# บทที่ 5

## สรุปผลการวิจัยและข้อเสนอแนะ

### 5.1 สรุปผลการวิจัย

ในงานวิจัยนี้ได้เสนออัลกอริทึมการแปลงจำนวนให้อยู่ในรูประบบจำนวนฐานสองที่มีน้ำหนักต่ำสุด ซึ่งดำเนินการตามอัลกอริทึมที่ 3.1 และอัลกอริทึมที่ 3.2 ตามลำดับ เพื่อส่งต่อผลลัพธ์ที่มีน้ำหนักต่ำสุดไปยังกระบวนการคูณสเกลาร์ในอัลกอริทึมที่ 3.3 ด้วยวิธีการของซามีร์ โดยจำเป็นต้องเพิ่มตัวดำเนินการใหม่อีกสองตัวคือ $-P$ และ $-3P$ เพื่อให้สามารถรองรับการคำนวณในชุดตัวเลข $\{\bar{3},\bar{1},0,1\}$ โดยกระบวนการของทุกขั้นตอนเป็นแบบเชื่อมตรงจึงสามารถรวมการทำงานเข้าด้วยกันเป็นสายท่อได้ ภายใต้ความหน่วงของการทำงานรวมเป็นสาม ทำให้สามารถเริ่มการคูณสเกลาร์ได้ทันทีเมื่อได้ค่านำออกแรกของการแปลงจำนวนให้อยู่ในรูปน้ำหนักต่ำสุดโดยไม่ต้องรอให้การแปลงดังกล่าวเสร็จสิ้นสมบูรณ์

การแปลงจำนวนให้อยู่ในรูปน้ำหนักต่ำสุดภายใต้ระบบจำนวนฐาน $\beta$ เมื่อ $\beta$ เป็นจำนวนเต็มที่มีค่ามากกว่าหรือเท่ากับสอง สามารถทำได้แบบเชื่อมตรง ตามที่เสนอในอัลกอริทึมที่ 4.1 ผลลัพธ์จะเป็นฐาน $\beta$ ภายใต้เซตตัวเลข $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ โดยกำหนดให้มีความหน่วงการทำงานคงที่คือสองซึ่งเพียงพอสำหรับการแปลงจำนวนให้อยู่รูปน้ำหนักต่ำสุด และได้เสนออัลกอริทึมสำหรับการคูณสเกลาร์ในระบบจำนวนฐาน $\beta$ อัลกอริทึมที่ 4.2 ซึ่งในการทำงานจะมีจำนวนของตัวดำเนินการเป็น $\beta+2$ เพื่อรองรับการทำงานในเซตตัวเลขดังกล่าว เช่น เมื่อกำหนดให้ $\beta=3$ จะต้องมีตัวดำเนินการในการคูณสเกลาร์ทั้งหมดห้าตัว คือ ตัวดำเนินการ *tripple* สำหรับการทวีคูณในแต่ละรอบ ตัวดำเนินการ $-4P$ $-P$ $+P$ และ $+2P$ สำหรับทำการบวกเมื่ออ่านบิตที่มีค่าน้ำหนักตรงกับตัวดำเนินการที่ต้องถูกเรียกใช้เข้ามา

นอกจากนี้ในงานวิจัยยังได้เสนอทฤษฎีบทที่ 3.1 3.2 และ 3.3 สำหรับสรุปการทำงานของอัลกอริทึมที่ 3.1 3.2 และ 3.3 ตามลำดับ ในการแปลงจำนวนให้อยู่ในรูประบบจำนวนฐานสองที่มีน้ำหนักต่ำสุดภายใต้เซตตัวเลข $\{\bar{3},\bar{1},0,1\}$ สำหรับการคูณสเกลาร์ในระบบจำนวนฐานสอง และเสนอทฤษฎีบทที่ 4.1 และ 4.2 สำหรับสรุปการทำงานของอัลกอริทึมที่ 4.1 และ 4.2 ตามลำดับ ในการแปลงจำนวนให้อยู่ในรูประบบจำนวนฐาน $\beta$ ที่มีน้ำหนักต่ำสุดภายใต้เซตตัวเลข $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ สำหรับการคูณสเกลาร์ในระบบจำนวนฐาน $\beta$ ซึ่งเมื่อรวมทำงานในระบบจำนวนฐานเดียวกันเข้าด้วยกันจะมีความซับซ้อนเชิงเวลาของการดำเนินการคือ $\Theta(n)$ เมื่อ $n$ คือขนาดของจำนวนนำเข้า

## 5.2 ข้อเสนอแนะ

การที่จะได้รูปแบบการแทนจำนวนที่ให้ค่าน้ำหนักต่ำสุดสำหรับการแปลงแบบเชื่อมตรง จำเป็นจะต้องกำหนดความหน่วงในการแปลง และเซตของตัวเลขที่ใช้ ให้เหมาะสมกับระบบจำนวนฐาน $\beta$ ที่เลือกใช้ ซึ่งในงานวิจัยนี้ได้กำหนดให้ค่าความหน่วงมีค่าคงที่เป็นสอง สำหรับการแปลงเซตตัวเลข $\{\bar{1},0,\ldots,(\beta-1)\}$ ไปเป็นเซตตัวเลข $\{(\overline{\beta+1}),\bar{1},0,\ldots,(\beta-1)\}$ โดยผลลัพธ์ที่ได้จะให้ค่าน้ำหนักต่ำสุดสำหรับเซตตัวเลขดังกล่าวในความหน่วงการทำงานเป็นสองเท่านั้น

ดังนั้นการเพิ่มค่าความหน่วงในการทำงานสามารถทำให้การแปลงจำนวนได้ค่าน้ำหนักที่ต่ำสุด ทั้งนี้จะขึ้นอยู่กับเซตตัวเลขที่เลือกใช้ด้วย ซึ่งหากเลือกใช้เซตตัวเลขไม่เหมาะสมกับค่าความหน่วงที่ใช้ก็ไม่สามารถได้การแปลงจำนวนที่ให้ค่าน้ำหนักต่ำสุดได้ ถึงแม้จะกำหนดให้ค่าความหน่วงมากเพียงใดก็ตาม เช่น กำหนดการแปลงจำนวนแบบเชื่อมตรงด้วยความหน่วงเป็นสอง จากค่านำเข้าในเซตตัวเลข $\{\bar{1},0,1\}$ เป็นค่านำออกในเซตตัวเลข $\{\bar{9},\bar{1},0,1\}$ ซึ่งจะไม่สามารถแปลงจำนวนเป็นบิต $\bar{9}$ ได้ เนื่องจากค่าความหน่วงสองไม่เพียงพอสำหรับการคำนวณค่าเชิงตัวเลขของ $\bar{9}$ เป็นต้น

# อภิธานศัพท์

## สัญกรณ์ทางคณิตศาสตร์

| | |
|---|---|
| $E_p(a,b)$ | แทนสมการในรูป $y^2 \bmod p = (x^3 + ax + b) \bmod p$ |
| $F_p$ | แทนขอบเขตจำกัด (finite field) |
| $k$ | แทนค่าจำนวนเฉพาะ $p$ (prime number $p$) |
| $G$ | แทนจุดบนเส้นโค้งอิลลิปติก |
| $P$ | แทนจุดบนเส้นโค้งอิลลิปติก |
| $\beta$ | beta: แทนเลขฐาน (base) |
| $\delta$ | delta: แทนค่าความหน่วงเชื่อมตรง (on-line delay) |
| $\eta$ | eta: แทนระบบจำนวนฐานสองแบบไม่มีเครื่องหมาย |
| $\mu$ | mu: แทนระบบจำนวนซ้ำซ้อนฐาน $\beta$ |
| $\omega$ | omega: แทนระบบจำนวนฐาน $\beta$ น้ำหนักต่ำสุด |

## ตัวย่อ

| | |
|---|---|
| EC | elliptic curve |
| ECC | elliptic curve cryptography |
| ECDLP | elliptic curve discrete logarithm problem |
| ISB | intermediate signed-binary |
| LSD | least significant digit |
| MSD | most significant digit |