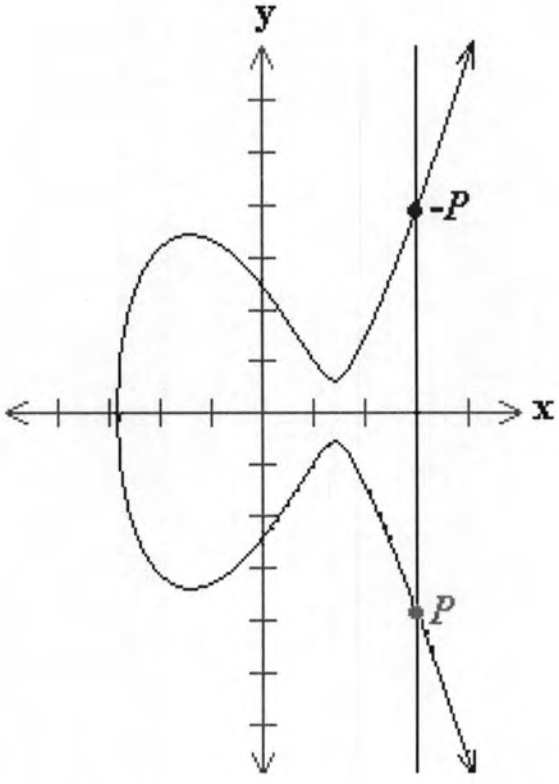
บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 กลุ่มเส้นโค้งอิลลิปติกบนขอบเขตจำกัด (elliptic curve groups over finite field)

รูปร่างของเส้นโค้งอิลลิปติก [1-2] ขึ้นอยู่กับสมการที่อยู่ในรูป $y^2 = x^3 + ax + b$ ซึ่งจะเขียนแทนด้วย $E(a,b)$ ก็ต่อเมื่อ $4a^3 + 27b^2 \neq 0$ โดยที่ x, y, a และ b เป็นจำนวนจริง (real number) ซึ่งแต่ละค่าของ a และ b จะให้เส้นโค้งอิลลิปติกที่แตกต่างกัน รูปกราฟของเส้นโค้งอิลลิปติกจะมีความสมมาตรกัน และแทนจุดใด ๆบนเส้นโค้งด้วย $P(x,y)$ ด้วยคุณสมบัติสมมาตรทำให้ได้จุดสะท้อนตามแนวแกนนอนแทนด้วย $-P(x,-y)$

ตัวอย่างที่ 2.1 *กราฟความสัมพันธ์ของจุดบนเส้นโค้งอิลลิปติก*
รูปแบบความสัมพันธ์ของจุด P และ $-P$ เมื่อ $a=-6$ และ $b=-6$ จะสามารถเขียนสมการได้เป็น $y^2 = x^3 - 6x - 6$ ได้ถูกแสดงดังรูปที่ 2.1



รูปที่ 2.1 รูปกราฟของสมการ $y^2 = x^3 - 6x - 6$

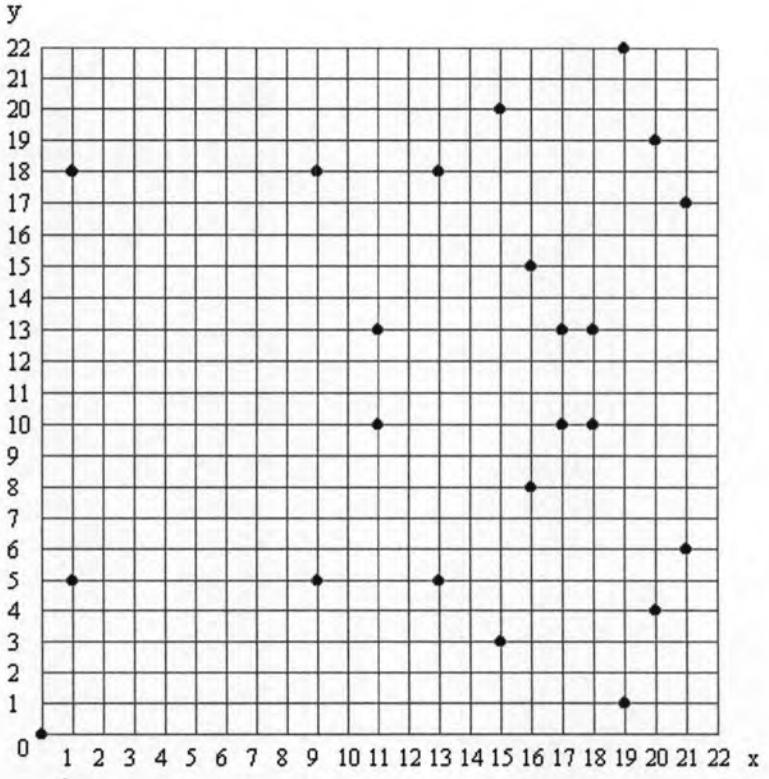
□

การจำกัดขอบเขต (finite field) ให้กับเส้นโค้งอิลลิปติก สามารถกระทำได้โดยเพิ่มขอบเขตจำกัด F_p โดยที่ p เป็นจำนวนเฉพาะค่าหนึ่ง ทำให้สามารถเขียนรูปสมการทั่วไปได้ใหม่เป็น $y^2 \bmod p = (x^3 + ax + b) \bmod p$ ซึ่งสามารถเขียนแทนด้วยรูปย่อ $E_p(a,b)$ ก็ต่อเมื่อ $(4a^3 + 27b^2) \bmod p \neq 0$ โดยที่ x, y, a และ b เป็นจำนวนที่อยู่ในขอบเขตจำกัด F_p

ตัวอย่างที่ 2.2 *ความสัมพันธ์ของสมการ และจุดบนขอบเขตจำกัด* F_p

กำหนด $E_{23}(1,0)$ สามารถเขียนเป็นสมการได้คือ $y^2 \bmod 23 = (x^3 + x) \bmod 23$ และจากสมการจะได้จุดทั้งหมด 23 จุด นั่นคือ

(0,0) (1,5) (1,18) (9,5) (9,18) (11,10) (11,13) (13,5) (13,18) (15,3) (15,20) (16,8) (16,15) (17,10) (17,13) (18,10) (18,13) (19,1) (19,22) (20,4) (20,19) (21,6) (21,17) ดังรูปที่ 2.2



รูปที่ 2.2 รูปกราฟของสมการ $y^2 = x^3 - x$ บนขอบเขตจำกัด F_{23}

□

2.2 การคูณจุดหรือสเกลาร์ (point or scalar multiplication)

การคูณจุด หรือเรียกว่าการคูณสเกลาร์ [2-4] เป็นการดำเนินการหลักของอีซีซี โดยมีรูปทั่วไปของการดำเนินการดังนี้

$$G = kP = \underbrace{P + P + \ldots + P}_{k}$$

โดยที่ G และ P แทนจุดใดๆบนเส้นโค้งอิลลิปติก และ k เป็นค่าสุ่มของจำนวนเฉพาะ ซึ่งการคูณสเกลาร์นั้นจะดำเนินการโดยใช้อัลกอริทึมการเพิ่มทวีคูณ (double and add algorithm) หรือเรียกว่าวิธีการฐานสอง (binary method) ดังแสดงในอัลกอริทึมที่ 2.1 โดยในที่นี้ค่า G ถูกตั้งต้นให้เป็นจุดอนันต์แทนด้วยศูนย์ และผลลัพธ์สุดท้ายจะถูกเก็บไว้ที่ G

อัลกอริทึมที่ 2.1 อัลกอริทึมการเพิ่มทวีคูณ

นำเข้า: ระบบจำนวนฐานสองของจำนวนเฉพาะ k

นำออก: ผลการคูณสเกลาร์ $G = kP$

$G = kP$

$k = (k_{t-1}, k_{t-2}, \ldots, k_0)$

$G = 0$

for i from $t-1$ down to 0 do

  $G = G + G$

  if $k_i = 1$ then

    $G = G + P$

return G

2.3 การดำเนินการเลขคณิตในการคูณสเกลาร์ (arithmetic in scalar multiplication)

กำหนด P, G และ R เป็นจุดบนกลุ่มเส้นโค้งอิลลิปติกบนขอบเขตจำกัด F_p [2-4] โดยที่ $P = (x_P, y_P)$ ซึ่งมี $-P = (x_P, -y_P \bmod p)$ และ $G = (x_G, y_G)$ โดยมีจุด $R = (x_R, y_R)$ เป็นผลลัพธ์ปัจจุบันจากการคำนวณบน $E_p(a,b)$ ซึ่งมีการดำเนินการเลขคณิตสองรูปแบบคือ

2.3.1 การบวกจำเพาะระหว่างจุด P และ G (adding distinct points P and G)

$P + G = R$ โดยที่

$s = ((y_P - y_G) \div (x_P - x_G)) \bmod p$ ซึ่ง s ก็คือค่าความชันของเส้นตรงที่ผ่านจุด P และ G

$x_R = (s^2 - x_P - x_G) \bmod p$

$y_R = (s(x_P - x_R) - y_P) \bmod p$

2.3.2 การเพิ่มทวีของจุด P (doubling the point P)

$2P = R$ เมื่อ $y_P \neq 0$

$s = ((3x_P^2 + a) \div 2y_P) \bmod p$

$x_R = (s^2 - 2x_P) \bmod p$

$y_R = (s(x_P - x_R) - y_P) \bmod p$

ตัวอย่างที่ 2.3 *การหา* $P+G$ *และ* $2P$ *จาก* $E_{23}(1,1)$ *เมื่อ* $P=(3,10)$ *และ* $G=(9,7)$

หา $P+G$ ได้จาก $s=((7-10)\div(9-3))\bmod 23 \quad =11$

$x_R=(11^2-3-9)\bmod 23 \quad =17$

$y_R=(11(3-17)-10)\bmod 23 \quad =20$

ดังนั้นจะได้ $P+G=(17,20)$

หา $2P$ ได้จาก $s=((3(3^2)+1)\div(2\times 10))\bmod 23 \quad =6$

$x_R=(6^2-(2\times 3))\bmod 23 \quad =7$

$y_R=(6(3-7)-10)\bmod 23 \quad =12$

ดังนั้นจะได้ $2P=(7,12)$ □

2.4 ปัญหาดิสครีทลอการิทึมของเส้นโค้งอิลลิปติก

เมื่อกำหนดขอบเขตจำกัด (finite field) ให้มีขนาดใหญ่เพื่อใช้สำหรับการเข้ารหัสลับด้วยเส้นโค้งอิลลิปติก ซึ่งในกระบวนการคูณสเกลาร์นั้น การที่จะทราบค่าจำนวนเต็มบวก k จากการคำนวณโดยกำหนดเพียงจุด P และค่า kP สามารถกระทำได้ยาก ซึ่งปัญหาดังกล่าวถูกเรียกว่า ปัญหาดิสครีทลอการิทึม [3] ดังตัวอย่างที่ 2.4

ตัวอย่างที่ 2.4 *ความซับซ้อนของดีสครีทลอการิทึมของเส้นโค้งอิลลิปติก*

กำหนด G และ P คือจุดบนเส้นโค้งอิลลิปติกซึ่งมีรูปย่อคือ $E_{23}(9,17)$ สามารถเขียนในรูปเต็มคือ $y^2 \bmod 23=(x^3+9x+17)\bmod 23$ แล้วคำนวณหา k ซึ่งทำให้ $G=kP$ เมื่อ $G=(4,5)$ และ $P=(16,5)$ วิธีการคือเริ่มต้นคำนวณ kP จาก $k=1$ จนกระทั่งพบผลลัพธ์ดังนี้

$P=(16,5)$	$2P=(20,20)$	$3P=(14,14)$
$4P=(19,20)$	$5P=(13,10)$	$6P=(7,3)$
$7P=(8,7)$	$8P=(12,17)$	$9P=(4,5)$

จะได้คำตอบคือ $k=1$ ซึ่งในความเป็นจริงแล้วในการเข้ารหัสจะใช้ $k=1$ เป็นจำนวนเฉพาะที่มีค่าใหญ่มากเพื่อยากต่อการทำบรูทฟอร์ส (brute-force) เพื่อหาผลลัพธ์ □

2.5 วิธีการของชามีร์ (Shamir's method)

ชามีร์ [6] ได้เสนอวิธีการคูณสเกลาร์โดยมีพื้นฐานการคำนวณอยู่บนระบบจำนวนฐานสอง และดำเนินการจากซ้ายไปขวา ซึ่งวิธีการนี้สามารถนำมาประยุกต์ใช้ในการคูณสเกลาร์ kP ได้อย่างมีประสิทธิภาพ โดยการแทนรูป k ในระบบจำนวนฐานสอง แล้วจึงคำนวณการเพิ่มทวีตามบิตนำเข้าทีละบิตจากซ้ายไปขวาจนครบทุกบิต ซึ่งความซับซ้อนของวิธีการนี้ขึ้นอยู่กับค่าน้ำหนักของ k กล่าวคือยิ่งมีบิตที่เป็นศูนย์มากก็จะคำนวณได้เร็วขึ้น

ตัวอย่างที่ 2.5 *การคูณสเกลาร์ kP ด้วยวิธีการของซามีร์*

ตารางที่ 2.1 การคำนวณ $61P$ ด้วยวิธีการของซามีร์ใช้เซตตัวเลข {0,1}

$k=61$	1	1	1	1	0	1
double	0	$2P$	$6P$	$14P$	$30P$	$60P$
$+P$	P	$3P$	$7P$	$15P$	-	$61P$

จากตารางที่ 2.1 การดำเนินการจะเริ่มด้วยการรับค่า k ซึ่งถูกเปลี่ยนให้อยู่ในรูประบบจำนวนฐานสอง โดยค่าเริ่มต้นในช่อง *double* จะถูกกำหนดให้เป็นศูนย์ เมื่อบิตแรกของ k ถูกอ่านเข้ามาจากซ้ายสุดหากพบว่ามีค่าเป็นหนึ่งก็ให้ทำการบวก P เพิ่มแล้วเก็บค่าลงในช่อง $+P$ แต่ถ้าบิตที่อ่านเข้ามาเป็นศูนย์ ก็ไม่ต้องทำการบวก P ปล่อยให้ช่อง $+P$ ว่างเปล่า หลังจากนั้นทำการทวีคูณ P เก็บค่าลงในช่อง *double* ในแต่ละรอบที่บิตถัดไปถูกอ่านเข้ามาจนครบ □

2.6 ระบบจำนวน (Number system)

ระบบจำนวน (β, D) ประกอบด้วยเลขฐาน (base) β โดยที่ β สามารถเป็นได้ทั้งจำนวนจริงหรือจำนวนเชิงซ้อนซึ่ง $\|\beta\|>1$ และชุดตัวเลขแบบจำกัด (finite digit set) D โดยที่สมาชิกในชุดตัวเลขที่เรียกว่าดิจิต (digit) สามารถเป็นได้ทั้งจำนวนจริงและจำนวนเชิงซ้อน

กำหนดให้มีจำนวนเต็ม X โดยที่ X สามารถแสดงได้ในระบบจำนวนเลขฐาน β ด้วยชุดตัวเลขแบบจำกัด D ดังนี้

$$X=(x_n x_{n-1}\ldots x_0 x_{-1}x_{-2}\ldots)\beta$$

ซึ่ง $x_i \in D$ โดยที่ $n\in Z, i\le n$ โดยค่าเชิงตัวเลข (numerical value) ของ X บนฐาน β สามารถคำนวณได้จากสมการ

$$\|X\|=\sum_{i=n}^{-\infty} x_i\beta^i$$

ซึ่งค่าเชิงตัวเลขทั้งหมดที่แสดงได้สามารถเขียนให้อยู่รูปของเซต $P[\beta, D]$ ได้ดังนี้

$$\mathrm{P}_n^m[\beta,D]=\left\{X=(x_n x_{n-1}\cdots x_{m+1}x_m)_\beta \,\middle|\, x_i\in D, m\le i\le n\right\}$$

$$\mathrm{P}_n[\beta,D]=\left\{X=(x_n x_{n-1}\cdots)_\beta \,\middle|\, x_i\in D, i\le n\right\}$$

โดย $P_n^m[\beta,D]$ และ $P_n[\beta,D]$ เท่ากับเซตจำกัดและเซตไม่จำกัดตามลำดับ โดยที่ n เป็นเลขชี้กำลังสูงสุด และ m เป็นเลขชี้กำลังต่ำสุด

ในระบบเลขฐานจำนวนเต็ม β ที่มีชุดตัวเลขอยู่ในรูป $C=\{c\in Z \mid 0\le c\le |\beta|-1\}$ เรียกว่า ชุดตัวเลขคาโนนิคอล (canonical digit set) ตัวอย่างเช่น สำหรับระบบเลขฐานสิบ จะได้ $\beta=10$ และชุดตัวเลขคาโนนิคอลคือ $\{c\in Z \mid 0\le c\le 9\}$

2.7 การแปลงแบบเชื่อมตรง (on-line conversion)

ระบบเลขคณิตแบบเชื่อมตรงถูกคิดค้นขึ้นเมื่อปี ค.ศ.1977 โดยเออเสกโกแวค และไทรเวดี [7] ซึ่งในการคำนวณเลขคณิตแบบเชื่อมตรงนี้ ระบบจำนวนที่ใช้คือ ระบบจำนวนซ้ำซ้อนแบบมีเครื่องหมายของอเวเซียนีส (Avizienis's signed-digit number system) [8]

แนวคิดของการคำนวณแบบเชื่อมตรงคือ การทำงานที่ทุกตัวดำเนินการกระทำไปในทิศทางเดียวกันแบบลำดับ (sequential) ผนวกเข้ากับ การทำงานแบบสายท่อ (pipeline) โดยอาศัยแนวคิดที่ว่า ตัวดำเนินการต่างๆ สามารถเริ่มต้นทำงานได้โดยไม่ต้องรอให้ตัวดำเนินการที่อยู่ในลำดับก่อนหน้าทำเสร็จเสียก่อน นอกจากนี้ การทำงานแบบเชื่อมตรงยังจำเป็นต้องใช้ระบบจำนวนซ้ำซ้อนด้วย และการคำนวณแบบเชื่อมตรง เป็นการคำนวณแบบลำดับเริ่มต้นจากดิจิตที่มีนัยสำคัญสูงสุด (most significant digit, MSD) ไปสู่ดิจิตที่มีนัยสำคัญต่ำสุด (least significant digit, LSD) การคำนวณจะกระทำทีละดิจิตจากซ้ายไปขวา

คุณสมบัติที่สำคัญอีกประการหนึ่งของเลขคณิตแบบเชื่อมตรงคือค่าความหน่วงเชื่อมตรง (on-line delay) δ ของตัวดำเนินการ ในบางกรณี การคำนวณแบบเชื่อมตรงไม่สามารถจะผลิตดิจิตแรกของคำตอบหรือจำนวนนำออก (output) ได้จากการคำนวณของดิจิตแรกของจำนวนนำเข้า (input) ได้เสมอไป การจะได้คำตอบจำเป็นต้องพิจารณาดิจิตของจำนวนนำเข้ามากกว่าหนึ่งดิจิตในการเริ่มต้นคำนวณ แต่ต่อจากนั้น การคำนวณสามารถทำได้ทีละดิจิต ในกรณีที่จำนวนของดิจิตที่ใช้เพื่อการผลิตดิจิตแรกของคำตอบเป็น $\delta+1$ ค่าความหน่วงเชื่อมตรงของตัวดำเนินการนั้นจะมีค่าเท่ากับ δ

จากงานวิจัย ของฟรูนี่ย์ และ อรรถสิทธิ์ สุรฤกษ์ [9] จะเห็นได้ว่าในการคำนวณแบบเชื่อมตรงสามารถทำได้แบบต่อเนื่องโดยจำเป็นต้องอาศัยระบบจำนวนซ้ำซ้อนแบบมีเครื่องหมาย เนื่องจากข้อดีของการคำนวณแบบเชื่อมตรงคือ การคำนวณสามารถทำได้โดยไม่จำเป็นต้องรอให้มีจำนวนนำเข้าเข้ามาทั้งหมดก่อนก็สามารถคำนวณหาจำนวนนำออกได้เลย ส่งผลให้เวลาที่ใช้มีความเร็วสูงขึ้น และผลลัพธ์ที่ได้สามารถนำไปคำนวณต่อได้เลย ทำให้การคำนวณอยู่ในรูปแบบการทำงานแบบสายท่อ ข้อดีอีกประการหนึ่งคือเมื่อนำวิธีการนี้มาทำให้เกิดผล (implement) ทรัพยากรที่ใช้ เช่น เรจิสเตอร์ (register) ไม่มีความจำเป็นต้องใช้มาก เนื่องจากดิจิตที่ใช้ในการคำนวณมีจำนวนน้อย ขึ้นอยู่กับค่าความหน่วงเชื่อมตรงที่กำหนด ดังนั้นการคำนวณแบบเชื่อมตรงนี้จึงสามารถประหยัดทรัพยากรลงได้มากทีเดียว ส่วนข้อเสียของการคำนวณแบบเชื่อมตรงคือ จำนวนดิจิตของจำนวนนำออกต้องเท่ากับจำนวนดิจิตของจำนวนนำเข้า ดังนั้นถ้าจะนำวิธีนี้มาใช้ในการทำให้เป็นบรรทัดฐานของจำนวนที่มีค่าน้ำหนักน้อยที่สุด ผลลัพธ์ที่ได้อาจไม่มีประสิทธิภาพที่ดี

2.8 การแทนฐานสองแบบมีเครื่องหมายในรูประหว่างกลาง (Intermediate Signed-Binary representation: ISB)

ความซ้ำซ้อน (redundant) เป็นคุณสมบัติสำคัญที่ทำให้ระบบจำนวนฐานสองแบบมีเครื่องหมายมีโอกาสแทนรูปจำนวนเต็มได้ด้วยน้ำหนักที่ต่ำ ซึ่งไอเอสบี (ISB) [10-13] เป็นวิธีการหนึ่งที่มีประสิทธิภาพในการเพิ่มความกำกวมให้กับระบบจำนวนฐานสอง โดยเมื่อระบบจำนวนฐานสองถูกเปลี่ยนให้อยู่ในรูปไอเอสบี จะมีลักษณะสำคัญดังนี้

1. จะไม่ปรากฏลำดับ $10...01$ หลังการแทนรูป
2. จะไม่ปรากฏลำดับ $\bar{1}0...0\bar{1}$ หลังการแทนรูป
3. จะไม่ปรากฏตัวเลขเดียวกันที่ไม่ใช่ศูนย์อยู่ติดกัน
4. บิตที่มีค่าน้ำหนักทางด้านซ้ายสุดจะมีค่าเป็นหนึ่ง และทางขวาสุดจะมีค่าเป็นลบหนึ่งเสมอ

ตัวอย่างที่ 2.6 *รูปแบบของไอเอสบี*

กำหนด $k = 53$ ซึ่งเขียนให้อยู่ในรูปจำนวนฐานสองแบบไม่มีเครื่องหมายคือ 110101 โดยจะมีรูปไอเอสบีได้คือ $10\bar{1}1\bar{1}1\bar{1}$ เนื่องจากความซ้ำซ้อนของระบบจำนวนฐานสองแบบมีเครื่องหมายทำให้สามารถเขียน k ในรูปอื่นคือ $100\bar{1}\bar{1}1\bar{1}$ ซึ่งรูปแบบดังกล่าวไม่ใช่ไอเอสบี □

2.9 การแลกเปลี่ยนกุญแจด้วยอีซีซี (ECC key exchange)

ตารางที่ 2.2 ขั้นตอนการสร้างกุญแจด้วยอีซีซี

1. ส่วนที่เป็นสาธารณะ (global public elements)	
$E_p(a,b)$ กลุ่มเส้นโค้งอิลลิปติกบนขอบเขตจำกัด F_p P จุดบนเส้นโค้งอิลลิปติกบนขอบเขตจำกัด F_p	
2. การสร้างกุญแจสาธารณะ (public key generation)	
ผู้ใช้ A ทำการสร้างกุญแจโดย เลือกจำนวนเต็ม k_A ทำการคำนวณกุญแจสาธารณะ $G_A = k_A P$	ผู้ใช้ B ทำการสร้างกุญแจโดย เลือกจำนวนเต็ม k_B ทำการคำนวณกุญแจสาธารณะ $G_B = k_B P$
3. การแจกจ่ายกุญแจสาธารณะ (public key distribution)	
ผู้ใช้ A ทำการส่ง G_A ให้ผู้ใช้ B	ผู้ใช้ B ทำการส่ง G_B ให้ผู้ใช้ A
4. การสร้างกุญแจลับ (secret key generation)	
Key = $k_A G_B$	Key = $k_B G_A$
5. ได้กุญแจที่ตกลงกันไว้คือ Key = $k_A k_B P$ $(G = kP)$	

จากตารางที่ 2.2 ถ้าระหว่างการแจกจ่ายกุญแจสาธารณะของผู้ใช้ A และ B นั้น หากสมมติว่า C เป็นผู้ไม่ประสงค์ดี ได้ทำการดักจับข้อมูล และสามารถที่จะขโมย G_A และ G_B ไปได้ก็เป็นการยากที่จะทราบได้ถึงค่าของ k ซึ่งในที่นี้คือ k_A และ k_B เนื่องจากติดตรงความซับซ้อนของปัญหาดิสครีทลอการิทึมของเส้นโค้งอิลลิปติกตามที่ได้อธิบายไว้ในหัวข้อ 2.4