網路安全的理論與實務

楊中皇 著

第六章 橢圓曲線密碼系統

http://crypto.nknu.edu.tw/textbook/

金禾圖書

伴 您 學 習 成 長 的 每 一 天

金禾資訊

第六章 橢圓曲線密碼系統

– 橢圓曲線密碼系統(ECC)簡介
– 橢圓曲線點乘法
– 橢圓曲線數位金鑰交換演算法(ECDH)
– 橢圓曲線數位簽章演算法(ECDSA)
– 橢圓曲線參數

橢圓曲線密碼系統(ECC)

- 橢圓曲線密碼系統（elliptic curve cryptosystem， ECC）
- 西元1985年由Koblitz與Miller各別提出的新型公開金鑰密碼學技術
- 國際標準如ISO 11770-3、ANSI X9.62、IEEE P1363 、FIPS 186-2等
- 橢圓曲線的技術不只能應用在密碼學加解密、數位簽章、金鑰交換等，也能應用於大數分解(factorization)與質數判斷(primality testing)
- 在相同的安全強度下，ECC的密碼學金鑰長度可遠較其他公開金鑰密碼系統(如RSA)小且處理速度較快，意即ECC每個金鑰位元所能提供的安全性遠超過其他公開金鑰密碼系統，這使得ECC非常適合利用於如智慧卡或手機無線行動裝置等記憶體有限的環境中

相同安全性時RSA與ECC金鑰長度比較

安全性 / 演算法	2^{80}	2^{112}	2^{128}	2^{192}	2^{256}
RSA長度(位元)	1024	2048	3072	7680	15360
ECC長度(位元)	160	224	256	384	512
RSA:ECC金鑰長度比	6:1	9:1	12:1	20:1	30:1

橢圓曲線

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- 滿足上述方程式的所有點(x, y)及一個無限遠點(point at infinity)∞所形成的集合，其中座標x與y屬於某個有限體(finite field)
- 橢圓曲線的級數(order)為曲線上包含無限遠點的所有點的數目。
- 有限體為質數體(prime field， GF(p))、二元體(binary field ，GF(2*n*))、最佳擴展體(optimal extension field ，GF (*pn*))等三種
- Hasse定理：如果採用有限體GF(q)則橢圓曲線的級數滿足

$$q+1-2\sqrt{q} \le order \le q+1+2\sqrt{q}$$

橢圓曲線範例一

- 質數體為GF(5)且橢圓曲線公式

  $y^2 = x^3 + x + 1$

- 這個橢圓曲線上的點，除無限遠點∞外，另有8個點：(0,1),(0,4),(2,1),(2,4),(3,1),(3,4),(4,3),(4,2)點的座標值屬於GF(5) 。
- 因為共有9點，所以此曲線的級數(order)為9。

橢圓曲線範例二

- 質數體爲GF(11)且橢圓曲線公式

  $y^2 = x^3 + x + 1$

- 這個橢圓曲線上的點，除無限遠點∞外，

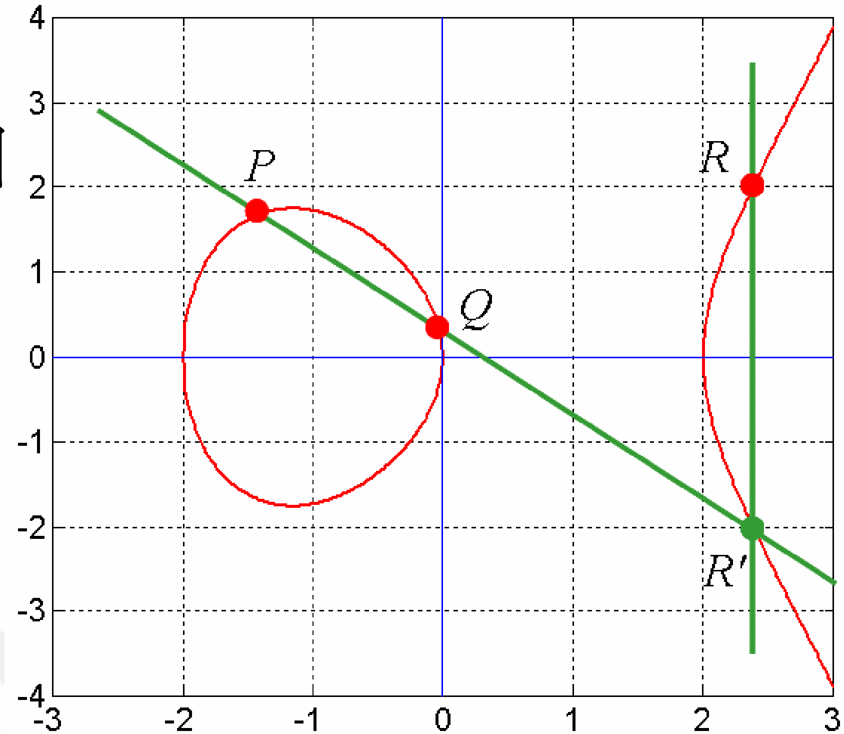
  另有13個點：

  (0,1),(0,10),(1,6),(1,5),(2,0),(3,8),(3,3),(4,6),(4,5),(6,6),(6,5),(8,2),(8,9) 點的座標值屬於GF(11) 。

- 因爲共有14點，所以此曲線的級數(order)爲14。

橢圓曲線加法()

- 幾何上如果要計算相異兩點*P*與*Q*的和，則我們先找出通過這兩點的直線，然後找出這條直線與橢圓曲線相交的第三點，再將此點對*x*軸做鏡射得到和。如果橢圓曲線上的某兩點共線的話，兩點相加之和就是∞。



橢圓曲線加法公式(質數體)

- 若$P = (x_1, y_1)$與$Q = (x_2, y_2)$爲橢圓曲線上的任意兩點，但$P \neq \infty \neq Q$，且選取質數體(此時橢圓曲線方程式爲 $y^2 = x^3 + ax + b$)，則我們有下列兩點加法的運算規則：
- 1. $P + \infty = \infty + P = P$
- 2. $P + (-P) = (x_1, y_1) + (x_1, -y_1) = \infty$
- 3. $P + Q = (x_3, y_3)$,

$$x_3 = \lambda^2 - x_1 - x_2 ,\ y_3 = \lambda (x_1 - x_3) - y_1,$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{如果 } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & \text{如果 } P = Q \end{cases}$$

橢圓曲線加法公式(二元體)

- 若$P = (x_1, y_1)$與$Q = (x_2, y_2)$爲橢圓曲線上的任意兩點，但$P \neq \infty \neq Q$，且選取二元體(此時橢圓曲線方程式爲 $y^2 + xy = x^3 + ax^2 + b$)，則規則3：
- $P + Q = (x_3, y_3)$,

$$x_3 = \begin{cases} \lambda^2 + \lambda + x_1 + x_2 + a & \text{如果} P \neq Q \\ \lambda^2 + \lambda + a & \text{如果} P = Q \end{cases}$$

$$y_3 = \lambda\,(x_1 + x_3) + x_3 + y_1$$

$$\lambda = \begin{cases} \dfrac{y_2 + y_1}{x_2 + x_1} & \text{如果} P \neq Q \\ x_1 + \dfrac{x_1}{y_1} & \text{如果} P = Q \end{cases}$$

橢圓曲線點的級數

- 加法公式的計算(加法、減法、乘法、除法/反元素)須在相關的有限體進行，若選取質數體時僅需進行模算術(modular arithmetic)，若選取二元體則需進行多項式計算(polynomail arithmetic)。
- 點乘法計算$k \bullet P$，其中k為正整數而P為橢圓曲線上的一個點
- 如果橢圓曲線上的一個點P我們找到最小的正整數n滿足$n \bullet P = \infty$ (無限遠點)，則n稱為點P的級數(order)，橢圓曲線上點的級數一定是曲線級數的因數。

質數體橢圓曲線加法範例一

- 質數體為GF(5)且橢圓曲線公式$y^2 = x^3 + x + 1$
- G=(0,1), 2G= (4,2), 3G=2G +G=(4,2), 4G=(3,4)，5G=(3,1)，6G=(2,4)，7G=(4,3)，8G=(0,4)，9G=∞。因為G =(0,1)時，9G=∞，所以此點G的級數為9。
- 若我們選G=(2,1)，則2G=(2,4)，3G=∞。因為G=(2,1)時，3G=∞，所以此點G的級數為3。

質數體橢圓曲線加法範例二

金禾資訊 伴您學習成長的每一天

- 質數體爲GF(11)且橢圓曲線公式$y^2 = x^3 + x + 1$
- 若我們選G=(0,1)，利用公式(6.5)計算，則我們有2G=(3,3)，3G=(6,6)， 4G=(6,5)， 5G=(3,8)，6G=(0,10)， 7G== ∞。因爲G=(0,1)時，7G= ∞，所以此點G的級數爲7。

Mathematica

- 橢圓曲線加法的Mathematica程式

```
If [Mod[x1 - x2, p] == 0,
    If [Mod[y1 + y2, p] == 0,
        slope = Mod[(3 x1^2 + g2) PowerMod[2 y1, -1, p], p]
    ],
    slope = Mod[(y2 - y1) PowerMod[x2 - x1, -1, p], p]
];
x3 =    Mod[slope^2 - x1 - x2, p];
y3 =    Mod[slope (x1-x3) - y1, p];
```

橢圓曲線密碼系統的實現的考慮

- 1. 有限體的選擇
- 2. 橢圓曲線的挑選
- 3. 有限體元素的運算(加法、減法、乘法、除法/反元素)
- 4. 橢圓曲線點的運算(加法、減法、乘法)

由左向右二元演算法計算 k • P

$$k \bullet P = \overbrace{P + P + \ldots + P}^{k\text{個點相加}} \qquad k = \sum_{i=0}^{t-1} k_i 2^i$$

Step 1. $Q \leftarrow \infty$ Step 2. for $i \leftarrow t\text{-}1$ downto 0 do $Q \leftarrow Q + Q$ If $k_i = 1$ then $Q \leftarrow Q + P$

圖6.4：由左向右二元演算法計算$k \bullet P$

參考資料

1. 楊中皇，橢圓曲線密碼系統軟體實現技術之探討，*資訊安全通訊*，第十一卷第一期，頁15~25，2005年1月。
2. ANSI X9.62, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 1998.
3. D.V. Bailey and C. Paar, "Efficient arithmetic in finite field extensions with applications in elliptic curve cryptograph," *J. Cryptology*, Vol. 14, No. 3, 2001, pp. 153-176.
4. D.M. Bressoud and S. Wagon, *A Course in Computational Number Theory*, Key College Publishing, 2000.
5. W. Dai, Crypto++ library, http://www.eskimo.com/~weidai/cryptlib.html
6. D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2004.
7. D. Johnson and A. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," Technical Report CORR 99-34, Centre for Applied Cryptographic Research, University of Waterloo, August 1999. http://www.cacr.math.uwaterloo.ca/ techreports/1999/corr99-34.pdf
8. LiDIA, http://www.informatik.tu-darmstadt.de/TI/LiDIA/
9. A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer, 1993.
10. NIST, *Digital Signature Standard (DSS)*, FIPS 186-2, October 2001, http://csrc.nist.gov/ publications/fips/ fips186-2/fips186-2-change1.pdf
11. NIST, *Recommendation on Key Management*, DRAFT Special Publication 800-57, J anuary 2003, http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf
12. PARI/GP, http://pari.math.u-bordeaux.fr/
13. J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.
14. S. Wolfram, *Mathematica Book*, 5th ed., Wolfram Research, Inc., 2003.