目錄

1 前言

數千年來，不論是君王或將領，都需要一套很有效率的通訊模式來治理國家、指揮軍隊。他們當然也深知萬一訊息落入不當人士裡， 讓敵國窺知機密，或讓反對勢力獲取關鍵資訊時，所會產生的嚴重後果。因此，在隨後的好幾個世紀裡，不斷的有一些高明的加密技術產生。

在19世紀Kerckhoffs的演說中，已經隱約透露出現代密碼學的原理：「沒有秘密算法，一切盡在密鑰中。」 可是，當時的加密體系仍然缺少數學背景，因而也缺少測量或評價這些體系抵抗攻擊的能力。 要是有人能最終達到密碼學的終極目標，即是找到百分之百無條件安全體系那該有多好。但事實上，是否存在這樣的密碼系統呢？ 答案是肯定的，的確存在有無法破解的密碼系統，如單次鑰匙簿密碼(One-time Pad)； 而且也存在有密碼系統如RSA者，只要執行妥當，在你有生之年也是無法破解的，即使破解了，也需耗費大量的時間及物資。

在現今這個網路通訊逐漸發達的社會上，有很多商業上的機密或私人的通訊，都會藉由網路來傳遞訊息。 因此網路上所流傳的資料的安全性就顯得格外重要，因此衍生出許多的密碼技術，如公開金鑰密碼系統、 數位簽署、秘密分享、橢圓曲線密碼系統等等，希望藉由資訊技術達到保護資訊安全的目的，所以密碼學已成為資訊科學中重要的一環。

本研究主要的論述，是以群體為導向的加密系統。因此，會先介紹最常使用的秘密分享系統， 而後是 ElGamal 密碼系統與

秘密分享所衍生的 Elgamal門檻密碼系統，並針對此系統做一分析。 之後再利用橢圓曲線密碼系統，將其改良，並探討此密碼系統之優缺點。

2 秘密分享

在這章節我們將介紹最受歡迎的幾個秘密分享系統，以及其推導之過程。

2.1 分散秘密

假設你擁有一個秘密，可用一個整數M來表示。你想把這個整數拆開成兩半給三毛與四郎， 使得他們當中的任何一人都無法從已知的那一部分得到完整的秘密M。那該如何解決此問題呢？其實答案就在問題中。首先，選取一隨機整數 r 交給三毛，而後再將整數 $M-r$ 交給四郎。 如果要重建此秘密 M ，三毛與四郎兩人僅需聚在一起，然後亮出各自擁有的數並相加即可。

但有一技術層面問題必先克服的，那就是我們不可能選取隨機整數使得所有的整數具有同等的可能性 (無限多個具有相同概率的數加在一起不可能會等於1)。所以我們選取一個整數 n ， n 會大過所有可能出現的訊息 M ，並將 M 與 r 看做模 n 下的數。如此一來，只要在模 n 數系下的每個整數之概率均為 $\frac{1}{n}$ ，那就毫無問題的可在 模 n 數系下隨機選取一整數 r 。

基於此想法，如果今天我們想將一個秘密 M 分散給 w 個人，那我們就在模 n 下選取 $w-1$ 個隨機整數 $r_1, r_2, \cdots, r_{w-1}$ (mod n) 並一一交給其中的 $w-1$ 個人，剩下的那個人則交給整數 $M-\sum_{k=1}^{w-1} r_k$ (mod n)。

2.2 門檻法 (Threshhold Schemes)

在上面我們所介紹的是將一秘密 M 分散給 w 個人。但那方

法必須所有 w 個人都參與，才能解出 M ，比較不實用。 現在我們介紹僅需部分的人參與即可重建整個訊息的方法。

定義： 令 $t \leq w$ 為兩正整數。一個(t, w)–門檻法乃是將訊息 M 分享給 w 位參與者的一種方法：在此方法中， 只需其中任何 t 位參與者就可重建訊息 M ，若少於 t 位便無法重建 M 。

Shamir門檻法： 在一九七九年由沙密爾(Shamir)所提出，所以稱之為沙密爾門檻法或拉格蘭茲內插法(Lagrange Interpolation Scheme)。 其演算法如下：

1. 選取一質數 p ，大於所有的訊息也大於所有參與者的人數。此處所有的計算都在模 p 的數系中進行。 若用合成數代替，那下面所得到的矩陣有可能沒有乘法反元素。

2. 將訊息 M 表示成模 p 數系中的一個數，而我們要將訊息 M 分享給 w 位參與者，但只需其中的 t 位便可解出此一訊息。

3. 隨機選取 $t-1$ 個稱之為 s_i , $i = 1, 2, \cdots, t-1$ 作為多項式 $s(x)$ 第 i 項係數， 然後將 M 放在此多項式的常數項位置。所以我們得到一多項式

$$s(x) = M + s_1 x + s_2 x^2 + s_3 x^3 + \cdots + s_{t-1} x^{t-1} \ (\bmod p)$$

其常數項就是原訊息 M ，亦即 $s(0) \equiv M \ (\bmod p)$。

4. 對這 w 位參與者，我們先選取相異的整數 $x_1, x_2, \cdots, x_w \pmod p$，然後再交給每個人一秘密數對 (x_i, y_i)，其中$y_i \equiv s(x_i) \pmod p$。例如：$1, 2, 3, \cdots, w$乃是這些 x 值既合理而又自然的一個選擇。 所以我們就將數對$(1, s(1)), (2, s(2)), \cdots, (w, s(w))$交給這 w 個人，一人一組。質數 p 是公開的，但多項式 $s(x)$ 則保密。

5. 假設現在有 t 個人聚在一起分享彼此間的數對。為了簡化符號，我們假設這些數對為$(x_1, y_1), (x_2, y_2), \cdots, (x_t, y_t)$ 準備尋回訊息 M 。

6. 假設有一個 $t-1$ 次的多項式 $s(x)$ ，我們從其中的 t 個點來重建這多項式，此處 $y_k \equiv s(x_k) \pmod p$ 所以得到

$$y_k(x_k) = M + s_1 x_k^1 + s_2 x_k^2 + s_3 x_k^3 + \cdots + s_{t-1} x_k^{t-1} \pmod p$$

$1 \le k \le t$ ，而我們的未知數為$s_i,\ i = 1, 2, \cdots, t-1$及 M 。

7. 將上面的 t 個同餘式寫成矩陣形式

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{t-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{t-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} M \\ s_1 \\ s_2 \\ \vdots \\ s_{t-1} \end{pmatrix} \equiv \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_t \end{pmatrix} \pmod p$$

此係數矩陣，暫且稱之為 V ，也就是 Vandermonde 矩陣。

我們知道，如果此矩陣的行列式值在模 p 下不等於零，則此矩陣有唯一的解。 此行列式值可被證明就是

$$\text{detV}=\prod_{1\le j<k\le t}(x_k-x_j)$$

此值只有當兩個 x_i 一樣時才是0 (mod p)(此處的 p 為質數)。所以只要 x_i 相異，則此系統有唯一解。

8. 現在我們換一個角度來重建多項式 $s(x)$ ，由此引導我們得到這個多項式的一個公式並且可推得訊息 M 得一個公式。 我們的目標是重建一多項式 $s(x)$ ，而其中的t個值為$(x_k,y_k),k=1,2,3,\cdots,t$，因此， 我們會想到 t 次多項式

$$u(x)=(x-x_1)(x-x_2)(x-x_3)\cdots(x-x_t)$$

對每一個 $k=1,2,3\cdots,t$ ，將 $u(x)$ 除以 $x-x_k$ 得到一個 $t-1$ 次多項式

$$u_k(x)=\prod_{\substack{j=1\\j\neq k}}^{t}(x-x_j)$$

此多項式滿足$u_k(x_j)=0,\forall j\neq k$，若$x_i$兩兩相異，則$u_k(x_k)\neq 0$。 所以將每一個$u_k(x)$單位化，亦即除以$u_k(x_k)$，稱之為$l_k(x)$。 因此得到

$$l_k(x)\equiv\frac{u_k(x)}{u_k(x_k)}\equiv\prod_{\substack{j=1\\j\neq k}}^{t}\frac{x-x_j}{x_k-x_j}\ (\text{ mod } p\ )$$

顯而易見，我們有

$$l_k(x_j) \equiv \begin{cases} 1 & k = j \\ 0 & k \neq j \end{cases} \quad (\bmod p)$$

因此我們得到拉格蘭茲內插多項式

$$L(x) = \sum_{k=1}^{t} y_k l_k(x) = \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \\ j \neq k}}^{t} \frac{x - x_j}{x_k - x_j}$$

這個多項式滿足所有的條件$L(x_j) = y_j, 1 \leq j \leq t$，因為

$$L(x_j) \equiv \sum_{k=1}^{t} y_k l_k(x_j) \equiv y_j l_j(x_j) + \sum_{\substack{j=1 \\ j \neq k}}^{t} y_k l_k(x_j) \equiv$$

$$y_j \cdot 1 + \sum_{\substack{j=1 \\ j \neq k}}^{t} y_k \cdot 0 \equiv y_j \quad (\bmod p)$$

因此，透過Vandermonde矩陣的證明，我們知道 $s(x)$ 為經過這些點的唯一的 $t-1$ 次多項式，所以得到$L(x) = s(x)$。

9. 如果要重建秘密訊息 M ，只需計算 $L(0)$ 之值。所以可推得秘密訊息的公式：

$$M \equiv \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \\ j \neq k}}^{t} \frac{-x_j}{x_k - x_j} \ (\bmod p)。$$

例子：假設我們有一個$(5,8)-$門檻法，其質數 $p = 987541$ 。
而其中的五份為

$$(9853, 853), (4421, 4387), (6543, 1234), (93293, 78428), (12398, 7563)$$

試求出訊息。
解: 使用拉格蘭茲內插法， 算出經過這五點之多項式在 Mathematics 中輸入指令如下：

```
PolynomialMod[InterpolatingPolynomial[
{{9853,853},{4421,4387},{6543,1234},{93293,78428},{12398,7563}}
,x],987541]
```

其輸出為 $M = 678987, s_1 = 14728, s_2 = 1651, s_3 = 574413, s_4 = 4567414$
所以解得此一多項式為

$$s(x) = 678987 + 14728x + 1651x^2 + 574413x^3 + 456741x^4 。$$

可得訊息 $M = 678987$。

3 Elgamal 門檻密碼系統

Elgamal 門檻法是一個以群體為導向而設計出來的密碼系統。其理論基礎是以 Elgamal 密碼系統與秘密分享中的沙密爾門檻法 衍生而出。以下便是 Elgamal 門檻密碼系統的演算法過程以及例子。

3.1 演算法

今 B 欲傳送訊息給 A ，步驟如下：

加密：

1. A 先選取一個大質數 p ，及其中一原根 α 。
2. A 選取密鑰 a ，且計算 $\beta = \alpha^a$。 A 將(p, α, β)公開，但 a 保持私密。
3. 透過一授權機制造一密鑰 a 的 (t, n) 門檻，其對應的多項式為：

   $$f(x) = a + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$$

   假設機制中的參與者 P_i 所持有之秘密參數為(x_i , s_i), $i = 1, 2, \cdots, n$ ，其中 $s_i \equiv f(x_i) \pmod{p-1}$ 。
4. 今 B 欲傳遞一訊息 m 給 A ， B 先隨機選取一整數 k ，並計算密文 $C_A = (\alpha^k, m\beta^k)$。
5. B 將密文 C_A 上傳至機制中。
6. 授權機制將密文 $C_A = C$ 做一分散的動作，即計算密文 $C_i = (x_i, \alpha^{ks_i}, m\beta^k)$, $i = 1, 2, \cdots, n$ 。

解密：

A 從機制傳送來的密文中，選取 t 份文件，即 $C = \{C_1, C_2, \cdots, C_t\}$ ，而後再計算 $\alpha^{ks_ib_i}$ ，其中

$$b_i \equiv \prod_{\substack{j=1 \\ j\neq i}}^{t} \frac{-x_j}{x_j - x_i} \ (\bmod\ p-1)$$

，然後計算 $\prod_{\substack{j=1 \\ j\neq i}}^{t} \alpha^{ks_ib_i} \equiv \alpha^{ak} \equiv \beta^k \ (\bmod\ p)$

並求 β^k 在模 p 之下的乘法反元素 β^{-k} 之後 $m\beta^k\beta^{-k} = m$ 即可解讀訊息 m 。

3.2 例 子

加密：

1. A 選取一質數 $p = 263$ ，及其原根 $\alpha = 193$ 。
2. A 選取密鑰 $a = 161$ ，且計算 $\beta = \alpha^a = 193^{161} \equiv 257 \ (\bmod\ 263)$ 。A 將(193 , 263 , 257)公開，但 $a = 161$ 保持私密。
3. 透過一授權機制造一密鑰 $a = 161$ 的$(3, 4)$門檻，其對應多項式為

$$s(x) \equiv 161 + 88x + 211x^2 \ (\bmod\ 262)$$

假設機制中的參與者 $\{P_1, P_2, P_3, P_4\}$ ，所持有之秘密數對為

$$\{ (1, s(1)), (2, s(2)), (3, s(3)), (4, s(4)) \}$$
$$= \{ (1, 198), (2, 133), (3, 220), (4, 221) \}$$

4. 今 B 欲傳遞一訊息 $m = 157$ ，先隨機選取一整數 $k = 95$ ，並計算密文 $C = (\alpha^k, m\beta^k) = (193^{95}, 157 * 257^{95}) \equiv (247, 139) \pmod{263}$

5. B 將密文 C 上傳至機制中。

6. 授權機制將傳送給 A 的密文 C 做一分散的動作，即計算密文 $\{C_i\}, i = 1, 2, 3, 4$

$$\begin{aligned} C_1 &= \{x_1, \alpha^{ks_1}, m\beta^k\} \\ &= \{1, 193^{95*198}, 157 * 257^{95}\} \\ &= \{1, 193^{208}, 139\} \\ &= \{1, 64, 139\} \end{aligned}$$

$$\begin{aligned} C_2 &= \{2, 7, 139\} \\ C_3 &= \{3, 95, 139\} \\ C_4 &= \{4, 58, 139\} \end{aligned}$$

解密：

A 從機制傳送來的密文中，選取 3 份文件，即 $C = \{C_1, C_2, C_4\}$ ，而後再計算 $\alpha^{ks_ib_i}$ ，其中

$$\begin{aligned} b_1 &\equiv \frac{-2}{2-1} \times \frac{-4}{4-1} \equiv \frac{8}{3} \equiv 90 \pmod{262} \\ b_2 &\equiv \frac{-1}{1-2} \times \frac{-4}{4-2} \equiv -2 \equiv 260 \pmod{262} \\ b_4 &\equiv \frac{-1}{1-4} \times \frac{-2}{2-4} \equiv \frac{1}{3} \equiv 175 \pmod{262} \end{aligned}$$

然後計算

$$\begin{aligned}\prod_{\substack{j=1\\ j\neq i}}^{3}\alpha^{ks_ib_i} &\equiv 64^{90}*7^{260}*58^{175} \ (\bmod 263)\\ &\equiv 49*102*155\\ &\equiv 155\equiv\beta^r\end{aligned}$$

即可求出 $m = m\beta^r\beta^{-r} = 139*155^{-1} = 139*56 \equiv 157 \ (\bmod 263)$

3.3 安全性之分析

在Elgamal門檻密碼系統中，隱含了一個重大的缺點。那就是在加密的過程中，傳送者 B 將密文傳送至授權機制時， 可利用解離散對數的困難度來面對攻擊者的攔截。然而，當授權機制將密文分散好欲傳送給接收者 A 時， 卻已將解離散對數的難題轉換成解拉格蘭茲內插法的問題了。雖然，Elgamal 門檻密碼系統是以分散密文來避免攻擊者的截取， 但是攻擊者若能截取到所有的 n 份密文時，那麼攻擊者只需了解每個 b_i 的求法，便能解出明文 m 了。 如此一來此加密系統的安全性反而相對的降低了，所以針對此問題我們做了一些改進，將在第五章來介紹。

4 橢圓曲線密碼系統

在1980年代的中期，米勒(Miller)與寇伯立茲(Koblitz)將橢圓曲線引進密碼術當中，從而設計了一套新的密碼系統。 橢圓曲線密碼系統相較於傳統密碼系統的優點之一，在於後者使用了相當大的鑰匙來保持安全性，而前者似乎不需要如此龐大的鑰匙便能提供某種程度的安全。

4.1 橢圓曲線

下列方程式的圖形我們稱之為橢圓曲線

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

在此處 a , b 為任何適用的集合，如有理數、實數、複數、模 p 之下的整數或有限數體。令 $E_p(a,b) = E \cup \{\infty\}$, 其中 $4a^3 + 27b^2 \neq 0$ 。而在此處的 ∞ 稱之為『無限遠點(Point at infinity)或零點(Zero point)』。 此點最簡單的一個處理方式就是將它看作在 y 軸的最上方。這可以放在投影幾何的背景下嚴密的處理，但上面直關的概念對我們來講已足夠了。可參考Silverman與Tate二人所合寫的書：橢圓曲線上的有理點(RationalPoint On EllipticCurves)。 若將 y 軸最下方的點看成最上方的點，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，就是右邊那個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，同常我們假設 三次多項式 $E : y^2 = x^3 + ax + b$ 沒有重根。

4.2 橢圓曲線上的加法律

現在回到我們原先的橢圓曲線 $E_p(a,b)$ 上，來看看橢圓曲線上的點是如何相加的。

1. 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 二點劃一直線 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 $-R$ (即 y 座標變號)，亦即 $P+Q+R=\infty$ 且 $P+Q=-R$ 。 其圖說明此性質。

2. 令 $P=(x_1,y_1), Q=(x_2,y_2)$為橢圓曲線上的兩點，並且 $P\neq Q$ ，則 $P+Q=(x_3,y_3)$ 。此處

$$\begin{aligned} x_3 &\equiv m^2-x_1-x_2 \qquad (\bmod p) \\ y_3 &\equiv m(x_1-x_3)-y_1 \quad (\bmod p) \end{aligned}$$

   其中的m為

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

3. 若將 P 加 ∞ ，又如何呢？經過 ∞ 及 P 的直線是垂直的，此直線與 E 相交的第三個交點為 $(x,-y)$ 。再將此點反射回去對稱於$x-$軸之點就是原來的 P 點。因此我們有

$$P+\infty=P$$

我們來看下列的例子：

考慮在模5之下的橢圓曲線

$$y^2 \equiv x^3 + 2x + 3 \ (\bmod 5)$$

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

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

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 1^2 - 1 - 3 \equiv 2 \quad (\bmod 5)$$

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

亦即 $P + Q = (2,0)$ 。 若要計算 $2P = P + P$ 的話，則要求其切線斜率 $\frac{dy}{dx}$ 在點 $P = (1,4)$ 的值如下：

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

並由公式得到

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 0^2 - 1 - 3 \equiv 1 \quad (\bmod 5)$$

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

最後的答案則是 $2P = (1,1)$ 。

上述的加法規則滿足一般的加法特性，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， $2P = P + P$ ， $3P = P + P + P$ ， $kP = P + P + \cdots + P$ ，以此類推。

4.3 橢圓曲線加密系統

在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易的一種方法，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，並且稍後會被解碼。在這裡要注意一點，我們不能單純的將訊息編碼成某個點的x或y座標， 因為並不是所有的這類座標都會落在 $E(\bmod p)$ 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$E(\bmod p)$。

首先，使用者 A 選擇一私密鑰匙 a_A ，然後在產生一公開鑰匙 $\beta_A = a_A\alpha$ 。同樣的使用者 B 也選擇一私密鑰匙 a_B ，然後在產生一公開鑰匙 $\beta_B = a_B\alpha$ 。

為了將加密後的訊息 P_m 傳送給 B ， A 選擇一隨機整數 k ，並且產生一個由兩點所組成密文 C_m 。

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

在這 A 用的是 B 的公開鑰匙 β_B 。為了解開密文， B 用自己的私密鑰匙成上第一點，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 值，所以即使 β_B 是公開的鑰匙，也沒人能移除 或隱藏用的 $k\beta_B$ 。

4.4 例子

考慮在模179之下的橢圓曲線

$$E : y^2 \equiv x^3 + 2x + 7 \ (\bmod 179)$$

以及橢圓曲線上的一點 $\alpha = (111, 11)$ ，在將此點及橢圓曲線 $E_{179}(2, 7)$ 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 $\beta_A \equiv 12 * (111, 11) \equiv (111, 168) \pmod{179}$ 。使用者 B 同樣選取一私密鑰匙 $a_B = 9$ ，並計算其公開鑰匙 $\beta_B \equiv 9 * (111, 11) \equiv (20, 23) \pmod{179}$ 。

若 A 要將訊息 $m = 5$ 加密後傳給 B ，其進行步驟如下：

1. 欲傳送訊息 $m = 5$ 加密後傳送給B，所以選擇 $K = 10$ 。可以成功的將 m 轉換成 $x = 5 * 10 + 1$ ， $y = 11$ 的點 $P_m = (51, 11)$。

2. 選取隨機整數 $k = 11$ 。

3. 計算

$$\begin{aligned} y_1 &\equiv k\alpha \pmod{p} \\ &\equiv 11 * (111, 11) \pmod{179} \\ &\equiv (152, 26) \end{aligned}$$

計算

$$\begin{aligned} y_2 &\equiv P_m + k\beta \pmod{p} \\ &\equiv (51, 11) + 11 * (20, 23) \pmod{179} \\ &\equiv (51, 11) + (164, 19) \\ &\equiv (156, 18) \end{aligned}$$

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

$$\begin{aligned} y_2 - a_B y_1 &\equiv P_m + k\beta_B - a_B(k\alpha) \ (\bmod\ p\ ) \\ &\equiv (51, 11) + 11 * (20, 23) - 9 * [11 * (111, 11)] \ (\bmod\ 179\ ) \\ &\equiv (51, 11) + (164, 19) - 9 * (152, 26) \\ &\equiv (51, 11) + (164, 19) - (164, 19) \\ &\equiv (51, 11) \\ &\equiv P_m \end{aligned}$$

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 $k\beta_B$

5 橢圓曲線版的 Elgamal 門檻密碼系統

由於橢圓曲線適用於 Elgamal 密碼系統中，相對之下，橢圓曲線也一樣能運用於 Elgamal 門檻密碼系統。 因此，接下來便是介紹橢圓曲線版的 Elgamal 門檻密碼系統演算法以及舉例。

5.1 演算法

加密：

1. A 選取一橢圓曲線 $E_p(a,b)$ ， p 是一個大質數，並選取曲線上的一點 α ,然後計算 α 的週期 λ 。

2. A 選取密鑰 a ，且計算 $\beta = a\alpha$ 。並將 (E, α, β) 公開，但 a 保持私密。

3. 透過一授權機制造一密鑰 a 的 (t,n) 門檻，其對應的多項式為：

   $$f(x) = a + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$$

   假設機制中的參與者 P_i 所持有之參數為(x_i , s_i), $i = 1, \cdots, n$，其中 $s_i = f(x_i) \pmod{\lambda}$

4. 今 B 欲傳遞一訊息 m 給 A ，先將 m 轉換成橢圓曲線上的一個點 P_m

5. B 隨機選取一整數 k ，並計算密文 $C_A = (k\alpha, P_m + k\beta)$

6. B 將密文 C_A 上傳至機制中。

7. 授權機制將密文 $C_A = C$ 做一分散的動作，即計算密文 $C_i = (x_i^a, ks_i\alpha, P_m + k\beta)$, $i = 1, 2, \cdots, n$ 。

解密：

A 從機制傳送來的密文中，選取 t 份文件，即$C = \{ C_1 , C_2 , \cdots , C_t \}$，並先使用自己的密鑰 a 解出每個 x_i 的值，而後再計算 $ks_ib_i\alpha$ ，

其中

$$b_i \equiv \prod_{\substack{j=1 \\ j\neq i}}^{t} \frac{-x_j}{x_j - x_i} \ \ (\bmod \lambda)$$

然後計算 $\sum_{\substack{j=1 \\ j\neq i}}^{t} ks_ib_i\alpha \equiv ka\alpha = \begin{cases} k\beta , & \text{if t is odd} \\ -k\beta , & \text{if t is even} \end{cases} \ (\bmod p)$

之後 $P_m + k\beta - k\beta = P_m$ 即可解讀訊息 P_m

5.2 例 子

1. (t 是奇數)加密:

   A 考慮在模263下的橢圓曲線

   $$E : y^2 \equiv x^3 + x + 6 \ \ (\bmod 263)$$

   並選取 $E_{263}(1, 6)$ 上的一點 $\alpha = (2, 4)$ ，並計算點 α 之秩 λ ，使得 $\lambda(2, 4) = \infty$ ， 即可求得 $\lambda = 274$ ，並將 $\alpha = (2, 4)$ 以及 $E_{263}(1, 6)$ 公開。

   選取密鑰 $a = 161$ ，以及一隨機整數 $k = 95$ ，且計算 $\beta = a\alpha = (37, 48)$ ， $k\beta = (172, 75)$ 。

   透過一授權機制造一密鑰為 $a = 161$ 的 $(3, 10)$ 門檻，其對應多項式為：

   $$s(x) = 161 + 88x + 211x^2$$

假設機制中的10位參與者所持有之秘密數對為

$$\begin{aligned} & \{\ (\ 1, s(1)\ ), (\ 2, s(2)\ ), (\ 3, s(3)\ ), \cdots, (\ 10, s(10)\ )\ \} \\ = \ & \{\ (1, 186), (2, 85), (3, 53), \cdots, (10, 221)\ \} \end{aligned}$$

今 B 欲傳遞一信息 $m = 5$ 給 A ，先將其轉換成橢圓曲線上的一點 $P_m = (51, 141)$ ，並計算密文

$$\begin{aligned} C &= \{\ k\alpha\ ,\ P_m + k\beta\ \} \\ &= \{(190, 122), (51, 141) + (172, 75)\} \\ &= \{(190, 122), (262, 261)\} \end{aligned}$$

而後 B 將密文 C ，上傳至機制中。

授權機制將傳送給 A 的密文 C 做一分散的動作，即計算密文 $\{C_i\}, i = 1, 2, \cdots, 10$

$$\begin{aligned} C_1 &= \{1^{161}, ks_1\alpha, P_m + k\beta\} \\ &= \{1, 186(190, 122), (51, 141) + (172, 75)\} \\ &= \{1, (51, 122), (262, 261)\} \end{aligned}$$

$$\begin{aligned} C_2 &= \{2^{161}, (87, 71), (262, 261)\} \\ C_3 &= \{3^{161}, (194, 21), (262, 261)\} \\ C_4 &= \{4^{161}, (219, 187), (262, 261)\} \\ &\vdots \\ C_{10} &= \{10^{161}, (219, 76), (262, 261)\} \end{aligned}$$

解密:

A 從機制傳送來的密文中，選取 3 份文件，即 $C = \{C_1, C_2, C_4\}$ ，並使用自己的密鑰解出每個 x_i 的值，即 $x_1 = 1, x_2 = 2, x_4 = 4$ ，而後再計算

$$\begin{aligned} b_1 &\equiv \frac{-2}{2-1} \times \frac{-4}{4-1} \equiv \frac{8}{3} \equiv 94 \pmod{274} \\ b_2 &\equiv \frac{-1}{1-2} \times \frac{-4}{4-2} \equiv -2 \equiv 272 \pmod{274} \\ b_4 &\equiv \frac{-1}{1-4} \times \frac{-2}{2-4} \equiv \frac{1}{3} \equiv 183 \pmod{274} \end{aligned}$$

然後計算

$$\begin{aligned} \Sigma\, ks_i b_i \alpha &\equiv 94(51, 122) + 272(87, 71) + 183(219, 187) \\ &\equiv (97, 193) + (141, 83) + (48, 42) \\ &\equiv (172, 75) \\ &\equiv k\beta \pmod{263} \end{aligned}$$

而

$$\begin{aligned} P_m &\equiv (262, 261) - (172, 75) \pmod{263} \\ &\equiv (262, 261) + (172, -75) \\ &\equiv (51, 141) \end{aligned}$$

即可解出我的信息。

2. (t 是偶數)加密:

考慮在模59下的橢圓曲線

$$E : y^2 \equiv x^3 + 2x + 6 \pmod{59}$$

並選取一個滿足 $E_{59}(2,6)$ 上的一點 $\alpha = (1,3)$ ，並計算點 α 之秩 λ ，使得 $\lambda(1,3) = \infty$ ，即可求得 $\lambda = 11$ ，並將 $\alpha = (1,3)$ 以及 $E_{59}(2,6)$ 公開。

選取密鑰 $a = 7$ ，以及一隨機整數 $k = 13$ ，並計算 $\beta = a\alpha = (54,15)$ ， $k\beta = (8,48)$ 。

透過一授權機制造一密鑰為 $a = 7$ 的 $(4,10)$ 門檻，其對應多項式為：

$$s(x) = 7 + x + x^2 + x^3$$

假設機制中的10位參與者所持有之秘密數對為

$$\begin{aligned} & \{\ (\ 1, s(1)\ ), (\ 2, s(2)\ ), (\ 3, s(3)\ ), \cdots, (\ 10, s(10)\ )\ \} \\ = \ & \{\ (1,10), (2,10), (3,2), \cdots, (10,6)\ \} \end{aligned}$$

今 B 欲傳遞一信息 $m = 5$ 給 A ，先將其轉換成橢圓曲線上的一點 $P_m = (51,3)$ ，並計算密文

$$\begin{aligned} C &= \{\ k\alpha\ ,\ P_m + k\beta\ \} \\ &= \{(20,50), (51,3) + (8,48)\} \\ &= \{(20,50), (57,17)\} \end{aligned}$$

而後 B 將密文 C ，上傳至機制中。

授權機制將傳送給 A 的密文 C 做一分散的動作，即計算密文 $\{C_i\}, i = 1, 2, \cdots, 10$

$$\begin{aligned} C_1 &= \{1^7, ks_1\alpha, P_m + k\beta\} \\ &= \{1, 10(20,50), (51,3) + (8,48)\} \end{aligned}$$

$$= \{1, (20, 9), (57, 17)\}$$

$$\begin{aligned} C_2 &= \{2^7, (20, 9), (57, 17)\} \\ C_3 &= \{3^7, (54, 44), (57, 17)\} \\ C_4 &= \{4^7, (13, 39), (57, 17)\} \\ &\vdots \\ C_{10} &= \{10^7, (1, 3), (57, 17)\} \end{aligned}$$

解密:

A 從機制傳送來的密文中，選取 4 份文件，即 $C = \{C_1, C_2, c_3, C_4\}$ ， 並使用自己的密鑰解出每個 x_i 的值，即 $x_1 = 1, x_2 = 2, x_3 = 3, x_4 = 4$ ， 而後計算 b_i 的值

$$\begin{aligned} b_1 &\equiv \frac{-2}{2-1} \times \frac{-3}{3-1} \times \frac{-4}{4-1} \equiv 7 \pmod{11} \\ b_2 &\equiv \frac{-1}{1-2} \times \frac{-3}{3-2} \times \frac{-4}{4-2} \equiv 6 \pmod{11} \\ b_3 &\equiv \frac{-1}{1-3} \times \frac{-2}{2-3} \times \frac{-4}{4-3} \equiv 7 \pmod{11} \\ b_4 &\equiv \frac{-1}{1-4} \times \frac{-2}{2-4} \times \frac{-3}{3-4} \equiv 1 \pmod{11} \end{aligned}$$

然後計算

$$\begin{aligned} \Sigma k s_i b_i \alpha &= 7(20, 9) + 6(20, 9) + 7(54, 44) + 1(13, 39) \\ &= (8, 11) + (1, 56) + (13, 39) + (13, 39) \\ &= (8, 11) \\ &= -k\beta \end{aligned}$$

所以真正的， $k\beta \equiv (8,-11) \equiv (8,48) \pmod{59}$

$$\begin{aligned} P_m &= (57,17) - (8,48) \\ &= (51,3) \end{aligned}$$

即可解出我的信息。

5.3 安全性之分析

在研究中，我們利用橢圓曲線去改良 Elgamal 門檻法群體加密系統，强化其加密性。因為橢圓曲線的關係， 將原本在 Elgamal 門檻法的數對，化成曲線上的點。也正因為如此，我們所分散的密文可能會造成重複的情況。比如說， 張三所得的密文為$\{1,(20,9)\}$，李四所得的密文為$\{2,(20,9)\}$，而六爺所得的密文為$\{5,(20,9)\}$。 相較於原本的 Elgamal 門檻法群體加密系統，其不同點在於，本系統會因參與者持有之參數的不同，但是卻擁有相同的密文。 此點容易混淆攻擊者的判斷，因為以群體為導向的密碼系統在解密的過程中需要特定的密文文件數目， 但現在密文文件的空間變小，可是解密的門檻卻沒有相對降低。所以對攻擊者而言，此點會造成截取資料上的困擾。 再者，因為橢圓曲線的關係，我們所求出的 $k\beta$ 值會因為選取門檻法的不同而產生共軛數的存在，這也是此系統的優點之一。 而在授權機制方面我們也稍作改變，當機制欲傳送密文給 A 時，我們將 A 登錄在機制的密碼當成密鑰， 對係數 x_i 做加密。如此一來，攻擊者即使獲取所有分散的密文，為了要解出 x_i 仍要面對解離散對數的問題。

然而 Elgamal 門檻密碼系統的缺點便在於我們所選取的質

數 p 可能必須有所選擇，避免我們在求 b_i 時 p 與 $x_j - x_i$ 不互質。 而這一點也是此密碼體系需要在改進之處。

References

[1] J. Pieprzyk,T. Hardjono,J. Seberry, Fundamentals of Computer Security, 361-366, 1998.

[2] N.Koblitz, Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203-209, 1987.

[3] V. S. Miller, Use of elliptic curves in cryptography. In H.C. Williams, editor, *Advances in Cryptology (CRYPTO'85)*. Lecture Notes in Computer Science No. 218, pages 417-426. Springer, Berlin Heidelberg New York, 1986.

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

[5] 賴溪松,韓亮,張真誠."近代密碼學及其應用",1995

[6] Lawrence C. Washington,Elliptic Curves Number Theory and Cryptography,159-173,2003