基於離散對數難題之新盲簽章

沈榮麟
國立臺北大學資訊工程學系
暨電機工程研究所教授
rlshen@mail.ntpu.edu.tw

林昱安
國立臺北大學電機工程研究所
碩士生
s79582501@webmail.ntpu.edu.tw

摘要

在 1983 年，D. Chaum 博士首先提出了盲簽章這個概念。在盲簽章流程中，簽章要求者要求簽章者簽署一個已經過加盲的文件，而簽章要求者可以從這盲簽章中得到正確的簽章。且當簽章要求者對外公佈簽章對，簽章者也無法對此簽章對做出追蹤。

在本研究中，我們以離散對數和 Harn 的廣義 ElGamal 數位簽章為基礎提出新的盲簽章演算法，並且詳細說明新盲簽章演算法的流程，最後說明我們所建構的新盲簽章滿足盲簽章所需要的四種性質：正確性、盲性、不可偽造性與不可追蹤性。

關鍵詞：盲簽章、數位簽章、離散對數難題

Abstract

In 1983, D. Chaum first introduced the concept of blind signature. In the blind signature scheme, the requester requests the signer to sign on a blinded message. The requester then derives the signature from the blind signature. When the requester releases the signature pair in public, the signer is unable to link this signature pair.

In this paper, we propose a novel blind signature scheme based on discrete logarithms problem and Harn's generalized ElGamal type digital signature schemes. Then we give the details of our new blind signature scheme. Finally, we shall examine the correctness, blindness, unforgeability, and untraceability of our proposed blind signature scheme.

Keywords: **Blind Signature, Digital Signature, Discrete Logarithms Problem.**

1. 前言

數位簽章(Digital Signature)[1]因為能提供身份認證(Authentication)、不可否認性(Non-Repudiation)、資料完整性(Data Integrity)及不可偽造(Unforgeablity)等安全性質，而在現今網路發達的社會裡佔了非常重要的位置，特別是在大型網路系統中密鑰的分配(Key Distribution)、身份認證(Authentication)以及電子商務(Electronic Commerce)等等用途被大量使用。

盲簽章(Blind Signature)是一個由數位簽章變形而來的簽章法，它在 1983 年由 D. Chaum[2, 3]提出了盲簽章的概念，D. Chaum 利用 RSA[4]提出第一個盲簽章來保護人們在網路上的交易，確保人們的私密資料不會遭有心人竊取，而在之後，因為有不同的需求及環境，而使盲簽章的研究更為深入，並且將此技術大量應用在需要隱私權保護(Privacy Protection)及匿名性(Anonymous)的環境當中，例如電子現金(Electronic Cash)[5]、電子投票(Electronic Voting)[6]等…。

在數位簽章的流程中，使用者分為兩種角色，分別為簽章者(Signer)及驗證者(Verifier)，簽章者使用自己的私密金鑰(Private Key)對欲簽章的文件(Message)作加密而求得數位簽章，傳送給驗證者後，驗證者可利用簽章者的公開金鑰(Public Key)驗證簽章是否正確。而在盲簽章的流程當中，不同於數位簽章，盲簽章的使用者共分為三種角色，分別為簽章要求者(Requester)、簽章者(Signer)以及驗證者(Verifier)，簽章要求者將所要簽章的文件先作加盲(Blinding)的運算，然後將此盲文件(Blind Message)傳送給簽章者，簽章者再利用自己的私密金鑰對此盲文件作簽章而得到盲簽章(Blind Signature)並將其傳回給簽章要求者，簽章要求者再對盲簽章作解盲的動作而得到正確的簽章，最後再將簽章驗證所需的資訊傳送給驗證者，驗證者使用簽章者的公開金鑰即可驗證簽章的正確性，進而作下一步的動作。

盲簽章和一般數位簽章的主要差異為[2, 3]：

1. 在一般的數位簽章中，簽章者知道其簽署的文件內容，但在盲簽章中，簽章者並不知道所簽署的文件內容。
2. 即使日後簽章要求者公佈簽章配對(Signature Pair)，簽章者也無法找到簽章配對和

當時所儲存的簽章紀錄之間的相互關係。

從盲簽章的相關文獻[2, 7-10]當中定義出了幾項盲簽章所要滿足的需求：正確性(Correctness)、盲性(Blindness)、不可偽造性(Unforgeability)和不可追蹤性(Untraceability)，以上這幾個盲簽章的需求將會在第二章說明。

因為盲簽章需滿足上面列出的四點需求，所以得知盲簽章能夠保護簽章要求者的隱私權，另外因為盲簽章是基於數位簽章而來，所以可以保證簽章的正確性且不會被偽造。

1.1 研究動機及目的

網際網路的便利，使得人們的生活中越來越仰賴網際網路，這使得人們在網路上的隱私更顯得重要，尤其是利用電子現金在網路上購物，或是電子選舉中的投票，這些網路上的應用均要保護使用者的身份而不被他人所知，故盲簽章的研究就更顯重要。

本研究將結合離散對數及 Harn 所提出的廣義 ElGamal 數位簽章[7]來建構盲簽章演算法，並期望此盲簽章演算法可以使人們在網路上交易的隱私權得到保護。

1.2 本文架構

本論文一共有五章。第一章為前言，首先先對數位簽章的應用面及重要性作簡短的介紹，說明為何需要使用盲簽章，並且對一般數位簽章和盲簽章的相異處做出說明，再來為本研究的動機和目的。第二章為文獻回顧，將說明本研究所使用到的技術及相關的研究。第三章為本研究的主體，說明如何將 Harn 所提出的廣義 ElGamal 數位簽章轉換成盲簽章演算法，並提出完整的盲簽章流程及架構。第四章將為本研究所提出的盲簽章演算法作盲簽章性質的說明，要成為一個好得盲簽章必須滿足正確性、盲性、不可偽造性和不可追蹤性。本章將會對所提出的盲簽章演算法作滿足上述性質的說明。最後一章則是為結論及未來研究方向。

2. 文獻回顧

本章針對本研究相關技術，提出精要的說明，包含：雜湊函數(Hash Function)[9]、基於離散對數(Discrete Logarithms Problem)的公鑰密碼系統[10]、盲簽章[2, 3]等相關技術以及盲簽章的應用等等…。

2.1 雜湊函數

訊息在網路上傳遞，往往會因為某些因素而使得訊息遺失或者因為有心人的攻擊而遭到竄改，所以需要作訊息確認(Message Authentication)[11]的動作，而雜湊函數就是最常拿來作訊息確認的技術。

使用在數位簽章的雜湊函數必須滿足下列條件[12]：

1. 雜湊函數對任意長度的資料，均產生固定長度的訊息摘要(Message Digest)。
2. 對輸入的任意資料，雜湊函數可藉由軟體或硬體輕易計算得到。
3. 需是單向函數(One-way Function)
4. 抗碰撞(Collision Resistance)：對雜湊函數 $h(\bullet)$ 來說，一個資料 m_1，要找到另一個資料 m_2 使得 $h(m_1) = h(m_2)$ 是不可能的。

除了訊息確認的用途之外，雜湊函數也常常在公鑰密碼系統中被合併使用，雜湊函數在公鑰密碼系統中使用可以使得在加解密的時候，減少許多運算次數，節省時間以提昇效率，所以不管在公鑰密碼系統的加解密、數位簽章及本研究所提到的盲簽章，都會使用到雜湊函數。

2.2 基於數學上兩大難題的公鑰密碼系統

公鑰密碼系統(Public Key Cryptosystem)[10]於 1976 年由 W. Diffie 和 M. Hellman 兩位學者首先提出其概念，現在的公鑰密碼系統大都基於 n 模餘群(n module)上的兩大難題：質因數分解及離散對數難題；質因數分解難題以 RSA 公鑰密碼系統[4]為代表，離散對數難題則以 ElGamal 公鑰密碼系統[8]為代表，下面將針對本研究所依據的 ElGamal 公鑰密碼系統來說明。

2.2.1 ElGamal 公鑰密碼系統

ElGamal 公鑰密碼系統[8]在 1985 年由 T. ElGamal 博士提出，ElGamal 公鑰密碼系統的安全性基於離散對數，以下就來簡述 ElGamal 公鑰密碼系統的加解密過程：

ElGamal 公鑰密碼系統一樣有兩個主要角色，接收者 Alice 及傳送者 Bob，Alice 鑰先產生一對金鑰，首先選擇一個大質數 p，選擇完

畢之後取得 p 的一個原根 α，再隨機選擇 x（$x < p$）作為私密金鑰，然後計算公開金鑰 $y = \alpha^x \bmod p$，得到公開金鑰為 (y, α, p)，私密金鑰為 x；這時 Bob 欲加密傳送文件 M 給 Alice，Bob 秘密選擇亂數 k（$0 \le k \le p-2$），計算 $a = \alpha^k \bmod p$，$b = y^k M \bmod p$，(a, b) 即為密文傳送給 Alice，Alice 再用其秘密金鑰解密得到文件 M。

ElGamal 公鑰密碼系統的安全性取決於離散對數難題，令 n、y、α 為非零的整數並滿足 $y \equiv \alpha^x \bmod n$，尋找 $x = \log_\alpha y$ 之問題即為離散對數問題，很明顯可以看出，給定 n、α 和 x 很容易求出 y，然而給定 n、α 和 y 卻很難得到 x，所以若可以解決離散對數難題，就等於破解了 ElGamal 公鑰密碼系統。

2.2.2 ElGamal 數位簽章

ElGamal 數位簽章[8]是基於離散對數難題，傳送者 Alice 欲簽署文件 M 給接收者 Bob，Alice 有公鑰 (y, α, p)、私鑰 x 和雜湊函數 $h(\bullet)$。

Alice 隨機選一整數 k 並使得 k 和 $\phi(p)$ 互質，Alice 計算 $r = \alpha^k \bmod p$ 以及簽章 $s^* = k^{-1}(h(M) - ar) \bmod \phi(p)$，然後將數位簽章 $s = (M, r, s^*)$ 傳給 Bob。Bob 收到數位簽章 s 之後使用 Alice 的公鑰 (y, α, p) 計算 $V_1 = y^r r^{s^*} \bmod p$ 及 $V_2 = g^{h(M)} \bmod p$，驗證 $V_1 = V_2$ 是否成立，若成立則簽章驗證成功，否則簽章驗證失敗。

2.2.3 Harn 提出的廣義 ElGamal 數位簽章

L. Harn 和 Y. Xu 兩位學者在 1994 年提出了基於 ElGamal 的廣義數位簽章(Generalized ElGamal Type Digital Signature)[7]，其中依據 ElGamal 公鑰密碼系統[8]的標準簽章方程式及驗證方程式，再加上對於安全性和可行性等等的討論，產生了十八個基於 ElGamal 數位簽章法的廣義 ElGamal 數位簽章，為方便說明，本小節均省略雜湊函數 $h(\bullet)$。

ElGamal 數位簽章[8]的簽章方程式為 $m = xr + ks \bmod \phi(p)$，驗證方程式為 $\alpha^m \equiv y^r r^s \bmod p$，為了不失一般性，Harn 將簽章方程式表示為 $ax = bk + c \bmod \phi(p)$，其中 (a, b, c) 代表參數 (m, r, s) 的集合，也就是說 a 可以代表參數 m 或是參數 rs，其餘以此類推；而簽章方程式可表示為 $y^a = r^b \alpha^c \bmod p$。以下就來說明 L. Harn 和 Y. Xu 兩位學者對建構廣義 ElGamal 數位簽章法所提出的幾項有關安全性的說明[7]：

1. 參數 s 和 m 不可合併在同一項，否則會使得他人成功偽造簽章。例如：簽章方程式若為 $x = rk + sm \bmod \phi(p)$，所產生出的簽章對為 (m, r, s)，偽造正確的簽章只需取 $m' = \beta m \bmod \phi(p)$ 並計算 $s' = \beta^{-1} s \bmod \phi(p)$，即可造出正確的簽章 (m', r, s')。
2. 參數 s 和 r 不可合併在同一項，否則也會使得他人偽造簽章成功。例如：簽章方程式為 $mx = k + rs \bmod \phi(p)$，驗證方程式為 $y^m = r\alpha^{rs} \bmod p$，偽造簽章者只要隨機取一整數 R 然後計算 r' 滿足 $y^m = r'\alpha^R \bmod p$，即可造出正確的簽章 (m, r', s')。（其中 $r's' = R \bmod \phi(p)$）
3. 簽章方程式必須式三個分開的項，如 $mx = rk + s \bmod \phi(p)$，若不為三個分開的項，例如：$(m + r)x = sk \bmod \phi(p)$，簽章偽造者即可取 m'，使得 $m - m' = \beta \bmod \phi(p)$ 且計算 $s' = (1 - \beta(m + r)^{-1})s \bmod \phi(p)$ 即可得到正確的簽章 (m', r, s')。

經過了一些討論，L. Harn 和 Y. Xu 兩位學者依據這些討論列出了十八個符合安全性等相關性質的廣義 ElGamal 數位簽章。

表 1 廣義 ElGamal 數位簽章[7]

編號	簽章方程式	驗證方程式
1	$mx = rk + s \bmod \phi(p)$	$y^m = r^r \alpha^r \bmod p$
2	$mx = sk + r \bmod \phi(p)$	$y^m = r^s \alpha^r \bmod p$
3	$rx = mk + s \bmod \phi(p)$	$y^r = r^m \alpha^s \bmod p$
4	$rx = sk + m \bmod \phi(p)$	$y^r = r^r \alpha^m \bmod p$
5	$sx = rk + m \bmod \phi(p)$	$y^s = r^r \alpha^m \bmod p$
6	$sx = mk + r \bmod \phi(p)$	$y^s = r^m \alpha^r \bmod p$
7	$rmx = k + s \bmod \phi(p)$	$y^{rm} = r\alpha^s \bmod p$
8	$x = mrk + s \bmod \phi(p)$	$y = r^{mr} \alpha^s \bmod p$
9	$sx = k + mr \bmod \phi(p)$	$y^s = r\alpha^{mr} \bmod p$
10	$x = sk + rm \bmod \phi(p)$	$y = r^s \alpha^{rm} \bmod p$
11	$rmx = sk + 1 \bmod \phi(p)$	$y^{rm} = r^s \alpha \bmod p$
12	$sx = rmk + 1 \bmod \phi(p)$	$y^s = r^{rm} \alpha \bmod p$
13	$(r + m)x = k + s \bmod \phi(p)$	$y^{r+m} = r\alpha^s \bmod p$
14	$x = (m + r)k + s \bmod \phi(p)$	$y = r^{m+r} \alpha^s \bmod p$
15	$sx = k + (m + r) \bmod \phi(p)$	$y = r^{m+r} \alpha^s \bmod p$
16	$x = sk + (r + m) \bmod \phi(p)$	$y = r^s \alpha^{r+m} \bmod p$
17	$(r + m)x = sk + 1 \bmod \phi(p)$	$y^{r+m} = r^s \alpha \bmod p$
18	$sx = (r + m)k + 1 \bmod \phi(p)$	$y^s = r^{r+m} \alpha \bmod p$

表 1 是十八個廣義 ElGamal 數位簽章的簽章方程式及驗證方程式，本研究依據編號第 13 個數位簽章，將其轉換成盲簽章且證明所轉換的盲簽章符合盲簽章性質，將會在第三章、第四章說明。

2.3 盲簽章及其相關研究

基本的數位簽章，就是將文件 m 利用私密金鑰 d 作加密得到數位簽章 s，驗收的時候再用公開金鑰 e 來驗證，但是在某些特殊的情形之下，例如電子現金的交易或是電子投票，這些情況則希望簽章者能夠在不知文件內容的情形下簽章而使文件能夠得到正確的驗證。

1983 年，D. Chaum 博士因鑑於網路的交易越來越頻繁，人們對隱私權的保護也越來越重視，所以提出了盲簽章這個概念[2]試圖解決這個問題。本小節將會介紹 D. Chaum 博士所提出的盲簽章概念和基於兩大難題所建構的盲簽章。

2.3.1 盲簽章的概念

D. Chaum 博士當時所提出的盲簽章概念是以電子交易的不可追蹤性為首要目標，該篇文獻[2]所提到的交易過程如下：

1.付款者(Payer)隨機選取 x 並使用計算函數 c (Commuting Function)計算 $c(x)$ 並將 $c(x)$ 傳給銀行(Bank)。

2.銀行利用私密金鑰作簽章的動作 $s'(c(x))$ 並且對付款者的銀行戶頭進行扣款，然後再將 $s'(c(x))$ 傳給付款者。

3.付款者利用反轉計算函數 c' 計算 $c'(s'(c(x))) = s'(x)$，然後再利用銀行的公開金鑰驗證 $s(s'(x))$ 是否等於 x？

4.付款者和銀行的交易結束之後，將 $s'(x)$ 及 $r(x)$ 傳送給收款者(Payee)，這裡的 $r(\bullet)$ 可看成是雜湊函數。

5.受款者計算 $r(s(s'(x)))$ 是否等於 $r(x)$，如果是則進行步驟 6。

6.受款者將 $s'(x)$ 及 $r(x)$ 傳送給銀行進行請款的動作。

7.銀行檢查 $r(s(s'(x)))$ 是否等於 $r(x)$，若相等則比對 $s'(x)$ 是否已存在資料庫中，若無則將此筆資料加入資料庫。

8.銀行將款項轉入受款者帳戶，並且通知付款者交易完成。

在同一年 D. Chaum 博士提出了利用 RSA 數位簽章修改得來的實際作法[3]。盲簽章的角色有三種：簽章要求者、簽章者及驗證者；盲簽章的過程分為五個階段：金鑰產生(Key Generation)、文件加盲(Blinding)、簽章(Signing)、解盲簽章(Unblinding)、驗證(Verifying)。

1.金鑰產生：
簽章者利用 RSA 公鑰密碼系統的方法產生兩把金鑰，公開金鑰 (e, n) 和私密金鑰 (d, n)，並且選擇一個雜湊函數 $h(\bullet)$。

2.文件加盲：
簽章要求者有一個文件 m，欲給簽章者作簽章的動作但不希望讓簽章者得知文件內容，所以簽章要求者隨機選擇一個整數 r 當作盲因子(Blind Factor)並計算盲文件 $\alpha = r^e \bullet h(m) \bmod n$，然後將 α 傳送給簽章者。

3.簽章：
簽章者收到 α 之後，計算 $t = \alpha^d \bmod n$，然後將 t 回傳給簽章要求者。

4.解盲簽章：
簽章要求者收到 t 之後，即可計算簽章 $s = t \bullet r^{-1} \bmod n$，然後將簽章對 (m, s) 送給驗證者。

5.驗證：
驗證者收到簽章對 (m, s)，即可使用 $h(\bullet)$ 和 (d, n) 來驗證簽章是否正確。

在盲簽章的基本概念中僅提到盲簽章需滿足簽章的不可偽造及盲性，而經過多年眾學者的研究，歸納出了盲簽章需滿足幾項特性[2, 7-10]：

1.正確性(Correctness)：經過盲簽章演算法計算過後所釋放出來的簽章對可以被使用簽章者公開金鑰的人正確的驗證。

2.盲性(Blindness)：簽章者在作簽章的時候並不知道所要簽章的文件內容，以達到簽章要求者的隱私保護。

3.不可偽造性(Unforgeability)：任何人若想偽造簽章也不能夠得到正確的驗證。

4.不可追蹤性(Untraceability)：當簽章要求者將簽章對公開，簽章者也無法經由當時的簽章紀錄而跟簽章對產生連結關係。

2.3.2 基於離散對數的盲簽章

J. L. Camenisch、J. M. Priveteau 和 M. A.

Stadler 三位學者在 1994 年首度提出以離散對數為基礎的盲簽章[13]。在該研究中，提出了兩個盲簽章演算法，第一個是由 DSA(Digital Signature Algorithm)[14]修改得來，第二個則是以 Nyberg-Rueppel 所提出的簽章演算法[15]為基礎修改得來。

第一個盲簽章演算法是由 DSA[14]變化而來，步驟如下：

1.初始化：

簽章者選擇一大質數 p 、 p 的質因數 q 和 p 的原根 g ，隨機選擇一數 x 作為私密金鑰($x \in Z_q$)並計算公開金鑰 $y = g^x \bmod p$ 。

2.加盲：

簽章要求者向簽章者提出欲簽章的要求，簽章者收到要求之後隨機產生一數 $\tilde{k} \in Z_q$ 並計算 $\tilde{R} = g^{\tilde{k}} \bmod p$ ，隨後確認是否滿足 $\gcd(\tilde{R}, q) = 1$ ，如果是則將 $\tilde{R}$ 傳送給簽章要求者，若不是則重新產生 $\tilde{k}$ 值。

簽章要求者收到 $\tilde{R}$ 之後，先確認是否滿足 $\gcd(\tilde{R}, q) = 1$ ，然後再隨機選取 α 、 $\beta \in Z_q$ ，選取完畢後計算 $R = \tilde{R}^{\alpha} g^{\beta} \bmod p$ ，再確認是否滿足 $\gcd(R, q) = 1$ ，如果是則計算 $\tilde{m} = \alpha m \tilde{R} R^{-1} \bmod q$ 並將 $\tilde{m}$ 傳送給簽章者，如果不是則重新選擇 α 、 β 。

3.簽章：

簽章者收到 $\tilde{m}$ 之後，計算 $\tilde{s} = \tilde{k}\tilde{m} + \tilde{R}x \bmod q$ 並將 $\tilde{s}$ 傳回給簽章要求者。

4.解盲簽章：

簽章要求者收到 $\tilde{s}$ 之後，計算 $s = \tilde{s} R \tilde{R}^{-1} + \beta m \bmod q$ 和 $r = R \bmod q$ ，最後得到簽章對 (m, r, s) 。

5.驗證：

驗證者可利用簽章者的公開金鑰驗證簽章是否正確，計算：

$T = (g^s y^{-r})^{m^{-1}} = g^{(\tilde{s}R\tilde{R}^{-1} + \beta m - xr)m^{-1}} = g^{\tilde{k}\alpha + \beta} = R \bmod p$

，然後驗證 $r = T \bmod q$ 是否正確。

提出的第二個盲簽章演算法是以 Nyberg-Rueppel[15]所提出的簽章法作修改，步驟如下：

1.初始化：

同上一個盲簽章演算法。

2.加盲：

簽章要求者向簽章者提出簽章的要求，簽章者收到要求後選一數 $\tilde{k} \in Z_q$ ，計算 $\tilde{r} = g^{\tilde{k}} \bmod p$ 之後將 $\tilde{r}$ 送給簽章要求者。

簽章要求者收到 $\tilde{r}$ 之後，隨機選取 $\alpha \in Z_q$ 、 $\beta \in Z_q^*$ ，然後計算 $r = m g^{\alpha} \tilde{r}^{\beta} \bmod p$ 和 $\tilde{m} = r\beta^{-1} \bmod q$ ，並將 $\tilde{m}$ 傳送給簽章者。

3.簽章：

簽章者收到 $\tilde{m}$ 之後，計算簽章 $\tilde{s} = \tilde{m}x + \tilde{k} \bmod q$ ，然後將盲簽章 $\tilde{s}$ 傳回給簽章要求者。

4.解盲簽章：

簽章要求者收到 $\tilde{s}$ 之後，計算 $s = \tilde{s}\beta + \alpha \bmod q$ ，得到簽章對 (m, r, s) ，並將簽章對送給驗證者。

5.驗證：

驗證者收到簽章對後可利用簽章者的公開金鑰驗證簽章是否正確：

$g^{-s} y^r r = m g^{-\tilde{s}\beta - \alpha + xr + \tilde{k}\beta + \alpha} = m g^{-\tilde{m}x\beta - \tilde{k}\beta + xr + \tilde{k}\beta} = m \bmod p$

分析：

J. L. Camenisch 等學者提出的第一個基於 DSA 變形而來的盲簽章，但在 1995 年，L. Harn 博士及提出分析並指出沒有滿足不可追蹤的性質，Harn 的分析[16]如下：

簽章要求者公佈簽章對 (m, r, s) 之後，因為簽章者留存 $(\tilde{m}, R, \tilde{k}, \tilde{s})$ ，故簽章者計算 $\alpha' = \tilde{m} m^{-1} R^{-1} r \bmod q$ 、 $\beta' = m^{-1}(s - \tilde{s} r R^{-1}) \bmod q$ 之後，再計算 $r = R^{\alpha'} g^{\beta'} \bmod p$ 則可得到兩者關聯，進而追蹤到該筆簽章對為哪位簽章要求者的，故不滿足盲簽章的不可追蹤性質。

另一個基於離散對數的盲簽章演算法是由 E. Mogammed 、 A. E. Emarah 和 Kh. EL-Shennawy 三位學者所提出[17]，他們在論文說明所提出的演算法會比基於 RSA 的盲簽章法更少運算，速度更快並滿足盲簽章應有的四個性質。

演算法步驟如下：

1.初始化：

簽章者依 ElGamal 數位簽章的方式產生公開金鑰和私密金鑰。

2.盲化：

簽章要求者有文件 m 需簽章者作簽章的動作。簽章要求者隨機選取 k $(1 < k < p-1)$ 並滿足 $\gcd(k, p-1) = 1$ ，然後計算 $r = \alpha^k \bmod (p-1)$ ，另外再選取一個盲因子 h 並滿足 $\gcd(h, p-1) = 1$ ，計算

$m' = h * m \bmod (p-1)$ 後再將 m' 和 r 傳送給簽章者。

3.簽章：

簽章者收到 m' 之後，計算盲簽章 $s' = (m' - xr) * k^{-1} \bmod (p-1)$，計算完畢之後將 s' 傳回給簽章要求者。

4.解盲簽章：

簽章要求者收到 s' 之後，計算 $s = xrk^{-1}(h^{-1}-1) + h^{-1}s' \bmod (p-1)$ 即可得到簽章，再把簽章對 (m, r, s) 傳送給驗證者驗證。

5.驗證：

驗證者收到簽章對 (m, r, s) 後，驗證者可使用簽章者的公開金鑰驗證該簽章對是否正確：

$$\alpha^m \equiv y^r r^s \bmod p$$

分析：

上面由 E. Mogammed 等學者所提出來的基於離散對數的盲簽章，雖然作者在該篇文章內說他們提出了一個比 RSA 盲簽章更有效率且滿足盲簽章四個性質的新盲簽章，但我們卻可以很容易看出該簽章在簽章者簽名的方程式有一個很大的問題，簽章式為 $s' = (m' - xr) * k^{-1} \bmod (p-1)$，當簽章要求者收到簽章之後，因為簽章要求者知道 (s', m', r, k^{-1}) 四個值，所以就可自行計算出簽章者的私密金鑰 x，之後簽章要求者就可以使用簽章者的私密金鑰自行做出可驗證的簽章，故我們可以說 E. Mogammed 等學者所提出的盲簽章法不安全。

3. 基於廣義 ElGamal 數位簽章的盲簽章法

本研究提出的盲簽章演算法是以離散對數難題及 Harn 所提出的廣義 ElGamal 數位簽章[7]作為基礎，本章將說明如何轉換 Harn 提出的廣義 ElGamal 數位簽章為盲簽章演算法及所產生出來的盲簽章演算法的可用性，並且在最後提出完整的新盲簽章演算法說明。

3.1 新盲簽章的建構

在說明如何轉換之前，首先要說明一些參數所代表的意義：

表 2 新盲簽章所使用的參數說明

簽章要求者		簽章者	
參數名稱	參數說明	參數名稱	參數說明
a, b, c	隨機選取並與 $\phi(p)$ 互質	p	大質數
m	文件	α	p 的原根
$\tilde{m}$	盲文件(經過文件加盲方程式得到)	y	公開金鑰（$y = \alpha^x \bmod p$）
k	$k = a\tilde{k} + bx + c$	x	私密金鑰，介於 $2 \sim (p-2)$ 之間
r	$r = \tilde{r}^a y^b \alpha^c \bmod$	$\tilde{k}$	整數，滿足 $\gcd(k, p-1) = 1$
s	簽章(經由解盲方程式得到)	$\tilde{r}$	$\tilde{r} = \alpha^{\tilde{k}} \bmod p$
		$\tilde{s}$	盲簽章(經由簽章方程式得到)
		$h(\bullet)$	雜湊函數

本研究將編號第十三個廣義 ElGamal 數位簽章轉換成盲簽章演算法，轉換過程如下：

以表 1 中編號第十三個廣義 ElGamal 數位簽章為例，其簽章式為

$$(r+m)x = k + s \quad (1)$$

在本研究的盲簽章演算法中，該簽章式同樣用於簽章，但所使用的參數卻有不同：

$$(\tilde{r}+\tilde{m})x = \tilde{k} + \tilde{s} \quad (2)$$

由式(2)可以得到：

$$x = \tilde{k}(\tilde{r}+\tilde{m})^{-1} + \tilde{s}(\tilde{r}+\tilde{m})^{-1} \bmod \phi(p) \quad (3)$$

我們令 $k = a\tilde{k} + bx + c$，將式(3)帶入此式可得：

$$k = a\tilde{k} + b\tilde{k}(\tilde{r}+\tilde{m})^{-1} + b\tilde{s}(\tilde{r}+\tilde{m})^{-1} + c \quad (4)$$

由式(1)可以得到

$$(r+m)x = k + s \Rightarrow (r+m)x - k - s = 0 \quad (5)$$

將式(3)、(4)代入式(5)

$$(r+m)x - k - s = 0$$

$$\Rightarrow (r+m)\tilde{k}(\tilde{r}+\tilde{m})^{-1} + (r+m)\tilde{s}(\tilde{r}+\tilde{m})^{-1}$$

$$-a\tilde{k} - b\tilde{k}(\tilde{r}+\tilde{m})^{-1} - b\tilde{s}(\tilde{r}+\tilde{m}) - c - s = 0$$

$$\Rightarrow \tilde{k}((r+m)(\tilde{r}+\tilde{m})^{-1} - a - b(\tilde{r}+\tilde{m})^{-1}) +$$

$$(r+m)\tilde{s}(\tilde{r}+\tilde{m})^{-1} - b\tilde{s}(\tilde{r}+\tilde{m}) - c - s = 0 \quad (6)$$

由式(6)可知：

$$(r+m)(\tilde{r}+\tilde{m})^{-1} - a - b(\tilde{r}+\tilde{m})^{-1} = 0 \quad (7)$$

$$(r+m)\tilde{s}(\tilde{r}+\tilde{m})^{-1} - b\tilde{s}(\tilde{r}+\tilde{m}) - c - s = 0 \quad (8)$$

由式(7)可以得到：

$$\tilde{m} = a^{-1}(r+m-b) - \tilde{r} \quad (9)$$

由 (8)可以得到：

$$s = a\tilde{s} - c \quad (10)$$

式(9)為文件加盲方程式，式(10)為解盲簽章方

程式。由以上的轉換我們可以得到文件加盲方程式和解盲簽章方程式。

3.2 基於廣義 ElGamal 數位簽章的新盲簽章

在 3.1 節已經說明可以利用 Harn 提出的編號第 13 個廣義數位簽章法經過轉換後得到盲簽章演算法，本節將說明這個盲簽章演算法的完整流程。

本研究的新盲簽章演算法和大部分的盲簽章演算法一樣，在流程中所參與的角色共有三類：簽章要求者、簽章者和驗證者。整個演算法的步驟共有五個：初始化、盲化、簽章、解盲簽章及驗證，詳細說明如下。

新盲簽章演算法一是基於 Harn 所提出的廣義 ElGamal 數位簽章演算法當中的編號第 13 個數位簽章(見表 1)轉換而來，以下是詳細的盲簽章演算法過程：

1. 初始化：

在初始化的過程中，簽章者需產生公開金鑰和私密金鑰。簽章者選擇一大質數 p 以及 p 的一原根 α ，另外選擇一數 x 作為私密金鑰並計算公開金鑰 $y=\alpha^x \bmod p$ ，計算完畢後簽章者得到公開金鑰 (y, α, p) 和私密金鑰 x 。

2. 盲化：

簽章要求者有文件 m 欲讓簽章者簽名並希望簽章者不知道其文件內容。首先向簽章者提出欲簽章的要求，簽章者收到簽章要求後隨機選擇一整數 $\tilde{k}$ ， $\tilde{k}$ 滿足 $\gcd(\tilde{k}, p-1)=1$ ，計算：

$$\tilde{r}=\alpha^{\tilde{k}} \bmod p$$

計算完畢之後將 $\tilde{r}$ 傳回給簽章要求者。

簽章要求者收到 $\tilde{r}$ 之後，隨機選取 (a, b, c) 且 (a, b, c) 三數與 $\phi(p)$ 互質，然後計算：

$$r=\tilde{r}^a y^b \alpha^c \bmod p$$

再將文件 m 經由雜湊函數 $h(\bullet)$ 計算後得到 $h(m)$ 。

然後將 $h(m)$ 加盲：

$$\tilde{m}=a^{-1}(r+h(m)-b)-\tilde{r} \bmod \phi(p)$$

加盲完成後把 $\tilde{m}$ 傳送給簽章者。

3. 簽章：

簽章者收到 $\tilde{m}$ 之後，計算盲簽章：

$$\tilde{s}=(\tilde{r}+\tilde{m})x-\tilde{k} \bmod \phi(p)$$

計算完畢後將 $\tilde{s}$ 回傳給簽章要求者。

4. 解盲簽章

簽章要求者收到簽章者送回的盲簽章 $\tilde{s}$ 之後，計算簽章：

$$s=a\tilde{s}-c \bmod \phi(p)$$

計算完畢就可以得到簽章對 (m, r, s) 。

5. 驗證：

驗證者收到簽章要求者所送過來的簽章對 (m, r, s) ，可使用簽章者所公佈的雜湊函數 $h(\bullet)$ 和公開金鑰作簽章的驗證：

$$V_1=y^{r+h(m)} \bmod p$$

$$V_2=r\alpha^s \bmod p$$

如果 $V_1=V_2$ 則簽章驗證正確，反之若 $V_1 \neq V_2$ 則簽章驗證失敗。

4. 所提出的新盲簽章相關特性說明

盲簽章需滿足正確性、盲性、不可偽造性和不可追蹤等性質。在這個章節，我們將對所提出的新盲簽章演算法做上列四種性質的說明。

新盲簽章演算法一的四個主要方程式：

簽章方程式： $(\tilde{r}+\tilde{m})x=\tilde{k}+\tilde{s} \bmod \phi(p)$

文件加盲方程式：

$\tilde{m}=a^{-1}(r+h(m)-b)-\tilde{r} \bmod \phi(p)$

解盲簽章方程式： $s=a\tilde{s}-c \bmod \phi(p)$

驗證方程式： $y^{r+h(m)}=r\alpha^s \bmod p$

4.1 正確性

簽章對 (m, r, s) 是經由盲簽章演算法流程而來，最後驗證可以使用 $y^{r+h(m)}=r\alpha^s \bmod p$ 來驗證：

$$y^{r+h(m)}=r\alpha^s \bmod p$$

$$\Leftrightarrow \alpha^{x(r+h(m))}=\alpha^k \alpha^s \bmod p$$

$$\Leftrightarrow x(r+h(m))=k+s \bmod \phi(p)$$

$$\Leftrightarrow x(r+h(m))=a\tilde{k}+bx+c+a\tilde{s}-c \bmod \phi(p)$$

$$\Leftrightarrow x(r+h(m))=a\tilde{k}+bx+a\tilde{s} \bmod \phi(p)$$

$$\Leftrightarrow x(r+h(m)-b)=a(\tilde{k}+\tilde{s}) \bmod \phi(p) \text{ 同乘 } a^{-1}$$

$$\Leftrightarrow xa^{-1}(r+h(m)-b)=(\tilde{k}+\tilde{s}) \bmod \phi(p) \text{ 同減 } x\tilde{r}$$

$$\Leftrightarrow xa^{-1}(r+h(m)-b)-x\tilde{r}=(\tilde{k}+\tilde{s})-x\tilde{r} \bmod \phi(p)$$

$$\Leftrightarrow x(a^{-1}(r+h(m)-b)-\tilde{r})=(\tilde{k}+\tilde{s})-x\tilde{r} \bmod \phi(p)$$

$$\Leftrightarrow x\tilde{m}=(\tilde{k}+\tilde{s})-x\tilde{r} \bmod \phi(p)$$

$$\Leftrightarrow (\tilde{r}+\tilde{m})x=\tilde{k}+\tilde{s} \bmod \phi(p)$$

4.2 盲性

盲性是盲簽章演算法裡的一個重要性質，指的是簽章要求者需要簽章者簽章，但簽章者是在不知文件內容的情況下簽名，在本小節提出的盲簽章演算法中，文件加盲方程式為：

$$\tilde{m} = a^{-1}(r + h(m) - b) - \tilde{r} \bmod \phi(p)$$

其中有參數 a 、 b 和 r 三個參數簽章者未知，故簽章者無法得知文件內容。

4.3 不可偽造性

我們所提出的盲簽章演算法在安全上是基於離散對數，所以只要離散對數問題沒有被解決，除了簽章者可簽署可供正確驗證的簽章外，任何人均不能仿造簽章而能被正確的驗證。

4.4 不可追蹤性

不可追蹤也是盲簽章的一個不可或缺的性質，當簽章要求者把簽章對 (m_i, r_i, s_i) 公佈之後，就算簽章者把所有的 $(\tilde{m}_i, \tilde{r}_i, \tilde{s}_i)$ 記錄下來，因為簽章要求者擁有 a 、 b 、 c 和 r 等秘密參數，所以簽章者無法找出該紀錄和簽章的相關性。

5. 結論及未來研究方向

在本研究中，我們提出了以離散對數難題和 Harn 提出的廣義 ElGamal 編號第 13 個數位簽章所建構的新盲簽章演算法。新盲簽章演算法的安全性是基於離散對數難題，如果離散對數難題沒辦法被破解，就等於我們所提出的演算法是安全的。另外，我們提出的盲簽章演算法滿足盲簽章所需的四個性質：正確性、盲性、不可偽造性和不可追蹤性，希望對往後網路上相關的交易，如電子現金交易或電子投票的應用上有很大的幫助。

在 1992 年，Solms 與 Naccache 兩位學者指出因為盲簽章不可追蹤的性質，會使得洗錢(money laundering)或是敲詐(blackmail)等非法活動變得更容易成功[18]，所以在 1995 年由 Stadler、Piveteau 及 Camenisch 等三位學者提出公平盲簽章(Fair Signatures)[19]的概念，就是在原本盲簽章的性質中，多加入了公平性(Fairness)的概念。主要是在盲簽章原本的三個角色：簽章要求者、簽章者和驗證者之外，多了一個仲裁者(Judge)的角色，以仲裁者的能力，使得原本不能追蹤的盲簽章可經由仲裁者出面追蹤到簽章對和簽章要求者之間的關係，未來的研究方向希望能將此盲簽章演算法延伸為公平盲簽章，若是簽章過程出現問題，便可經由仲裁者的介入，使得問題得到解決。

參考文獻

[1] S. G. Aki, "Digital Signatures: A Tutorial Survey," *Computer*, vol. 16, pp. 15-24, 1983.

[2] D. Chaum, "Blind signatures for untraceable payments", Crypto'82," Springer-Verlag, 1983.

[3] D. L. Chaum, "Blind signature systems," US Patent 4,759,063, 1988.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120-126, 1978.

[5] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Proceedings on Advances in cryptology* Santa Barbara, California, United States: Springer-Verlag New York, Inc., 1990.

[6] L. C. David, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, pp. 84-90, 1981.

[7] L. Harn and Y. Xu, "Design of generalised ElGamal type digital signature schemes based on discrete logarithm," *Electronics Letters*, vol. 30, pp. 2025-2026, 1994.

[8] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *Information Theory, IEEE Transactions on*, vol. 31, pp. 469-472, 1985.

[9] J. M. Alfred, A. V. Scott, and C. V. O. Paul, *Handbook of Applied Cryptography*: CRC Press, Inc., 1996.

[10] W. Diffie and M. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, pp. 644-654, 1976.

[11] G. Tsudik, "Message authentication with one-way hash functions," in *INFOCOM '92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE*, 1992, pp. 2055-2059 vol.3.

[12] J. Nechvatal, "Public-Key Cryptography," in *In Contemporary Cryptology-The Science of Information Integrity*, G. J. Simmons, Ed.: IEEE Press, 1992, pp. 177-288.
[13] J. L. Camenisch, J. M. Piveteau, and M. A. Stadler, "Blind signatures based on the discrete logarithm problem," *Advances in Cryptology–EUROCRYPT'94 (LNCS 950)*, pp. 428–432, 1995.
[14] P. U. B. Fips, "186-2, Digital Signature Standard (DSS)," *National Institute of Standards and Technology (NIST)*, 2000.
[15] N. Kaisa and A. R. Rainer, "A new signature scheme based on the DSA giving message recovery," in *Proceedings of the 1st ACM conference on Computer and communications security* Fairfax, Virginia, United States: ACM, 1993.
[16] L. Harn, "Cryptanalysis of the blind signatures based on the discrete logarithm problem," *Electronics Letters*, vol. 31, 1995.
[17] E. Mohammed, A. E. Emarah, and K. El-Shennawy, "A blind signature scheme based on ElGamal signature," in *EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA*, 2000, pp. 51-53.
[18] S. von Solms and D. Naccache, "On blind signatures and perfect crimes," *Computers and Security*, vol. 11, pp. 581-583, 1992.
[19] M. Stadler, J. M. Piveteau, and J. Camenisch, "Fair blind signatures," *Advances in Cryptology-Eurocrypt'95*, pp. 209-219, 1995.