การหาผลเฉลยปัญหาลอการิทึมวิยุตเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง

Solving an Elliptic Curve Discrete Logarithm Problem over Field of Characteristic Two

พิเชษฐ เชี่ยวธนะกุล

Bhichate Chiewthanakul

อาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น อำเภอเมือง จังหวัดขอนแก่น 14002

Lecturer in Department of Computer Engineering, Faculty of Engineering, Khon Kaen University, Amphoe Muang, Khon Kaen 14002

E-mail: bhichi@kku.ac.th

บทคัดย่อ

การรักษาความปลอดภัยของวิทยาการเข้ารหัสลับเส้นโค้งเชิงวงรี ขึ้นอยู่กับความยากของปัญหาลอการิทึมวิยุตเส้นโค้งเชิงวงรี (อีซีดีแอ็ลพี) เส้นโค้งเชิงวงรีที่ศึกษาในที่นี้ เป็นเส้นโค้งเชิงวงรีที่นิยามเหนือฟิลด์ลักษณะเฉพาะสอง ปัจจุบันวิธีการทั่วไป ที่จะหาผลเฉลยอีซีดีแอ็ลพีที่มีขนาดใหญ่ หมายถึง การเปลี่ยนแปลงเกี่ยวกับวิธีเบบี้สเต็ปไจแอนท์สเต็ป วิธีการเหล่านี้ทำงานสำหรับทุกอีซีดีแอ็ลพี เนื่องจากกรุ๊ปวัฏจักรจำกัด โดยปกติขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ปถูกใช้สำหรับกรุ๊ปของยูนิตมอดุโลจำนวนเฉพาะ บทความนี้นำเสนอการเปลี่ยนแปลงใหม่เกี่ยวกับขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ปที่จะโจมตีกรุ๊ปอื่น ที่เรียกว่ากรุ๊ปของเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง ผลการศึกษานี้แสดงให้เห็นว่าความซับซ้อนเชิงเวลาและพื้นที่ของแผนวิธีที่นำเสนอดีกว่าของการคำนวณบรูทฟอร์ซ

คำสำคัญ: *วิทยาการเข้ารหัสลับเส้นโค้งเชิงวงรี ลอการิทึมวิยุตเส้นโค้งเชิงวงรี เบบี้สเต็ปไจแอนท์สเต็ป*

Abstract

The security of elliptic curve cryptography is based on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). Elliptic curves studied here are elliptic curves defined over fields of characteristic two. Currently, the general methods to solve ECDLPs are variants of baby-step giant-step method. These methods work for every ECDLP because of the finite cyclic group. Usually the baby-step giant-step algorithm is used for the group of units modulo prime. In this paper, we present a new variant of baby-step giant-step scheme to attack other groups called groups of elliptic curve over characteristic two fields. The results of this study showed that time and space complexity of this scheme is better than the naive brute force calculation.

Keywords*: elliptic curve cryptography, elliptic curve discrete logarithm, baby-step giant-step*

1. บทนำ

การนำเสนอวิทยาการเข้ารหัสลับกุญแจสาธารณะ (Diffie and Hellman, 1976) นับเป็นการเริ่มต้นใช้คณิตศาสตร์อธิบายสมมุติฐานปัญหาลอการิทึมวิยุต ต่อการได้เกณฑ์วิธี (protocol) การสร้างกุญแจ หลังจากนั้น ได้มีการนำเสนอแผนวิธีอีกมากมายที่ใช้ปัญหาลอการิทึมวิยุต (Girault, 1991) และ (PUB, 2000) และความปลอดภัยของปัญหานี้ได้มีการศึกษาอย่างแพร่หลาย (Odlyzko, 2000) ผลการศึกษาส่วนใหญ่พบว่ามีการประยุกต์ใช้งานวิธีเบบี้สเต็ปไจแอนท์สเต็ป ซึ่งมีข้อดีคือ สามารถทำงานได้กับทุกกรุ๊ป และวิธีแบบโร (rho method) ซึ่งมีข้อดีคือ ใช้ทรัพยากรในการคำนวณน้อยกว่า แต่มีข้อจำกัดคือ สามารถทำงานได้ในบางกรุ๊ป (Pollard, 1978) ขั้นตอนวิธี (algorithm) เหล่านี้ถูกใช้เพื่อการกู้ค่าลอการิทึมวิยุต และปัจจุบันนี้ใช้สำหรับอ้างอิงเพื่อหาขอบเขตความปลอดภัยล่างสำหรับลอการิทึมวิยุตลักษณะเด่นอีกประการหนึ่งของปัญหาลอการิทึมวิยุต คือ ในการแสดงตัวตนหรือแผนวิธีการสร้างลายเซ็นนั้น สามารถใช้วิธีคำนวณบางส่วนล่วงหน้าได้ ส่งผลให้การพิสูจน์ตัวตนหรือลายเซ็นสามารถบูรณาการในชิบ (chip) ราคาไม่แพงได้ (Schnorr, 1990) เพราะใช้เพียงการดำเนินการคูณมอดุลาร์ (modular multiplication) หนึ่งครั้ง และหนึ่งครั้งในการบวกมอดุลาร์ (modular addition) ในขณะที่การตรวจสอบลายเซ็นในวิทยาการเข้ารหัสลับแบบอาร์เอ็สเอ (RSA) กลับใช้การคำนวณด้วยค่าใช้จ่ายที่มากกว่า กล่าวคือ ใช้อย่างน้อยมากกว่าหนึ่งเลขชี้กำลังมอดุลาร์ (modular exponential)

วิทยาการเข้ารหัสลับเส้นโค้งเชิงวงรี (Elliptic Curve Cryptography) เรียกแบบย่อว่าอีซีซี (ECC) อยู่บนพื้นฐานของโครงสร้างพีชคณิตของเส้นโค้งเชิงวงรีเหนือฟิลด์จำกัด ถูกคิดค้นในปีค.ศ. 1985 โดย Miller (1986) และ Koblitz (1987) จัดเป็นอีกทางเลือกหนึ่งของกลไกแบบวิทยาการเข้ารหัสลับกุญแจสาธารณะ สิ่งที่แตกต่างอย่างเด่นชัดจากวิทยาการเข้ารหัสลับแบบอาร์เอ็สเอ คือ ความปลอดภัยของวิทยาการเข้ารหัสลับเส้นโค้งเชิงวงรี ขึ้นอยู่กับความยากของปัญหาลอการิทึมวิยุต ส่วนความปลอดภัยของวิทยาการเข้ารหัสลับอาร์เอ็สเอขึ้นอยู่กับความยากของการแยกตัวประกอบ

จุดเด่นที่สำคัญคือ ที่ระดับความปลอดภัยเท่ากันวิทยาการเข้ารหัสลับเส้นโค้งเชิงวงรีใช้กุญแจขนาดเล็กกว่ามากเมื่อเทียบกับวิทยาการเข้ารหัสลับแบบอาร์เอ็สเอ นอกจากนี้ วิทยาการเข้ารหัสลับเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสองใช้ขนาดกุญแจเล็กกว่าวิทยาการเข้ารหัสลับเส้นโค้งเชิงวงรีเหนือฟิลด์เฉพาะ ที่ความปลอดภัยระดับเดียวกัน (Bos et al., 2009) ดังนั้นในการวิจัยนี้จึงศึกษาการหาผลเฉลยปัญหาลอการิทึมวิยุตเส้นโค้งเชิงวงรีเหนือฟิลด์เฉพาะสอง

บทความนี้มีการจัดลำดับเนื้อหาในการนำเสนอดังต่อไปนี้ วัตถุประสงค์ของงานวิจัยแสดงในหัวข้อที่ 2 หลังจากแนะนำขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ปในหัวข้อที่ 3 แล้ว ในหัวข้อที่ 4 อธิบายการเปลี่ยนแปลงใหม่เกี่ยวกับขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ป สำหรับกรุ๊ปของเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง หัวข้อที่ 5 แสดงตัวอย่างการประยุกต์เชิงตัวเลขสำหรับแผนวิธีที่นำเสนอ และบทสรุปในหัวข้อที่ 6

2. วัตถุประสงค์

1. เพื่อประยุกต์เครื่องมือในพีชคณิตนามธรรมสำหรับพัฒนาวิธีการส่งกฎการดำเนินการทวิภาคของกรุ๊ปของยูนิตมอดุโลจำนวนเฉพาะไปดำเนินการทวิภาคภายใต้กฎของกรุ๊ปการบวกของเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง ซึ่งเป็นเรขาคณิตนอกแบบยุคลิด

2. เพื่อพัฒนาการเปลี่ยนแปลงใหม่เกี่ยวกับขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ปที่สามารถโจมตีกรุ๊ปเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง โดยสามารถหาผลเฉลยปัญหาลอการิทึมวิยุตเส้นโค้งเชิงวงรีได้อย่างถูกต้อง และมีประสิทธิภาพที่ดี

3. เพื่อนำเสนอตัวอย่างการประยุกต์แผนวิธีที่ได้พัฒนาขึ้นด้วยโปรแกรมเซจ ซึ่งเป็นโปรแกรมแบบโอเพนซอร์สที่มีประสิทธิภาพ เหมาะสำหรับการศึกษาระดับสูง

3. ขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ป

ในหัวข้อนี้ แนะนำขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ป (Baby-Step Giant-Step algorithm) ปรากฏใน (พิเชษฐ เชี่ยวธนะกุล, 2556) และ (Cohen, 1993) เริ่มต้นด้วยการกำหนดสัญกรณ์ (notation) ในงานวิจัยดังต่อไปนี้

สัญกรณ์ 1 ให้ $\mathbb{G} =< g >$ แทน กรุ๊ปวัฏจักรจำกัด (finite cyclic group) ถูกก่อกำเนิดด้วยสมาชิก g ภายใต้การดำเนินการคูณ ให้ n แทน อันดับ (order) ของ $\mathbb{G}$ แล้วผลที่ได้คือ $\mathbb{G} = \{g^i : i \in \{0,1,\dots,n-1\}\}$ สำหรับสมาชิก h ใน $\mathbb{G}$ นิยาม *ลอการิทึมวิยุต (discrete logarithm)* ของ h ในฐาน g เขียนแทนด้วย $\log_g h$ หมายถึง จำนวนเต็ม x ที่ไม่เป็นลบและมีค่าน้อยกว่า n ที่ซึ่ง $h = g^x$ และนิยาม *ปัญหาลอการิทึมวิยุต (discrete logarithm problem)* หมายถึง การคำนวณ $\log_g h$ เมื่อกำหนดค่า g และ h ใน $\mathbb{G}$

ขั้นตอนวิธีแบบเบบี้สเต็ปไจแอนท์สเต็ปเป็นขั้นตอนวิธีทั่วไปสำหรับปัญหาลอการิทึมวิยุต ถูกนำเสนอโดยแชงซ์ (Shanks) (Cohen,1993) มีความซับซ้อนเชิงเวลา (time complexity) เท่ากับ $O(\sqrt{n})$ ปฏิบัติการคูณในกรุ๊ป

ขั้นตอนการทำงานเป็นดังนี้ ให้ $m = \lceil \sqrt{n} \rceil$ หมายถึง จำนวนเต็มค่าน้อยสุดที่มากกว่าหรือเท่ากับ $\sqrt{n}$ และสำหรับแต่ละสมาชิก $h \in \mathbb{G}$ จะมี $x = \log_g h$ ซึ่ง $x < n$ และ $x = jm + i$ โดยที่ i และ j เป็นจำนวนเต็มบางตัวซึ่ง $0 \le i, j < m$ จากความสัมพันธ์นี้ส่งผลให้ $h = g^{\log_g h} = g^{jm+i}$ และได้สมการที่ (1)

$$hg^{-jm} = g^i \qquad (1)$$

สำหรับบางค่าของจำนวน i และ j ดังนั้นเมื่อพิจารณาสองรายการต่อไปนี้

$$(1, g, g^2, \dots, g^{m-2}, g^{m-1})$$

และ

$$(h, hg^{-m}, hg^{-2m}, \dots, hg^{-(m-2)m}, hg^{-(m-1)m})$$

ข้อมูลในรายการทั้งสองมีการชน (collisions) และด้วยการชนมากที่สุดจำนวนสองคู่ นั่นคือ มีคู่ $(g^{i_0}, hg^{-j_0 m})$ และคู่ $(g^{i_1}, hg^{-j_1 m})$ ที่ซึ่ง $g^{i_0} = hg^{-j_0 m}$ และ $g^{i_1} = hg^{-j_1 m}$ สำหรับ $k = 0, \dots, m-1$ นั้น มีค่าของ x ได้จากคู่ที่มีค่า j_k ต่ำสุด แล้ว $x = i_k + j_k m$ และได้ขั้นตอนวิธีที่ 1 สำหรับความซับซ้อนเชิงเวลาของขั้นตอนวิธี ขึ้นอยู่กับการคำนวณของรายการทั้งสองเป็นหลักที่มีจำนวนสมาชิกเป็น m ดังนั้น ความซับซ้อนเชิงเวลาของขั้นตอนวิธีนี้เท่ากับ $O(\sqrt{n})$ ปฏิบัติการคูณในกรุ๊ป และความซับซ้อนเชิงพื้นที่ (space) เท่ากับจำนวน $O(\sqrt{n})$ สมาชิกในกรุ๊ป

ขั้นตอนวิธี 1 เบบี้สเต็ปไจแอนท์สเต็ป

Input: กรุ๊ปวัฏจักร $\mathbb{G}$ ของอันดับ n ด้วยตัวก่อกำเนิด g และสมาชิก h

Output: ค่าของ x ที่ซึ่ง $g^x = h$

$m = \lceil \sqrt{n} \rceil$

forall i ที่ซึ่ง $0 \leq i \leq m-1$ do

คำนวณ g^i และเก็บค่าคู่ (i, g^i) ในตาราง

endfor

คำนวณ g^{-m}

$y \leftarrow h$

for $j = 0$ to $(m-1)$ do

if y เป็นองค์ประกอบที่สอง (g^j) ของคู่ใดๆในตาราง then

$x \leftarrow jm + i$

else

$y \leftarrow y \cdot g^{-m}$

endif

endfor

4. การเปลี่ยนแปลงใหม่เกี่ยวกับขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ป

เริ่มต้นด้วยการแนะนำเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง แบบเส้นโค้งคอบลิทซ์ (Koblitz curve) ในหัวข้อ 4.1 แล้วหัวข้อ 4.2 วิเคราะห์การเปลี่ยนแปลงใหม่เกี่ยวกับขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ปเหนือเส้นโค้งคอบลิทซ์

4.1 เส้นโค้งคอบลิทซ์

เส้นโค้งเชิงวงรีถูกพัฒนาจากทฤษฎีของฟังก์ชันอิลลิปติก (Elliptic function) ในการวิเคราะห์เชิงซ้อน ซึ่งเป็นฟังก์ชันผกผันของปริพันธ์เชิงวงรี (Elliptic integral) ไวแยร์สทราสส์ (Weierstrass) ได้ค้นพบฟังก์ชันอิลลิปติกอย่างง่าย และได้มีการนำไปเชื่อมโยงกับเส้นโค้งเชิงวงรีเป็นอย่างมาก จึงมีการเรียกสมการของไวแยร์สทราสส์ ว่าสมการเส้นโค้งเชิงวงรี เซตของผลเฉลยภายใต้การดำเนินการทวิภาคของสมการไวแยร์สทราสส์มีโครงสร้างเป็นกรุ๊ปการบวก รายละเอียดเกี่ยวข้องกับโครงสร้างของสมการไวแยร์สทราสส์มีมากมายสามารถศึกษาได้ใน (Cohen, 1993) และ (Hoffstein, et al., 2008) สมการของเส้นโค้งคอบลิทซ์จัดเป็นสมการไวแยร์สทราสส์รูปแบบหนึ่ง มีโครงสร้างการคำนวณที่สอดคล้องกับโครงสร้างฮาร์ดแวร์ของดิจิทัลคอมพิวเตอร์ จึงนำมาศึกษาในงานวิจัยนี้ ต่อไป กำหนดสัญกรณ์ (notation) ที่ใช้ในการวิจัย สำหรับรายละเอียดเชิงลึกทางพีชคณิตสามารถศึกษาได้ใน (Lang, 2002) และ (Stewart, 2003) ส่วนรายละเอียดทางเรขาคณิตเชิงเลขคณิตสามารถศึกษาใน (Schmitt and Zimmer, 2003)

สัญกรณ์ 2 ให้ F_2 แทน ฟิลด์ลักษณะเฉพาะสอง (characteristic two field) แล้วส่งผลให้ $2 = 0$ สำหรับจำนวนเต็มบวก k ให้ F_{2^k} หมายถึง ริงพหุนามผลหาร (quotient polynomial ring) เหนือ F_2 ที่มีจำนวนสมาชิก 2^k ที่ซึ่งเป็นฟิลด์ และให้ $\mathbb{GF}(2^k)$ แทนกาลัวส์ฟิลด์ (Galois field) ที่มีจำนวนสมาชิก 2^k โดยทฤษฎีบทหลักมูลทางพีชคณิตส่งผลให้ F_{2^k} และ $\mathbb{GF}(2^k)$ มีสัณฐานเหมือนกัน (isomorphic)

บทนิยาม 1 *เส้นโค้งคอบลิทซ์* หมายถึง เส้นโค้งเชิงวงรีนิยามเหนือ F_2 ที่สอดคล้องกับสมการที่ (2)

$$\mathbf{E}_a: Y^2 + XY = X^3 + aX^2 + 1 \qquad (2)$$

เมื่อ $a \in \mathrm{F}_2$ และสัญกรณ์ $\mathbf{E}_a$แทนเส้นโค้งคอบลิทซ์เช่นเดียวกับปรากฏใน (Hoffstein, et al., 2008) เพื่อให้เกิดความสะดวกในการเชื่อมโยงกับงานวิจัยที่เกี่ยวข้องและเกิดความแตกต่างจากเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสองอื่น

จุดเด่นของเส้นโค้งคอบลิทซ์คือ มีโครงสร้างการคำนวณที่สอดคล้องกับโครงสร้างฮาร์ดแวร์ของดิจิทัลคอมพิวเตอร์ที่ใช้แพร่หลายในปัจจุบัน

(Hankerson et al., 2004) และสามารถประยุกต์วิธีการส่งโฟรเบนิอุส (Frobenius map) (Hoffstein, et al., 2008) เพื่อลดจำนวนครั้งของการดำเนินการกรุ๊ปในเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง จึงส่งผลให้ความซับซ้อนเชิงเวลาลดลงมาก เมื่อทำการเข้ารหัสลับและการถอดรหัสลับ ให้ $\#\mathbf{E}_a$ แทนจำนวนจุดในเส้นโค้งคอบลิทซ์ และให้ t แทนรอยโฟรเบนิอุส (Trace of Frobenius) สำหรับบทนิยามของรอยโฟรเบนิอุส มีความเกี่ยวข้องกับทฤษฎีบทมากมาย และไม่ได้เกี่ยวข้องกับงานวิจัยนี้โดยตรง ดังนั้น สามารถศึกษาได้ใน (Hoffstein, et al., 2008) จากทฤษฎีบทของฮาสส์ (Theorem of Hasse) ปรากฏใน (Hoffstein, et al., 2008) ได้ความสัมพันธ์ $\#\mathbf{E}_a = 3 - t$ ที่ซึ่ง $|t| \leq 2\sqrt{2}$ เพราะว่าจำนวนจุดเป็นจำนวนเต็มบวก และจะมีค่ามากสุดเมื่อ $t = -\lceil 2\sqrt{2} \rceil = -2$ ดังนั้น $1 \leq \#\mathbf{E}_a \leq 5$ เนื่องจากจำนวนจุดบนเส้นโค้งเชิงวงรีในสมการที่ (2) มีไม่เกิน 5 จุด และสำหรับจำนวนเฉพาะ p ที่ยกกำลังด้วย k จะมีฟิลด์ F_{p^k} ที่มีจำนวนสมาชิก p^k เสมอ ดังนั้น จึงสามารถประยุกต์เส้นโค้งคอบลิทซ์ได้ดังสมการที่ (3)

$$\mathbf{E}(\mathrm{F}_{2^k}): Y^2 + XY = X^3 + aX^2 + 1 \qquad (3)$$

โดยที่ $a \in F_{2^k}$ และสัญกรณ์ $\mathbf{E}(\mathrm{F}_{2^k})$ แทนเส้นโค้งคอบลิทซ์เหนือฟิลด์ F_{2^k} เช่นเดียวกับปรากฏใน (Cohen, 1993) และ (Hoffstein, et al., 2008) เพื่อให้เกิดความสะดวกในการเชื่อมโยงกับงานวิจัยที่เกี่ยวข้องและสะดวกในการพัฒนาโปรแกรม

สำหรับการดำเนินการทวิภาค (binary operation) ของสมาชิกในเส้นโค้งคอบลิทซ์ค่อนข้างซับซ้อนเพราะอยู่ภายใต้กฎเรขาคณิตนอกแบบยุคลิด (non-Euclidean geometry) รายละเอียดสามารถศึกษาได้ใน (Hankerson et al., 2004) และ (Schmitt and Zimmer, 2003)

ต่อไป ผู้วิจัยจะแสดงตัวอย่างการประยุกต์สมการที่ (3) ด้วยเซจ (SAGE: System for Algebra and Geometry Experimentation) จัดเป็นโปรแกรมแบบโอเพนซอร์ส (open source) (Stein et al., 2014) และเป็นอีกทางเลือกหนึ่งจากแมธิแมติกา (Mathematica) ซึ่งเป็นซอฟต์แวร์ลิขสิทธิ์ที่ต้องได้รับอนุญาตก่อนสำหรับตัวอย่างนี้ ผู้วิจัยใช้เซจรุ่น 6.4.1 ภายใต้ระบบปฏิบัติการลินุกซ์มินท์ 17.1 เมท 64-บิต (Linux Mint 17.1 Mate 64-bit) บนเครื่องเดลล์ (Dell) รุ่นอินสไปรอน 1420 (Inspiron 1420) ซีพียูอินเทลคอร์ทูดูโอ (Intel core 2 duo) ความเร็ว 2.1 GHz หน่วยความจำ 4 GBytes

ตัวอย่าง 1 ให้ $k = 4$ แล้วสามารถก่อกำเนิดฟิลด์ F_{2^k} ได้ด้วยคำสั่ง

```
sage: k=4;F.<x>=GF(2^k);F
```

F_{2^4}

แล้วแสดงสมาชิกทั้งหมดและจำนวนสมาชิกใน F_{2^4} ด้วยคำสั่งตามลำดับ

```
sage: list(F);len(F)
```

$[0, x, x^2, x^3, x + 1, x^2 + x, x^3 + x^2, x^3 + x + 1, x^2 + 1, x^3 + x, x^2 + x + 1, x^3 + x^2 + x, x^3 + x^2 + x + 1, x^3 + x^2 + 1, x^3 + 1, 1]$, 16

จากนั้นสุ่มค่า a และกำเนิดเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง ได้ด้วยคำสั่ง

```
sage: lst=list(F)
sage: a=lst[randrange(0,len(F))];a
```

$x^3 + x^2 + x$

```
sage: E=EllipticCurve(F,[1,a,0,0,1]);E
```

$y^2 + xy = x^3 + (x^3 + x^2 + x)x^2 + 1$

แสดงกรุ๊ปการบวกเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง ได้ด้วยคำสั่ง

```
sage: list(E)
```

$[(0 : 1 : 0), (0 : 1 : 1), (x : x^3 + x^2 : 1), (x : x^3 + x^2 + x : 1), (x + 1 : x^2 + 1 : 1), (x + 1 : x^2 + x : 1), (x^2 : x : 1), (x^2 : x^2 + x : 1), (x^2 + 1 : 1 : 1), (x^2 + 1 : x^2 : 1), (x^3 + 1 : x^2 + x : 1), (x^3 + 1 : x^3 + x^2 + x + 1 : 1), (x^3 + x + 1 : 1 : 1), (x^3 + x + 1 : x^3 + x : 1), (x^3 + x^2 + 1 : 0 : 1), (x^3 + x^2 + 1 : x^3 + x^2 + 1 : 1), (x^3 + x^2 + x : x^2 + 1 : 1), (x^3 + x^2 + x : x^3 + x + 1 : 1)]$

และคำนวณจำนวนจุดใน **E** ด้วยคำสั่ง

```
sage: order(E)
```

16

ในตัวอย่างที่ 1 แสดงให้เห็นว่าสามารถประยุกต์สมการที่ (3) เพื่อก่อกำเนิดเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสองได้ จำนวนจุดบนเส้นโค้งเชิงวงรีหรือขนาดของกรุ๊ปนี้จะขึ้นอยู่กับจำนวนเต็ม k เมื่อค่า k มากจะได้จำนวนจุดมาก แต่เมื่อค่า k น้อยจะได้จำนวนจุดน้อย

4.2 ขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ปเหนือเส้นโค้งคอบลิทซ์

ความสัมพันธ์ระหว่างกรุ๊ปจำกัดการคูณ และเส้นโค้งคอบลิทซ์ ได้มีการศึกษาใน (ปานดาว แก้วมณี และ ศิวารุจ พรรคชัย, 2555) บอกให้ทราบว่า มีสัณฐานเหมือนกันระหว่างกรุ๊ปจำกัดและภาพของกรุ๊ปจำกัด (image of finite group) ซึ่งเป็นกรุ๊ปเส้นโค้งคอบลิทซ์ ดังนั้น จึงได้ประพจน์ที่ 1

ประพจน์ที่ 1 ให้ p แทนจำนวนเฉพาะ และ F_p เป็นฟิลด์จำกัด และให้ $\mathbf{E}(\mathrm{F}_{2^k})$ เป็นเส้นโค้งคอบลิทซ์ แล้วกรุ๊ปของยูนิตมอดุโลจำนวนเฉพาะเขียนแทนด้วย $\mathbf{F}_p^*$ มีสัณฐานเหมือนกันกับกรุ๊ปเส้นโค้งคอบลิทซ์

การพิสูจน์ ให้ p แทนจำนวนเฉพาะ และ F_p เป็นฟิลด์จำกัด แล้วเซตย่อย $\mathrm{F}_p\backslash\{0\}$ ของ F_p ภายใต้กฎการคูณเป็นกรุ๊ปของ ยูนิตมอดุโลจำนวนเฉพาะ เขียนแทนด้วย $\mathbf{F}_p^*$ เพราะว่ามีสัณฐานเหมือนกันระหว่างกรุ๊ปจำกัด และกรุ๊ปเส้นโค้งคอบลิทซ์ จึงสมมุติ φ เป็นสมสัณฐาน (isomorphism) เพื่อการส่งระหว่างกรุ๊ป ดังสมการที่ (4)

$$\varphi: \mathbf{F}_p^* \rightarrow \mathbf{E}(\mathrm{F}_{2^k}) \qquad (4)$$

แล้วกรุ๊ปของยูนิตมอดุโลจำนวนเฉพาะ มีสัณฐานเหมือนกันกับกรุ๊ปการบวกของเส้นโค้งคอบลิทซ์

ประพจน์ที่ 1 บอกเป็นนัยว่า มีการส่งที่คงสภาพกรุ๊ปและความสัมพันธ์ของสมาชิกในกรุ๊ประหว่างกรุ๊ปของยูนิตมอดุโลจำนวนเฉพาะและกรุ๊ปการบวกของเส้นโค้งคอบลิทซ์ หรือกล่าวในเชิงการประยุกต์ว่าการดำเนินการคูณในกรุ๊ปของยูนิตมอดุโลจำนวนเฉพาะมีผลลัพธ์ในทำนองเดียวกันกับการดำเนินการบวกในเส้นโค้งคอบลิทซ์ แล้วจึงได้ประพจน์ที่ 2

บทนิยาม 2 ให้ x เป็นจำนวนเต็มบวก และให้ P และ Q อยู่ใน $\mathbf{E}(\mathrm{F}_{2^k})$ ที่ซึ่ง $Q = \underbrace{P + \cdots + P}_{x \text{ การบวกบน } \mathbf{E}(\mathrm{F}_{2^k})}$ เขียนแทนด้วย $Q = xP$ แล้วเรียกปัญหาการหาค่า x เมื่อทราบค่า P และ Q ว่า *ปัญหาลอการิทึมวิยุตเส้นโค้งเชิงวงรี (อีซีดีแอ็ลพี)*

ประพจน์ที่ 2 ให้ P และ Q อยู่ใน $\mathbf{E}(\mathrm{F}_{2^k})$ ที่มีจำนวนสมาชิก n ให้ $m = \lceil \sqrt{n} \rceil$ และสำหรับ i, j เป็นจำนวนเต็มที่ไม่เป็นลบค่าน้อยกว่า m แล้วได้ความสัมพันธ์

$$Q - (jm)P = iP \qquad (5)$$

การพิสูจน์ ให้ g และ h อยู่ใน $\mathbb{F}_p^*$ และให้ $\varphi: \mathbb{F}_p^* \to \mathbf{E}(\mathrm{F}_{2^k})$ เป็นสมสัณฐานที่ซึ่ง $P = \varphi(g)$ และ $Q = \varphi(h)$ เมื่อพิจารณาสมการที่ (1) แล้วได้ $\varphi(hg^{-jm}) = Q - (jm)P = \varphi(g^i) = iP$ ดังนั้น $Q - (jm)P = iP$

ประพจน์ที่ 2 บอกเป็นนัยว่าสามารถเปลี่ยนกฎการคำนวณใน ขั้นตอนวิธีที่ 1 แล้วได้ขั้นตอนวิธีที่สามารถหาผลเฉลย ปัญหาลอการิทึมวิยุตเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง ดังขั้นตอนวิธีที่ 2 เพราะว่ากรุ๊ปของยูนิตมอดุโลจำนวนเฉพาะมีสัณฐานเหมือนกันกับกรุ๊ปการบวกของเส้นโค้งคอบลิทซ์ ดังนั้นจำนวนครั้งของการดำเนินการกรุ๊ปของขั้นตอนวิธีที่ 2 จึงเท่ากับการดำเนินการกรุ๊ปในขั้นตอนวิธีที่ 1 นั่นคือความซับซ้อนเชิงเวลาของขั้นตอนวิธีนี้เท่ากับ $O(\sqrt{n})$ ปฏิบัติการบวกในกรุ๊ป และความซับซ้อนเชิงพื้นที่ (space) เท่ากับจำนวน $O(\sqrt{n})$ สมาชิกในกรุ๊ปดีกว่าเวลาการทำงานเท่ากับ $O(n)$ ของการคำนวณบรูทฟอร์ซธรรมดา

ขั้นตอนวิธี 2 เบบี้สเต็ปไจแอนท์สเต็ปเหนือเส้นโค้งคอบลิทซ์

Input: กรุ๊ปวัฏจักร $\mathrm{E}(\mathrm{F}_{2^k})$ ของอันดับ n ด้วยตัวก่อกำเนิด P และสมาชิก Q

Output: ค่าของ x ที่ซึ่ง $xP = Q$

$m = \lceil \sqrt{n} \rceil$

forall i ที่ซึ่ง $0 \le i \le m-1$ do

คำนวณ iP และเก็บค่าคู่ (i, iP) ในตาราง

endfor

คำนวณ $(-m)P$

$y \leftarrow Q$

for $j = 0$ to $(m-1)$ do

if y เป็นองค์ประกอบที่สอง (jP) ของคู่ใดๆในตาราง then

$x \leftarrow jm + i$

else

$y \leftarrow y + (-m)P$

endif

endfor

5. ตัวอย่างการประยุกต์เชิงตัวเลข

หัวข้อนี้นำเสนอตัวอย่างการประยุกต์เบบี้สเต็ปไจแอนท์สเต็ปเหนือเส้นโค้งคอบลิทซ์ดังที่แสดงในขั้นตอนวิธีที่ 2 ด้วยโปรแกรมเซจ

ตัวอย่าง 2 ให้ $k = 10$ แล้วสามารถก่อกำเนิดฟิลด์ F_{2^k} และสุ่มเส้นโค้งเชิงวงรี $\mathrm{E}(\mathrm{F}_{2^k})$ ได้ด้วยคำสั่ง

```
sage: k=10;F.<x>=GF(2^k);lst=list(F)
sage: a=lst[randrange(0,len(F))]
sage: E=EllipticCurve(F,[1,a,0,0,1]);E
```

สุ่มได้สมการ $\mathrm{E}: y^2 + xy = x^3 + (x^8 + x^7 + x^6 + x^5 + x^2)x^2 + 1$ แล้วคำนวณตัวก่อกำเนิดเส้นโค้งเชิงวงรีแทนด้วยจุด P จากนั้นสุ่มจุด Q ด้วยคำสั่ง

```
sage: P=E.gens()[0]
sage: Q=randrange(1,order(E))*P;
sage: P
```

ได้ $P = (x^8 + x^7 + x^6 + x^3 + x^2 + 1, x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + x)$ และ

```
sage: Q
```

$Q = (x^8 + x^7 + x^6 : x^9, 1)$

แล้วใช้ขั้นตอนวิธีที่ 2 โดยเขียนโปรแกรมในรูปฟังก์ชันได้ดังต่อไปนี้

```
sage:
#-------------------------------------------------------------
#Algorithm Baby-step giant-step for ECC_Char2
# function ECC_Baby_Gian(P,y,n)
#-------------------------------------------------------------
def EEC_BaBy_Gian(P,y,n):
```

```
        m=1+floor(sqrt(n))
#-------------------------------------------------------------
#Generate First Table:
#-------------------------------------------------------------
        table_st=[]
        for j in range(m):
                table_st.append((j*P))
#-------------------------------------------------------------
#Generate Second Table:
#-------------------------------------------------------------
        table_nd=[]
        for j in range(len(table_st)):
                table_nd.append(table_st[j])
        table_nd.sort()
#-------------------------------------------------------------
        P_inv = -P
        P_ninv = m*P_inv
        j=0
        flag=true
        while flag:
                gamma1=y+j*P_ninv
                if gamma1 in table_nd:
                        i=table_st.index(gamma1)
                        flag=false
                else:
                        j=j+1
        x=j*m+i
        return x
#-------------------------------------------------------------
```

จากนั้นใช้ฟังก์ชัน ECC_Baby_Gian(P,y,n) หาผลเฉลย

```
sage: x=EEC_BaBy_Gian(P,Q,n);x
        59
```

แล้วได้ $x = 59$

ท้ายสุด ลองตรวจคำตอบ

```
sage: bool(Q==x*P)
        true
```

แสดงว่าหาผลเฉลยได้ถูกต้อง

6. บทสรุป

การรักษาความปลอดภัยของวิทยาการเข้ารหัสลับเส้นโค้งเชิงวงรีขึ้นอยู่กับความยากของปัญหาลอการิทึมวิยุตเส้นโค้งเชิงวงรี (อีซีดีแอ็ลพี) โดยศึกษาเส้นโค้งวงรีที่นิยามเหนือฟิลด์ลักษณะเฉพาะสองปัจจุบัน วิธีการทั่วไปที่จะหาผลเฉลยอีซีดีแอ็ลพีที่มีขนาดใหญ่ หมายถึง การเปลี่ยนแปลงเกี่ยวกับวิธีเบบี้สเต็ปไจแอนท์สเต็ป วิธีการเหล่านี้ทำงานสำหรับทุกอีซีดีแอ็ลพีเพราะเป็นการคำนวณเหนือกรุ๊ปวัฏจักรจำกัด โดยปกติขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ปถูกใช้สำหรับกรุ๊ปของยูนิตมอดุโลจำนวนเฉพาะ ในบทความนี้เรานำเสนอการเปลี่ยนแปลงใหม่เกี่ยวกับขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ปที่จะโจมตีกรุ๊ปอื่น ที่เรียกว่ากรุ๊ปของเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง โดยการใช้เครื่องมือทางพีชคณิตเพื่อเปลี่ยนกฎการคำนวณในขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ปเหนือกรุ๊ปการคูณ ให้อยู่ในรูปกฎการบวกในเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง แล้วได้ขั้นตอนวิธีเบบี้สเต็ปไจแอนท์สเต็ปเหนือเส้นโค้งคอบลิทซ์ ผลการศึกษานี้แสดงให้เห็นว่าขั้นตอนวิธีสามารถหาผลเฉลยได้ถูกต้อง โดยเวลาการทำงานและความซับซ้อนพื้นที่ของขั้นตอนวิธีนี้เท่ากับ $O(\sqrt{n})$ ดีกว่าเวลาการทำงานเท่ากับ $O(n)$ ของการคำนวณบรูทฟอร์ซธรรมดา

7. กิตติกรรมประกาศ

ผู้เขียนขอขอบคุณศาสตราจารย์ซิลเวอร์แมน โจเซฟ แห่งมหาวิทยาลัยเบราว์ ณ โรดไอแลนด์ ศาสตราจารย์สไตล์ วิลเลียม แห่งมหาวิทยาลัยวอชิงตัน ณ เมืองซีแอตเติล และศาสตราจารย์มาซู แบร์รี่ แห่งมหาวิทยาลัยฮาร์วาร์ด ณ เมืองเคมบริดจ์ ที่ได้สร้างแรงบันดาลใจให้กับผู้เขียน

8. เอกสารอ้างอิง

ปานดาว แก้วมณี และ ศิวารุจ พรรคชัย. (2555). แผนวิธีแบบอสมมาตรด้วยเส้นโค้งเชิงวงรีเหนือฟิลด์ลักษณะเฉพาะสอง. ค้นเมื่อ 8 ธันวาคม 2557 จาก http://mis.en.kku.ac.th/administrator/doc_upload/20130313184509.pdf

พิเชษฐ เชี่ยวธนะกุล. (2556). วิทยาการรหัสลับเชิงคณิตศาสตร์. มหาวิทยาลัยขอนแก่น.

Bos, J. W., Kaihara, M. E., Kleinjung, T., Lenstra, A. K., and Montgomery, P. L. (2009). On the security of 1024-bit rsa and 160-bit elliptic curve cryptography. IACR Cryptology ePrint Archive, 2009, 389.

Cohen, H. (1993). A course in computational algebraic number theory. Springer.

Diffie, W., and Hellman, M. E. (1976). New directions in cryptography. Information Theory, IEEE Transactions on, 22(6): 644–654.

Girault, M. (1991). Self-certified public keys. In Advances in Cryptology-EUROCRYPT'91 (pp.490–497).

Hankerson, D., Vanstone, S., and Menezes, A. J. (2004). Guide to elliptic curve cryptography. Springer.

Hoffstein, J., Pipher, J. C., and Silverman, J. H. (2008). An introduction to mathematical cryptography. Springer.

Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177): 203–209.

Lang, S. (2002). Algebra. (Third edition). Springer.

Miller, V. S. (1986). Use of elliptic curves in cryptography. In Advances in Cryptology-CRYPTO'85 Proceedings (pp. 417–426).

Odlyzko, A. (2000). Discrete logarithms: The past and the future. In Towards a Quarter-Century of Public Key Cryptography (pp. 59–75). Springer.

Pollard, J. M. (1978). Monte carlo methods for index computation (mod p). Mathematics of computation, 32(143): 918–924.

PUB, F. (2000). Digital signature standard (dss).

Schmitt, S., and Zimmer, H. G. (2003). Elliptic Curves: A computational approach (Vol. 31). Walter de Gruyter.

Stein, W. A., et al. (2014). Sage Mathematics Software (Version 6.4.1). The Sage Development Team, http://www.sagemath.org.