2.13 เส้นโค้งอิลลิปติก

นิยามเส้นโค้งอิลลิปติก (Elliptic curve) เป็นเซตคำตอบของสมการที่อยู่ในรูป

$$y^2 = x^3 + ax + b \qquad (2.7)$$

ค่า $(a, b) \in R$ หรือ สัมประสิทธิ์เป็นจำนวนจริงและ $4a^3 + 27b^3 \neq 0$

การบวกบนเส้นโค้งอิลลิปติก

ถ้าให้ P และ Q เป็นจุดบนเส้นโค้งอิลลิปติกโดย $P = (x_1, y_1)$ และ $Q = (x_2, y_2)$ แล้ว $P + Q = (x_3, y_3)$

1.การบวกบนเส้นโค้งอิลลิปติกของจุด $P + Q$ ในกรณี $P \neq Q$ เส้นที่ลากผ่านจุด P และ Q สามารถแสดงได้โดยสมการ

$$y = m(x - x_1) + y_1 \qquad (2.8)$$

จากสมการ m เป็นค่าความชัน การหาผลเฉลยของ x_3 เป็นการหาจุดที่สะท้อนจากจุดตัดที่เหลือของเส้นตรงคือจุดตัด x_1และx_2 แทนค่าสมการเส้นตรง (2.8) ลงสมการเส้นโค้งอิลลิปติก (2.7)

$$(m(x - x_1) + y_{\ 1})^2 = x^3 + ax + b$$

ได้ว่า

$$x^3 - m^2x^2 + (a + 2m^2x_1 + 2my_{\ 1})x + (b - m^2x_1^2 + 2x_1y_1 + y_1^2) = 0 \quad (2.9)$$

จากสมการ $x^3 + ax + b$ ที่มีผลเฉลย $x_1, x_2,$ และ x_3 คือ

$$x^3 + ax + b = (x - x_1)(x - x_2)(x - x_3)$$

$$= x^3 - (x_1 + x_2 + x_3)x^2 - (x_1x_2 + x_1x_3 + x_2x_3)x - (x_1x_2x_3)$$

ดังนั้นจากสมการ (2.9) เทียบสัมประสิทธิ์ที่ x^2 ได้ว่า

$$x_3 = m^2 - x_1 - x_2$$

เนื่องจากผลเฉลย $P + Q$ ค่าผลลัพธ์ของจุด (x_3, y_3) เป็นจุดสะท้อนจากจุดตัดของเส้นตรงในสมการ (2.8) ที่สมมาตรในแกน x ดังนั้น

$$y_3 = m(x_1 - x_3) - y_1$$

2.การบวกบนเส้นโค้งอิลลิปติกของจุด $P + Q$ เมื่อ $P = Q$ ในกรณีนี้จุด $(x_1, y_1) = (x_2, y_2)$ ค่าความชัน m หาได้โดยการอนุพันธ์สมการเส้นโค้งอิลลิปติก (2.7)

$$\frac{dy^2}{dx} = \frac{d}{dy}(x^3 + ax + b)$$

$$2y\frac{dy}{dx} = 3x_1^2 + a$$

$$m = \frac{dy}{dx} = \frac{3x_1^2+a}{2y}$$

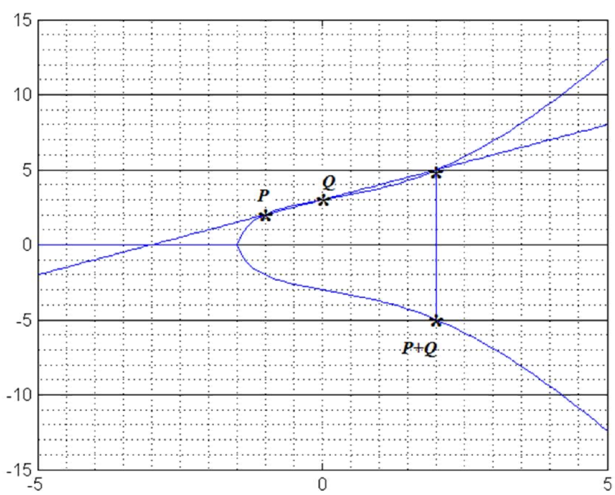
ดังนั้นการบวกบนเส้นโค้งอิลลิปติก $P + Q = (x_3, y_3)$ แสดงได้

$$x_3 = m^2 - x_1 - x_2 \qquad (2.10.1)$$

$$y_3 = m(x_1 - x_3) - y_1 \qquad (2.10.2)$$

m เป็นค่าความชันหาได้จาก

$$m = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{ถ้า } P \neq Q \\ \frac{3x_1^2+a}{2y} & \text{ถ้า } P = Q \end{cases}$$



รูปที่ 2.1 $P + Q$ *ในกรณี* $P \neq Q$

ตัวอย่างที่ 2.29 สมการเส้นโค้งอิลลิปติก $y^2 = x^3 + 4x + 9$ โดย $P = (-1,2)$ และ $Q = (0,3)$ หาผลบวกของ $P + Q$ จากรูปที่ 2.1 เส้นตรงที่ผ่านจุด P, Q มีสมการ $y = x + 3$ จาก

$$y^2 = x^3 + ax + b$$
$$(x + 3)^2 = x^3 + 4x + 9$$
$$x^3 - x^2 - 2x = 0$$

ผลเฉลยของ x คือ

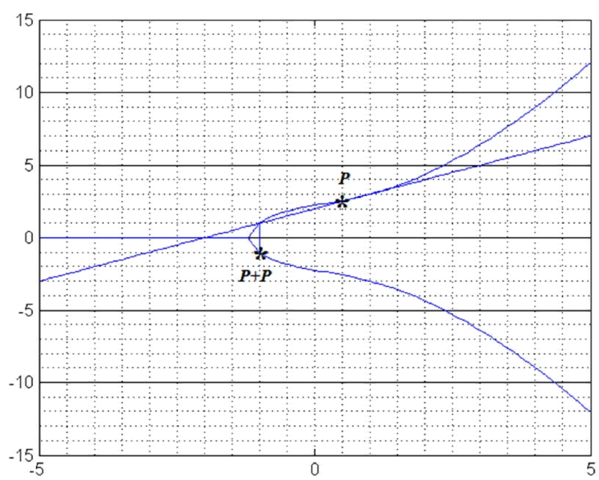
$$x^3 - x^2 - 2x = x(x+1)(x-2)$$

จากจุด P, Q ที่ $x_1 = -1, x_2 = 0$ ดังนั้น $x_3 = 2$ และสมการเส้นตรงที่ผ่านจุด x คือ $y = x + 3 = 5$ ที่จุด y_3 เป็นจุดที่สะท้อนจุดตัดของเส้นตรงกับเส้นโค้งอิลลิป ติกที่สมมาตรบนแกน x ดังนั้น $y_3 = -5$ ในกรณีหาผลบวกโดยใช้สมการ (2.10.1) และ (2.10.2) ผลเฉลย $(x_1, y_1) = (-1,2)$ และ $(x_2, y_2) = (0,3)$

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{3-2}{0-(-1)} = 1$$

$$x_3 = m^2 - x_1 - x_2 = (1)^2 - (-1) - (0) = 2$$

$$y_3 = m(x_1 - x_3) - y_1 = 1(-1-2) - 2 = -5$$



รูปที่ 2.2 $P + Q$ *ในกรณี* $P = Q$

ตัวอย่างที่ 2.30 สมการเส้นโค้งอิลลิปติก $y^2 = x^3 + 3x + 5$ โดย $P = (1,3)$ หา $P + P$ จากรูปที่ 2.2 ค่าความชันที่จุด P หาได้จาก

$$m = \frac{3x_1^2 + a}{2y} = \frac{3(1)^2 + 3}{2(3)} = 1$$

$$x_3 = m^2 - x_1 - x_2 = (1)^2 - (1) - (1) = -1$$

$$y_3 = m(x_1 - x_3) - y_1 = 1(1-(-1)) - 3 = -1$$

ข้อสังเกตเพิ่มเติมในการบวกบนเส้นโค้งอิลลิปติก

1. การบวก $P+Q$ เมื่อ P และ Q อยู่บนเส้นโค้งตรงข้ามกันสมมาตรบนแกน x หรือ $Q=-P$ ในกรณีนี้ค่าความชันของเส้นตรงที่ตัดผ่านจุด P และ Q มีค่าเป็น ∞ จากสมการ (2.10.1) และ (2.10.2) ทำให้ค่า $x_3 = y_3 = \infty$ หรือ $P+Q$ มีผลลัพธ์ที่จุด ∞ หรือเขียนได้ $P+(-P)=O_\infty$ โดย O_∞ แทนจุดที่ ∞
2. การบวก $P+P$ เมื่อ P อยู่บนจุดยอดเส้นโค้ง ในกรณีนี้ค่าความชันของเส้นตรงที่ตัดผ่านจุด P เป็นเส้นสัมผัสเส้นโค้งมีค่าเป็น ∞ เช่นเดียวกับกรณีผ่านมาดังนั้น $P+P$ จึงมีผลลัพธ์ที่เป็น ∞ แต่เนื่องจาก P เป็นจุดเดียวกันเขียนได้ $P+O_\infty = P$

ทฤษฎีบท 2.6 ถ้า E เป็นเส้นโค้งอิลลิปติกการบวกมีสมบัติเป็นกรุปโดย
1. $P+O_\infty = O_\infty + P = P$ สำหรับทุกจุด P บน E (มีเอกลักษณ์)
2. $P+(-P)=O_\infty$ สำหรับทุกจุด P บน E (มีตัวผกผัน)
3. $(P+Q)+R = P+(Q+R)$ สำหรับทุกจุด P, Q, R บน E (เปลี่ยนหมู่)
4. $P+Q=Q+P$ สำหรับทุกจุด P, Q บน E (สลับที่)

เส้นโค้งอิลลิปติกภายใต้การมอดุโลจำนวนเฉพาะ
นิยาม ถ้า P เป็นจำนวนเฉพาะ $P > 3$ และ $(a,b) \in Z_p$ หรือเป็นจำนวนเต็ม
โดย $4a^3 + 27b^3 \neq 0 \ mod \ p$ แล้ว เส้นโค้งอิลลิปติกภายใต้การมอดุโลจำนวนเฉพาะเป็นเซตของจุด (x,y) ที่อยู่ในระนาบ Z_p ที่ทำให้สมการ

$$y^2 \equiv x^3 + ax + b \ mod \ p$$

เป็นจริง

ตัวอย่างที่ 2.31 แสดงจุด (x,y) ทั้งหมดบนเส้นโค้งอิลลิปติก $y^2 \equiv x^3 + x + 1 \ mod \ 23$
จากสมการเป็นการมอดุโลภายใต้ $p \equiv 3 mod \ 4$ ดังนั้นจากทฤษฎีบทของออยเลอร์ ถ้าหาก $a \ mod \ p$ และ a เป็นค่าส่วนค้างกำลังสองของ p แล้วผลเฉลยของ $\sqrt{a} mod \ p$ หาได้จาก $a^{(p+1)/4} mod \ p$ จุดบนเส้นโค้ง $y^2 \equiv x^3 + x + 1 \ mod \ 23$ แสดงได้

x	$y^2 \equiv x^3 + x + 1 \ mod \ 23$	QR	y	(x,y)
0	0	yes	1,22	(0,1), (0,22)
1	3	yes	7,16	(1,7), (1,16)
2	11	no	$-$	$-$
3	8	yes	10,13	(8,10), (8,13)
4	0	no	$-$	(4,0)

5	16	yes	4,19	(5,4), (5,19)
6	16	yes	4,19	(6,4), (6,19)
7	6	yes	11,12	(7,11), (7,12)
8	15	no	−	−
9	3	yes	7,16	(9,7), (9,16)
10	22	no	−	−
11	9	yes	3,20	(11,3), (11,20)
12	16	yes	4,19	(12,4), (12,19)
13	3	yes	7,16	(9,7), (9,16)
14	22	no	−	−
15	10	no	−	−
16	19	no	−	−
17	9	yes	3,20	(17,3), (17,20)
18	9	yes	3,20	(18,3), (18,20)
19	2	yes	5,18	(19,5), (19,18)
20	17	no	−	−
21	14	no	−	−
22	22	no	−	−

ทฤษฎีบท 2.7 จุดบนเส้นโค้งอิลลิปติก E รวมทั้งจุด O_∞ มีสมบัติเป็นกรุปวัฏจักรย่อยหรือทุกจุดอาจเป็นกรุปวัฏจักรขึ้นอยู่กับเงื่อนไขของจุดที่เป็นตัวกำเนิด

ตัวอย่างที่ 2.32 จากจุด (x, y) ของเส้นโค้งอิลลิปติก $y^2 \equiv x^3 + x + 1 \ mod\ 23$
ในตัวอย่างที่ 2.31 จำนวนจุด (x, y) ทั้งหมดรวมจุดที่ O_∞ มีจำนวน 28 จุด
ถ้าให้ $P = (3,10)$ เป็นจุดบนเส้นโค้งอิลลิปติกแล้วจุด $2P$ หาได้จาก

$$2P = P + P = (x_3, y_3)$$

$$m = \frac{3x_1^2+a}{2y} modp = \frac{3(3)^2+1}{2(10)} = \frac{5}{20} mod23 = 6$$

$$x_3 = (m^2 - x_1 - x_2)modp = ((6)^2 - (3) - (3))mod23 = 7$$

$$y_3 = (m(x_1 - x_3) - y_1)modp = (6(3 - 7) - 10)mod23 = 12$$

$$2P = (x_3, y_3) = (7,12)$$

ที่จุด $3P$

$$3P = 2P + P$$

$$m = \frac{y_2-y_1}{x_2-x_1} modp = \frac{12-10}{7-3} = \frac{1}{2} mod23 = 12$$

$$x_3 = (m^2 - x_1 - x_2)\ modp = ((12)^2 - (3) - (7))mod23 = 19$$

$y_3 = (m(x_1 - x_3) - y_1) mod p = (1(3 - 19) - 10) mod 23 = 5$

$3P = (x_3, y_3) = (19,5)$

สำหรับจุด

$4P = 3P + P = (17,3)$

$5P = 4P + P = (9,16)$

$6P = 3P + P = (12,4)$

$7P = 6P + P = (11,13)$

$8P = 7P + P = (13,16)$

$9P = 8P + P = (0,1)$

$10P = 9P + P = (6,4)$

$11P = 10P + P = (18,20)$

$12P = 11P + P = (5,4)$

$13P = 12P + P = (1,7)$

$14P = 13P + P = (4,0)$

$15P = 14P + P = (1,16)$

$16P = 15P + P = (5,19)$

$17P = 16P + P = (18,3)$

$18P = 17P + P = (6,19)$

$19P = 18P + P = (0,22)$

$20P = 19P + P = (13,7)$

$21P = 20P + P = (11,20)$

$22P = 21P + P = (12,19)$

$23P = 22P + P = (9,7)$

$24P = 23P + P = (17,20)$

$25P = 24P + P = (19,18)$

$26P = 25P + P = (7,11)$

$27P = 26P + P = (3,13)$

ที่จุด $28P = 27P + P$

$$m = \frac{y_2 - y_1}{x_2 - x_1} modp = \frac{13-10}{3-3} = \infty$$

$x_3 = (m^2 - x_1 - x_2)\ modp = \infty$

$y_3 = (m(x_1 - x_3) - y_1) modp = \infty$

$28P = (x_3, y_3) = O_\infty$

ที่จุด $29P = 28P + P = O_\infty + P = P$

ที่จุด $30P = 29P + P = P + P = 2P$

อันดับและจำนวนจุดของเส้นโค้งอิลลิปติกภายใต้การมอดุโลจำนวนเฉพาะ

จากการบวกของจุดเส้นโค้งอิลลิปติกภายใต้การมอดุโลจำนวนเฉพาะในตัวอย่างที่ 2.32 เป็นการคูณจุดด้วยค่าคงที่ หลังจาก $28P$ มีค่าเท่ากับ O_∞ แล้วค่าต่อไปซ้ำกับค่า $P, 2P..3P$ ตามลำดับ ดังนั้นอันดับของสมการ $y^2 \equiv x^3 + x + 1\ mod\ 23$

มีขนาดเท่ากับจำนวนจุดทั้งหมดคือ 28 โดยค่า P เริ่มต้นที่ทำให้มีขนาดลำดับเท่ากับจำนวนจุดนี้เรียกว่าตัวกำเนิดแบบปฐมภูมิซึ่งทำให้จุดทั้งหมดบนเส้นโค้งอิลลิปติกเป็นกรุปวัฏจักร โดยตัวกำเนิดที่ทำให้จุดเป็นกรุป $E(Z_p)$ แสดงได้

ลำดับ	จุดเริ่มต้น
28	$(0,1), (0,22), (1,7), (1,16), (3,10), (3,13)$ $(9,7), (9,16)(18,3), (18,20)(19,5), (19,18)$
14	\\$(6,4), (6,19), (7,11), (7,12), (12,4), (12,19)$
7	$(5,4), (5,19)(13,7), (13,16)(17,3), (17,20)$
4	$(11,3), (11,20)$
1	$(4,0)$

สำหรับจุดบน $f(x) = y^2 \equiv x^3 + ax + b\ mod\ p$ เกิดขึ้นเมื่อ

1. $f(x)$ เป็นค่าส่วนค้างกำลังสองของ p ทำให้มีจุดสองจุด $(x, \pm y)$
2. $f(x)$ หาร p ลงตัวทำให้มีจุดหนึ่งจุดที่ $(x, 0)$

ดังนั้นจำนวนจุดหรือ $\# E(a,b)$ ของ $f(x)$ มีขนาด

$$\# E(a,b) = \sum_{i=0}^{p-1}(1 + \frac{f(x)}{p})$$

ถ้าหาก p มีขนาดใหญ่มากๆแล้ว การหาจำนวนจุดประมาณได้จากทฤษฎีของ Hasse โดยขอบเขตของจุดคือ

$$p + 1 - 2\sqrt{p} \leq \# E(a,b) \leq p + 1 + 2\sqrt{p}$$

หรือ

$$\# E(a,b) = p + 1 + t$$

โดย $|t| \leq 2\sqrt{p}$

ในกรณี $p \equiv 2mod3$ และ $a = 0$ กรุปของ $E_p(0,b)$ เป็นกรุปวัฏจักรมีขนาดอันดับเท่ากับ $p + 1$

ในกรณี $p \equiv 3mod4$ และ $b = 0$ ค่า a เป็นส่วนตกค้างของ p กรุปของ $E_p(a,0)$ เป็นกรุปวัฏจักรมีขนาดอันดับเท่ากับ $p + 1$

5.8 ระบบรหัสลับแบบกุญแจสาธารณะใช้เส้นโค้งอิลลิปติก

การเข้ารหัสลับแบบเส้นโค้งอิลลิปติกเสนอโดย [7,8] อาศัยหลักการของสมการเส้นโค้งอิลลิปติกภายใต้มอดุโลจำนวนเฉพาะ pคือ $f(x) = y^2 \equiv x^3 + ax + b \; mod \; p$ ที่มีลำดับขนาด N เส้นโค้งอิลลิปติกสามารถใช้เป็นฟังก์ชันทางเดียวที่เป็นปัญหาเส้นโค้งอิลลิปติกดิสครีตลอการิทึม(Elliptic Curve Discrete Logarithm Problem:

ECDLP) ได้ถ้าค่า p มีขนาดใหญ่มากๆ ค่า P และ Q เป็นจุดบนเส้นโค้งอิลลิปติกหรือเป็นกรุป $E(Z_p)$ และ d เป็นจำนวนเต็ม $d \in (0, n-1)$ จาก

$$Q = dP = \underbrace{P + P + P \dots . + P}_{d \; time}$$

ถ้าให้ d และจุด P แล้วการหาจุด Q จากการคูณจำนวนเต็ม d กับจุด P กระทำได้ง่าย แต่ถ้าหากให้จุด P และจุด Q แล้ว การหาค่า d กระทำได้ยาก

การหา dP หรือการคูณจุด (point multiplier) กระทำได้โดยขั้นตอนวิธีการเพิ่มสองเท่าและการบวก (Double and Add) โดยการแทนค่า d อยู่ในรูป

$$d = \sum_{i=0}^{t-1} d_i 2^i \qquad (5.11)$$

การคูณค่า d และ P

$dP = \left(\sum_{i=0}^{t-1} d_i 2^i\right) P = d_{t-1}2^{t-1}P + d_{t-2}2^{t-2}P + d_1 2P + d_0 P$ (5.12)

ขั้นตอนวิธีของสมการ (5.12) แสดงได้

```
Double and Add (input d, P,output Q )
. Q = O∞
 For  i = t − 1  to 0
   Q = 2Q
.   IF  d_i = 1  Then Q = Q + P
  End
 Return Q
```

ตัวอย่างที่ 5.9 แสดงการคูณ $Q = 26P$

$d = 26 = d_4d_3d_2d_1d_0 = (11010)_2$

$i = 4$	$d_4 = 1$	$Q = O_\infty$	$Q = O_\infty + P = P$
$i = 3$	$d_3 = 1$	$Q = 2Q = 2P$	$Q = Q + P = 2P + P = 3P$
$i = 2$	$d_2 = 0$	$Q = 2Q = 6P$	
$i = 1$	$d_1 = 1$	$Q = 2Q = 12P$	$Q = Q + P = 12P + P = 13P$
$i = 0$	$d_0 = 0$	$Q = 2Q = 26P$	

ขนาดความซับซ้อนของขั้นตอนวิธีการขึ้นอยู่กับค่า d ที่มีขนาดสูงสุดซึ่งไม่เกินขนาดของจำนวนเฉพาะ p ที่มีขนาด k บิต การวนกระทำประกอบด้วยการยกกำลังและการบวก ดังนั้นค่าความซับซ้อนมีขนาด $O(k^3)$ ในขณะที่การหาค่า d จากการให้จุด P และจุด Q การหาที่เป็นไปได้ทั้งหมดต้องกระทำ $n-1$ ค่า ซึ่งมีขนาดเท่ากับจำนวนเฉพาะ p ดังนั้นความซับซ้อนขั้นตอนวิธีของการหาค่า d เป็นเอกซ์โพเนนเชียลเท่ากับ $O(2^k)$

ในทางปฏิบัติ NIST [9] ได้แนะนำเส้นโค้งอิลลิปติกภายใต้มอดุโลจำนวนเฉพาะขนาดใหญ่คือ $E: y^2 \equiv x^3 - 3x + b \bmod p$ ค่า p สร้างจากจำนวนเฉพาะแบบแมร์แซน ที่มีรูปแบบ $2^m \pm 2^n + 1$ มีขนาดบิตต่าง ๆดังนี้

192 บิต $p = 2^{192} - 2^{64} - 1$

224 บิต $p = 2^{224} - 2^{96} + 1$

256 บิต $p = 2^{256} - 2^{224} + 2^{192} - 2^{96} - 1$

521 บิต $p = 2^{521} + 1$

ความสอดคล้องระหว่างกรุป Z_p^* และกรุป $E(Z_p)$แสดงได้ตามตาราง

กรุป	Z_p^*	$E(Z_p)$
สมาชิก	จำนวนเต็ม $\{1,2,.p-1\}$	จุด(x,y) บน E รวมทั้งจุด O_∞
การกระทำ	การคูณภายใต้การมอดุโล	การบวกจุด
ปัญหา *DLP*	ให้ $g \in Z_p^*, X = g^x mod p$ หา x	ให้$P \in E(Z_p), Q = dP$หา d

5.8.1 การตกลงสร้างกุญแจ Diffie-Hellman ใช้เส้นโค้งอิลลิปติก

การตกลงกุญแจแบบนี้เป็นหนึ่งในมาตรฐานของ IEEE[9] การสร้างกุญแจระหว่าง A และ B ค่าพารามิเตอร์สาธารณะของทั้งสองคือเส้นโค้งอิลลิปติกและจุดบนเส้นโค้ง

$$E: y^2 \equiv x^3 + ax + b \ mod \ p$$

p เป็นจำนวนเฉพาะ p มีขนาดใหญ่และจุด $P = (x,y)$ เป็นสมาชิกปฐมฐานให้กำเนิดสมาชิกทั้งหมดเป็นกรุปวัฏจักรมีลำดับขนาด $\#E - 1$

ในการตกลงกุญแจ

1. ที่ A ทำการเลือกค่าลับ $n_A \in \{1,2,.\#E-1\}$ และที่ B ทำการเลือกค่าลับ $n_B \in \{1,2,.\#E-1\}$
2. A คำนวณ $Q_A = n_A P$ ส่งให้ B และ B คำนวณ $Q_B = n_B P$ ส่งให้ A
3. ค่ากุญแจกุญแจเซสชัน K_{AB} ของ A และ B หาได้โดย

ที่ A คำนวณกุญแจ $K_{AB} = n_A Q_B = n_A n_B P$ และ B คำนวณกุญแจ $K_{AB} = n_B Q_A = n_B n_A P$

ตัวอย่างที่ 5.10 A และ B ทำการตกลงสร้างกุญแจโดยใช้เส้นโค้งอิลลิปติก $E: y^2 \equiv x^3 + 2x + 2 \ mod \ 17$ เลือกจุดที่เป็นสมาชิกปฐมฐาน $P = (5,1)$

จากตัวกำเนิดทำการหาจุดทั้งหมดบนเส้นโค้งได้คือ

$P = (5,1)$	$11P = (13,10)$
$2P = (6,3)$	$12P = (0,11)$
$3P = (10,6)$	$13P = (16,4)$
$4P = (3,1)$	$14P = (9,1)$
$5P = (9,16)$	$15P = (3,16)$
$6P = (16,13)$	$16P = (10,11)$
$7P = (0,6)$	$17P = (6,14)$
$8P = (13,7)$	$18P = (5,16)$

$9P = (7,6)$ $\qquad$ $19P = O_\infty$
$10P = (7,11)$

ในการตกลงสร้างกุญแจ

1. ที่ A ทำการเลือกค่าลับ $n_A = 3$ และที่ B ทำการเลือกค่าลับ $n_B = 10$

2. A คำนวณ $Q_A = n_A P = 3P = 3(5,1) = (10,6)$ ส่งให้ B และ

B คำนวณ $Q_B = n_B P = 10P = 10(5,1) = (7,11)$ ส่งให้ A

3. ค่ากุญแจกุญแจเซสชัน K_{AB} ของ A และ B หาได้จาก

ที่ A คำนวณกุญแจ $K_{AB} = n_A Q_B = 10(3P) = 10(10,6) = (13,10)$

และ B คำนวณกุญแจ $K_{AB} = n_B Q_A = 3(10P) = 3(7,11) = (13,10)$

ข้อสังเกต $K_{AB} = 3(10P) = 10(3P) = 30P$ ด้วยคุณสมบัติที่ตัวกำเนิด $P = (5,1)$ เป็นการสร้างกรุปวัฏจักรซึ่งขนาดลำดับเท่ากับ19 โดยจุดที่ $20P = P$ และ$21P = 2P$ ตามลำดับแล้ว ดังนั้นที่จุด $30P = 11P$