักต่ำสุด

1.6 ผลงานที่ตีพิมพ์จากวิทยานิพนธ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้รับการตีพิมพ์เป็นบทความทางวิชาการในหัวเรื่องดังต่อไปนี้

1.6.1 "On-line Elliptic Scalar Multiplication in Signed-Binary Number Representation System" โดย ตะวัน ฉายกลิ่น และอรรถสิทธิ์ สุรฤกษ์ ในงานประชุมวิชาการ 5th International Joint Conference on Computer Science and Software Engineering (JCSSE2008) ณ Felix River Kwai Resort จ.กาญจนบุรี ประเทศไทย ระหว่างวันที่ 7-9 พฤษภาคม พ.ศ.2551 (Full Paper)

1.6.2 "A Minimum Weight On-line Binary Digit Conversion Algorithm" โดย ตะวัน ฉายกลิ่น และอรรถสิทธิ์ สุรฤกษ์ ในงานประชุมวิชาการ 12th National Computer Science and Engineering Conference (NCSEC2008) ณ Long Beach Garden Hotel and Spa พัทยา จ.ชลบุรี ประเทศไทย ระหว่างวันที่ 20-21 พฤศจิกายน พ.ศ. 2551 (Full Paper)