# 目錄

# 1 簡介

現在隨著科技進步，人與人之間溝通頻繁，更需要精密的保密措施，尤其是網路的發達，資訊的傳遞越來越透明化，隨時都有機密外洩的危險。利用電子系統來保護資料和傳達訊息，對於我們生活中，已經是不可或缺的一部分。大家對於密碼的第一印象應該是很複雜的東西，或者是一堆很大的數字，這些看法其實都沒錯，很多密碼系統的確是數字組成，在經過轉換之後，才能破解。現在密碼技術已經進步不少，要破解是不容易，只有依賴更強大的破解方法才能夠辦到。

網路通訊是現在人常用的通訊方法，開放性的網路環境是相當危險的，任何有心人士都可以窺探網路世界的秘密，如果要保護網路世界的安全，必須有相關的安全機制。常用的防火牆和密碼驗證，就是相關的做法，但是在即時通訊中，常常爲了便利忽略安全的重要性，攻擊者容易從通訊過程盜取重要資訊，例如是信用卡資料。

另外，現在各種科技公司隨著市場需求日異擴大，員工人數成長，隨之開會的規模也是越來越大，所以，召開網路會議已經是常見的形式。我們就秘密的網路會議來說，如果要保護會議中訊息的安全性，必須在召開會議之前，讓主席和所有參與者共享相同的會議鑰匙，確認會議的合理性。然而在開放式的網路環境中，主席如何將會議鑰匙安全的分派給各位參與者，在密碼學的研究上稱做會議鑰匙分配協定。

而建立鑰匙過程中可能出現的攻擊者，我們可以分成以下三種。
(1) 竊聽者：這種攻擊者藉由觀察主席傳送的訊息，企圖推導有關的訊息，例如主席的私密鑰匙、參與者的私密鑰匙、會議鑰匙等等。
(2) 惡意的攻擊者：這類型攻擊者可能會假冒主席開會，假冒參與者進行會議，或是故意傳送錯誤訊息干擾會議進行，讓會議的參與者無法重建會議鑰匙。

(3) 不誠實的參與者：這類攻擊者是屬於參與者成員之一，在會議進行中，干擾其他參與者，使得誠實的參與者無法重建正確會議鑰匙。

綜合以上的安全性討論，我們可以知道會議鑰匙分配協定，除了必須滿足機密性外，還必須滿足鑑別性，機密性的要求是必須確保只有參與者可以解出會議鑰匙，其他人沒有足夠資訊能夠推導出來，並且只有會議參與者能夠計算出相同的會議鑰匙。鑑別性則是要求參與者必須能驗證接收到的會議鑰匙訊息，已確認該訊息是主席所傳送，防止有人假冒主席身分來開會。

# 2 背景知識

## 2.1 秘密分享

我們先想像一個情形，如果你中了樂透或是統一發票頭獎，突然多出一筆錢，你會怎麼處理，是存入銀行呢？還是分給家人？當然，存入銀行以後應該是留給孩子，但是，銀行保險箱號碼應該給誰呢？每個孩子都有一份的話，不知道何時哪一個貪心的小孩會全部領走，而你又不希望大家失和，以爲你是自私的。你應該如何處理呢？或許我們可以用秘密分享的觀念來處理這個問題。

接著我先提一下秘密分散的想法，假設你擁有一個秘密，先用整數$A$代替。你想先做的是把秘密分成兩半，一半分給小明，另一半給大毛。如此一來，他們二人無法知道完整的秘密，也不會獲得利益。除非他們二人一起合作，才可以重建秘密。其實，這個想法不難，我們只要將秘密分成兩個整數，其中之一爲$s$，另外一個爲$A-s$，小明和大毛只要一起將兩個數相加，就可以將秘密$A$回復。

我們會發現一個技術問題，因爲不可能隨機選取一個整數，使得所有的整數都具有相同可能性(無限多個具有相同機率的數加在一起不可能會是1)。所以我們可以選一個整數$n$，這個數會大過所有可能出現的信息$A$，並將$A$和$s$看作模$n$中的數。所以，只要定義在模$n$數系中每一整數之機率爲$1/n$，那就沒有問題可以在模$n$中選取一個隨機整數了。

寫到這裡，大家應該會問一個問題，秘密可不可以分給三個人、四個人、或是更多人呢？答案是肯定的。三個人我們可以這樣做，分成$s$，$r$，$A-s-r$，那麼只要三者將秘密集合，就可以知道原來的$A$。一般來說，我們想將$A$分散給$m$個人，那麼我們必須分成$x_1, x_2, x_3, \cdots, x_{m-1} (\mathrm{mod}\ n)$，並

且交給其中$m-1$個人，剩下那個人則給整數$A-\sum_{k=1}^{m-1}x_k \pmod{n}$。

### 2.1.1 門檻法

在第一節我們提到了分享秘密的方法，大家應該會發現問題，我們將秘密分散給多數的擁有者，然而，秘密重建時，卻需要所有人都在場，秘密才可以重建。如果有人缺席，那要怎麼處理？所以我們可以思考一下，是否有只需要一部份人就可以完成的方法，這就是我接下來要提到的門檻法。

在美國和蘇俄冷戰時期，兩國常常用威力強大的軍事武器彼此牽制，例如核子武器。但是，這樣機密的設備安全一定要更加慎重，擁有決定權的人士也要有一定影響力，才能確保軍事設施的安全性。在電影中常看到，一個飛彈按鈕有三把鑰匙孔，只要兩把鑰匙同時在場，就可以開啓按鈕。

那麼像這種情況當然不適用前一節的秘密分享法，因爲將秘密分給三巨頭，如總統、副總統和國防部長，不一定三人會有時間同時出現，或許有人出國去了，所以秘密分想法是有困難的，也不太符合緊急狀況的情形。

因爲有太多的不定因素，秘密分享法是不太實用，我們可以改用門檻法來解決類似問題，也就是說，只要部份的秘密擁有者，我們就可以回復秘密。以下，我先簡單介紹門檻法的基本定義。

定義：令$t \leq w$，$t$和$w$爲兩個正整數，如果我們要使用一個$(t,w)$門檻法，這是將訊息$M$分給$w$位秘密擁有者的方法，在這個方法中，只需要其中任何$t$位擁有者，我們就可以回復秘密$M$，假如少於$t$個便沒辦法重建

$M$。

1979年，由沙密爾提出的方法，稱作沙密爾門檻法或是拉格蘭茲內插法，是來自於我們高中所學過的簡單代數，例如已知兩點可以決定一條直線，已知三點可以決定一個二次式等等。以下就是這個方法的內容。

首先選取一個質數$p$，大於所有的訊息也大於所有參與者人數。此處所有計算都在模$p$數系中進行的，假若用合成數代替，那麼下面所得到的矩陣可能沒有乘法反元素。

將信息$M$表示成模$p$數系中的一個數，而我們的目標是要將信息$M$分享給$w$位參與者，但只要其中任何的$t$位就可以重建此一信息$M$，先隨機的選取模$p$下$t-1$個整數稱之爲$s_i$，$i=1,2,3,\cdots,t-1$作爲多項式$s(x)$第$i$項的係數，然後將信息$M$安置在常數項的位置。所以我們得到一個多項式

$$s(x) = M + s_1x + s_2x^2 + s_3x^3 + \cdots + s_{t-1}x^{t-1} \pmod{p}$$

其常數項就是原信息$M$，亦即$s(0) \equiv M(\mathrm{mod}p)$。對這$w$位參與者，我們先選取相異的整數$x_1, x_2, x_3, \cdots, x_w(\mathrm{mod}\ p)$，然後再交給每個人一秘密數對$(x_i, y_i)$，其中$y_i \equiv s(x_i) \pmod{p}$。舉例來說：$1,2,3,\cdots,w$乃是這些$x$值既合理又自然的一個選擇，所以我們將數對

$$(1, s(1)), (2, s(2)), (3, s(3)), \cdots, (w, s(w))$$

交給這$w$個人，一人一個。質數$p$是所有人都知道的，但多項式$s(x)$則保持秘密。

### 2.1.2 分析

Shamir門檻法秘密分享有三個主要的問題：

1. 不能有效地防止分發者的欺騙，即是分發者在分發子秘密時，可能會給某個分享者分發假的子秘密，使在恢復秘密的成員無法恢復出正確的秘密，多數的文獻忽略了這一點。

2. 不能抵抗分享者的欺騙，即是有些分享者在恢復秘密時提供假的子秘密，而使其他的成員無法恢復正確的秘密。

3. 在恢復秘密的階段，參與秘密恢復的成員會將自己的子秘密交付給一位合成者，由合成者來代表所有參與者恢復共享秘密，大部份的文獻中，合成者本身就是參與秘密恢復的共享者，這就難以保證合成者在恢復秘密後不會提供假的秘密給其他參與秘密恢復的分享者。

## 2.2 動態秘密分享

在本章中，我們提出基於離散對數問題的動態秘密分享策略；此策略不僅檢測出包括分發者在內的所有參與者的欺騙行爲，又可以無限次分發且還原不同的秘密，並具有結構簡單、安全性高等優點。與已有可驗證的秘密分享方案相比較，此驗證計算複雜度較小，數據傳輸量小，因此效率較高。 其演算法如下：

### 2.2.1 秘密分發階段

1. $U_D$ 是系統秘密的分發者， $U_D$ 選取一個大質數 $p$ 及模 $p$ 的一個原根 $g$ , $p$ 大於所有的訊息也大於所有參與者的人數。 $U_i$ 是第 $i$ 個參與者，其身份識別碼爲 $\delta_i$ $(i = 1, 2, \cdots, w)$。

2. 將訊息 $k$ 表示成模 $p$ 數系中的一個數，而我們要將訊息 $k$ 分享給 $w$ 位參與者，但只需其中的 $t$ 位便可解出此一訊息。 $U_D$ 先計算 $K = g^k \pmod p$。

3. 每一個 $U_i$ $(i = 1, 2, \cdots, w)$ 隨機選一整數 $x_i$ 爲私鑰，算出 $X_i = g^{x_i}$ 並傳送給 $U_D$ 。

4. $U_D$ 隨機選取 $t$ 個整數 $a_j$ $(j = 0, 1, 2, \cdots, t-1)$ 作爲多項式 $f(x)$ 中 $x^j$ 項的係數。所以得到一多項式

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{t-1} x^{t-1} \pmod{p-1},$$

   $U_D$ 計算 $s = k + a_0 \pmod{p-1}$ , 並算出 $A_j = g^{a_j} \pmod p$ , $j = 0, 1, 2, \cdots, t-1$; 以及每一個 $f(\delta_i) \pmod{p-1}$ , $i = 1, 2, \cdots, w$ 。

5. $U_D$ 隨機選取整數 $r$ , 並計算 $R = g^r \pmod p$。
   對 $i = 1, \cdots, w$ 算出 $b_i = f(\delta_i) + X_i{}^r \pmod p$, 以及 $c_i = s + X_i{}^r \pmod p$。

6. $U_D$ 將 $p$ , $g$ , $R$ , $K$ ; $b_i$ , $c_i$ , $\delta_i$ ( $i = 1, \cdots, w$ ) ; $A_j$ ( $j = 0, 1, \cdots,$ $t-1$ ) 公開。

### 2.2.2 訊息驗證階段

1. 每一個 $U_i$ $(i = 1, 2, \cdots, w)$ 使用其私鑰 $x_i$ 算出 $R^{x_i} \pmod p$ 稱之爲 $D_i$ , 然後算出 $B_i = b_i - D_i \pmod p$ 及 $C_i = c_i - D_i \pmod p$。

2. 每一個 $U_i$ $(i = 1, 2, \cdots, w)$ 可驗證下列等式是否成立

$$g^{C_i} = K \cdot A_0 \pmod{p}, \quad g^{B_i} = \prod_{j=1}^{t} {A_{j-1}}^{{\delta_i}^{j-1}} \pmod{p}$$

若等式成立，說明了 $U_D$ 沒有欺騙行爲。

若等式不成立，則公開 $U_D$ 的欺騙行爲。

#### 2.2.3 證明驗證成立

1. 驗證 $g^{C_i} = K \cdot A_0 \pmod{p}$

證明：

因爲 $D_i = R^{x_i} = (g^r)^{x_i} = (g^{x_i})^r = {X_i}^r \pmod{p}$

所以 $C_i = c_i - D_i = s + {X_i}^r - {X_i}^r = s \pmod{p}$

又因爲 $s = k + a_0 \pmod{p-1}$

$\Rightarrow C_i = (k + a_0) + n \cdot (p-1)$

且 $K = g^k \pmod{p-1}$，$A_0 = g^{a_0} \pmod{p-1}$

$\therefore g^{C_i} = g^{(k + a_0) + n \cdot (p-1)} = g^k \cdot g^{a_0} \cdot g^{n \cdot (p-1)} = K \cdot A_0 \cdot (g^{p-1})^n$

$= K \cdot A_0 \pmod{p}$ 因此得到左式＝右式，故得證。

2. 驗證 $g^{B_i} = \prod_{j=1}^{t} {A_{j-1}}^{{\delta_i}^{j-1}} \pmod{p}$

證明：

因爲 $D_i = {X_i}^r \pmod{p}$

所以 $B_i = b_i - D_i = f(\delta_i) + {X_i}^r - {X_i}^r = f(\delta_i) \pmod{p}$

已知 $A_i = g^{a_i} \pmod{p}$

將 $\delta_i$ 代入 $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{t-1} x^{t-1} \pmod{p-1}$

得到

$f(\delta_i) = (a_0 + a_1 \delta_i + a_2 {\delta_i}^2 + a_3 {\delta_i}^3 + \cdots + a_{t-1} {\delta_i}^{t-1}) + n \cdot (p-1)$

$\therefore$左式$= g^{f(\delta_i)} = g^{(a_0 + a_1 \delta_i + a_2 {\delta_i}^2 + a_3 {\delta_i}^3 + \cdots + a_{t-1} {\delta_i}^{t-1}) + n \cdot (p-1)}$

$= g^{(a_0 + a_1 \delta_i + a_2 {\delta_i}^2 + a_3 {\delta_i}^3 + \cdots + a_{t-1} {\delta_i}^{t-1})} \cdot (g^{p-1})^n$

$= g^{(a_0 + a_1 \delta_i + a_2 {\delta_i}^2 + a_3 {\delta_i}^3 + \cdots + a_{t-1} {\delta_i}^{t-1})} \pmod{p}$

$= g^{a_0} \cdot g^{a_1 \delta_i} \cdot g^{a_2 {\delta_i}^2} \cdot \cdots \cdot g^{a_{t-1} {\delta_i}^{t-1}}$

$= (g^{a_0}) \cdot (g^{a_1})^{\delta_i} \cdot (g^{a_2})^{{\delta_i}^2} \cdot \cdots \cdot (g^{a_{t-1}})^{{\delta_i}^{t-1}}$

$$= A_0 \cdot {A_1}^{\delta_i} \cdot {A_2}^{{\delta_i}^2} \cdot \cdots \cdot {A_{t-1}}^{{\delta_i}^{t-1}}$$
$$= \prod_{j=1}^{t} {A_{j-1}}^{{\delta_i}^{j-1}} = \text{右式，故得證。}$$

#### 2.2.4 秘密還原階段

1. 假設有 $t$ 位說是 $U_1$ , $U_2$ ,$\cdots$, $U_t$ 共同還原秘密。每個參與的成員 $U_i$ 將各自的 $B_i$ 傳送給合成者 $U_A$ 。

2. 合成者 $U_A$ 首先驗證 $g^{B_i} = \prod_{j=1}^{t} {A_{j-1}}^{{\delta_i}^{j-1}} \pmod p, i = 1 ,\cdots, t$是否成立。若成立，說明分享者 $U_i$ 沒有欺騙行爲；若不成立，則要求其重新發送自己手中的資訊。

3. 當 $U_A$ 獲得一組數據 ( $\delta_i$ , $B_i$ ), $i = 1 ,\cdots, t$,由Lagrange內插多項式求出經過此 $t$ 點的 $t-1$ 次多項式 $L(T)$ ,並將 $L(0)$ 告知參與秘密還原的分享者。

4. 分享者驗證 $A_0 = g^{L(0)} \pmod p$ 是否成立，如果成立，則說明 $U_A$ 沒有欺騙行爲，最後，分享者 $U_i$ 計算 $C_i - L(0)$ ；就是所要求的秘密 $k$ ,因爲 $C_i = s$ ,$L(0) = a_0$

## 2.3 橢圓曲線

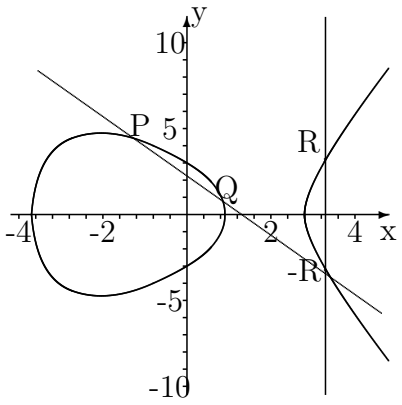
在1980年代的中期，米勒(Miller)與寇伯立茲(Koblitz)將橢圓曲線引進密碼術當中，從而設計了一套新的密碼系統。橢圓曲線密碼系統相較於傳統密碼系統的優點之一，在於後者使用了相當大的鑰匙來保持安全性，而前者似乎不需要如此龐大的鑰匙便能提供某種程度的安全。下列方程式的圖形我們稱之爲橢圓曲線

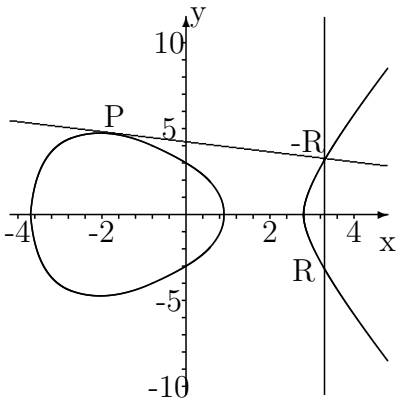
$$E : y^2 \equiv x^3 + ax + b \pmod{p}$$

在此處 $a$ , $b$ 爲任何適用的集合，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 $\infty$ 稱之爲『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，但上面直觀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)；或L.C. Washington的Elliptic Curves Number Theory and Cryptography。若將 $y$ 軸最下方的點看成最上方的點，則 $\infty$ 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，通常我們假設三次多項式 $E : y^2 = x^3 + ax + b$ 沒有重根。

### 2.3.1 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。




圖一橢圓曲線上$P+Q=R$　　圖二橢圓曲線上$P+P=R$

1. 橢圓曲線 $E$ 上的相異兩點 $P$ 及 $Q$ 相加，可經由圖一中觀察 $P+Q=R$ ，如下：經過 $P$ 及 $Q$ 二點劃一直線 $L$ 。直線 $L$ 與橢圓曲線 $E$ 交於 $-R$ ，然後取 $E$ 上與 $-R$ 對稱於$x$-軸的點 $R$ (即 $y$ 座標變號)。

2. 橢圓曲線 $E$ 上的一點 $P$ ，計算 $P+P=R$ ，可經由圖二中觀察 $P+Q=R$ ，如下：經過 $P$ 點畫橢圓曲線 $E$ 的切線 $L$ 。直線 $L$ 與橢圓曲線 $E$ 交於 $-R$ ，然後取 $E$ 上與 $-R$ 對稱於$x$-軸的點 $R$ 。

3. 加法單位元素：我們發現 $P+\infty=P$ ，因爲經過 $P$ 與 $\infty$ 點的直線是垂直$x$-軸的，所以此直線將會與 $E$ 自然相交於 $-P$ ，而再取對稱點即爲 $P$ ，使得 $P+\infty=P$ 。同時亦可證明此加法具有結合性與交換性：

$$(P+Q)+R=P+(Q+R)$$

$$P+Q=Q+P$$

因此，橢圓曲線 $E$ 上的點在此加法運算之下則形成一個交換群，無限遠的點 $\infty$ 就是橢圓曲線的加法單位元素。

4. 橢圓曲線加法運算的公式：

令 $P=(x_1,y_1),Q=(x_2,y_2)$ 爲橢圓曲線上的兩點，並且 $P\neq Q$ ，則

$P+Q=R=(x_3,y_3)$ 。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$m$爲

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

**2.3.2** 如何用橢圓曲線上的點來表示明文？

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。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$j=0,1,\cdots,K-1$，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？僅需計算$\frac{x}{K}$，取其整數部分即可。所以$m=[\frac{x}{K}]$，此處$[\frac{x}{K}]$爲高斯符號，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$0\le m\le 16$。

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$50, 51, \cdots, 59$。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：$m = [\frac{51}{11}] = 5$。

#### 2.3.3 橢圓曲線加密系統

在現有的數種橢圓曲線的加/解密方法中，我們只看其中最簡易的一種方法。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，因爲並不是所有的這類座標都會落在$E(\text{mod } p)$ 上。在一個鑰匙交換系統中，其加/解密系統需要兩個參數，$\alpha$和橢圓曲線$E(\text{mod } p)$。

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 $\beta_B = a_B\alpha$ 。

爲了將訊息 $P_m$ 加密後傳送給 $B$ ， $A$ 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 $\beta_B$ 。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 $k$ 值，所以即使 $\beta_B$ 是公開的鑰匙，也沒人能移除或隱藏用的 $k\beta_B$ 。

# 3 會議鑰匙分配系統

主席計算會議鑰匙分配的計算成本和參與者人數成正比，此系統利用利用鑑別加密法和$(t,n)$門檻秘密分享法所設計，達到降低成本的優點，此系統可以讓參與者鑑別會議鑰匙是否爲主席所分派，另外也考慮了參與者無法開會的情形，因此利用了$(t,n)$門檻法的限制，參與者人數必須達到門檻值以上，才能重建會議鑰匙以進行會議。系統分爲系統初始、次鑰匙分派、出席會議宣告、會議鑰匙產生四階段，以下介紹各階段過程：

## 3.1 系統初始階段

系統管理者建立並定義下列參數與函數：

$p$：爲一個大質數

$q$：爲一個$p-1$的大質因數

$g$：爲模$p$的一個原根

$H(.)$：表示一個Hash函數

然後系統公佈以上函數和參數。

系統使用者必須先向系統註冊，每位參與者選擇一把各自的私密鑰匙$x_i \in Z_q^*$，並計算對應的公開鑰匙$y_i = g^{x_i} (\mathrm{mod} p)$，然後將公開鑰匙送給系統認證並公佈。

## 3.2 次鑰匙分派階段

假設$U_1, U_2, \cdots, U_n$爲會議參與者，$U_c$爲會議主席，主席選擇一個會議鑰匙$CK$，然後建立一個秘密多項式，利用此多項式計算每一個參與者的次鑰匙$K_i$，利用鑑別加密法產生這些次鑰匙的鑑別加密訊息$(C_i, R_i, S)$與會議鑰匙簽章$(R,S)$，合稱爲會議鑰匙訊息，然後廣播給參與者。主席執行以下步驟：

1. 假設$t$是會議門檻值(會議合法人數)，主席$U_c$建立一個$t-1$次方的多項式$f(x)$：

$$f(x) = CK + a_1x^1 + a_2x^2 + \cdots + a_{t-1}x^{t-1}(\mathrm{mod}p)$$
$$\text{其中}\, a_i \in \mathrm{Z}_p(i = 1, 2, \cdots, t-1)\, \text{且}\, a_{t-1} \neq 0$$

2. 根據秘密多項式$f(x)$，計算參與者的次鑰匙$K_i$：

$$K_i = f(i)(\mathrm{mod}p)$$

3. 從系統中取得一個時戳$T$與選擇一個隨機亂數$v \in \mathrm{Z}_q$，計算
   $A = g^v(\mathrm{mod}p)$
   $B_i = y_i^v(\mathrm{mod}p)$
   $C_i = K_i \cdot \mathrm{B}_i(\mathrm{mod}q)$
   $R_i = H(K_i \| A)(\mathrm{mod}q)$
   $R = H(CK \| A)(\mathrm{mod}q)$
   $S = v - H(T \| R \| R_1 \| R_2 \| \cdots \| R_n) \cdot \mathrm{x}_c(\mathrm{mod}q)$
   其中$(C_i, R_i, S)$爲主席對次鑰匙產生的鑑別加密訊息，$(R, S)$爲主席對會議鑰匙產生的簽章訊息。

4. 將會議鑰匙訊息$(C_1, C_2, \cdots, C_n, R, R_1, R_2, \cdots, R_n, S, T, t)$廣播給參與者$U_i$。

### 3.3 出席會議宣告階段

出席會議的參與者$U_i$收到會議鑰匙訊息$(C_1, C_2, \cdots, C_n, R, R_1, R_2, \cdots, R_n, S, T, t)$之後，使用參與者本身的私密鑰匙從會議鑰匙訊息中解出次鑰匙$K_i$並驗證次鑰匙的有效性，已確認次鑰匙是否爲主席分派，假如證明了次鑰匙是有效的，則將次鑰匙經過廣播通道傳送給其他參與者，作爲出席會議宣告。

參與者$U_i$執行下列步驟：

1. 驗證會議鑰匙訊息中$T$的正確性，假如不正確則中斷會議鑰匙建立程序，避免接收訊息的重送攻擊。

2. 使用私密鑰匙計算

$$A' = g^S \cdot y_c^{H(T\|R\|R_1\|R_2\cdots\|R_n)} (\mathrm{mod} p)$$
$$K_i = C_i \cdot ((\mathrm{A}')^{x_i} \mathrm{mod} p)^{-1} (\mathrm{mod} q)$$

3. 驗證下列等式：
   $R_i = H(K_i \| A') (\mathrm{mod} q)$
   如果上式成立，則$U_i$確認$(C_i, R_i, S)$爲主席對次鑰匙$K_i$的簽章，證明$K_i$確實爲主席所分派，如果不成立，表示有人假冒主席身分開會，必須中斷會議。

4. 把通過認證的次鑰匙$K_i$，經由廣播通道傳送給其他參與者，作爲出席會議的宣告。

### 3.4 會議鑰匙產生階段

會議參與者$U_j$接收到其他參與者$U_i$經由廣播傳送的次鑰匙$K_i$之後，必須驗證次鑰匙$K_i$的有效性，確認是否爲主席所分派，若次鑰匙有效，代表$U_i$有參與會議資格，視爲合法的參與者，當會議參與者$U_j$收到有效的次鑰匙數目大於門檻值，即可利用這些次鑰匙重建出秘密多項式，計算主席的會議鑰匙，之後，會議參與者$U_j$還要驗證主席對會議鑰匙的簽章是否有效，確認此會議鑰匙確實爲主席分派。會議參與者$U_j$進行以下步驟：

1. 根據接收到的次鑰匙$K_i$，對應主席之前廣播的$R_i$，驗證下列等式：
   $R_i = H(K_i \| A') (\mathrm{mod} q)$
   如果上式成立，則會議參與者$U_j$確認$K_i$確實爲主席分派給$U_i$，代表$U_i$具有開會資格，如果不成立，把不正確的次鑰匙排除。

2. 當得到$t$把以上的有效次鑰匙時，表示參加會議人數超過最低門檻，參與者可以建立一個Lagrange多項式，重建秘密多項式$f(x)$。

3. 根據重建的多項式$f(x)$，計算出會議鑰匙$CK$：
   $CK = f(0) (\mathrm{mod} p)$

4. 根據計算出的會議鑰匙，對應主席之前廣播的$R$，驗證：
   $R = H(CK \| A') (\mathrm{mod} q)$
   如果上式成立，則$U_j$確認(R,S)爲主席對會議鑰匙$CK$的簽章，證明$CK$確實是主席分派的，若不成立，代表主席傳送錯誤的次鑰匙，造成重建時的錯誤

# 4 動態會議鑰匙分配系統

承接上一章的會議鑰匙分配系統，在這裡我們加入橢圓曲線來代替Hash函數，可以減少計算的複雜度，和使用電腦運算的困難性。以下介紹動態會議鑰匙分配系統的過程。

## 4.1 系統初始階段

1. 主席選取一個大質數$p$及模$p$的原根$g$，$p$大於所有的訊息也大於所有參與者的人數，$U_i$是第$i$個參與者，其身分識別碼爲$\delta_i(i = 1, 2, \cdots, w)$。

2. 主席將會議鑰匙$k$表示成模$p$數系中的一個數，而我們要將會議鑰匙$k$分享給$w$位參與者，但其門檻值爲$t$，主席先計算$K = g^k(\mathrm{mod}p)$。

## 4.2 次鑰匙分派階段

1. 主席隨機選取$t$個整數$a_j(j = 0, 1, 2, \cdots, t-1)$作爲多項式$f(x)$中$x^j$項的係數，所以得到一多項式

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1}(\mathrm{mod}p - 1)$$

接著主席計算$s = k + a_0(\mathrm{mod}p - 1)$，並算出每一個$A_j = g^{a_j}(\mathrm{mod}p)$，$j = 0, 1, 2, \cdots, t-1$；以及每一個$f(\delta_i)(\mathrm{mod}p - 1)$，$i = 1, 2, \cdots, w$。

2. 主席選取一橢圓曲線$E_p(a, b)$，並公開之；每一個參與者$U_i$在橢圓曲線$E_p(a, b)$上選取一點$\alpha_i$，再隨機選取一整數$x_i$爲私密鑰匙，然後去計算$\beta_i = x_i\alpha_i$並將$\alpha_i$，$\beta_i$公開，但是$x_i$保持私密。

3. 主席將其$f(\delta_i)$轉換成$E_p(a, b)$上的一點$P_i$，並將$s$轉換成$E_p(a, b)$上的一點$Q$。選取隨機整數$r$，並算出$z_{1i} = r\alpha_i, z_{2i} = P_i + r\beta_i, z_{3i} = Q + r\beta_i$，

將數對$(z_{1i}, z_{2i}, z_{3i})$傳給$U_i$，$i = 1, 2, \cdots, w$。

4. 主席將下列參數公開：$p, g, K, z_{1i}, z_{2i}, z_{3i}, \delta_i (i = 1, \cdots, w), A_j (j = 0, 1, \cdots, t-1)$

### 4.3 驗證公開訊息階段

1. 每一個參與者$U_i$使用私密鑰匙$x_i$計算$b_i = z_{2i} - x_i z_{1i}$及$c_i = z_{3i} - x_i z_{1i}$，再將$b_i, c_i$回復其原值分別爲$B_i, C_i$。(此$b_i$即$P_i$,$c_i$即$Q$,所以$B_i$就是$f(\delta_i)$,$C_i$就是$s$)

2. 每一個參與者$U_i$可驗證下列等式是否成立
$g^{C_i} = K \cdot \mathrm{A}_0 (\mathrm{mod} p)$,$g^{B_i} = \Pi_{j=1}^{t} A_{j-1}^{\delta_i^{j-1}} (\mathrm{mod} p)$
若等式成立，說明了主席沒有欺騙行爲；若是不成立，則公開主席的欺騙行爲。

### 4.4 會議鑰匙還原階段

假設有$t$位參與者共同還原秘密，說是$U_1, U_2, \cdots, U_t$，每個參與還原鑰匙的參與者將將自己本身的$b_i$加密後傳送給合成者，再由合成者還原會議鑰匙。

1. 每一個參與者$U_i$用合成者$U_A$的$\alpha_A, \beta_A$，以及參與者本身手上的$x_i, b_i$算出$e_{1i} = x_i \alpha_A, e_{2i} = b_i + x_i \beta_A$，再將數對$(e_{1i}, e_{2i})$傳給合成者$U_A$。

2. 合成者$U_A$得到一組$(e_{1i}, e_{2i})$，$i = 1, 2, \cdots, t$之後，使用自己的私密鑰匙$x_A$解出$e_{2i} - x_A e_{1i}$，再回復其原值$T_i (i = 1, \cdots, t)$。

3. 合成者$U_A$首先驗證

$$g^{T_i} = \Pi_{j=1}^{t} A_{j-1}^{\delta_i^{j-1}} (\mathrm{mod} p), i = 1, \cdots, t$$

(因爲$T_i$就是之前的$B_i$，$i = 1, \cdots, t$)
若成立，說明參與還原者$U_i$沒有欺騙行爲；若是不成立，則要求參與還原者$U_i$重新發送自己手上的資訊。

4. 當合成者$U_A$算好一組數據$(\delta_i, T_i)$，$i = 1, \cdots, t$，經由Lagrange內插多項式求出$L(T)$，並計算其常數項$L(0)$，再將$L(0)$表示爲橢圓曲線$E_p(a, b)$上的一點$R$，合成者$U_A$再計算$m_{1i} = x_A\alpha_i, m_{2i} = R + x_A\beta_i (i = 1, \cdots, t)$，並將數對$(m_{1i}, m_{2i})$傳送給每一個參與還原會議鑰匙的參與者$U_i$。

5. 參與者$U_i$利用自己的私密鑰匙$x_i$計算$n_i = m_{2i} - x_i m_{1i} (i = 1, \cdots, t)$，再將$n_i$回復其原值$N_i$ (此時$n_i$就是$R$,因而$N_i$就是$L(0)$)，參與者$U_i$驗證$A_0 = g^{N_i} (\mathrm{mod} p)$是否成立，若是成立，說明合成者$U_A$沒有欺騙行爲；若是不成立，則要求合成者$U_A$重新發送計算結果。最後，參與者$U_i$計算會議鑰匙$k = C_i - N_i (\mathrm{mod} p - 1)$。

# 5 結論

## 5.1 安全性分析

在上一章我們介紹了動態會議鑰匙分配系統，接著將動態會議鑰匙分配系統做安全性上的分析。

1. 首先我們先討論，攻擊者是否可以從公開資訊中得到會議鑰匙，攻擊者可以得到包括橢圓曲線$E_p(a,b)$，每個參與者選取的隨機點$\alpha_i$，$\beta_i$，等參數，但是整個系統經過橢圓曲線運算之後，還原時必須經過離散對數的運算，這是有其困難性，再加上攻擊者並不知道會議參與者的私密鑰匙$x_i$，是無法得知會議鑰匙的。

2. 若是攻擊者竊取會議參與者的鑰匙來參加會議又該如何應對？爲了安全起見，每次主席可以選取不同會議鑰匙，所以每次計算的次鑰匙也會不同，而在還原階段時，合成者可以檢驗出鑰匙的合法性，也就是有效性，相對可以得知有攻擊者參與這次會議。

3. 假如主席有私心想要欺騙參與者，自己獨享會議鑰匙又該如何？在會議參與者都提供自己的私密鑰匙之後，主席卻故意傳送不正確的相關訊息給參與者，意圖蒙騙參與會議的成員，但是，在訊息驗證階段每位參與者可以藉著驗證相關等式，來證明主席的欺騙行爲，所以這種攻擊者想要冒充主席身分或是主席本身想要獨享秘密，都是不可行的。

4. 如果會議參與者沒有足夠的參與者鑰匙是否可以解出會議鑰匙呢？由於在還原階段，有效的次鑰匙是需要檢驗的，若是沒有足夠的次鑰匙，是無法重建秘密多項式，僞造的鑰匙經過檢驗是會被淘汰的，如此一來，有效的次鑰匙數目低於會議參與的合法人數，

是無法重建會議鑰匙。所以，攻擊者沒有足夠的次鑰匙或是僞造次鑰匙的攻擊行爲，都是會被檢驗出來。

## 5.2 結語

在本篇論文中，我們利用橢圓曲線來改善原本的會議鑰匙分配系統，原系統在資訊的背景中使用了Hash函數作爲檢驗相關訊息的方法，但是，缺點是計算量通常很大，也比較複雜，對於要使用紙筆計算是不可能的，而對於橢圓曲線來說，計算量和數據可以較小，也可以使用紙筆計算，增加不少便利性。而會議的參與者，他們無法知道其他參與者的訊息，也就無法知道會議鑰匙。另外，會議鑰匙是可以無限次更新，只要主席重複分配動作即可。在分配過程中，主席難以避免會分配假訊息給參與者，造成回復會議鑰匙的錯誤，或是一些相關的錯誤訊息，在我們的驗證過程中做了有效的確認，防止這類情形發生。對於最後要把鑰匙回復的合成者，在回復過程中可能的作假行爲，也就是不提供相關訊息給其他參與者，也做了相關的驗證步驟。在這個會議鑰匙分配系統中，攻擊者可以獲得包括橢圓曲線在內的公開訊息，但是，卻無法得知主席或是其他參與者的私密鑰匙，基於運算離散對數的困難性，攻擊者是無法得知會議鑰匙。

## References


[1] A Shamir, How to share a secret[J]. Comm. ACM, 1979,22(11)：612-613

[2] H. M. Sun S. P. Shieh Construction of dynamic threshold schemes[J], Electronics Letters, 1994, 30(24)：2023-2025

[3] E. Dawson Multisecret - sharing scheme based on one - way function[J] , Electronics Letters 1995

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

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

[6] 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, pp. 417-426, Springer, Berlin Heidelberg New York, 1986.

[7] ElGamal,T. Public key cryptosystem and a signature scheme based on discrete logarithms,IEEE Transactions on Information Theory,31,4,pp.469-472,1985.

[8] Hoster,P.Michels,M. and Petersen,H. Uthenticated encryption schemes with low communication costs[J],Electronics Letters,30,15,pp.1212-1213,1994.

[9] Nyberg,K.and Rueppel,R.A. Essage recovery for signature schemes based on the discrete logarithm？ Advances in Cryptology Eurcrypt？ 4,pp.182-193,1995.

[10] Wu,T.S.and Hsu,C.L. Onvertible authenticated encryption scheme？ The Journal of System and Software,62,3,pp.205-209,2002.

[11] 沈淵源,密碼學之旅與MATHEMATICA 同行全華科技圖書股份有限公司, 2006

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

[13] 陳明裕,可鑑別的門檻會議金鑰分配系統,私立東吳大學,碩士論文,2002

[14] 翁榮茂,橢圓曲線版的ElGamal門檻密碼系統,私立東海大學,碩士論文, 2005

[15] 林靜慧,橢圓曲線版的動態秘密分享,私立東海大學,碩士論文,2006

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

[17] Silverman, Joseph H./Tate, John : Rational Points on Elliptic Curves, Undergraduate Texts in Math, Springer - Verlag, New York, 1992