東　海　大　學
應　用　數　學　研　究　所
碩　士　論　文

橢圓曲線版的ElGamal數位簽署及其變形

指導教授：沈淵源

研究生：林文儀

中華民國九十二年七月

橢圓曲線版的ElGamal數位簽署及其變形

研　究　生：林文儀　　Student：Wen-Yi Lin

指 導 教 授：沈淵源　　Advisor：Yuan-Yuan Shen

東　海　大　學

應　用　數　學　研　究　所

碩　士　論　文

A Thesis

Submitted to the Institute of Applied Mathematics

College of Science

Tunghai University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Applied Mathematics

June 2003

Taichung, Taiwan, Republic of China.

中華民國九十二年七月

摘　要

本篇論文的主要目的在探討橢圓曲線版的數位簽署，並採用ElGamal公開鑰匙密碼系統來對此橢圓曲線加以簽署，以及改良的方法，並且對此橢圓曲線同步進行加密且簽署的過程，來增加橢圓曲線密碼系統的變化。如此一來，橢圓曲線密碼系統不再是那樣的單調，可依需要來做不同的變化，更能提供給大家一個新的思考方向。

Abstract

In this thesis, we are concerned with the elliptic curves digital signature, and adopt ElGamal public key cryptosystem to come the elliptic curves signature, there are various (better) ways adding to this elliptic curves synchronize encryption and signature process. Therefore, the elliptic curves cryptosystem would not be as monotonous; instead, It can be altered depending on different necessities; moreover, it provides everyone a new way of thinking.

目　　錄

第一章

密碼系統簡介

1.1 密碼系統

早在人類發明電腦之前，資訊安全就是人類社會一個重要的議題。但隨著電腦與網路的發展，越來越多的資訊透過電子型態進行交換，而電腦網路的開放性引發了許多資訊安全上的問題，因此資訊安全也越來越受到重視。

在古希臘羅馬時代，人們就使用了密碼的技術。當時使用的方法很簡單，將原始的文件資料明文中每個字母向右移動 (或迴轉) 三個位置，也就是 A 變成 D，B 變成 E，而 X 變成 A。經過這樣的轉換後資料就成了密文，接收資

料的人再將密文反向運算，即可得出原始的文件內容。不管明文或密文，其組成最小單位我們稱之爲信息單元(Message unit)。將明文的信息單元轉換爲密文的信息單元我們稱之爲加密(Enciphering)，而其逆過程則稱之爲解密(Deciphering)。我們可將整個架構表示如下圖：

$$\begin{aligned} \mathcal{P} &= \{\text{所有可能的明文信息單元}\} \\ \mathcal{C} &= \{\text{所有可能的密文信息單元}\} \\ f &= \text{加密函數，此函數爲一對一函數} \end{aligned}$$

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$$

這樣的系統我們稱爲一個密碼系統(Cryptosystem)。

1.2 公開鑰匙密碼系統

公開鑰匙演算法用一把鑰匙來加密，並且用另一把不同但相關的鑰匙來解密。而這些演算法具下列重要特性：

1. 兩把相關鑰匙的任一把皆可用來加密，而另一把則用來解密。
2. 如果只知道加密演算法與加密鑰匙的話，我們是無法求出解密鑰匙的。此外有些演算法〈例如RSA〉同時

具備下列特性：

公開鑰匙加密的流程其基本步驟如下：

(1) 網路中的每個終端機系統都會產生一組鑰匙，用來對信息加密。

(2) 每個系統都會將其加密鑰匙公佈在一個公開的註冊或檔案，這把鑰匙就稱爲公開鑰匙(public key)，另一把鑰匙就保留私用。

(3) 如果A想要送信息給B，他就用B的公開鑰匙加密該信息。

(4) 當B收到這個信息後，用他的私密鑰匙(private key)將之解密。其他任何人都沒有辦法解密，因爲只有B知道自己的私密鑰匙。

第二章

ElGamal 密碼系統

ElGamal於一九八五年所提出的密碼系統[1]。這個系統是一個非定性的(non-deterministic)系統。因爲密文不僅僅與明文有關，而且跟加密者在加密時所選取的隨機整數有關。所以同一明文就會產生許許多多不同的密文。

2.1 ElGamal 密碼系統

假設 B 要傳遞信息 m 給 A。首先 A 選取一個大質數 p 及一個整數 $\alpha \pmod p$，同時 A 也選取一秘密整數 a 並計算 $\beta \equiv \alpha^a \pmod p$。$A$ 將 (p, α, β) 公開，但將 a 保持私密。B 則根據 A 所公開的鑰匙，選取一個隨機整數 k 並算出 y_1 與

y_2，此處

$$y_1 \equiv \alpha^k \quad , \quad y_2 \equiv m\beta^k \pmod{p}。$$

B將密文y_1, y_2送出給A，然後A據此解密如下：

$$m \equiv y_2 y_1^{-a} \pmod{p}。$$

2.2 ElGamal的數位簽署

假設A要簽署一份文件m。首先他選擇一個大質數p及一個原根α，然後選取一個介於1與$p-2$之間的整數a並且計算$\beta \equiv \alpha^a \pmod{p}$。其公開的參數爲$p$，$\alpha$和$\beta$。整個系統的安全性完全是建立在$a$的私密性上。敵對者想從$(p, \alpha, \beta)$來決定$a$是困難重重，因爲離散對數問題被認爲是困難的。

A要簽署一信息m，他可進行如下得到簽署文(m, r, s)：

1. 選取一秘密隨機整數k使得$gcd = (k, p-1) = 1$。

2. 計算$r \equiv \alpha^k \pmod{p}$。

3. 計算$s \equiv k^{-1}(m - ar) \pmod{p-1}$。

4. 簽署後的信息爲 (m, r, s)。

B 可以驗證此簽名的有效性，其步驟如下：

1. 下載 A 的公開鑰匙 (p, α, β)。

2. 計算 $v_1 \equiv \beta^r r^s \pmod{p}$ 以及 $v_2 \equiv \alpha^m \pmod{p}$。

3. 接受此爲有效簽名 $\Longleftrightarrow v_1 = v_2$。

驗證此簽名的步驟爲何如此？其原因如下：

$$\text{因爲} \quad s \equiv k^{-1}(m - ar) \pmod{p-1}$$

$$\Longrightarrow \quad sk \equiv m - ar \pmod{p-1}$$

$$\Longrightarrow \quad m \equiv ks + ar \pmod{p-1}$$

$$\text{所以} \quad v_2 \equiv \alpha^m \equiv \alpha^{ks+ar} \equiv (\alpha^a)^r(\alpha^k)^s \equiv \beta^r r^s \equiv v_1 \pmod{p}$$

2.3 安全性分析及討論

1. 本簽署系統的安全性係基於解離散對數之困難上。若能解離散對數，則由β及α，可求出A之密匙a，因此本系統就不安全。

2. 若第三者想要僞造一合法簽署文，任選其r(或s)，想要求出s(或r)滿足$\alpha^m \equiv \beta^r r^s \pmod{p}$，則面臨解離散對數問題。

3. 若第三者已獲得一明文m及簽署文$\{r, s\}$，想要由$s \equiv k^{-1}(m - ar) \pmod{p-1}$求出$a$。則因式中有兩個未知數$a$及$k$，所以無法求得$a$。但若$A$利用相同的$k$對$m_1$、$m_2$簽署兩次，其簽署文分別爲$\{r, s_1\}$及$\{r, s_2\}$，則第三者可利用$m \equiv ar + ks \pmod{p-1}$來解聯立方程式

$$m_1 \equiv ar + ks_1 \pmod{p-1}$$

$$m_2 \equiv ar + ks_2 \pmod{p-1}$$

因爲有兩個方程式和兩個變數(a和k)，則a可被求出。所以，爲了避免此情形發生，k不可重複使用。

4. 第三者可以僞造m之合法簽署文$\{r, s\}$，但m無法事先固定。此僞造方法如下[2]：

假設第三者選取亂數i及j，滿足$1 < i, j < p-1$並且$gcd(j, p-1) = 1$。再計算

$$\begin{aligned} r &\equiv \alpha^i \beta^j \pmod{p} \\ s &\equiv -rj^{-1} \pmod{p-1} \\ m &\equiv -rij^{-1} \pmod{p-1} \end{aligned}$$

由此三式可得

$$\begin{aligned} \beta^r r^s &\equiv \beta^{\alpha^i \beta^j} (\alpha^i \beta^j)^{-\alpha^i \beta^j j^{-1}} \pmod{p} \\ &\equiv \beta^{\alpha^i \beta^j} \alpha^{-ij^{-1} \alpha^i \beta^j} \beta^{-\alpha^i \beta^j} \pmod{p} \\ &\equiv \alpha^{-ij^{-1} \alpha^i \beta^j} \pmod{p} \\ &\equiv \alpha^{-rij^{-1}} \pmod{p} \\ &\equiv \alpha^m \pmod{p} \end{aligned}$$

因此$\{r, s\}$爲m之合法簽署文。此僞造過程中，由於對m並沒有控制能力，故ElGamal簽署仍爲安全。

第三章

橢圓曲線與密碼系統

在一八九零年代的中期，米勒(Miller[3])與寇伯立茲(Koblitz[4])將橢圓曲線引進密碼術(cryptography)當中，而藍斯特(Lenstra[5])則指出如何使用橢圓曲線來分解因數。從此開始，橢圓曲線在密碼學的許多地方。扮演著一個重要的角色。優點之一是與傳統密碼系統使用相當大的鑰匙來比較，橢圓曲線看起來似乎提供了某種程度的安全水準。

3.1 橢圓曲線(Elliptic Curves)

下列的方程式我們稱之爲橢圓曲線

$$E:\ y^2 = x^3 + ax + b$$

此處的a , b佈於任何適用的集合如有理數、實數、複數、模p下之整數或有限數體。在任何的橢圓曲線的定義中都有一個元素∞，稱之爲「無限遠點(Point at infinity)或零點(Zero point)」。此無限遠點最簡單的一個處理方式就是將此點看作在y-軸的最上方。這可以放在投影幾何的背景下嚴密地處理，但上面直觀的概念對我門來講已足夠了。我們可以參考Silverman與Tate二人所合寫的書《橢圓曲線上的有理點(Rational Points On Elliptic Curves[8])》。若將y-軸最下方的點看成是最上方的點。則∞也是位於y-軸的最下方。在實數的領域下，圖形只有兩種可能的形式，就是看右邊那個的三次多項式有三個相異的實根或是一個實根而定。重根的情況又另當別論，通常我們假設三次多項式x^3+ax+b沒有重根。請參考下面之圖形。

3.2 橢圓曲線上的加法律

對橢圓曲線加密系統(Elliptic Curves Cryptosystem)而言,我們所關心的是在有限體內的橢圓曲線。在密碼學上特別的是取p的同餘的橢圓曲線，此處p爲質數。其定義如下。挑選兩個小於p的非負整數，滿足

$$4a^3 + 27b^2 \pmod{p} \neq 0$$

則$E_p(a,b)$表示取p的同餘的橢圓曲線，其元素(x,y)是一對小於p的非負整數，滿足

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

，以及無限遠點∞。因此對橢圓曲線來說，我們只對$(0,0)$到(p,p)間滿足方程式(取p之同餘)的非負整數點有興趣。通常這些點可由下列方式列出：

1. 對每個滿足$0 \leq x < p$的x來說，計算$x^3 + ax + b \pmod{p}$。
2. 檢查上一步所產生的結果是否有平方根(取p的同餘)[6]。如果沒有的話，則$E_p(a,b)$沒有此x的點。如果有的話，會有兩個平方根y(除非此y值爲0)。這些

(x, y) 值爲 $E_p(a, b)$ 上的點。

$E_p(a, b)$ 上的加法規則與圖上的幾何技巧是相對應的。對所有的點 $P, Q \in E_p(a, b)$ 來說，其加法如下：

1. ∞ 爲加法單位元素。因此 $\infty = -\infty$；對任何在橢圓曲線上的點 P 而言， $P + \infty = P$。

2. 垂直線會和曲線相交於兩點，這兩點具有相同的 x 座標，如果 $P = (x, y)$，則 $P + (x, -y) = \infty$。點 $(x, -y)$ 爲負 P，記爲 $-P$。請注意 $(x, -y)$ 爲橢圓曲線上的點 (也就是在 $E_p(a, b)$ 上)。所以一點的負點會有相同的 x 座標，但是 y 座標變成負的。其圖說明此性質。

3. 給予不同 x 座標的兩點 P 及 Q 相加的話。可得到在橢圓曲線上的第三點如下：經過 P 及 Q 二點畫一直線 L(若 $P = Q$，則取切線)。直線 L 與橢圓曲線交於 R，然後求其 x-軸的對稱點 $-R$(亦即 y 座標變號)，亦即 $P + Q + R = \infty$ 且 $P + Q = -R$。其圖說明此性質。

4. 令 $P = (x_1, y_1)$，$Q = (x_2, y_2)$ 爲橢圓曲線上之兩點，並且 $P \neq -Q$，則 $P + Q = (x_3, y_3)$。

此處

$$x_3 \equiv m^2 - x_1 - x_2 \pmod{p}$$

$$y_3 \equiv m(x_1 - x_3) - y_1 \pmod{p}$$

其中的m爲

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

我們來看下列的例子：

考慮在模5之下的橢圓曲線

$$E: \ y^2 \equiv x^3 + 2x + 3 \pmod{5}。$$

滿足$E_5(2,3)$的點爲$(1,1)$, $(1,4)$, $(2,0)$, $(3,1)$, $(3,4)$, $(4,0)$及∞。

令$P = (1,4)$且$Q = (3,1)$，則$m \equiv \frac{1-4}{3-1} \equiv 1 \pmod{5}$。

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 1^2 - 1 - 3 \equiv 2 \pmod{5}。$$

$$y_3 \equiv m(x_1 - x_3) - y_1 \equiv 1(1-2) - 4 \equiv 0 \pmod{5}。$$

亦即$P + Q = (2,0)$。

若要計算$2P = P + P$的話，則求其切線斜率$\frac{dy}{dx}$在點$P(1,4)$的值如下：

$$m \equiv \frac{3x_1^2 + a}{2y_1} \equiv \frac{3(1)^2 + 2}{2(4)} \equiv \frac{5}{8} \equiv \frac{0}{3} \equiv 0 \pmod 5。$$

並由公式得到

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 0^2 - 1 - 3 \equiv 1 \pmod 5。$$

$$y_3 \equiv m(x_1 - x_3) - y_1 \equiv 0(1 - 2) - 4 \equiv 1 \pmod 5。$$

最後的答案則是$2P = (1,1)$。

上述的加法規則滿足一般加法特性，像交換性與結合性。橢圓曲線上一點P乘上一整數k的定義，就像把P加k次一樣。因此，$2P = P + P$，$3P = P + P + P$，以此類推。

3.3 如何用橢圓曲線上的點來表示明文？

在大部分的密碼系統，我們必須有一套方法將原信息轉換成一個數值，以方便在此數值上做數學運算。同樣地，爲了要使用橢圓曲線，我們需要一套方法將信息轉換成橢圓曲線上的一點。然後橢圓曲線密碼系統再執行某種橢圓曲線上的運算於此點，如此得到一個新的點當成原信息的密文。

將明文信息編碼而成爲橢圓曲線上之點的問題，並不像傳統的情況那樣簡單。特別而言，還找不到一個在多項式時間內、定性的演算法，可供你在任意的橢圓曲線 $E \pmod{p}$ 上完成此任務。然而，的確存在有快速機率式的方法來產生橢圓曲線上的點，而這些點可用來對明文信息加以編碼。這些方法有一個共同性，即產生橢圓曲線上一點失敗的概率是小的。適當的選取參數，可使得這個失敗的概率如你之意的小，如 $1/2^{30}$。

這裡有一個 Koblitz 的方法。其想法如下：令 $E : y^2 \equiv$

$x^3+ax+b \pmod p$ 爲一橢圓曲線。已經數字化的信息 m 將看成是這橢圓曲線上的某一點的 x 座標。然而，m^3+am+b 在模 p 之下是平方數的概率至少 $1/2$。因此我們在 m 後面接上一個位元成爲另一個數，稱之爲 x，藉著調整此位元直到我們得到一個 x 使得 x^3+ax+b 在模 p 之下爲平方數。

更明確地說，令 K 爲一個大整數使得將信息編碼成爲橢圓曲線上的點時，其失敗率爲 $1/2^K$ 是可接受的。假設 m 滿足 $(m+1)K < p$，將此信息 m 表示成一個形如 $x = mK + j$ 的數，此數 $0 \le j \le K$。對 $j = 0, 1, \ldots, K-1$，計算 x^3+ax+b 並計算在模 p 之下的平方根。若有一平方根 y，則取 $P_m = (x, y)$，否則將 j 增加 1 形成新的 x，然後重複上述的步驟。如此這般地，直等到找著了一個平方根或是 $j = K$。如果 j 總是等於 K，那麼對這個信息而言，我們的任務就無法達成。因爲 x^3+ax+b 大約有一半的時間是一個平方數，所以我們大約有 $1/2^K$ 失敗的機會。

由點 $P_m = (x, y)$，如何回復到原信息呢？那簡單之至，僅需計算 $\frac{x}{K}$，取其整數部分即可。所以我們有 $m = [\frac{x}{K}]$，

此處$[\frac{x}{K}]$爲高斯符號，指的就是小於或等於$\frac{x}{K}$的最大整數。

例題：

令$p = 179$且假設我們的橢圓曲線爲$y^2 = x^3 + 2x + 7$。若可以接受$1/2^{10}$的失敗率，則取$K = 10$。因爲我們要求$(m+1)K < 179$，故$0 \leq m \leq 16$。假設我們的信息爲$m = 5$。考慮形如$mK + j = 50 + j$的m值，可能的選擇爲$50, 51, \ldots, 59$。對$x = 51$，我們得到

$$x^3 + 2x + 7 \equiv 121 \pmod{179}\ ,\ 11^2 \equiv 121 \pmod{179}$$

因此我們用點$P_m = (51, 11)$來表示信息$m = 5$。因此信息m可還原如下：$m = [\frac{51}{10}] = 5$。

3.4 橢圓曲線加密法

已有文獻分析了現有的數種橢圓曲線的加/解密方法。在這裡，讓我們來看看最簡單的一種。首先系統將要送的明文m編碼成橢圓曲線上的點P_m。點P_m會被加密成密文，並且稍後會被解密。要注意的是我們不能單純地將信息編碼成某個點的x或y座標，因爲並不是所有的這類座標都會$E \pmod p$在上。在一個鑰匙交換系統中，其加/解密系統需要兩個參數，α和橢圓曲線$E \pmod p$。

首先，使用者A選擇一私密鑰匙$a_{_A}$，然後再產生一公開鑰匙$\beta_A = a_{_A}\alpha$。

同樣地使用者B也選擇一私密鑰匙$a_{_B}$，然後再產生一公開鑰匙$\beta_B = a_{_B}\alpha$。

爲了將加密後的信息P_m傳送給B，A選擇一隨機正整數k，並且產生一個由兩個點所組成的密文C_m。

$$C_m = \{k\alpha\ ,\ P_m + k\beta_B\}$$

請注意，A用的是B的公開鑰匙β_B。爲了解開密文，B用自己的私密鑰匙乘上第一點，再用第二點減去得到的結

果，可得

$$P_m + k\beta_B - a_{_B}(k\alpha) = P_m + k(a_{_B}\alpha) - a_{_B}(k\alpha) = P_m$$

A藉由加上$k\beta_B$來隱藏訊息P_m。除了A之外沒人知道k的值，所以即使β_B是公開的鑰匙，也沒人能移除隱藏用的$k\beta_B$。然而，A在信息中加入了移除隱藏的「線索」，如果有人知道私密鑰匙$a_{_B}$的話，就可以移除$k\beta_B$。給定α和$k\alpha$，攻擊者必須計算出才能破解，但這是很困難的。

此方法有可能不是很實用，但我們也可以用Menezes-Vanstone[2]方法來做加密，因爲此方法在加密時不需先將信息m轉換成橢圓曲線上的點即可做加密的動作。

例題：

考慮在模179之下的橢圓曲線

$$E:\ y^2 \equiv x^3 + 2x + 7 \pmod{179}。$$

並在其上選取一點$\alpha = (111, 11)$再將此$(111, 11)$,及橢圓曲線$E_{179}(2, 7)$公開。

使用者A選取一私密鑰匙$a_A = 12$，然後A產生一公開鑰匙$\beta_A \equiv 12 * (111, 11) = (111, 168) \pmod{179}$。

使用者B同樣地選擇一私密鑰匙$a_B = 9$，並且計算其公開鑰匙$\beta_B \equiv 9 * (111, 11) = (20, 23) \pmod{179}$。

若A要將信息$m = 5$加密後傳送給B，其進行步驟如下：

1. 欲傳送信息$m = 5$，所以選擇$K = 10$。可以成功的將m轉換成爲$x = 5*10+1 = 51$，$y = 11$的點$P_m = (51, 11)$。

2. 選取隨機整數$k = 11$。

3. 計算 $y_1 \equiv k\alpha \pmod{p}$

$$\equiv 11 * (111, 11) \pmod{179}$$

$$\equiv (152, 26)$$

3. 計算 $y_2 \equiv P_m + k\beta_B \pmod{p}$

$$\equiv (51, 11) + 11 * (20, 23) \pmod{179}$$

$$\equiv (51, 11) + (164, 19) \pmod{179}$$

$$\equiv (156, 18)$$

因此A所產生的密文$C_m = \{(152, 26), (156, 18)\}$。

B 可由 A 所產生的密文 C_m 來加以解密：

計算 $y_2 - a_{_B} y_1 \pmod{p}$

$$\equiv P_m + k\beta_B - a_{_B}(k\alpha) \pmod{p}$$

$$\equiv (51, 11) + 11 * (20, 23) - 9 * [11 * (111, 11)] \pmod{179}$$

$$\equiv (51, 11) + (164, 19) - 9 * (152, 26) \pmod{179}$$

$$\equiv (51, 11) + (164, 19) - (164, 19) \pmod{179}$$

$$\equiv (51, 11) \pmod{179}$$

$$\equiv P_m$$

因此，A 藉由加上 $k\beta_B$ 來隱藏訊息 P_m。除了 A 之外沒人知道 k 的值，所以即使 β_B 是公開的鑰匙，也沒人能移除隱藏用的 $k\beta_B$。

第四章

橢圓曲線版的數位簽署

ElGamal密碼系統是專門爲簽署而設計的。其不同於RSA的一個特色就是對任何的一個信息有多種不同的簽署法。由於橢圓曲線能運用於ElGamal密碼系統中，相對之下，那橢圓曲線一樣也能運用於ElGamal數位簽署中。因此在下面的4.1節裡我們所討論的就是有關於橢圓曲線版的ElGamal數位簽署。

4.1 橢圓曲線版的ElGamal數位簽署

令$E : y^2 \equiv x^3 + ax + b \pmod{p}$爲一橢圓曲線，在其上選取一秩$(order)$爲$n \in \mathbb{N}$的點$\alpha = (x, y)$，並將$\alpha$及$E_p(a, b)$

對所有密碼系統的參與者而言都是公開的。假設A想要利用橢圓曲線來簽署一份文件m，首先他選取一秘密隨機整數a，且a必須落在區間$[1, n-1]$裡，並且計算一等式$\beta \equiv a\alpha \pmod{p}$，此$\alpha, \beta \in E_p(a, b)$。則$\beta$爲$A$的公開鑰匙，而$a$是爲秘密鑰匙。

使用者A對此信息m加以簽署，其步驟如下：

1. 選取一介於1與n之間的秘密整數k，使得$gcd(k, n) = 1$。
2. 計算$\gamma \equiv k\alpha \equiv (x_1, y_1) \pmod{p}$。
3. 計算$s \equiv k^{-1}(m - ax_1) \pmod{n}$。
4. 因此簽署爲(m, γ, s)。

B的驗證程序如下：

1. 下載A的公開鑰匙(E_p, α, β)。
2. 計算$v_1 \equiv x_1\beta + s\gamma \pmod{p}$以及$v_2 \equiv m\alpha \pmod{p}$。
3. 接受此爲有效簽署$\Longleftrightarrow v_1 = v_2$。

驗證此簽名的步驟爲何如此？其原因如下：

$$
\begin{aligned}
\text{因爲} \quad s &\equiv k^{-1}(m - ax_1) \pmod{n} \\
\Longrightarrow \quad sk &\equiv m - ax_1 \pmod{n} \\
\Longrightarrow \quad m &\equiv ks + ax_1 \pmod{n} \\
\text{所以} \quad v_2 &\equiv m\alpha \\
&\equiv (ks + ax_1)\alpha \\
&\equiv ks\alpha + ax_1\alpha \\
&\equiv s\gamma + x_1\beta \\
&\equiv v_1 \pmod{p}
\end{aligned}
$$

所以$v_1 = v_2$得證，因此使用者B接受此簽署。

例題：

考慮在模179之下的橢圓曲線

$$E:\ y^2 \equiv x^3 + 2x + 7 \pmod{179}。$$

選取一個滿足$E_{179}(2,7)$上的點$\alpha = (111,11)$，使得$n * (111,11) = \infty$，其中$n = 13$。使用者A選取隨機整數$a = 12$，且$a \in (1,13)$，並計算$\beta = 12\alpha = (111,168) \pmod{179}$，此$\alpha, \beta \in E_{179}(2,7)$。因此$A$將$((111,11),\ (111,168),\ E_{179}(2,7))$公開。

A對信息$m = 5$簽署，其步驟如下：

1. 選取隨機整數$k = 11$，使得$gcd(11,13) = 1$。

2. 計算 $\gamma \equiv k\alpha \pmod{p}$

$$\equiv 11 * (111,11) \pmod{179}$$

$$\equiv (152,26)$$

3. 計算 $s \equiv k^{-1}(m - ax_1) \pmod{n}$

$$\equiv 6 * (5 - 12 * 152) \pmod{13}$$

$$\equiv 6$$

4. 因此簽署爲$(5\ ,\ (152,26)\ ,\ 6)$。

B的驗證程序如下：

1. 下載A的公開鑰匙$(E_{179}(2,7)\ ,\ (111,11)\ ,\ (111,168))$。

2. 計算 $v_1 \equiv x_1\beta + s\gamma \pmod{p}$

$$\equiv 152 * (111,168) + 6 * (152,26) \pmod{179}$$

$$\equiv (20,156) + (111,11) \pmod{179}$$

$$\equiv (164,160)$$

計算 $v_2 \equiv m\alpha \pmod{p}$

$$\equiv 5 * (111,11) \pmod{179}$$

$$\equiv (164,160)。$$

3. 因此得到$v_1 = v_2$，所以此簽署是有效的。

4.2 橢圓曲線改良版的ElGamal數位簽署

令$E: y^2 \equiv x^3 + ax + b \pmod{p}$爲一橢圓曲線，在其上選取一秩$(order)$爲$n \in \mathbb{N}$的點$\alpha = (x, y)$，並將$\alpha$及$E_p(a, b)$對所有密碼系統的參與者而言都是公開的。假設$A$想要利用橢圓曲線來簽署一份文件$m$，首先他選取一秘密隨機整數$a$，且$a$必須落在區間$[1, n-1]$裡，並且計算一等式$\beta \equiv a\alpha \pmod{p}$，此$\alpha, \beta \in E_p(a, b)$。則$\beta$爲$A$的公開鑰匙，而$a$是爲秘密鑰匙。

使用者A對此信息m加以簽署，其步驟如下：

1. 選取一介於1與n之間的秘密整數k，使得$gcd(k, n) = 1$。
2. 計算$\gamma \equiv k\alpha \equiv (x_1, y_1) \pmod{p}$。
3. 計算$s \equiv a^{-1}(x_1 k - m) \pmod{n}$。
4. 因此簽署爲(m, γ, s)。

B的驗證程序如下：

1. 下載 A 的公開鑰匙 (E_p, α, β)。

2. 計算 $v_1 \equiv x_1\gamma - s\beta \pmod{p}$ 以及 $v_2 \equiv m\alpha \pmod{p}$。

3. 接受此爲有效簽署 $\Longleftrightarrow v_1 = v_2$。

我們說明此驗證試行的通的。因爲

$$\begin{aligned} v_1 &\equiv x_1\gamma - s\beta \\ &\equiv x_1 k\alpha - sa\alpha \\ &\equiv x_1 k\alpha - [a^{-1}(x_1 k - m)]a\alpha \\ &\equiv x_1 k\alpha - x_1 k\alpha + m\alpha \\ &\equiv m\alpha \\ &\equiv v_2 \pmod{p} \end{aligned}$$

所以 $v_1 = v_2$ 得證，因此使用者 B 接受此簽署。

例題：

考慮在模179之下的橢圓曲線

$$E:\ y^2 \equiv x^3 + 2x + 7 \pmod{179}。$$

選取一個滿足$E_{179}(2,7)$上的點$\alpha = (111,11)$，使得$n * (111,11) = \infty$，其中$n = 13$。使用者A選取隨機整數$a = 12$，且$a \in (1,13)$。並計算$\beta = 12\alpha = (111,168) \pmod{179}$，此$\alpha, \beta \in E_{179}(2,7)$。因此$A$將$((111,11),\ (111,168),\ E_{179}(2,7))$公開。

A對信息$m = 5$簽署，其步驟如下：

1. 選取隨機整數$k = 11$，使得$gcd(11,13) = 1$。

2. 計算 $\gamma \equiv k\alpha \pmod{p}$

$$\equiv 11 * (111,11) \pmod{179}$$

$$\equiv (152,26)$$

3. 計算 $s \equiv a^{-1}(x_1 k - m) \pmod{n}$

$$\equiv 12 * (152 * 11 - 5) \pmod{13}$$

$$\equiv 10$$

4. 因此簽署爲$(5\ ,\ (152,26)\ ,\ 10)$。

B的驗證程序如下：

1. 下載A的公開鑰匙$(E_{179}(2,7)\ ,\ (111,11)\ ,\ (111,168))$。

2. 計算 $v_1 \equiv x_1\gamma - s\beta \pmod{p}$

$$\equiv 152 * (152,26) - 10 * (111,168) \pmod{179}$$

$$\equiv (164,19) + (112,-3) \pmod{179}$$

$$\equiv (164,160)$$

計算 $v_2 \equiv m\alpha \pmod{p}$

$$\equiv 5 * (111,11) \pmod{179}$$

$$\equiv (164,160)。$$

3. 因此得到$v_1 = v_2$，所以此簽署是有效的。

4.3 同時達到秘密通訊和數位簽署

令 $E : y^2 \equiv x^3 + ax + b \pmod{p}$ 爲一橢圓曲線，在其上選取一秩 $(order)$ 爲 $n \in \mathbb{N}$ 的點 $\alpha = (x, y)$，並將 α 及 $E_p(a, b)$ 對所有密碼系統的參與者而言都是公開的。

4.3.1 系統參數相同時

使用者 A 與 B 其系統參數 (p, α) 相同，個人私密鑰匙求法如下：

1. A 選擇一小於 n 的整數 $a_{_A}$，此 $a_{_A}$ 爲 A 的私密鑰匙，然後 A 產生一公開鑰匙 $\beta_A \equiv a_{_A}\alpha \pmod{p}$；公開鑰匙爲 $E_p(a, b)$ 上的一點。

2. B 同樣地選擇一私密鑰匙 $a_{_B}$，並且計算其公開鑰匙 $\beta_B \equiv a_{_B}\alpha \pmod{p}$。

3. A 生成密鑰 $K = a_{_A}\beta_B$，B 生成密鑰 $K = a_{_B}\beta_A \pmod{p}$。

步驟 3 的兩個運算會產生相同的結果，因爲

$$a_{_A} \times \beta_B = a_{_A} \times (a_{_B} \times \alpha) = a_{_B} \times (a_{_A} \times \alpha) = a_{_B} \times \beta_A$$

若A欲秘密傳送明文$m(1 \leq m \leq p-1)$，並且同時對m做簽署，然後傳送給B。其進行步驟如下：

使用者A首先對信息m加密，得到密文$C = \{\gamma, \delta\}$。然後再對密文C加以簽署，得到簽署文$S = \{x_1, s\}$。

1. A任選一介於1及n之間的整數k，使得$gcd(k, n) = 1$。

2. 將信息m轉換成橢圓曲線上的點P_m。

3. 加密：
$$\gamma \equiv k\alpha \pmod{p}$$
$$\delta \equiv P_m + k\beta_B \pmod{p}$$

4. 簽署：
$$\gamma \equiv k\alpha \equiv (x_1, y_1) \pmod{p}$$
$$s \equiv k^{-1}(m - a_{_A} x_1) \pmod{n}$$

B收到$\{C, S\}$後，先進行解密的動作，以求得信息m；然後再執行驗證，確定是否爲A傳送過來的。

1. 解密：
$$P_m \equiv \delta - a_{_B}\gamma \pmod{p}$$

2. 將此橢圓曲線上的點P_m轉換成原來的信息m。

3. 驗證：　　$v_1 \equiv x_1\beta_A + s\gamma \pmod{p}$

$v_2 \equiv m\alpha \pmod{p}$

我們說明此驗證是行的通的。

$$\begin{aligned}
\text{因爲} \quad s &\equiv k^{-1}(m - a_{_A}x_1) \pmod{n} \\
\Longrightarrow \quad sk &\equiv m - a_{_A}x_1 \pmod{n} \\
\Longrightarrow \quad m &\equiv ks + a_{_A}x_1 \pmod{n} \\
\text{所以} \quad v_2 &\equiv m\alpha \\
&\equiv (ks + a_{_A}x_1)\alpha \\
&\equiv ks\alpha + a_{_A}x_1\alpha \\
&\equiv s\gamma + x_1\beta_A \\
&\equiv v_1 \pmod{p}
\end{aligned}$$

所以$v_1 = v_2$得證，因此使用者B接受此簽署。

例題：

考慮在模179之下的橢圓曲線

$$E:\ y^2 \equiv x^3 + 2x + 7 \pmod{179}$$

並選取一個滿足$E_{179}(2,7)$上的點$\alpha = (111,11)$，使得$n(111,11) = \infty$，其中$n = 13$，並將$(111,11)$及$E_{179}(2,7)$公開。

使用者A的系統參數爲$(179,(111,11))$，私密鑰匙$a_{_A} = 12$，

其公開鑰匙爲$\beta_A = 12 * (111,11) = (111,168) \pmod{179}$。

使用者B的系統參數爲$(179,(111,11))$，私密鑰匙$a_{_B} = 9$，

其公開鑰匙爲$\beta_B = 9 * (111,11) = (20,23) \pmod{179}$。

若A要傳送信息m，並同時對m做簽署，然後傳送給B。

其進行步驟如下：

A的加密及簽署：

1. 選取一整數$k = 11$，使得$gcd(11,13) = 1$。

2. 欲傳送信息$m = 5$，所以選擇$K = 10$。可以成功的將m轉換成爲$x = 5*10+1 = 51$，$y = 11$的點$P_m = (51,11)$。

3. 加密：

   計算 $\gamma \equiv k\alpha \pmod{p}$

$$\equiv 11 * (111, 11) \pmod{179}$$

$$\equiv (152, 26)$$

計算 $\delta \equiv P_m + k\beta_B \pmod{p}$

$$\equiv (51, 11) + 11 * (20, 23) \pmod{179}$$

$$\equiv (51, 11) + (164, 19) \pmod{179}$$

$$\equiv (156, 18)。$$

4. 簽署：

計算 $\gamma \equiv k\alpha \pmod{p}$

$$\equiv 11 * (111, 11) \pmod{179}$$

$$\equiv (152, 26)$$

計算 $s \equiv k^{-1}(m - a_{_A}x_1) \pmod{n}$

$$\equiv 6 * (5 - 12 * 152) \pmod{13}$$

$$\equiv 6。$$

因此密文$C = \{(152, 26), (156, 18)\}$，簽署文$S = \{152, 6\}$。

B收到$\{C, S\}$後進行解密及驗證：

1. 解密：

計算 $\delta - a_{_B}\gamma \equiv (156, 18) - 9 * (152, 26) \pmod{179}$

$$\equiv (156, 18) + (164, -19) \pmod{179}$$

$$\equiv (51, 11)$$

$$\equiv P_m \circ$$

2. 取其點 P_m 中的 x 座標 51，得 $[\frac{51}{10}] = 5$ 爲原來的信息 m。

3. 驗證：

計算 $x_1\beta_A + s\gamma \equiv 152 * (111, 168) + 6 * (152, 26) \pmod{179}$

$$\equiv (20, 156) + (111, 11) \pmod{179}$$

$$\equiv (164, 160)$$

$$\equiv v_1$$

計算 $m\alpha \equiv 5 * (111, 11) \pmod{179}$

$$\equiv (164, 160)$$

$$\equiv v_2 \circ$$

4. 因此得到 $v_1 = v_2$，所以此簽署是有效的。

4.3.2 系統參數不相同時

使用者A與B其系統參數分別爲(p_A, α_A)及(p_B, α_B)，個人私密鑰匙分別爲a_A及a_B，個人公開鑰匙分別爲$\beta_A \equiv a_A\alpha_A \pmod{p_A}$及$\beta_B \equiv a_B\alpha_B \pmod{p_B}$。

若A欲秘密傳送信息$m(1 \leq m \leq p_B - 1)$，並且同時對m做簽署，然後傳送給B。首先A必須選取一橢圓曲線$E : y^2 \equiv x^3 + ax + b \pmod{p_A}$，並在其上選取一秩$(order)$爲$n \in \mathbb{N}$的點$\alpha_A = (x, y)$，並將$\alpha_A$及$E_{p_A}(a, b)$公開。其進行的步驟如下：

使用者A對信息m加密，得到密文$C = \{\gamma, \delta\}$。然後再對密文C加以簽署，得到簽署文$S = \{\gamma_A, s\}$。

1. A任意選取一整數k，使得$gcd(k, n) = 1$。

2. 將信息m轉換成橢圓曲線上的點P_m。

3. 加密：
$$\gamma \equiv k\alpha_B \pmod{p_B}$$
$$\delta \equiv P_m + k\beta_B \pmod{p_B} \tag{4.1}$$

3. 簽署：
$$\gamma_A \equiv k\alpha_A \equiv (x_1, y_1) \pmod{p_A}$$
$$s \equiv k^{-1}(m - a_A x_1) \pmod{n} \tag{4.2}$$

B收到$\{C, S\}$後，先進行解密的動作，以求得信息m；然後再執行驗證，確定是否爲A傳送過來的。

1. 解密：　　$P_m \equiv \delta - a_{_B}\gamma \pmod{p_{_B}}$　　(4.3)

2. 將此橢圓曲線上的點P_m轉換成原來的信息m。

3. 驗證：　　$v_1 \equiv x_1\beta_A + s\gamma_{_A} \pmod{p_{_A}}$　　(4.4)

$$v_2 \equiv m\alpha_{_A} \pmod{p_{_A}} \qquad (4.5)$$

Reblocking問題的討論

若先執行加密再簽署時，因爲A和B之系統參數不同，分別爲$p_{_A}$和$p_{_B}$，所以有可能造成Reblocking問題。

1. 當$p_{_B} < p_{_A}$時，在解密時因(4.1)式解密出來(4.3)式的m和原來信息(4.1)式中的m相同，所以不會造成Reblocking。但在驗證時因$p_{_B} < p_{_A}$時，則

   (a) 當$p_{_A} > n$時，

      i. 若$n > p_{_B}$，則(4.1)式和(4.2)式中的m相同。

      ii. 若$n < p_{_B}$，則(4.1)式和(4.2)式中的m相同。

因爲在(4.2)式中的m和(4.1)式中的m不相同，之間相差了n倍，由於一秩($order$)爲$n \in \mathbb{N}$的點α_A，會變成單位元數。因此，在(4.4)式和(4.5)式中可知v_1和v_2之間只差n倍，所以不會產生Reblocking的問題。

(b) 當$n > p_A$ ($i.e.\ n > p_B$)時，則(4.1)式和(4.2)式中的m相同。

因此由$(a), (b)$可得(4.1)式解密出來的信息m和(4.2)式中的m相同，所以在驗證時(4.4)式和(4.5)式等號會相等(因爲$a_A x_1 + ks = m \pmod{n}$)，因此不會造成Reblocking。

2. 當$p_B > p_A$時，在解密時因爲(4.1)式所解出來(4.3)式的m和原來(4.1)式中的信息m相同，所以不會造成Reblocking。但驗證時因$p_B > p_A$時，則

(a) 當$p_A > n$ ($i.e.\ p_B > n$)，若$m > n$則(4.2)式中的m和(4.1)式中的m會不相同，之間相差了n倍，由於一秩($order$)爲$n \in \mathbb{N}$的點α_A，會變成單位元數。因此，在(4.4)式和(4.5)式中可知v_1和v_2之間只差n倍，所以不會產生Reblocking的問題。

(b) 當 $n > p_A$ 時，

i. 若 n 也大於 p_B $(i.e.\ n > p_B)$，則 (4.1) 式和 (4.2) 式中的 m 相同。

ii. 若 $n < p_B$ $(i.e.\ p_B > n)$，則 (4.2) 式中的 m 和 (4.1) 式中的 m 不相同，之間相差了 n 倍，由於一秩 $(order)$ 爲 $n \in \mathbb{N}$ 的點 α_A，會變成單位元數。因此，在 (4.4) 式和 (4.5) 式中可知 v_1 和 v_2 之間只差 n 倍，所以不會產生 Reblocking 的問題。

因此由 $(a), (b)$ 可得 (4.1) 式解密出來的信息 m 和 (4.2) 式中的 m 相同，所以在驗證時 (4.4) 式和 (4.5) 式等號會相等 (因爲 $a_A x_1 + ks = m \pmod{n}$)，因此不會造成 Reblocking。

由上可知雖然 p_A，p_B 不同，但並不會影響其解密和驗證的過程。

例題1： $P_A > P_B$

使用者A的系統參數爲$(191,(125,5))$，私密鑰匙$a_{_A}=12$，

其公開鑰匙爲$\beta_A = 12*(125,5) = (182,62) \pmod{191}$。

使用者B的系統參數爲$(179,(111,11))$，私密鑰匙$a_{_B}=9$，

其公開鑰匙爲$\beta_B = 9*(111,11) = (20,23) \pmod{179}$。

若A要傳送信息m，並同時對m做簽署，然後傳送給B。

首先A考慮在模191之下的橢圓曲線

$$E:\ y^2 \equiv x^3 + 2x + 7 \pmod{191}$$

並選取一個滿足$E_{191}(2,7)$上的點$\alpha_{_A} = (125,5)$，使得$n(125,5) = \infty$，其中$n = 96$，並將$(125,5)$及$E_{191}(2,7)$公開。其進行步驟如下：

A的加密及簽署：

1. 選取一整數$k = 11$，使得$gcd(11,96) = 1$。

2. 欲傳送信息$m = 5$，所以選擇$K = 10$。可以成功的將m轉換成爲$x = 5*10+1 = 51$，$y = 11$的點$P_m = (51,11)$。

3. 加密：

   計算 $\gamma \equiv k\alpha_{_B} \pmod{p_{_B}}$

$$\equiv 11 * (111, 11) \pmod{179}$$

$$\equiv (152, 26)$$

計算 $\delta \equiv P_m + k\beta_B \pmod{p_B}$

$$\equiv (51, 11) + 11 * (20, 23) \pmod{179}$$

$$\equiv (51, 11) + (164, 19) \pmod{179}$$

$$\equiv (156, 18)。$$

4. 簽署：

計算 $\gamma_A \equiv k\alpha_A \pmod{p_A}$

$$\equiv 11 * (125, 5) \pmod{191}$$

$$\equiv (123, 4)$$

計算 $s \equiv k^{-1}(m - a_A x_1) \pmod{n}$

$$\equiv 35 * (5 - 12 * 123) \pmod{96}$$

$$\equiv 67。$$

因此密文$C = \{(152, 26), (156, 18)\}$，簽署文$S = \{(123, 4), 67\}$。

B收到$\{C, S\}$後進行解密及驗證：

1. 解密：

計算 $\delta - a_B\gamma \equiv (156, 18) - 9 * (152, 26) \pmod{179}$

$$\equiv (156, 18) + (164, -19) \pmod{179}$$

$$\equiv (51, 11)$$

$$\equiv P_m \circ$$

2. 取其點 P_m 中的 x 座標 51，得 $[\frac{51}{10}] = 5$ 爲原來的信息 m。

3. 驗證：

計算 $x_1\beta_A + s\gamma_A \equiv 123 * (182, 62) + 67 * (123, 4) \pmod{191}$

$$\equiv (96, 168) + (157, 118) \pmod{191}$$

$$\equiv (43, 12)$$

$$\equiv v_1$$

計算 $m\alpha_A \equiv 5 * (125, 5) \pmod{191}$

$$\equiv (43, 12)$$

$$\equiv v_2 \circ$$

4. 因此得到 $v_1 = v_2$，所以此簽署是有效的。

例題 2：　$P_B > P_A$

使用者 A 的系統參數爲 $(179, (111, 11))$，私密鑰匙 $a_A = 12$，

其公開鑰匙爲 $\beta_A = 12 * (111, 11) = (111, 168) \pmod{179}$。

使用者 B 的系統參數爲 $(191, (125, 5))$，私密鑰匙 $a_B = 9$，

其公開鑰匙爲 $\beta_B = 9 * (125, 5) = (190, 189) \pmod{191}$。

若 A 要傳送信息 m，並同時對 m 做簽署，然後傳送給 B。

首先 A 考慮在模 179 之下的橢圓曲線

$$E: \ y^2 \equiv x^3 + 2x + 7 \pmod{179}$$

並選取一個滿足 $E_{179}(2, 7)$ 上的點 $\alpha_A = (111, 11)$，使得 $n(111, 11) = \infty$，其中 $n = 13$，並將 $(111, 11)$ 及 $E_{179}(2, 7)$ 公開。其進行步驟如下：

A 的加密及簽署：

1. 選取一整數 $k = 11$，使得 $gcd(11, 13) = 1$。

2. 欲傳送信息 $m = 5$，所以選擇 $K = 10$。可以成功的將 m 轉換成爲 $x = 5 * 10 + 4 = 54$，$y = 2$ 的點 $P_m = (54, 2)$。

3. 加密：

   計算 $\gamma \equiv k\alpha_B \pmod{p_B}$

   $\equiv 11 * (125, 5) \pmod{191}$

   $\equiv (123, 4)$

   計算 $\delta \equiv P_m + k\beta_B \pmod{p_B}$

   $\equiv (54, 2) + 11 * (190, 189) \pmod{191}$

$$\equiv (54,2)+(114,1) \pmod{191}$$

$$\equiv (102,37)。$$

4. 簽署：

計算 $\gamma_{_A} \equiv k\alpha_{_A} \pmod{p_{_A}}$

$$\equiv 11*(111,11) \pmod{179}$$

$$\equiv (152,26)$$

計算 $s \equiv k^{-1}(m-a_{_A}x_1) \pmod{n}$

$$\equiv 6*(5-12*152) \pmod{13}$$

$$\equiv 6。$$

因此密文$C=\{(123,4),(102,37)\}$，簽署文$S=\{(152,26),6\}$。

B收到$\{C,S\}$後進行解密及驗證：

1. 解密：

計算 $\delta - a_{_B}\gamma \equiv (102,37)-9*(123,4) \pmod{191}$

$$\equiv (102,37)+(114,-1) \pmod{191}$$

$$\equiv (54,2)$$

$$\equiv P_m。$$

2. 取其點P_m中的x座標54，得$[\frac{54}{10}]=5$爲原來的信息m。

3. 驗證：

計算 $x_1\beta_A + s\gamma_A \equiv 152*(111,168)+6*(152,26) \pmod{179}$

$\equiv (20,156)+(111,11) \pmod{179}$

$\equiv (164,160)$

$\equiv v_1$

計算 $m\alpha_A \equiv 5*(111,11) \pmod{179}$

$\equiv (164,160)$

$\equiv v_2$。

4. 因此得到$v_1 = v_2$，所以此簽署是有效的。

Mathematica的指令及程式

Mathematica指令　　在Mathematica中有兩個指令，說明如下：

• $addell\ [\ \{x1, y1\}, \{x2, y2\}, a, b, n\ ]$　　計算在模p之下橢圓曲線

$$E: \quad y^2 = x^3 + ax + b \pmod{n}$$

上兩點(x_1, y_1)與(x_2, y_2)之和。所有的數$x_1, x_2, y_1, y_2, a, b, n$都是整數。若$n$爲合成數而計算兩點與之和時得求某個數在模$n$之下的乘法反元素與$n$的最大公因數既不是1也不是$n$，則輸出的東西爲此最大公因數而非兩點之和。

• $multell\ [\ \{x, y\}, m, a, b, n\ ]$　　列舉在模n之下橢圓曲線

$$E: \quad y^2 = x^3 + ax + b \pmod{n}$$

上一點$P = (x, y)$的倍數：$P,\ 2P,\ 3P,\ \ldots,\ mP$。

若需要求某個數在模n之下的乘法反元素且此數與n的最大公因數既不是1也不是n，則整個計算停止但輸出此最大公因數。這個指令可用來分解大約是8位數的整數，所用的值大約100：當然有可能需要是幾條不同的橢圓曲線。

Mathematica程式　　上面兩個指令其程式如下：

```
addell[p1, p2, a, b, n]:=Module[z,m,x3,y3,p3,z=0;z1=1;
    If[p1==”infinity”,”infinity”, p3=p2;z=1,” ”];
        If[z == 1, ” ”,
    If[p2 == ”infinity”, ”infinity”, p3 = p1; z = 1, ” ”]];
        If[z == 1, ” ”,
    If[p1[[1]] == p2[[1]]  p1[[2]] == p2[[2]] == 0,
        p3 = ”infinity”, ”infinity”; z = 1, ” ”]];
        If[z == 1, ” ”,
    If[p1[[1]] == p2[[1]]  p1[[2]] != p2[[2]],
        p3 = ”infinity”, ”infinity”; z = 1, ” ”]];
        If[z == 1, ” ”,
    If[p1 == p2  GCD[p1[[2]], n] != 1  GCD[p1[[2]], n] != n,
        z = 1;
        z1 = GCD[p1[[2]], n], ” ”]];
        If[z == 1, ” ”,
    If[p1 == p2, m = Mod[(3*p1[[1]]^2 + a)*PowerMod[2*p1[[2]], -1,n],n];
        z= 1;x3=m^2-p1[[1]]-p2[[1]];
        y3=m*(p1[[1]] - x3)-p1[[2]];
        p3=Mod[x3,y3,n],” ”]];
        If[z== 1,””,
    If[GCD[p2[[1]]-p1[[1]],n]! = 1,z= 1;
        z1=GCD[p2[[1]]-p1[[1]],n],” ”]];
```

```
    If[z== 1," ",m=Mod[(p2[[2]]−p1[[2]])∗PowerMod[p2[[1]]−p1[[1]], −1,n],n];
    x3=m^2 - p1[[1]] - p2[[1]];
    y3 = m*(p1[[1]] - x3) - p1[[2]];p3 = Mod[x3, y3, n]];
    If[z1 == 1, p3, "factor=", z1]];

multell[p1, m, a, b, n] := Module[z, z = p1;
  For[i = 1, i ¡ m  z[[Length[z]]][[1]] != "factor=", i++,
  z = Append[z, addell[p1, z[[Length[z]]], a, b, n]]]; z]
```

參考文獻

[1] Elgamal, T.: A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, Advances in cryptology: Procedings of CRYPTO 84, Springer-Verlag, 1985, 10-18. Also appeared in IEEE Transactions on Information Theory, 31(1985), 469-472.

[2] Douglas R. Stinson : Cryptography Theory and Practice, 1956.

[3] Miller, V. : Use of elliptic curves in cryptography. Lecture Notes in computer science, 218(1986), 417-426. (Advances in Cryptology-CRYPTO'85).

[4] Koblitz, N. : Elliptic Curve Cryptosystem, Math. Comp. 48(1987), 203-209.

[5] Lenstra, H. W. Jr. : Factoring integers with elliptic

curves, Annals of Math. (2) 126(1987), 649-673.

[6] James K. Strayer : Elementary Number Theory, 1994.

[7] 賴溪松, 韓亮, 張真誠. " 近代密碼學及其應用," 1995.

[8] Silverman, Joseph H./Tate, Jhon: Rational Points on Elipitic Curves,

[9] 顏嵩銘, "公開金匙密碼系統之設計與運用法," 國立成功大學電機工程研究所博士論文,1994.