行政院國家科學委員會專題研究計畫 成果報告

數位簽章之非對稱式潛隱通道之研究(第 3 年)
研究成果報告(完整版)

計 畫 類 別 ：個別型
計 畫 編 號 ：NSC 96-2221-E-006-199-MY3
執 行 期 間 ：98 年 08 月 01 日至 99 年 07 月 31 日
執 行 單 位 ：國立成功大學資訊工程學系（所）

計 畫 主 持 人：黃宗立

計畫參與人員：碩士班研究生-兼任助理人員：黃正傑
碩士班研究生-兼任助理人員：謝朝任
博士班研究生-兼任助理人員：楊竣崴

處 理 方 式 ：本計畫涉及專利或其他智慧財產權，2 年後可公開查詢

中 華 民 國 99 年 10 月 29 日

數位簽章之非對稱式潛隱通道之研究

三年期之第三年

期末報告

計劃主持人：黃宗立 教授

中華民國 九十八 年 十 月

第一章、導論

1.1 前言

潛隱通道（subliminal channel）以不為外人察覺的方式傳遞重要的資訊，其提供了較加密技術更為安全且隱密的通訊方法。因此更適用於重要的情報傳輸或極機密資訊的傳遞。

雖然目前已有許多潛隱通道協定提出，但皆需要訊息傳送者事先與接收者協議一把私密金鑰，此一限制造成潛隱通道在實用上的諸多不便，例如：私密金鑰必須仰賴安全的金鑰分配協定產生、訊息傳送者無法隨機指定接收者等，尤其若利用電子簽章方式建構潛隱通道，則傳送者更必須將其全部或部分之簽章金鑰與接收者共享，同時由於必須事先完成私密金鑰協議，因此這些潛隱通道協定無法用於大量用戶彼此間的訊息傳遞。

為改善上述缺點，吾人近年即積極研究一種非對稱式的潛隱通道，即在不需事先協議私密金鑰的前提下，傳送者可直接運用接收者的公開金鑰建立潛隱通道。本研究計劃的目的即期望以現有研究成果為基礎，提出植基於各種有名的數位簽章策略下之非對稱式潛隱通道協定，並進一步研究訂定非對稱式潛隱通道的建構法則，使後續的研究者或使用者能以此建構法則，評估、判斷某一簽章協定能否被用以建立潛隱通道，以及其可行之建構方法。

「基礎協定發展階段」（第一年）：本階段研究重點主在藉由先期之研究經驗，深入分析現有著名之數位簽章協定的特性，並依據非對稱式潛隱通道的安

全需求，釐清運用接收者的公開金鑰建立非對稱式潛隱通道所可能遭遇之問題與限制，並依據非對稱式潛隱通道的特性，研究在現有之數位簽章協定中建立非對稱潛隱通道之可行性與可行作法。

「建構法則研擬階段」(第二年)：本階段主在延續第一年之研究成果，分析在第一年所發展之非對稱式潛隱通道協定的過程中，其作法上的異同，進而研擬出建構非對稱潛隱通道的一般法則，使未來使用者能依據此通用的建構法則，判斷某一數位簽章協定是否可以用以建立非對稱式潛隱通道以及建構潛隱通道之可行方法。此階段在規劃上將以簽章內是否含亂數、簽章是否具有匿名性，以及傳送者想達到的訊息傳遞功能等三項作為不同的非對稱式潛隱通道的區分依據，利用此分類探討於數位簽章協定中建構非對稱式潛隱通道的通用法則，並期望對這些法則的做法進行說明並找出相關的實例。

「安全證明分析階段」(第三年)：本階段研究重點在針對所提出之非對稱式潛隱通道協定的安全性以及建構法則的正確性提出驗證與分析，我們將根據過去研究可證明之安全分析和各類簽章所累積的成果與經驗，採取正規的安全證明分析模式，除了分析證明我們先前所提出之非對稱式潛隱通道協定確實達到潛隱通道所要求之安全特性外，並據以確認我們所提出之建構法則的正確性，同時以我們的分析證明邏輯，做為未來延續研究發展非對稱式潛隱通道協定安全分析之參考。

1.2 研究動機

在資訊網路發達的今日，密碼學已被廣泛的應用，以確保資訊傳遞的安全。在許多實際的應用環境中，對於機密資訊的交換，除了強調必須確保資料的安全性與完整性之外，往往更重視資料傳遞過程的隱密性。例如：情報人員為能蒐集敵人的情資，經常必須深入敵陣，甚至臥底於敵人的組織當中，適時地將所蒐集的情資回傳所屬的情報單位，而敵方組織很可能為了防堵洩密事件的發生，會對於組織中的成員採取嚴密監控，除明令禁止個人對外進行秘密通訊外，更對所屬人員所傳遞之各種訊息、文件，進行查驗與紀錄，在此情況下，情報人員若將所蒐集之情資採一般加密與直接通訊方式對外傳送，幾乎是不被允許的，而且極可能因此而洩漏身份，所以情報人員與情資接收單位必須建立一個秘密且安全的通訊管道，此秘密通訊管道所必須達到的安全需求，就情報人員而言，必須能讓其順利地將蒐集的情資安全、秘密的對外傳送，且外人無法偵知此通訊管道的存在，就接收情資的一方而言，則必須有能力將所接收的情資予以解密，同時能確認傳送者的身份，以確保資訊來源的正確性。又例如在一個階層式的組織當中，為落實作業紀律的要求，高階人員被授與得以監看低階人員的通信內容，假設此組織中某位低階人員無意間發現其上一級主管有不法之情事發生，而欲向更高階之主管檢舉時，在此情形下，該低階人員亦必須透過秘密的通信管道與更高階之主管建立聯繫，而接受檢舉之主管，則必須能確認檢舉者之身份，以避免落入處理黑函的非議。

1984 年 Simmons[1]首先以兩位監獄犯人在典獄長監控下建立秘密通訊管道，協商逃獄計畫為例，提出了潛隱通道(Subliminal Channel)的觀念，並於 1993 年[2]將潛隱通道植入數位簽章中，用以傳遞潛隱訊息(subliminal messages)。在 Simmons[2]所提出運用數位簽章建立潛隱通道的作法中，簽署者所產生之簽章在外人的眼中就和一般數位簽章一樣，並無任何差異，也可以

很容易地驗證該簽章的正確性；然而對於特定的接收者而言，該簽章隱藏著潛隱訊息，特定的接收者可運用事前與簽署者所共享之秘密金鑰，將潛隱訊息自數位簽章中解密取得，因此外人無法查覺簽署者與特定的接收者之間正秘密地傳遞訊息，進而達到安全通訊的目的。

Simmons 之所以運用數位簽章做為建立潛隱通道之媒介，主要是因為數位簽章本身不可偽冒(Unforgeability)與不可否認(Undeniability)之特性，恰巧滿足潛隱通道所需身份識別、確認資訊來源的安全需求。本研究亦將考慮運用各種有名的電子簽章技術來產生非對稱式的潛隱通道。

1.3 章節概要

這份報告接下來的內容安排如下：

- 第二章，說明相關的密碼學技術簡介，並且介紹較經典的數位簽章(digital signature)，潛隱通道系統。
- 第三章，回顧前二年計劃中，所提出之潛隱通道系統。
- 第四章，簡介亂數神諭(random oracle model)所定義的潛隱通道系統之一般化模組，並且證明非對稱式潛隱通道系統的安全性。
- 第五章為計畫成果自評。

第二章、密碼學技術簡介

2.1 數位簽章

數位簽章不同於一般的手寫簽章，是因數位簽章的結果與簽章明文內容息息相關，並不能夠單純地以簽章外表進行人工的模仿。數位簽章不可否認的特性，正可完整地代表了簽署者的認可，而數位簽章的不可偽冒性也提供絕佳的身份識別功能。一般而言，數位簽章多由三個元素所組成：隨機選取之亂數、雜湊函數及簽署者之個人私密金鑰。以下依序介紹雜湊函數、公開金鑰架構與數位簽章。

(1) 雜湊函數 h( ) (Hash Function)

雜湊函數為一至少含有以下特性之函數：

1. 對於任意長度明文的輸入，輸出固定長度的雜湊函數值。
2. 對於一雜湊函數值 Y，要找尋一 X 使 h(X)=Y 在計算上為不可能。
3. 對於一明文 X_1 要找尋另一明文 X_2 使得其具有相同雜湊值：$h(X_1) = h(X_2)$ 在計算上為不可能。
4. 要找到任意一對不同的明文(X_1 , X_2)使得其具有相同雜湊值：$h(X_1) = h(X_2)$在計算上為不可能。

簡言之，一安全之雜湊函數需具備單向性(One-Way)及不可碰撞性(Collision-Free)。

(2) 公開金鑰密碼系統(Public Key Cryptosystem)

在公開金鑰密碼系統中，每個使用者在金鑰產生階段都會拿到一對金鑰─公鑰(Public Key)及私鑰(Private Key)。公鑰為公開資訊並且有憑証中心CA(Certificate Authority)証明此公鑰與持有人的關係；私鑰則由使用者自行秘密地保管。此一系統能夠提供加密與簽章的效果。

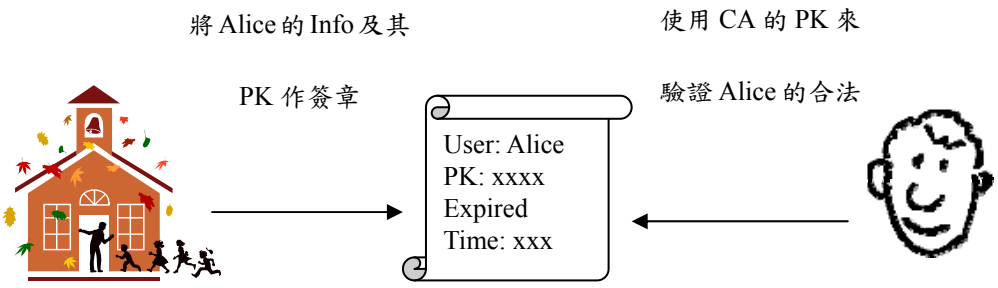


圖 1、公開金鑰系統

(3) 數位簽章(Digital Signature)

數位簽章為公開金鑰密碼系統的應用，利用圖 2 可了解數位簽章與公開金鑰的運作及數位簽章的驗證流程。在此小節中，除了說明數位簽章的兩種現行技術並對此些技術的相關簽章方法做介紹外，也說明數位簽章與隨機亂數在數位簽章裡所扮演的角色及重要性。

現行之技術分為：固定式(Deterministic)與機率式(Probabilistic)數位簽章兩種。固定式簽章的代表為 RSA[3]。RSA 簽章的建立僅由私鑰與明文所組成，同一位簽署者對同一份明文產生的數個簽章，將會相同；機率式簽章的代表為

ElGamal [3]。ElGamal 簽章的建立除了由私鑰與明文組成外，更加入了隨機選取的亂數以提供更高的安全性，藉以防止存在性偽冒(Existentially Forgery)[4]。在圖 2 當 Alice 欲產生一個數位簽章時，通常先將欲簽署之明文 M 通過雜湊函數得到固定長度的雜湊值 h(M)，再將私鑰及雜湊值代入簽章演算法便得到對於此一明文的數位簽章 S。驗證時，接收者 Bob 先依相同雜湊函數算出 h(M)，並將此雜湊值、簽章 S 及簽署者之公鑰作為驗證演算法的輸入值，驗證成功則代表此一簽章確為 Alice 所簽署。

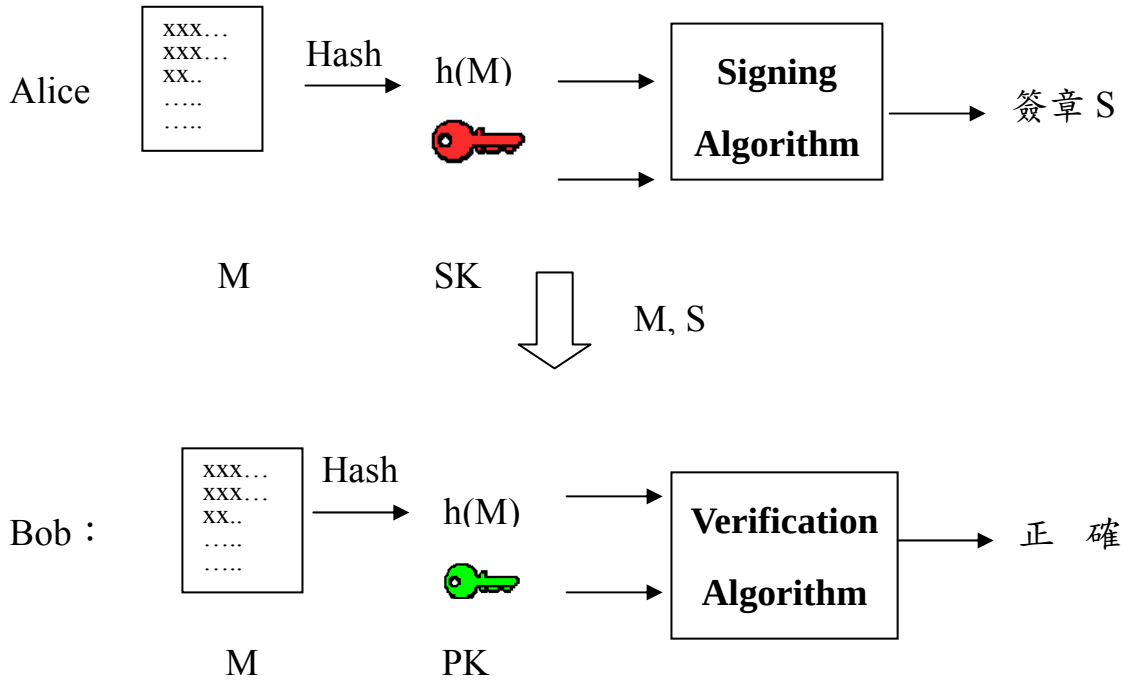


圖 2、數位簽章及驗證流程

以下就說明固定式跟機率式數位簽章的相關簽章方法。首先是屬於固定式簽署方式的 RSA 簽章方法[5]，即一個明文對應到一個簽章，再來是屬於機率式簽署方式的 ElGamal 簽章方法[6]和 Schnorr 簽章方法[7]。其中 RSA 和 ElGamal 簽章方法和加解密方式很相似。

2.1.1 RSA 加解密/簽章方法

在 Diffie-Hellman 提出公開金鑰密碼系統架構時，其實他們並不清楚單向暗門函數是否存在，然而在 1987 年，美國麻省理工學院的三位教授 Rivest、Shamir 及 Adleman(RSA)首先提出了一種基於因數分解的指數函數作為單向暗門函數，為公開金鑰密碼系統架構打開了一片天，而往後許多的加解密/簽章方法都是從這個方法變化而來，其重要性不言而喻。以下為簡介 RSA 加解密/簽章方法的細節。

系統初始階段：

1. 選取兩個大質數 p,q 。
2. 計算 $n = p \times q$ 和 $\phi(n) = (p-1)(q-1)$ 。
3. 選取一個數 e 使得 $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$ 。
4. 計算 $d = e^{-1} \bmod \phi(n)$ ，即 $ed = 1 \bmod \phi(n)$ 。
5. 每位使用者的公鑰為 $\{e_i, n_i\}$ ，其私鑰為 $\{d_i\}$ 。

加密階段：

令欲加密的明文為 M ，且 $M < n$ 。某使用者為 A，其公鑰為 $\{e_A, n_A\}$ ，其私鑰為 $\{d_A\}$ 。當使用者 B 想要加密明文 M 給使用者 A 時，即可用 A 之公鑰 $\{e_A, n_A\}$ 來對該明文 M 加密，其密文為 $C = M^{e_A} \bmod n_A$ 。

解密階段：

當使用者 A 接到密文C想要解開時，他只需要拿自己之私鑰$\{d_A\}$來解密，其解密過程為：$M = C^{d_A} \bmod n_A$，則使用者 A 就可以得到明文M。其解密的細節如下：

$$\begin{aligned} C^{d_A} \bmod n_A &= M^{e_A d_A} \bmod n_A \\ &= M \end{aligned}$$

簽章階段：

令欲簽署的明文為M，且$M < n$。簽署者為 A，其公鑰為$\{e_A, n_A\}$，其私鑰為$\{d_A\}$。當使用者 A 想要簽署明文M時，即可用其私鑰$\{d_A\}$來對該明文M簽章，其簽章為$s = M^{d_A} \bmod n_A$。

驗證階段：

當接收者拿到簽章s欲驗證是否為 A 所簽時，接收者就可以拿 A 的公鑰$\{e_A, n_A\}$來做驗證，其驗證式為：$M = s^{e_A} \bmod n_A$，若這個式子相等，則表示此簽章s為 A 對明文M之簽章。其驗證細節如下：

$$\begin{aligned} s^{e_A} \bmod n_A &= M^{d_A e_A} \bmod n_A \\ &= M \end{aligned}$$

2.1.2 ElGamal 加解密/簽章方法

在 1985 年，ElGamal 提出了一種機率式的簽署方式，即對於每個明文 M ，可能有許多個合法的簽章，而且相較於RSA方法將安全性植基於因數分解上，ElGamal 簽署之安全性是基於解離散對數之困難度上。以下就是 ElGamal 簽章方法的細節。

系統初始階段：

1. 選取一個大質數 p 和一個模 p 的原根 g 。
2. 每位使用者任選一個整數 x_i ，而且 $1 < x_i < p-1$ ，而其公鑰為 $y_i = g^{x_i} \bmod p$ ，其私鑰為 x_i 。

加密階段：

令欲加密的明文為 M ，且 $1 \le M \le p-1$ 。某使用者為 A，其公鑰為 $y_A = g^{x_A} \bmod p$ ，其私鑰為 x_A 。當使用者 B 想要加密明文 M 給使用者 A 時，即可用 A 之公鑰 y_A 來對該明文 M 加密，其方法如下：

1. 選取一個亂數 k ，其中 $\gcd(k, p-1) = 1$ 。
2. 計算 $r = g^k \bmod p$ 。
3. 計算 $C = My_A^{\,k} \bmod p$ 。
4. 則密文為 (r, C) 。

解密階段：

當使用者 A 接到密文(r,C)想要解開時，他只需要拿自己之私鑰x_A來解密，其解密過程為：$M=\frac{C}{r^{x_A}} \bmod p$，則使用者 A 就可以得到明文$M$。其解密細節如下：

$$\begin{aligned}\frac{C}{r^{x_A}} \bmod p &= My_A{}^k (r^{x_A})^{-1} \bmod p \\ &= Mg^{x_A k}(g^{kx_A})^{-1} \bmod p \\ &= M\end{aligned}$$

簽章階段：

令欲簽署的明文為M，且$1 \le M \le p-1$。簽署者為 A，其公鑰為$y_A = g^{x_A} \bmod p$，其私鑰為x_A。當使用者 A 想要簽署明文M時，即可用其私鑰x_A來對該明文M簽章，其方法如下：

1. 選取一個亂數k，其中$\gcd(k, p-1)=1$。
2. 計算$r = g^k \bmod p$。
3. 計算$M = x_A r + ks \bmod p-1$或$s = k^{-1}(M - x_A r) \bmod p-1$。
4. 則 A 對該明文M簽章為(r,s)。

驗證階段：

當接收者拿到簽章(r,s)欲驗證是否為 A 所簽署時，接收者就可以拿 A 的公鑰y_A來做驗證，其驗證式為：$g^M = y_A{}^r r^s \bmod p$。若這個式子相等，則表示此

簽章(r,s)為 A 對明文M之簽章。其驗證細節如下：

$$g^M \bmod p = g^{x_A r} g^{ks} \bmod p$$
$$= g^{x_A r + ks} \bmod p$$

2.1.3 Schnorr 加解密/簽章方法

在 1989 年，Schnorr 也提出了一個機率式的簽章方法，而這個方法和 ElGamal 簽章方法相同，其安全性也是植基於解離散對數之困難度上，但其和 ElGamal 簽章方法不同的是 Schnorr 簽章較短，而且計算較快。

系統初始階段：

1. 取兩個大質數p和q使得$q \mid p-1$且$q \geq 2^k$，其中k是系統的安全係數。
2. 選取一個生成子g且能形成大小為q的乘法群。
3. 單向雜湊函數 h()，其輸出值屬於Z_q。
4. 對於每個人選取其私鑰為$x_i \in Z_q$，其相對應之公鑰為$y_i = g^{x_i} \bmod p$

簽章階段：

令欲簽署的明文為M。簽署者為 A，其公鑰為$y_A = g^{x_A} \bmod p$，其私鑰為x_A。當使用者 A 想要簽署明文M時，即可用其私鑰x_A來對該明文M簽章，其方法如下：

1. 選取一個亂數k，其中$1 \leq k \leq p-1$。

2. 計算 $r = g^k \bmod p$ 。

3. 計算 $e = h(r, M)$ 。

4. 計算 $s = k - x_A e \bmod p$ 。

5. 則 A 對明文 M 的簽章為 (e,s) 。

驗證階段：

當接收者拿到簽章 (e,s) 欲驗證是否為 A 所簽署時，接收者就可以拿 A 的公鑰 y_A 來做驗證，其驗證式如下：

1. 接收者先計算 $r' = g^s y_A{}^e \bmod p$ 。

2. 再檢查 $h(r', M) = e$ ，若這個式子相等，則可確定此簽章 (e,s) 為 A 對明文 M 之簽章。其驗證細節如下：

$$\begin{aligned} g^s y_A{}^e \bmod p &= g^{k - x_A e} g^{x_A e} \bmod p \\ &= g^k \bmod p \\ &= r \bmod p \end{aligned}$$

以上為三種簽章方式的加解密、簽章與驗證的運作過程。而數位簽章的特性在於其有不可否認性，亦即只有知道私鑰的人才能簽出合法的數位簽章，而其另一個重要特性：不可偽冒性則是簽章演算法的重點。不可偽冒性基本上是仰賴於現今已知之難題：離散對數難題(DLP)、質因數分解(IFP)等，此外安全的數位簽章通常還必須能抵抗其他相關之攻擊，例如： No Message Attack、Adaptive Chosen-Message Attack 及存在性偽冒(Existentially Forgery)[4]等。此外，就現今數位簽章安全性的證明而言，只有機率式簽章演算法，因為其隨機亂數的加入，使得其具備抵禦存在性偽冒攻擊的能力，而固定式簽章演算法如

RSA[3]則無法防止此種攻擊。

2.2 潛隱通道

然而，一般的密碼系統雖可將重要文件由明文加密轉變成為密文，但密文傳遞的過程，卻也明確透露送方與收方正進行秘密資訊的交換，而惡意的第三者亦可輕易地在網路上攔截、蒐集傳遞中之密文，以進行各種可能的破密分析。不同於一般的密碼系統，潛隱通道的發展除可提供送方與收方一個安全的通信管道外，最重要的是，第三者無法從送方與收方的通信過程中偵知兩人正秘密地進行重要資訊的交換，因此，相較於傳統密碼系統，潛隱通道在機密資訊傳遞方面，提供了更高的安全性與隱密性，也更適用於重要的情報傳輸或極機密資訊的傳遞。

為了能確認潛隱訊息的來源，現有潛隱通道的建立通常均依附在電子簽章協定中，利用電子簽章所具備之不可否認性，來達到確認傳送者身份的目的。簡言之，送方通常是利用其個人的電子簽章來藏匿與傳遞潛隱訊息給特定的接收者，此電子簽章對一般人而言如同普通的電子簽章一樣，僅能驗證簽署者的身份與簽章的正確性，而無法偵知其中隱含著潛隱訊息，但就特定的接收者而言，卻能從該簽章中萃取出潛隱資訊。

在研究上，潛隱通道基本上係屬於資訊隱藏 (Steganography)的技術範疇，資訊隱藏係將資訊以不可偵測、私密地傳送給另一方的統稱，而用來將訊息以不可偵測的方式傳送的管道則稱之為潛隱通道(Subliminal Channel)，故潛隱通道為資訊隱藏的實際作法。資訊隱藏的基礎概念在於收發雙方可利用事前共享的金鑰來達到將秘密訊息嵌入一般的訊息中傳送，且只有握有此把金鑰的接收

者便能夠獲得秘密訊息。資訊隱藏技術依隱藏方式又可區分為二個層面：語言學(Linguistic)的與技術(Technical)層面上的。語言學上的資訊隱藏係指將秘密訊息隱藏於手寫(Hand-write)的文章；技術層面則泛指非語言學方面者均屬此類。一個稱之為成功的資訊隱藏基本上需要有如下特性：

1. 不可分辨性(Indistinguishability)：任何人均無法判別一份資訊中是否有隱藏秘密訊息，因而無法偵測出潛隱通道是否存在。此也代表含有潛隱訊息的簽章與不含有潛隱訊息的原始簽章是無法分辨的，故也保有原有數位簽章的安全性。如何証明二個簽章演算法所算出之簽章符合不可分辨性？是否會有一組簽章值代入某個演算法便能得知是否隱藏著潛隱訊息？証明方法如下：假設一普通之簽章演算法 A 及另一用來隱藏潛隱訊息之簽章演算法 B，二者輸出的格式皆同，驗證程序也皆同。若針對任一訊息 m，經由 A 演算法及 B 演算法所得出之簽章 S_1、S_2，若 $S_1 = S_2$ 恆成立，則不可分辨出是否有隱藏潛隱訊息。

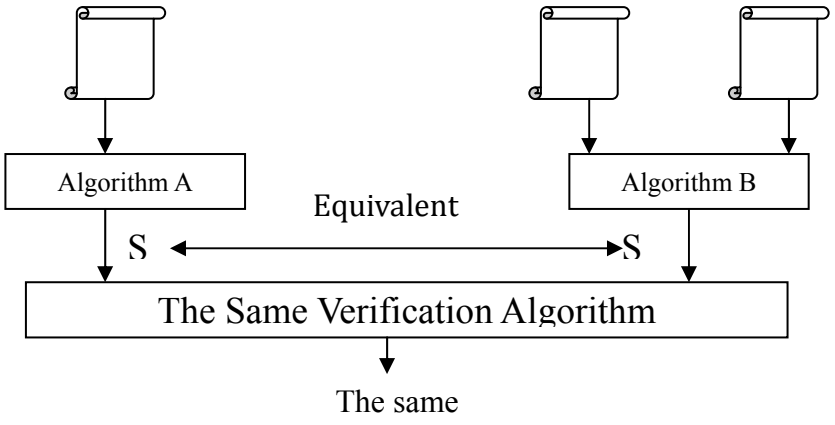


圖 3、不可分辨性

2. 不可萃取性(Inextractability)：除握有金鑰者，其餘任何人均無法從資料中取得秘密訊息。

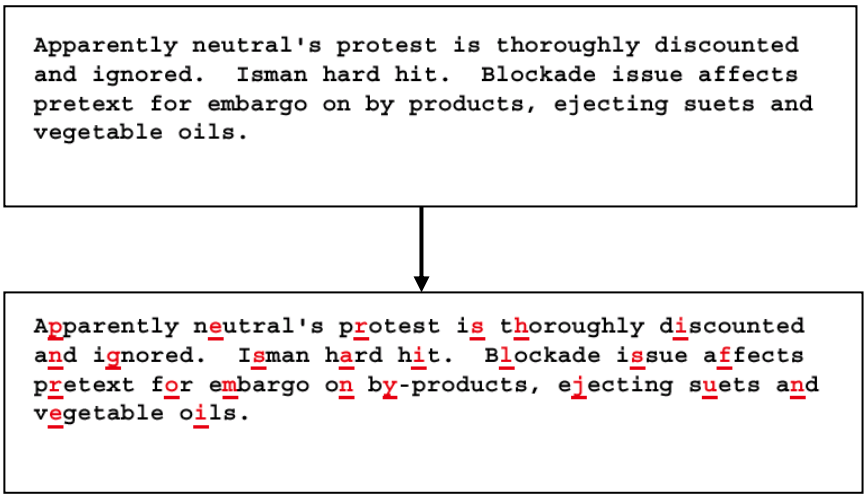


圖 4、Linguistic – 每第二個字元之集合為隱藏

以潛隱通道而言，Simmons 於 1994 將潛隱通道植入數位簽章裡，並定義出了寬頻 (Broadband) 潛隱通道及窄頻(Narrowband)潛隱通道。對於與一訊息 M 相對應及內藏潛隱訊息 M'的簽章 S，分類寬頻及窄頻的方法如下：

- α：簽章 S 的總位元數
- β：為提供防止偽冒、篡改所需之位元數
- 寬頻(Broadband)：若潛隱訊息 M'之位元數等於或接近$\alpha-\beta$。
- 窄頻(Narrowband)：若潛隱訊息 M'之位元數遠少於或使用部份$\alpha-\beta$。

所以資訊隱藏與一般密碼學(Cryptosystem)不同之處在於一般密碼學的加密只符合私密性，並沒有不可偵測性，即使非秘密訊息的接收者也能夠知道此

一傳送的資訊裡有隱藏著某個秘密訊息。因此，一般加密的技術並不能套用先前所提到的應用環境中。

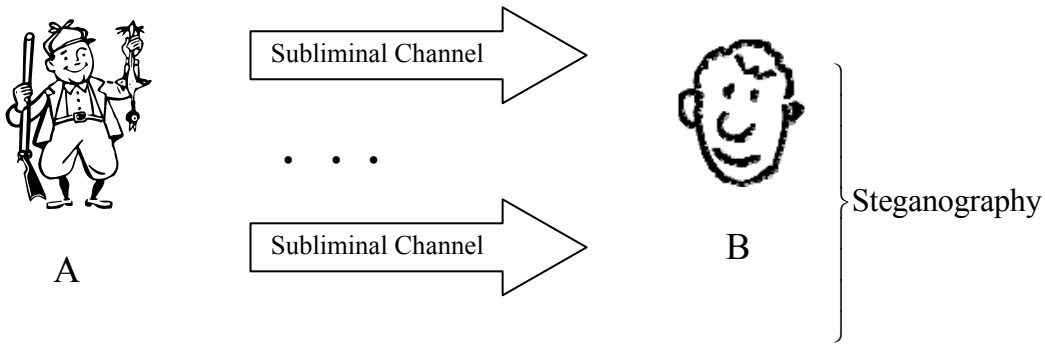


圖 5、潛隱通道為資訊隱藏的實現

現今的潛隱通道基本上都是配合數位簽章來實作，藉由數位簽章的不可否認性(non-repudiation)來避免潛隱訊息成為黑函。自 Simmons 於 1994 首先將潛隱通道植入數位簽章之後，潛隱式通道有其應用環境與使用之必要性，因此陸續有許多學者投入，發展出不同的潛隱通道簽章[8,9,10,11,12]，在這些潛隱通道簽章中，其安全性多植基於因數分解[11]、離散對數[12]及植基於 Pairing[8]的數學難題上。

2.2.1 Harn & Gong 的植基於因數分解之潛隱通道簽章

在 Harn 及 Gong[11]的架構裡，有著二個潛隱通道：*p-Channel* 及 *q-Channel*，在這每個通道與一潛隱接收者共享一私鑰以達到傳送潛隱訊息。

系統初始階段：

1. 選擇四個大質數 p,q,p',q'，且使得 $p=2p'+1, q=2q'+1$，並計算 $N=pq$

2. α：為一生成子，其形成一大小為$(p-1)(q-1)$之循環群

3. 選擇二個私鑰$x_p \in [1-p-1], x_q \in [1, q-1]$且必須為偶數，$x_p$與在$p-Channel$的接收者共享；$x_q$與在$q-Channel$的接收者共享。

其中，$y_p = \alpha^{x_p} \bmod p, y_q = \alpha^{x_q} \bmod q, y = CRT(y_p, y_q, p, q)$；

$x = CRT(x_p, x_q, \phi(p), \phi(q))$，CRT 為中國餘數定理。

因此，簽署者的私鑰為(p, q, x_p, x_q, x)

$p-Channel$接收者的私鑰為(p, x_p)

$q-Channel$接收者的私鑰為(q, x_q)

公鑰為(α, N, y)

簽章產生階段：

假設m為一有意義訊息的雜湊值，$m_p \in [1, p-1], m_q \in [1, q-1]$分別為二個通道的潛隱訊息且為偶數。要分別隱藏此二個潛隱訊息至$p-Channel, q-Channel$執行如下：

1. 計算$r_p = \alpha^{m_p} \bmod p, r_q = \alpha^{m_q} \bmod q$及$r = CRT(r_p, r_q, p, q)$

2. 計算$m_{pq} = CRT(m_p, m_q, \phi(p), \phi(q))$在所得之二值裡選取較小值。

3. 求得$s = rmx - m_{pq} \bmod \phi(N)$

(r, s)　為訊息雜湊值為m的簽章並且隱藏著潛隱訊息m_p, m_q

簽章驗證階段：

若符合 $y^{rm} = r\alpha^{s} \bmod N$ 則為一對訊息雜湊值為 m 之合法簽章

取出潛隱訊息階段：

根據中國餘數定理，以下算式成立。

$$rmx = (m_{pq} + s) \bmod N \tag{1}$$

$$rmx_{p} = (m_{p} + s) \bmod \phi(p) \tag{2}$$

$$rmx_{q} = (m_{q} + s) \bmod \phi(q) \tag{3}$$

所以 $p-Channel, q-channel$ 的潛隱接收者可分別利用 $x_{p}, \phi(p)$ 及 $x_{q}, \phi(p)$ 於(2)式及(3)式取得 m_{p}, m_{q} 。

在 Harn 的寬頻潛隱通道簽章裡，$p-Channel$ 及 $q-Channel$ 的潛隱訊息的長度共有 $|\phi(p)|+|\phi(q)|$，簽章 (r,s) 長度共為 $|N|+|\phi(N)|$，又 r 為提供防止偽冒使用(不知私鑰的情況下，若先決定 s ，則必須選一 r 並使得其能通過驗證式)，所以根據定義 $\alpha-\beta=|\phi(N)|=|\phi(p)|+|\phi(q)|$，故其為寬頻潛隱通道。在這寬頻通道裡，共謀攻擊能夠經由他們彼此所持有的私鑰來求得簽署者的私鑰，往後便能偽冒簽署者作簽章的動作。因此他們又提出了窄頻潛隱通道簽章以抵抗這種攻擊。

2.2.2 Harn & Gong 的植基於因數分解之窄頻潛隱通道簽章

在窄頻潛隱通道簽章裡，新增了第三個只有簽署者知道的通道 $r-Channel$ 。如同 p、$q-Channel$ ，在 $r-Channel$ 裡也有相對應的私鑰 (r, x_{q}) 及公鑰 $(y_{r} = \alpha^{x^{r}} \bmod r)$ 。

初始階段：

與寬頻潛隱通道簽章之初始階段相同，唯一不同者為需選擇一 $r = 2r'+1$ 並且使 $y = CRT(y_p, y_q, y_r, p, q, r), x = CRT(x_p, x_q, x_r, \phi(p), \phi(q), \phi(r)), N = pqr$

簽章產生階段：

選一潛隱訊息 m_r，其餘皆與之前相同，但並無實際 $r - Channel$ 接收者。

在窄頻潛隱簽章裡，他們解決了共謀的問題，但卻也因為 N 的變大使得每次的簽章長度增加了 log$r$ 個位元。因此 J. K. Jan[11]等人後來提出植基於離散對數的潛隱通道簽章，在他們的窄頻部份也能夠抵抗共謀問題。

2.2.3 Lee & Lin 的植基於離散對數之寬頻潛隱通道簽章

J. K. Jan 於 1999 年提出植基於離散對數之潛隱通道簽章(寬頻及窄頻)，雖然能夠傳送潛隱訊息，但於 2003 年由 Lee 及 Lin 等人指出其潛隱通道簽章會被中間者將潛隱訊息作更改而使得潛隱通道接收者收到錯誤的潛隱訊息，並且簽章依然能通過驗證。於是 Lee 及 Lin[12]提出修改使得這個問題得以解決。因此我們將 J. K. Jan 的寬頻潛隱通道數位簽章，經過了 Lee 及 Lin 改良後展現出來。

系統初始階段：

1. 選取一大質數 p 且存在另一大質數 q 符合 $q \mid p$。

2. 選取二個生成子 g_1, g_2 且皆能形成大小為 q 的循環群。

3. 選取 x_1, x_2 為私鑰，相對應的公鑰為 $y = g_1^{-x_1} \cdot g_2^{-x_2} \bmod p$

4. 單向雜湊函數 h(・)

因此，簽署者的私鑰為 (x_1, x_2)，公鑰為 (y, g_1, g_2, p, q)

第一潛隱通道接收者的私鑰為 x_1

第二潛隱通道接收者的私鑰為 x_2

簽章產生階段：

令 m 為欲簽署之明文，$m_1, m_2 \in [1, q-1]$ 分別為欲傳給第一及第二潛隱通道接收者的潛隱訊息。要分別隱藏此二潛隱訊息，作法如下：

1. 計算 $r = g_1^{m_1} \cdot g_2^{m_2} \bmod p$

2. 計算 $e = h(r \| m)$

3. 根據私鑰求得 $s_1 = m_1 + ex_1 \bmod p, s_2 = m_2 + ex_2 \bmod p$

(e, s_1, s_2) 為訊息 m 的簽章並且隱藏著潛隱訊息 m_1, m_2。

簽章驗證階段：

若符合下式，(e, s_1, s_2) 則為一對訊息 m 之合法簽章。

$e = h(g_1^{s_1} \cdot g_2^{s_2} \cdot y^e \| m)$

取出潛隱訊息階段：

第一潛隱通道的接收者，因為知道x_1，故可取得潛隱訊息($m_1 = s_1 - ex_1$)。同樣的方法第二潛隱通道的接收者也能取出潛隱訊息$m_2 = s_2 - ex_2$

而在 Lee 及 Lin 這個架構裡，潛隱訊息的長度共有$2\log q$，簽章(e, s_1, s_2)長度共為$|e|+2|q|$，又e為提供防偽冒用(在不知私鑰的情況下，若先決定s_1, s_2，則必須選一e並使得其能通過驗證式)，所以根據定義$\alpha - \beta = 2|q|$，故為寬頻潛隱通道。因為第一通道及第二通道的接收者各知道簽署者一半的私鑰，所以這種寬頻的潛隱通道簽章依舊會遭到共謀攻擊。接下來將介紹經過 Lee 及 Lin 改良 J. K. Jan 窄頻潛隱通道簽章，這樣的改良不但能夠抵擋共謀攻擊，且保証潛隱接收者能夠收到正確無誤的潛隱訊息。

2.2.4 Lee & Lin 的植基於離散對數之窄頻潛隱通道簽章

在窄頻潛隱通道簽章裡，新增了第三個只有簽署者知道的潛隱通道。因為共謀需要所有通道接收者的合作，而又無實際上的第三潛隱接收者，故能防止共謀。

初始階段：

與寬頻潛隱通道簽章之初始階段相同，唯一不同者如下：

1. 選擇一生成子g_3使得此生成子在模p之下能產生大小為q的循環群。

2. 選取第三把私鑰x_3，相對應的公鑰為$y = g_1^{x_1} \cdot g_2^{x_2} \cdot g_3^{x_3} \bmod p$

3. 將x_1, x_2秘密地與第一、第二通道接收者共享，保持x_3的私密性。

簽章產生階段：

1. 選一潛隱訊息m_3，計算$r = g_1^{m_1} \cdot g_2^{m_2} \cdot g_3^{m_3} \bmod p$。

2. 計算$e = h(r \| m)$。

3. 依序根據私鑰x_1, x_2, x_3算出s_1, s_2, s_3並發送出去。

簽章驗證階段與取出潛隱訊息階段的作法皆相同。因為是窄頻的架構，共謀也只有洩露x_1與x_2，缺少另一把私鑰x_3，共謀者不能偽冒簽署者簽章。

2.2.5 Zang et al. 的植基於 Weil Pairing 的潛隱通道簽章

此簽章其難題為 GDH(Gap Diffie Hellman)。因此在介紹他們的架構前先簡述 Weil Pairing 及在橢圓曲線上的 DLP、DDH、CDH 及 GDH[13]。我們舉個例子，假設G為在橢圓曲線下的一個加法子群，一點P為其生成子，且形成大小為質數q之循環群；G_2為一乘法群且其階數(Order)亦為q。現有一函數$e: G \times G \to G_2$能將二個橢圓曲線上的點映射到整數加法群G_2裡的一個元素。這

種 Bilinear Pairing 符合如下特性：

- Bilinear：令 P_1, P_2, P, Q 為橢圓曲線上四個點，則以下條件成立

$$e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$$

$$e(aP, bQ) = e(aP, bQ) = e(P, P)^{ab}$$

- Non-degenerate：存在一點 $P \in G$ ，使得 $e(P, P) \neq 1$
- Computable：存在一快速的演算法能求出 $e(P, Q)$

DLP (Discrete Logarithm Problem)

在橢圓曲線上存在著離散對數問題：當給予二點 aP 及 P ，要算出 a 為不可能。

DDH (Decision Diffie-Hellman Problem)

給定二點 aP, bP ，其中 $a, b \in Z_q^*$ ，要計算 abP 為一難題。

CDH (Computational Diffie-Hellman Problem)

給定三點 aP, bP, cP ，其中 $a, b, c \in Z_q^*$ ，要判斷是否 $c = ab$ 為一難題。

GDH(Gap Diffie-Hellman Problem)

當 DDH 為容易而 CDH 為困難者稱之為 GDH。

在 e 函數這種映射(Mapping)下，DDH 變得不再是難題：給定 aP, bP, cP ，可由

$e(aP, bP) = e(P, P)^{ab}$ 是否等於 $e(cp, p) = e(P, P)^c$ 來判斷是否 $c = ab$ 。因此在此情況下稱為 GDH 群。

而 Zang et al.的潛隱式數位簽章[8]，是植基於 ID 的 Weil Pairing。在植基於 ID 的這種架構下，每個人都有自己的 ID，而私鑰是由系統依據各人 ID 及系統的私鑰所運算出來再秘密地發給各人。因此，不像公開金鑰系統一樣能確保私鑰只有自己知道。

系統初始階段：

$s \in Z_q^*$、$sP \in G_1$ 分別為系統的私鑰及公鑰

$e: G_1 \times G_1 \to G_2$，$P$ 為橢圓曲線上一點並為能產生大小為 q 之加法群的生成子。

$H(\bullet): \{0,1\}^* \to Z_q$，能將任意長度的訊息轉換成固定長度位元數之正整數。

$H_2(\bullet): \{0,1\}^* \to G_1$，能將任意長度的訊息轉換成固定長度位元數且於 G_1 上一點。

$Q_{ID} = H_2(ID)$：為 G_1 上之一點，由個人 ID 經由 $H_2(\bullet)$ 所求得。

$S_{ID} = sQ_{ID}$：為雜湊值為 Q_{ID} 相對應的私鑰，由系統算出 s 倍 Q_{ID} 所得。

簽署者將私鑰 S_{ID} 秘密地傳送給潛隱接收者，與之共享。

簽章產生階段：

令 m 為欲簽署之明文，m_{Sub} 為欲潛隱訊息且為 G_1 上之一點，要將此潛隱訊息

傳送給接收者，作法如下：

1. 計算 $r = e(m_{Sub}, P)$

2. 計算 $v = H(m, r)$

3. 依據私鑰算出 $U = vS_{ID} + m_{Sub}$

(U, v) 為訊息 m 的簽章並且隱藏著潛隱訊息 m_{Sub} 。

簽章驗證階段：

接收到簽章 (U, v) 後，依下式算出 r ，再代入 $v = H(m, r)$ 驗證簽章的正確性。

$$r = e(U, P) \cdot e(Q_{ID}, sP)^{-v} = e(U, P) \cdot e(-vS_{ID}, P) = e(m_{Sub}, P)$$

取出潛隱訊息階段：

因為潛隱接收者知道簽署者之私鑰 S_{ID} ，故可取得潛隱訊息 $m_{Sub} = U - vS_{ID}$ 。

在這個潛隱通道簽章裡，潛隱訊息長度為 m_{Sub} ，簽章為 (U, v) 又 v 為用來防止偽冒用(在不知私鑰的情況下，若先決定 v ，則必須選一 U 並使得其能通過驗證式)，所以根據定義顯示，潛隱訊息 m_{Sub} 的長度等於 U 的長度為寬頻潛隱通道。相同地，在這寬頻通道裡，潛隱接收者因為知道簽署者之私鑰，能夠偽冒簽署者。

2.2.6 Zang et al. 的植基於 Bilinear Pairing 之窄頻潛隱通道簽章

此窄頻潛隱通道簽章，並不像先前二個架構般地新增簽署者之私鑰並秘密

保存來達到窄頻防止共謀，而是將與潛隱接收者共享的東西更改。簽署者跟潛隱接收者間不再事先共享私鑰，取而代之的是一個亂數，但代價卻是潛隱接收者得進行小幅度的暴力搜尋法取出潛隱訊息。另外，也不能於不同簽章裡隱藏相同的潛隱訊息。

系統初始階段：

一切與寬頻架構一樣，不同處為簽署者事先選取一亂數 $k' \in Z_q^*$，並算出 $r' = e(P,P)^{k'}$，再選擇一數 l 使 $l << q$，將 r'、l 秘密傳送給予潛隱接收者。

簽章產生階段：

令 m 為欲簽署之明文，$m' \in [1, l-1]$ 為潛隱訊息。要將潛隱訊息隱藏於簽章中傳送給潛隱接收者作法如下：

1. 計算 $r = e(P,P)^{k'+m'}$
2. 計算 $v = H(m,r)$
3. 依據私鑰算出 $U = vS_{ID} + m' + k'$

   (U,v) 為訊息 m 的簽章並且隱藏著潛隱訊息 m_{Sub}。

簽章驗證階段：

與寬頻部份之驗證程序相同。

取出潛隱訊息階段：

1. 計算 $r / r' = e(P, P)^{m'}$

2. 利用暴力攻擊法找出 m'

在此窄頻潛隱簽章架構中，接收者需要利用暴力攻擊法來找出潛隱訊息，所以參數 l 勢必得遠小於 q ，因此所能傳送的能力與先前技術相較下來得差。

2.2.7 Okamoto 簽章

現有文獻中所提出的潛隱通道協定均屬於「對稱式潛隱通道協定」，亦即潛隱訊息的傳送者必須事先將其全部或部分之簽章金鑰與接收者共享，只有如此接收者才有能力從傳送者的電子簽章中讀取潛隱訊息，此一特性造成對稱式潛隱通道協定應用上的限制與不便，例如：傳送者必須依賴安全的金鑰分配協定來分配其簽章金鑰給接收者、潛隱接收者無法隨機指定，以及潛隱接收者很可能利用傳送者的簽章金鑰偽造傳送者簽章等。簡言之，「對稱式潛隱通道協定」存在有以下三種限制：

1. 需要事先共享一份相同的金鑰。
2. 能夠形成不同群體的潛隱接收者之數量有限─若簽署者能共享之私鑰有 k 把，則最多只能分成 k 個不同群的潛隱接收者。
3. 需要小幅度的暴力攻擊法找尋出潛隱訊息─如 Zang 等人的方法，但形成潛隱接收群之數量不限。

Jan et al. [10]則在 1999 年提出了架構在 Okamoto[14]的簽章系統上的潛隱通道，做出一個不用事先共享私鑰的窄頻潛隱通道簽章，以下就介紹 Okamoto 簽章作法和 Jan 等人的作法，其細節如下。

- Okamoto 簽章

系統初始階段：

1. 選取一大質數 p 且存在另一大質數 q 符合 $q \mid p$。

2. 使用者選取二個生成子 g_1, g_2 且皆能形成大小為 q 的循環群。

3. 選取 x_1, x_2 為私鑰，相對應的公鑰為 $y = g_1^{-x_1} \cdot g_2^{-x_2} \bmod p$

4. 單向雜湊函數 h(・)

因此，簽署者的私鑰為 (x_1, x_2)，公鑰為 (y, g_1, g_2, p, q)

簽章產生階段：

令 m 為欲簽署之明文，作法如下：

1. 計算 $r = g_1^{k_1} \cdot g_2^{k_2} \bmod p$

2. 計算 $e = h(r \| m)$

3. 根據私鑰求得 $s_1 = k_1 + ex_1 \bmod p, s_2 = k_2 + ex_2 \bmod p$

(e, s_1, s_2) 為訊息 m 的簽章。

簽章驗證階段：

若符合下式，(e, s_1, s_2) 則為一對訊息 m 之合法簽章。

$$e = h(g_1^{s_1} \cdot g_2^{s_2} \cdot y^e \| m)$$

2.2.8 Jan et al. 的簽章架構

其重點在於利用 Okamoto 的簽章中簽署者所擁有的兩個私密金鑰與兩個不同的潛隱接收者建立兩道不同的潛隱通道 (如圖 6)。

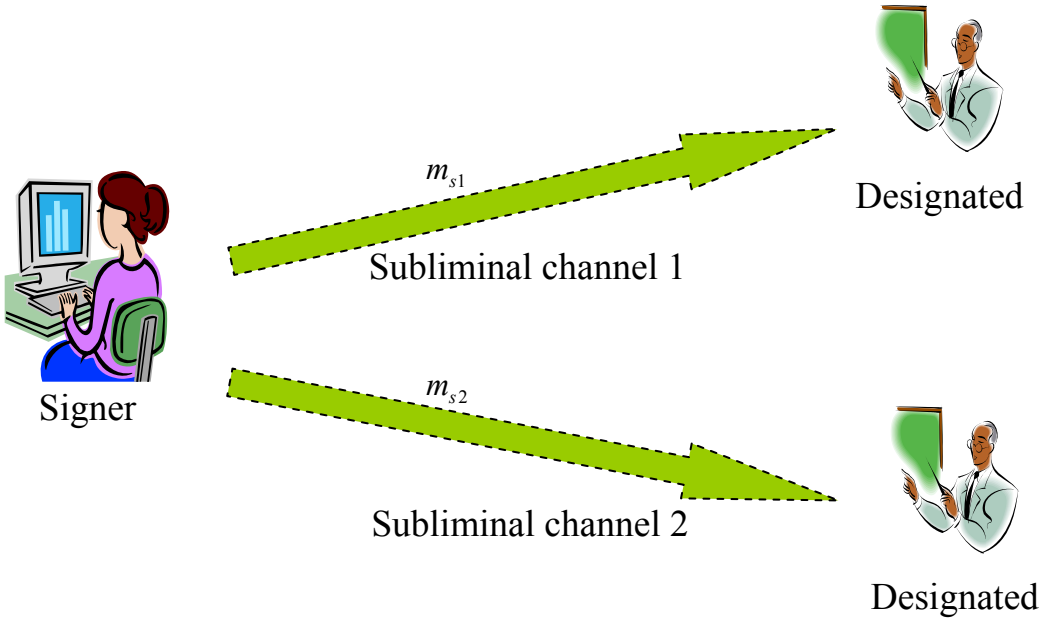


圖 6、Jan 等人提出的潛隱通道示意圖

其運作流程如下：

步驟 1 環境設定：

系統選取兩個大質數 p ，q ，其中 $q \mid p-1$。設定使用者 U_i 的私密金鑰為 $(x_{i1}, x_{i2}) \in_R Z_q^*$ ，公開金鑰為 $y_i = g^{-x_{i1}} g^{-x_{i2}} \bmod p$ 。

注意：潛隱傳送者(即簽章簽署者) U_π 與兩位潛隱接收者，假設為 R_i 及 R_j ，必須

事前共享一把秘密金鑰，即U_π需傳送一把私密金鑰$x_{\pi 1}$給R_i，並傳送另一把私密金鑰$x_{\pi 2}$給R_j。

步驟 2 簽章簽署：

簽署者在簽署文件M的過程中首先計算出$e=(g^{m_{s1}}g^{m_{s2}} \bmod p \| M)$，並將欲傳送給潛隱接收者$R_i$的潛隱訊息$m_{s1} \in Z_q^*$藏於簽章中的$s_1=(m_{s1}+ex_{\pi 1}) \bmod q$，接著將欲傳送給潛隱接收者$R_j$的潛隱訊息$m_{s2} \in Z_q^*$藏於簽章中的$s_2=(m_{s2}+ex_{\pi 2}) \bmod q$。

步驟 3 簽章驗證：

驗證方式與 Okamato 的方式相同，驗證者以簽署者的公開金鑰y_π來驗證簽章(e,s_1,s_2)及文件M：$H(g^{s_1}g^{s_2}y_\pi{}^e \| M) \stackrel{?}{=} e$。

步驟 4 潛隱訊息萃取：

潛隱接收者R_i以與潛隱傳送者共享的秘密金鑰$x_{\pi 1}$來萃取潛隱訊息：$m_{s1}=(s_1-ex_{\pi 1}) \bmod q$，潛隱接收者$R_j$以與潛隱傳送者共享的秘密金鑰$x_{\pi 2}$來萃取潛隱訊息：$m_{s2}=(s_2-ex_{\pi 2}) \bmod q$。

此系統的分析：

1．與 Simmons[2]的系統有相同的限制，由於潛隱傳送者在事前需與潛隱接收者共享秘密金鑰，使得潛隱傳送者無法任意挑選潛隱接收者。

2．雖然每位潛隱接收者只擁有部分潛隱傳送者的私密金鑰，但只要兩位潛隱接收者合作的話，就可導出潛隱接收者完整的私密金鑰，故潛隱接收者還是有可能可以偽冒簽章。

2.3 非對稱式潛隱通道簡例說明

從以上的研究不難發現利用對稱式金鑰的潛隱通道建構方式，都存在金鑰共享所產生的數種問題，為了解決在對稱式潛隱通道的此數種問題，我們在先期研究中，即考量把原有須利用雙方事先共享秘密金鑰的方式改以運用潛隱接收者的公開金鑰的方式來解決，如此簽署者與潛隱接收者便能夠在不需事先執行私密金鑰分配作業，而得到用以建立潛隱通道的金鑰，這也就不會有對稱式潛隱通道的三種問題，對於此種利用公開金鑰來建立潛隱通道的方式，吾人定義為非對稱式潛隱通道。以下我們提出一個植基於 Okamoto 簽章的非對稱式潛隱通道簡例做說明，此簡例並不代表最終之研究成果，其安全性、有效性和隱蔽性仍需日後嚴密之探討。

系統初始階段：

1. 選取一大質數 p 且存在另一大質數 q 符合 $q \mid p$。
2. 單向雜湊函數 h(・)
3. 一系統生成子 g

各使用者自行作如下動作：

1. 選取α, t_1, t_2並形成二個大小為q循環群的生成子g_1, g_2，其中

   $g_1^{\alpha} = g_2 \bmod p$,

   $g_1 = g^{t_1} \bmod p, g_2 = g^{t_2} \bmod p$

2. 選取x_1, x_2為私鑰，相對應的公鑰為$y = g_1^{-x_1} \cdot g_2^{-x_2} \bmod p$

因此，簽署者的私鑰為$(x_1, x_2, \alpha, t_1, t_2)$，公鑰為$(y, g_1, g_2, p, q)$

簽章產生階段：

令m為欲簽署之明文，$m' \in [1, q-1]$為簽署者 A 欲傳給潛通道接收者 B 的隱訊息。令簽署者與潛隱接收者之參數分別如下：

$t_1, t_2, \alpha, g_1, g_2, x_1, x_2, y_A = g_1^{-x_1} \cdot g_2^{-x_2} \bmod p, g_1^{\alpha} = g_2 \bmod p, g_1 = g^{t_1} \bmod p, g_2 = g^{t_2} \bmod p$

$t_3, t_4, \beta, g_3, g_4, x_3, x_4, y_B = g_3^{-x_3} \cdot g_4^{-x_4} \bmod p, g_3^{\beta} = g_4 \bmod p, g_3 = g^{t_3} \bmod p, g_3 = g^{t_3} \bmod p$

要隱藏此潛隱訊息於簽章裡，作法如下：

1. 計算與潛隱訊接收者 B 的 Diffie-Hellman 金鑰

   $k_{ab} = y_B^{t_1 x_1 + \alpha t_2 x_2} = y_A^{t_3 x_3 + \beta t_4 x_4} = g^{(t_1 x_1 + \alpha t_2 x_2)(t_3 x_3 + \beta t_4 x_4)} \bmod p$

2. 任選$k \in Z_q^*$並計算$r = g_1^k \cdot g_2^{m' + K_{ab}} \bmod p$

3. 計算$e = h(r \| m)$

4. 根據私鑰求得$s_1 = k + e x_1 \bmod p, s_2 = m' + K_{ab} + e x_2 \bmod p$

5. 再求得$s_1' = k + e(x_1 + \alpha x_2) \bmod p, s_2' = m' + K_{ab} \bmod p$

(e, s_1', s_2')為訊息m的簽章並且隱藏著潛隱訊息m'。

簽章驗證階段：

若符合(2.4)式，(e,s_1',s_2')則為一對訊息m之合法簽章。

$$e = h(g_1^{s_1'} \cdot g_2^{s_2'} \cdot y^e \parallel m)$$

$$\begin{aligned} h(g_1^{s_1'} \cdot g_2^{s_2'} \cdot y^e \parallel m) &= h(g_1^{k+e(x_1+\alpha x_2)} \cdot g_2^{m'+K_{ab}} \cdot g_1^{-ex_1} \cdot g_2^{-ex_2} \parallel m) \\ &= h(g_1^{k} \cdot g_1^{ex_1} \cdot g_2^{ex_2} \cdot g_2^{m'+K_{ab}} \cdot g_1^{-ex_1} \cdot g_2^{-ex_2} \parallel m) \\ &= h(g_1^{k} \cdot g_2^{m'+K_{ab}} \parallel m) = h(r \parallel m) = e \end{aligned}$$

取出潛隱訊息階段：

潛隱接收者可由簽章(e,s_1',s_2')裡的s_2'使用與簽署者之間的 Diffie-Hellman 金鑰來還原出潛隱訊息$m' = s_2' - K_{ab}$。

在這潛隱通道簽章裡，簽署者能夠隨時地決定潛隱接收者而不需要事前與他們共享金鑰，而是利用公開金鑰系統的觀念算出 Diffie-Hellman 金鑰。在我們的窄頻架構裡，不但不會遭受到因與潛隱訊息共享私鑰而遭偽冒，也不需要做小幅度的暴力攻擊法來取出潛隱訊息。

然而，從上述之簡例亦不難發現，並非任意之簽章即可用來做非對稱潛隱通道，其必需俱備某些特質；同時非對稱式潛隱通道之建構方法，亦不如想像中的容易，尤其如何證明其安全性、隱密性等更是一個很大的課題。這些在在需要時間來定義、分析與證明。由於非對稱式潛隱通道至今並未有統整的研究，本研究計劃的目的即期望以現有研究成果為基礎，提出植基於數位簽章協定下

之非對稱式潛隱通道協定，並進一步研究訂定非對稱式潛隱通道的建構法則，使後續的研究者或使用者能以此建構法則，評估、判斷某一簽章協定能否被用以建立潛隱通道，以及其可行之建構方法。同時，在非對稱式潛隱通道協定的安全分析方面，由於正規化的證明為目前密碼學研究領域中被公認較嚴謹的安全分析方法，因此本計劃將以正規化之證明模式驗證我們所提出非對稱式潛隱通道協定的安全性，同時據以確認通用建構法則的正確性，並提供未來進行非對稱式潛隱通道協定研究時安全分析之參考。

第三章、非對稱式潛隱通道之設計

3.1 架構在 Okamato 的簽章系統上的非對稱式潛隱通道

在這裡我們將先介紹 Okamoto 的數位簽章，接著再將非對稱式潛隱通道之架構在 Okamoto 的數位簽章之上。最後介紹我們所設計之架構在環簽章的非對稱式潛隱通道。

Okamoto 數位簽章

系統初始階段：

1. 選取一大質數 p 且存在另一大質數 q 符合 $q \mid p$。
2. 使用者選取二個生成子 g_1, g_2 且皆能形成大小為 q 的循環群。
3. 選取 x_1, x_2 為私鑰，相對應的公鑰為 $y = g_1^{-x_1} \cdot g_2^{-x_2} \bmod p$
4. 單向雜湊函數 h(・)

因此，簽署者的私鑰為 (x_1, x_2)，公鑰為 (y, g_1, g_2, p, q)

簽章產生階段：

令 m 為欲簽署之明文，作法如下：

1. 計算 $r = g_1^{k_1} \cdot g_2^{k_2} \bmod p$
2. 計算 $e = h(r \| m)$
3. 根據私鑰求得 $s_1 = k_1 + ex_1 \bmod p, s_2 = k_2 + ex_2 \bmod p$

(e, s_1, s_2) 為訊息 m 的簽章。

簽章驗證階段：

若符合下式，(e, s_1, s_2) 則為一對訊息 m 之合法簽章。

$$e = h(g_1^{s_1} \cdot g_2^{s_2} \cdot y^e \| m)$$

架構在 Okamato 的簽章系統上的非對稱式潛隱通道

我們的潛隱通道植基於 Okamoto 的架構，不同處在於當形成簽章 (e, s_1, s_2) 之後，簽署者再依據二生成子 g_1, g_2 之冪次方倍數差來調整簽章使之變成 (e, s_1', s_2')。各階段之作法如下：

系統初始階段：

1. 選取一大質數 p 且存在另一大質數 q 符合 $q \mid p$。

2. 單向雜湊函數 h(・)

3. 一系統生成子 g

各使用者自行作如下動作：

2. 選取 α, t_1, t_2 並形成二個大小為 q 循環群的生成子 g_1, g_2，其中

$$g_1^{\alpha} = g_2 \bmod p,$$

$$g_1 = g^{t_1} \bmod p, g_2 = g^{t_2} \bmod p$$

2. 選取 x_1, x_2 為私鑰，相對應的公鑰為 $y = g_1^{-x_1} \cdot g_2^{-x_2} \bmod p$

因此，簽署者的私鑰為$(x_1, x_2, \alpha, t_1, t_2)$，公鑰為$(y, g_1, g_2, p, q)$

簽章產生階段：

令m為欲簽署之明文，$m' \in [1, q-1]$為簽署者 A 欲傳給潛通道接收者 B 的隱訊息。令簽署者與潛隱接收者之參數分別如下：

$$t_1, t_2, \alpha, g_1, g_2, x_1, x_2, y_A = g_1^{-x_1} \cdot g_2^{-x_2} \bmod p, g_1^{\alpha} = g_2 \bmod p, g_1 = g^{t_1} \bmod p, g_2 = g^{t_2} \bmod p$$

$$t_3, t_4, \beta, g_3, g_4, x_3, x_4, y_B = g_3^{-x_3} \cdot g_4^{-x_4} \bmod p, g_3^{\beta} = g_4 \bmod p, g_3 = g^{t_3} \bmod p, g_3 = g^{t_3} \bmod p$$

要隱藏此潛隱訊息於簽章裡，作法如下：

1. 計算與潛隱訊接收者 B 的 Diffie-Hellman 金鑰

$$k_{ab} = y_B^{t_1 x_1 + \alpha t_2 x_2} = y_A^{t_3 x_3 + \beta t_4 x_4} = g^{(t_1 x_1 + \alpha t_2 x_2)(t_3 x_3 + \beta t_4 x_4)} \bmod p$$

2. 任選$k \in Z_q^*$並計算$r = g_1^k \cdot g_2^{m' + K_{ab}} \bmod p$

3. 計算$e = h(r \| m)$

4. 根據私鑰求得$s_1 = k + e x_1 \bmod p, s_2 = m' + K_{ab} + e x_2 \bmod p$

5. 再求得$s_1' = k + e(x_1 + \alpha x_2) \bmod p, s_2' = m' + K_{ab} \bmod p$

(e, s_1', s_2')為訊息m的簽章並且隱藏著潛隱訊息m'。

簽章驗證階段：

若符合驗證式，(e, s_1', s_2')則為一對訊息m之合法簽章。

$$e = h(g_1^{s_1'} \cdot g_2^{s_2'} \cdot y^e \| m)$$

$$
\begin{aligned}
h(g_1^{s_1'} \cdot g_2^{s_2'} \cdot y^e \parallel m) &= h(g_1^{k+e(x_1+\alpha x_2)} \cdot g_2^{m'+K_{ab}} \cdot g_1^{-ex_1} \cdot g_2^{-ex_2} \parallel m) \\
&= h(g_1^{k} \cdot g_1^{ex_1} \cdot g_2^{ex_2} \cdot g_2^{m'+K_{ab}} \cdot g_1^{-ex_1} \cdot g_2^{-ex_2} \parallel m) \\
&= h(g_1^{k} \cdot g_2^{m'+K_{ab}} \parallel m) = h(r \parallel m) = e
\end{aligned}
$$

取出潛隱訊息階段：

潛隱接收者可由簽章(e, s_1', s_2')裡的s_2'使用與簽署者之間的 Diffie-Hellman 金鑰來還原出潛隱訊息$m' = s_2' - K_{ab}$。

3.2 架構在環簽章的非對稱式潛隱通道

系統初始階段：

1. 取兩個大質數p和q使得$q \mid p-1$且$q \geq 2^k$，其中k是系統的安全係數。
2. 選取一個生成子g且能形成大小為q的乘法群。
3. 單向雜湊函數 h()，其輸出值屬於Z_q。
4. 對於每個環簽章的成員A_i選取其私鑰為$x_i \in Z_q$，其相對應之公鑰為$y_i = g^{x_i} \bmod p$，其中$i \in \{1,...,n\}$。而潛隱訊息接受者其私鑰為$x_R \in Z_q$，其相對應之公鑰為$y_R = g^{x_R} \bmod p$。

環簽章產生階段：

令欲簽署之明文為m，潛隱訊息為$M_{sub} \in Z_q$(注 1)，而潛隱訊息發送者為A_s，其中$s \in \{1,...,n\}$。做法如下：

1. 選取亂數 $k_i \in Z_q$ 並計算 $r_i = g^{k_i} \bmod p$ ，對於所有的 $i = \{1,...,n\}, i \neq s, sub$ 。

2. 再用仿效 ElGamal 的加密法把潛隱訊息 M_{sub} 藏在 r_{sub} 裡，所以 A_s 計算 $r_{sub} = y_R^{k_n} \cdot M_{sub} \bmod p$ ，其中 y_R 是潛隱訊息接收者的公鑰， k_n 是算出 r_n 的亂數次方。

3. 計算 $e_i = h(r_i \| m)$ ，其中 $i \neq s$ 。

4. 選取一個亂數 $k_s \in Z_q$ ，並計算 $r_s = g^{k_s} \cdot \prod_{i \neq s} y_i^{-e_i} \cdot r_{sub}^{-1} \bmod p$ 和 $e_s = h(r_s \| m)$ 。

5. 最後 A_s 再用自己的私鑰求得 $\sigma = \sum_{i \neq sub} k_i + e_s x_s \bmod q$ 。

6. $(m, r_1, ..., r_n, e_1, ..., e_n, \sigma)$ 為訊息 m 的環簽章並且隱藏著潛隱訊息 M_{sub} 。

環簽章驗證階段：

若符合 $g^{\sigma} = r_1 \cdot ... \cdot r_n \cdot y_1^{e_1} \cdot ... \cdot y_n^{e_n} \bmod p$ ，其中 $e_i = h(r_i \| m)$ ， $i = \{1,...,n\}$ ，則任何人都可以確定 $(m, r_1, ..., r_n, e_1, ..., e_n, \sigma)$ 為訊息 m 的合法環簽章。驗證的細節如下：

$$
\begin{aligned}
g^{\sigma} &= r_1 \cdot ... \cdot r_n \cdot y_1^{e_1} \cdot ... \cdot y_n^{e_n} \\
&= g^{\sum_{i \neq sub, s} k_i} \cdot r_{sub} \cdot g^{k_s} \cdot \prod_{i \neq s} y_i^{-e_i} \cdot r_{sub}^{-1} \cdot y_1^{e_1} \cdot ... \cdot y_n^{e_n} \\
&= g^{\sum_{i \neq sub} k_i} \cdot y_s^{e_s} \\
&= g^{\sum_{i \neq sub} k_i} \cdot g^{x_s e_s} \\
&= g^{\sum_{i \neq sub} k_i + x_s e_s}
\end{aligned}
$$

取出潛隱訊息階段：

當潛隱訊息接收者收到這個環簽章時，他就可以用他的私鑰 x_R 來取出潛隱

訊息 $M_{sub} = r_{sub} \cdot (r_n^{x_R})^{-1} \bmod p$，因為潛隱訊息接收者不知道潛隱訊息傳送者是誰，所以他必需對除了 r_n 之外的每個 r_i 做測試，看是否解出來的 M_{sub} 是有意義的訊息。若潛隱訊息接收者在收到這個環簽章前，就已經接到密報，知道這個環簽章中的某一個 r_i 藏有給他的潛隱訊息，那他就不用對每個做測試即可直接用他的私鑰去取出潛隱訊息。

3.3 非對稱潛隱通道之建構法則

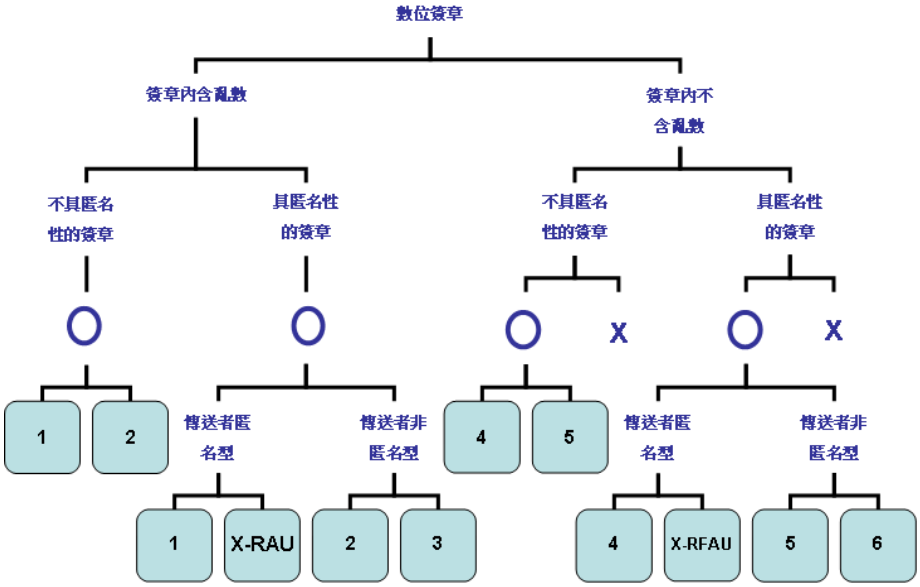
在本節中，將提出一個完整的非對稱潛隱通道之建構法則，針對不同分類的數位簽章，提出其對應的架構設計方法。此建構法則根據以下 3 點作為建構不同的非對稱潛隱通道的依據：

1．簽章值的型式：可分"簽章內含亂數/簽章內不含亂數"。簽章內含亂數意指簽署者簽署出的簽章中內含簽署者任意選取的亂數值；簽章內不含亂數意指簽章中的值都是由簽署者計算出來、而非任意選取的亂數值。

2．簽署者的可識別性：可分"不具匿名性/具匿名性"的簽章。不具匿名性的簽章意指當驗證者驗證完簽章的正確性後可以得知簽署者明確的身份；具匿名性的簽章意指當驗證者驗證完簽章的正確性後，不可得知簽署者的明確身份，如環簽章或群體簽章。

3．欲達到的功能：針對具匿名性的簽章，依傳送者想達到的功能可分"

匿名型/非匿名型”。匿名型意指潛隱接收者無法得知傳送者的真實身份；非匿名型意指潛隱接收者可得知傳送者的真實身份。



依上述的分類依據，非對稱潛隱通道系統共可分為以下六種作法(圖 3-1)：

圖 7、非對稱潛隱通道系統建構法則示意圖

圖中○表示可以建立非對稱潛隱通道系統，×則表示無法建立非對稱潛隱通道系統。在這些作法中，我們不考慮修改明文來建立非對稱潛隱通道系統，因為修改明文需使用暴力法來藏匿密文，且遇到明文無法修改的情況時便無法建立潛隱通道，故在我們所提出的建構法則中的作法皆以不改變明文的前提下進行藏匿潛隱訊息。

3.3.1 Method–1

這類型的作法使用公開金鑰加密法去藏匿潛隱訊息於簽章中屬於亂數值的部分，並視簽章系統的環境選擇適合的加密法，如 ElGamal 加密法或 ID-based 加密法。要注意的是公開金鑰加密法會產生兩個密文值，故當簽章中的個數不足時無法適用此作法(X-RAU)。

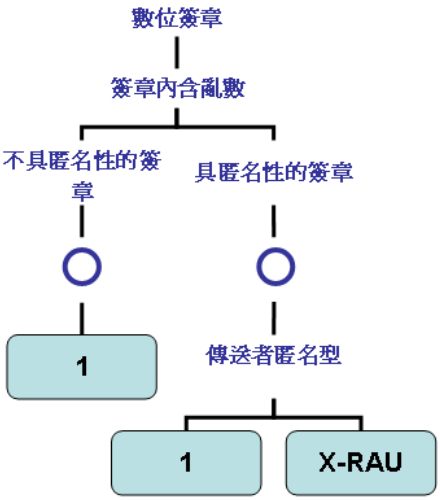


圖 8、Method-1 示意圖

我們以 M. Michels 等人[15]的簽章系統為實例說明如何建立 method-1 的非對稱潛隱通道系統：

步驟 1 環境設定：

設定系統參數 *params*：

$$params = \{p, q, g, H()\},$$

其中 p ，q 為兩個大質數且 $q \mid p-1$ ，g 為 Z_q^* 之生成子，$H : \{0,1\}^* \to Z_q$ 為雜湊

函數。

步驟 2　金鑰產生：

使用者 U_i 任意選擇兩整數 $x_i, z_i \in_R Z_q^*$ 為其私密金鑰，並以 $y_i = g^{x_i} \bmod p, u_i = g^{z_i} \bmod p$ 作為相對應的公開金鑰。使用者 U_i 的公私金鑰對即為 $(y_i, u_i), (x_i, z_i)$。令簽署者的公私金鑰對為 $(y_S, u_S), (x_S, z_S)$；而指定接收者的公私金鑰對為 $(y_R, u_R), (x_R, z_R)$。

步驟 3　簽章簽署及驗證：

輸入一訊息 M 及潛隱訊息 m_s。每位簽署者執行以下步驟去產生簽章：

choose random $: t, k \in_R Z_q^*$

$T = g^t \bmod p, r = g^k \bmod p$

$T \cdot t \cdot h(m) \cdot z = x_S \cdot r + k \cdot s + 1 \pmod q$

$\xrightarrow{T, r, s}$

$d = y_R^k m_s$

$a, b \in_R Z_p^*$

$ch = (T^{Th(m)})^a g^b \bmod p$

$\xleftarrow{ch}$

$h_1 = ch \cdot g^t \bmod p$

$h_2 = h_1^{z_S} \bmod p$

$\xrightarrow{(h_1, h_2)}$

$\xleftarrow{a, b}$

$ch \overset{?}{=} (T^{Th(m)})^a g^b \bmod p$

$\xrightarrow{d}$

$h_1 \overset{?}{=} (T^{Th(m)})^a g^{b+d}$

$h_2 \overset{?}{=} (y^r r^s g)^a u^{b+d}$

步驟 4 潛隱訊息萃取：

指定接收者以其秘密金鑰萃取潛隱訊息：$m_s = d \cdot (r)^{-x_R} \bmod q$ 。

3.3.2 Method–2

這類型的作法使用 Diffie-Hellman 金鑰配合簽章中的簽章值來藏匿潛隱訊息於簽章中屬於亂數值的部分。配合簽章中的簽章值來加密可避免相同傳送者傳送相同的潛隱訊息給相同的接收者時產生相同的簽章值，因而破壞不可分辨性。

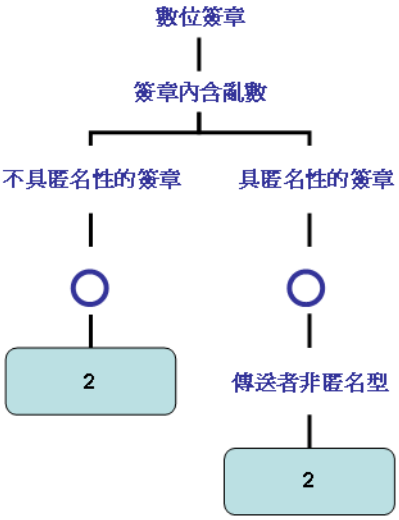


圖 9、Method-2 示意圖

我們以 J. K. Liu 等人[16]的簽章系統為實例說明如何建立 method-2 的非對稱潛隱通道系統：

步驟 1 環境設定：

設定系統參數 *params*：

$$params = \{q, g, G, H_1(), H_2()\},$$

其中 G 為 order 為一大質數 q 之循環群，g 為 G 之生成子，$H_1 : \{0,1\}^* \to Z_q$、$H_2 : \{0,1\}^* \to G$ 為雜湊函數。

步驟 2 金鑰產生：

使用者 U_i 任意選擇一整數 $x_i \in_R Z_q^*$ 為其私密金鑰，並計算 $y_i = g^{x_i} \bmod p$ 作為相對應的公開金鑰，使用者 U_i 的公私金鑰對即為 (y_i, x_i)。令環成員 U_{S_i} 的公私金鑰對為 (y_{S_i}, x_{S_i})；而指定接收者的公私金鑰對為 (y_R, x_R)。

步驟 3 簽章簽署：

令 $L = (U_{S_1}, ..., U_{S_n})$ 代表所有的環成員。真實簽署者 U_{S_π} 執行以下步驟產生簽章：

1． 計算 $h = H_2(L)$ 及 $y_0 = h^{x_{S_\pi}}$ 。

2． 選擇 $r_i \in_R Z_q, i = 1, ..., n, i \neq \pi, p$ ， $c_i \in_R Z_q, i = 1, ..., n, i \neq \pi$ 及 $k \in_R Z_q$ ，其中 $p \in \{1, ..., n\}$ 。

3． 藏匿潛隱訊息：$r_p = (H_1(y_R^{x_{S_\pi}})^{c_p} \cdot m_s) \bmod q$ 。

4． 計算 $z_i^{'} = g^{r_i} y_i^{c_i}$ ， $z_i^{''} = h^{r_i} y_0^{c_i}$ 及 $z_\pi^{'} = g^k$ ， $z_\pi^{''} = h^k$ 。

5． 計算 c_π 使得 $c_1 + ... + c_\pi ... + c_n \bmod q = H_1(L \| y_0 \| M \| z_1^{'} \| ... \| z_n^{'} \| z_1^{''} \| ... \| z_n^{''})$ 。

6． 計算 $r_\pi = k - c_\pi x_{S_\pi} \bmod q$ 。

7． 輸出簽章 $(y_0, r_1, ..., r_n, c_1, ..., c_n)$ 。

步驟 4　簽章驗證：

驗證者取得文件 M 及簽章後，進行下列步驟去驗證簽章的合法性：

$$\sum_{i=1}^{n} c_i \bmod q = H_1(L \| y_0 \| M \| g^{r_1} y_{S_1}^{c_1} \| ... \| g^{r_n} y_{S_n}^{c_n} \| h^{r_1} y_0^{c_1} \| ... \| h^{r_n} y_0^{c_n}) \text{ 。}$$

步驟 5　潛隱訊息萃取：

指定接收者以其秘密金鑰萃取潛隱訊息：$m_s = r_p \cdot H_1(y_{S_\pi}{}^{x_R})^{-c_p}$ 。

3.3.3 Method–3

這類型的作法使用公開金鑰加密法去藏匿潛隱訊息於簽章中屬於亂數值的部分，可視簽章系統的環境去選擇適合的加密法。因為我們想要使用公開金鑰加密法去達到傳送非匿名型的功能，故需消除具匿名性簽章的匿名性，使接收者萃取出潛隱訊息時可以得知傳送者的身份。

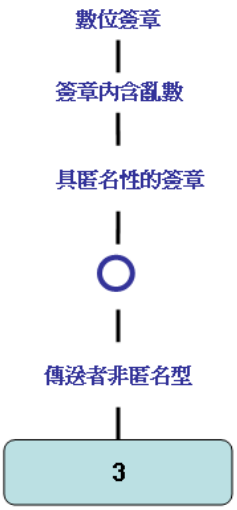


圖 10、Method-3 示意圖

我們以 J. K. Liu 等人[16]的簽章系統為實例說明如何建立 method-3 的非對稱潛隱通道系統：

步驟 1 環境設定：

此步驟與 method-2 所舉的例子相同。

步驟 2 金鑰產生：

此步驟與 method-2 所舉的例子相同。

步驟 3 簽章簽署：

令 $L = (U_{S_1},...,U_{S_n})$ 代表所有的環成員。真實簽署者 U_{S_π} 執行以下步驟產生簽章：

1． 計算 $h = H_2(L), y_0 = h^{x_{S_\pi}}$ 。

2． 選擇 $r_i \in_R Z_q, i = 1,...,n, i \neq \pi, p$ ， $c_i \in_R Z_q, i = 1,...,n, i \neq \pi$ 及 $k \in_R Z_q$ ，其中 $p \in \{1,...,n\}$ 。

3． 藏匿潛隱訊息：$r_p = H_2(y_R{}^k) \cdot m_s \bmod q$ 。

其餘步驟 4,5,6,7 與 method-2 所舉的例子相同。

步驟 4 簽章驗證：

此步驟與 method-2 所舉的例子相同。

步驟 5 潛隱訊息萃取：

指定接收者以其秘密金鑰萃取潛隱訊息：$m_s = r_p \cdot H_2(g^{r_\pi} y_{S_\pi}{}^{c_\pi})^{-x_R} \bmod q$ 。

3.3.4 Method–4

這類型的作法使用公開金鑰加密法去藏匿潛隱訊息於簽章的非亂數中，可視簽章系統的環境去選擇適合的加密法。藏匿潛隱訊息於簽章中的非亂數值後，會改變原簽章的簽署方式，故需對其它的簽章值作調整使驗證式可以通過。另外有些情況當簽章中的個數不足時無法適用此作法(X-RFAU)。

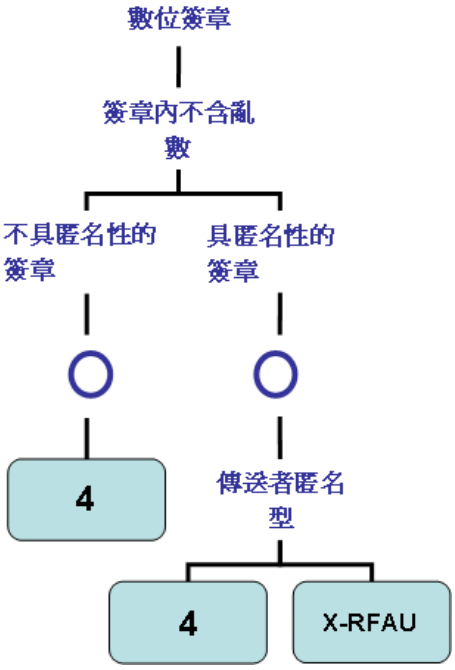


圖 11、Method-4 示意圖

Li 等人[17]在 2005 年提出了一篇架構在 Herranz 等人[8]提出的環簽章上的潛隱通道，利用環簽章的匿名特性來發展一個具有匿名性的潛隱通道。其運作流程如下：

步驟 1 環境設定：

系統選取兩個大質數 p ，q ，其中 $q \mid p-1$ ，以及生成子 g 及雜湊函數 $H:\{0,1\}^* \to Z_q$ 。假設環共有 n 個成員，每個成員 U_i 的私密金鑰為 $x_{u_i} \in_R Z_q^*$ ，公開金鑰為 $y_{u_i} = g^{x_{u_i}} \bmod p$ ，其中 $i = 1,...,n$ 。而潛隱接收者 R 的私密金鑰為 $x_r \in_R Z_q^*$ ，公開金鑰為 $y_r = g^{x_r} \bmod p$ 。

步驟 2 環簽章簽署及藏匿潛隱訊息：

欲簽署之文件為 M ，簽署者 U_s 欲傳送之潛隱訊息為 m_s ，U_s 進行以下步驟去藏匿潛隱訊息 m_s ：

1．選取一亂數值 $k_n \in_R Z_q^*$，用 ElGamal encryption 將潛隱訊息 m_s 藏於 r_1 中：

$r_1 = (y_r^{k_n} m_s^{H(y_r^{k_n})}) \bmod p$ ，並計算 $r_n = g^{k_n} \bmod p$ 。

2．選取一亂數值 $k_i \in_R Z_q^*$ ，並計算 $r_i = g^{k_i} \bmod p$ ，其中 $i = 2,...,n-1, i \neq s$ 。

3．選取一亂數值 $k_s \in_R Z_q^*$，並計算 $r_s = (g^{k_s} r_s^{-1} r_n^{-1} \prod_{i \neq s, i=1}^{n} y_{u_i}^{-H(M,r_i)}) \bmod p$。若 $r_s = 1$ 或 $r_s = r_i$, $i = 1,...,n, i \neq s$ ，則重新挑選 $k_s \in_R Z_q$ 並計算 r_s 。

4．計算 $e_i = H(r_i \| M)$ ，其中 $i = 1,...,n$ 。

5．計算 $\sigma = (k_s + \sum_{i \neq s, i=2}^{n-1} k_i + x_s e_s) \bmod q$ 。

6．輸出藏有潛隱訊息 m_s 之環簽章：$(M, r_1,...,r_n, e_1,...,e_n, \sigma)$ 。

步驟 3 環簽章驗證：

驗證者以下列步驟驗證環簽章 $(M, r_1,...,r_n, e_1,...,e_n, \sigma)$ ：

1．驗證 $e_i \stackrel{?}{=} H(r_i \| M)$ 。

2．驗證 $g^{\sigma} \stackrel{?}{=} (r_1 \cdots r_n \cdot y_1^{e_1} \cdots y_n^{e_n}) \bmod p$ 。

步驟 4　萃取潛隱訊息：

潛隱接收者 R 以其私密金鑰為 x_r 去取出潛隱訊息 m_s 如下：$m_s = (r_1 \cdot (r_n^{x_r})^{-1})^{(H(r_n^{x_r}))^{-1}} \bmod p$ 。

3.3.5 Method–5

這類型的作法使用 Diffie-Hellman 金鑰配合簽章中的簽章值為加密法藏匿潛隱訊息於簽章的非亂數中。配合簽章中的簽章值來加密可避免相同傳送者傳送相同的潛隱訊息給相同的接收者時產生相同的簽章值而破壞不可分辨性。藏匿潛隱訊息於簽章中的非亂數值後，會改變原簽章的簽署方式，故需對其它的簽章值作調整使驗證式可以通過。

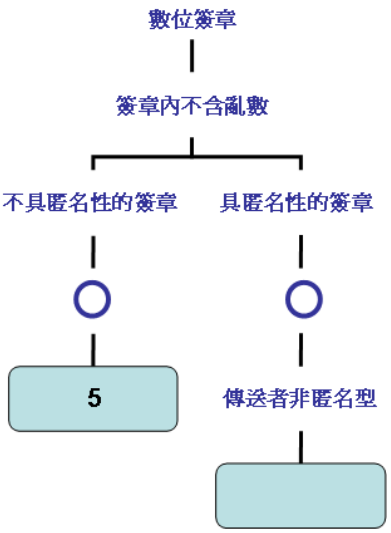


圖 12、Method-5 示意圖

我們以 C. F. Chang 等人[18]的系統做些微修改來說明如何建立 method-5 的非對稱潛隱通道系統：

步驟 1 環境設定：

設定系統參數 *params*：

$$params=\{p,q,g,H()\},$$

系統選取兩個大質數 p，q，其中 $q \mid p-1$。g 是 Z_q^* 內 order 為 q 之生成子。$H()$ 為輸出值至 Z_q^* 之雜湊函數。

步驟 2 金鑰產生：

每個使用者 U_i 選擇 $(t_{i1},t_{i2}) \in Z_q^*$，$(x_{i1},x_{i2}) \in_R Z_q^*$，並計算 $g_{i1}=g^{t_{i1}}$, $g_{i2}=g^{t_{i2}}$，$\beta_i=(t_{i2}t_{i1}^{-1}) \bmod q$ 及 $y_i=g_1^{-x_{i1}}g_2^{-x_{i2}} \bmod p$。使用者 U_i 的私密金鑰即為 $(t_{i1},t_{i2},\beta_i,x_{i1},x_{i2})$，公開金鑰為 (g_{i1},g_{i2},y_i)。令簽署者 U_π 之公私金鑰對為 $(g_{\pi 1},g_{\pi 2},y_\pi)$ 及 $(t_{\pi 1},t_{\pi 2},\beta_\pi,x_{\pi 1},x_{\pi 2})$；指定接收者 U_R 之公私金鑰對為 (g_{R1},g_{R2},y_R) 及 $(t_{R1},t_{R2},\beta_R,x_{R1},x_{R2})$。

步驟 3 簽章簽署：

簽署者 U_π 執行以下步驟產生簽章：

1．簽署者在簽署文件 M 的過程中首先計算出與潛隱接收者 R 共享的 Diffie-Hellman 金鑰: $K_{\pi R}=y_R^{\,t_{\pi 1}x_{\pi 1}+t_{\pi 2}x_{\pi 2}} \bmod q$。

2．選取任意值 $r_{\pi 1},r_{\pi 2} \in_R Z_q$，接著算出 $r=(g_{\pi 1}^{\,r_{\pi 1}}g_{\pi 2}^{\,r_{\pi 2}}) \bmod p$，$e=H(r \| M)$、$\tilde{s_1}=(r_{\pi 1}+ex_{\pi 1}) \bmod q$、$\tilde{s_2}=(r_{\pi 2}+ex_{\pi 2}) \bmod q$。

3．將欲傳送給潛隱接收者 R 的潛隱訊息 $m_s \in Z_q^*$ 藏於簽章的

$s_2 = (m_s + eK_{\pi R}) \bmod q$ ， $s_1 = \tilde{s_1} + \beta_\pi \cdot (\tilde{s_2} - s_2) \bmod q$ 中。

4．輸出簽章 $\sigma = \{e, s_1, s_2\}$ 。

步驟 4 簽章驗證：

驗證方式與 Okamato 的方式相同，驗證者以簽署者的公開金鑰 y_π 來驗證簽章 $\{e, s_1, s_2\}$ ： $H(g_{\pi 1}{}^{s_1} g_{\pi 2}{}^{s_2} y_\pi{}^{e} \bmod p \,\|\, M) \stackrel{?}{=} e$ 。

步驟 5 潛隱訊息萃取：

潛隱接收者 R 以自己的私密金鑰與簽署者的公開金鑰去求出 Diffie-Hellman 金鑰 : $K_{\pi R} = y_\pi{}^{t_{R1}x_{R1} + t_{R2}x_{R2}} \bmod q$ 。接著用 $K_{\pi R}$ 來萃取潛隱訊息： $m_s = (s_2 - K_{\pi R}) \bmod q$ 。

3.3.6 Method–6

這類型的作法使用公開金鑰加密法去藏匿潛隱訊息於簽章的非亂數中，可視簽章系統的環境去選擇適合的加密法。因為我們想要使用公開金鑰加密法去達到傳送非匿名型的功能，故需消除具匿名性簽章的匿名性，使接收者萃取出潛隱訊息時可以得知傳送者的身份。藏匿潛隱訊息於簽章中的非亂數值後，會改變原簽章的簽署方式，故需對其它的簽章值作調整使驗證式可以通過。

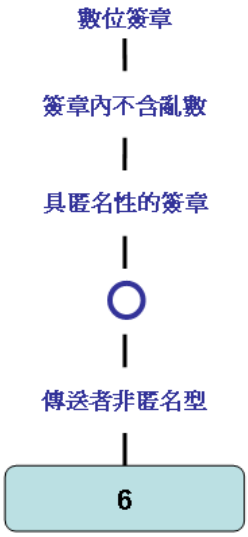


圖 13、 Method-6 示意圖

我們以 Herranz 等人[19]的簽章系統為實例說明如何建立 method-4 的非對稱潛隱通道系統：

步驟 1 環境設定：

設定系統參數 *params*：

$$params=\{p,q,g\},$$

系統選取兩個大質數 p ，q ，其中 $q \mid p-1$。g 是 Z_q^* 內 order 為 q 之生成子。

步驟 2 金鑰產生：

使用者 U_i 任意選擇一整數 $x_i \in_R Z_q^*$ 為其私密金鑰，並以 $y_i = g^{x_i} \bmod p$ 作為相對應的公開金鑰，使用者 U_i 的公私金鑰對即為 (y_i, x_i)。令環成員 U_{S_i} 的公私金鑰對為 (y_{S_i}, x_{S_i}) ，而指定接收者的公私金鑰對為 (y_R, x_R) 。

步驟 3 簽章簽署：

令 $L=(U_{S_1},...,U_{S_n})$ 代表所有的環成員。真實簽署者 U_{S_π} 執行以下步驟產生簽章：

1．選擇 $k_t,k_\pi \in_R Z_q^*$，接著藏匿潛隱訊息 m_s 如下：$r_t=(y_R{}^{k_t+k_\pi}\cdot m_s) \bmod p$。

2．接著計算 $r_{t+1}=g^{k_t} \bmod p$，其中 $t\in\{1,...,n\}\setminus\pi$。

3．選擇 $k_i \in_R Z_q^*$ 並計算 $r_i=g^{k_i} \bmod p$，其中 $i=1,...,n, i\neq\pi,t,t+1$。

4．計算 $r_\pi=((\prod_{i=1,i\neq\pi}^{n} y_{S_i}{}^{-H(M,r_i)})\cdot r_t^{-1}\cdot r_{t+1}{}^{-1}) \bmod p$ 及 $h_i=H(M,r_i)$，其中 $i=1,...,n$。

5．計算 $\sigma=(k_\pi+\sum_{i=1,i\neq\pi,t,t+1}^{n} k_i + x_{S_\pi}h_\pi) \bmod q$。

6．輸出藏有潛隱訊息 m_s 之環簽章：$(r_1,...,r_n,h_1,...,h_n,\sigma)$。

步驟 4 簽章驗證：

驗證者以下列步驟驗證環簽章 $(M,r_1,...,r_n,e_1,...,e_n,\sigma)$：

1．驗證 $e_i \stackrel{?}{=} H(r_i \| M)$。

2．驗證 $g^\sigma \stackrel{?}{=} (r_1\cdots r_n\cdot y_1{}^{h_1}\cdots y_n{}^{h_n}) \bmod p$。

步驟 5 潛隱訊息萃取：

指定接收者 R 以其私密金鑰為 x_R 去取出潛隱訊息 m_s 如下：

$m_s=r_t\cdot(r_{t+1}\cdot g^\sigma\cdot(\prod_{i=1,i\neq\pi,t,t+1}^{n} r_i^{-1})\cdot y_{S_\pi}{}^{-h_\pi})^{-x_R} (\bmod p)$。

第四章、亂數神諭 Random Oracle Model

4.1 亂數神諭簡介

安全性分析為驗證密碼系統是否達到預期安全目標最重要的評估依據。由於不嚴謹的安全性分析，往往導致無法查出密碼系統執行過程中可能的安全漏洞，甚或造成使用者難以彌補之損失。因此，如何建立足以信賴之安全分析模式，已為研究、設計密碼系統不可或缺的一環。在過去，運用密碼系統所發展出來的各種應用協定的安全性分析，大多採取「說明」與「列舉」的方式行之，亦即列舉出一些常見的攻擊法，並且一一說明這些攻擊法對這些協定是無效的。然而，真正破解的這些協定的攻擊法，往往都是這些攻擊法的變形，但是因為協定的設計沒有考慮到這些變形的攻擊，所以造成了執行上的安全漏洞。而近年來，在安全分析上，多已採用正規證明 (formal proof)的分析方法[20, 21, 22]，其中又以亂數模型(Random Oracle Model)的證明方式最為普遍。亂數模型的證明方法通常分為三個階段：

1. 模型(Model)

   在這個階段中，我們塑造一個攻擊者(Adversary)出來，並且定義出攻擊者的能力。一個攻擊者最基本的能力就是控制網路和執行協定(executing protocol)。為了提高我們協定的安全度，我們必須適當的增加攻擊者的能力，當攻擊者能力越高時，我們要證明出一個協定是安全的困難度便越高，但反過來說，若能在攻擊者能力越強的情況之下來證明一個協定是安全的，則可以保證此協定的安全度越高。

2. 定義(Definition)

   在這個階段中，我們必須把此協定所利用之基本的安全假設找出來，並且用正規的數學模型來定義這些安全假設。例如說某個協定的安全性是植基

於一個安全的加密系統,則我們就必須在此階段用正規的數學模型來定義何謂一個安全的加密系統,也就是要定出一個安全的加密系統所必須滿足的條件。如果一個協定中所利用的安全假設不只一項,則我們必須把所有用到的安全假設全部在此階段中定義出來。

3. 證明(Proof)

在此階段中,我們是利用反證法的方式來證明一個協定的安全性。舉例來說,若我們假設存在一個安全的加密系統 (這個假設的安全定義必須事先定義在第二階段),則某協定是安全的。那我們要利用的反證法便是:如果有一個攻擊者A(A的能力事先定義在第一階段)能夠破解協定P的話,則我們可以推導出將會存在一個攻擊者F可以破解一個安全的加密系統。但由於我們已假設加密系統是安全的,因此矛盾,所以攻擊者 A 並無法破解協定 P。

由於正規化的證明雖為公認較嚴謹的安全分析方法,但其分析技巧與證明細節頗為複雜,一般而言,並不容易理解與學習,所幸我們的研究團隊曾投入相當大的心力鑽研這方面的研究,且曾於 2001 年與 2002 年分別執行相關的研究計畫,因此我們已累積了很好的研究經驗與成果。根據我們的研究結果,運用「亂數模型」正規的證明非對稱潛隱通道協定是可行的,關鍵重點在如何建立基本的安全假設,並據此反證若能破解我們所提出的非對稱式潛隱通道,就必定能構建出一位攻擊者來破解原有基本的安全假設。對此關鍵重點,我們將從深入探討簽章的安全假設著手,找出可以做為基本安全假

設的特性，再依「模型」、「定義」與「證明」的敘述流程，逐步分析我們所提出非對稱式潛隱通道協定的安全性。

4.2 非對稱潛隱通道之安全性分析

要證明一個非對稱潛隱通道系統的安全性，我們依以下四節所介紹的程序去分析：

4.2.1．正規模型及系統安全性之定義。

4.2.2．選擇適合證明用的 security assumption。

4.2.3．依正規模型的流程(game)去證明。

4.2.4．分析證明流程中的 advantage。

這四個程序將在以下章節作詳細介紹。

4.2.1 正規模型及系統安全性之定義

我們以正規模型來定義非對稱潛隱通道系統的安全性定義。

正規模型：

我們以一個要破解非對稱潛隱通道系統(asymmetric subliminal channel(**ASC**))的 adversary 與一個提供環境參數的 challenger 去進行一個 game 來描述我們的正規模型。這個 game 共有五個步驟：

Setup：

輸入一個安全參數 k ，challenger 以此演算法來產生 game 所需的參數並傳送給 adversary。

Phase 1：

Adversary 可向 challenger 發出簽章的請求，challenger 會回送一個可能藏有潛隱訊息的簽章，或一個沒有藏有潛隱訊息的簽章。

Challenge：

Adversary 輸出一個明文 $\tilde{M}$ 及潛隱訊息 $\tilde{m}$ 給 challenger。challenger 根據其所選的亂數值 $c \in_R \{0,1\}$ 來決定是否將 $\tilde{m}$ 藏匿於簽章 $\tilde{\sigma}$ 中，若 $c = 0$ 則不藏匿 $\tilde{m}$，$c = 1$ 則藏匿 $\tilde{m}$ 於 $\tilde{\sigma}$ 中。最後將 $\tilde{\sigma}$ 送回給 adversary。

Phase 2：

與 Phase 1 相同。

Response：

Adversary 輸出 c' 代表對 $\tilde{\sigma}$ 是否藏有潛隱訊息的猜測值。

根據以上的 game，我們定義若存在一多項式時間的 adversary A，其贏得 game 的 advantage 為：

$Adv_{ASC,A} = \left| \Pr[c' = c] - \frac{1}{2} \right|$ 。

安全性定義：

若一個非對稱潛隱通道系統是安全的話即代表對於任何的多項式時間的 adversary，其擁有的 advantage 是可忽略的。

4.2.2 Security Assumptions

依非對稱潛隱通道系統的安全性定義中可得知欲破解我們的系統，即去判斷一個簽章是一個普通的簽章或是由非對稱潛隱通道系統產生的簽章，這是一個分辨的動作。而決定類的假設(decisional assumption)所架構的也是一種分辨性的難題。因此我們配合數位簽章系統的環境去選擇適合的 decisional assumption。而現行的 decisional assumption 大致可歸納為表 1 這四種：

表 1、decisional assumption 列表

Assumption 名稱	適用環境
Decision Diffie-Hellman (DDH) assumption	適合用於 discrete logarithm 的環境
Hash Diffie-Hellman (HDH) assumption	適合用於 discrete logarithm 並有使用 hash function 的環境
Decision Bilinear Diffie-Hellman (DBDH) assumption	適合用於 bilinear pairing 為架構的環境
Decision Hash Bilinear Diffie-Hellman (DHBDH) assumption	適合用於 bilinear pairing 為架構並有使用 hash function 的環境。

這四種 assumption 的詳細描述如下：

1． Decision Diffie-Hellman (DDH) assumption

decision Diffie-Hellman problem：

Φ : DDH parameter generator
k : a sufficiently large input
A : polynomial time adversary
$\langle q, G, g \rangle \leftarrow \Phi(k)$
$g \in G; a_1, a_2, a_3 \in Z_q^*$

$$\mathrm{Adv}(k)_{\Phi,A} = \left| \begin{matrix} \Pr[A(g, g^{a_1}, g^{a_2}, g^{a_3})] = 1 \\ -\Pr[A(g, g^{a_1}, g^{a_2}, g^{a_1 a_2})] = 1 \end{matrix} \right| \geq \varepsilon(k)$$

decision Diffie-Hellman assumption：

adversary A 的 advantage 是可以忽略的。

2． Hash Diffie-Hellman (HDH) assumption

hash decision Diffie-Hellman problem：

Φ : HDH parameter generator
k : a sufficiently large input
A : polynomial time adversary
$\langle q, G, g \rangle \leftarrow \Phi(k)$
$g \in G; a_1, a_2 \in Z_q^*, R \in_R \{0,1\}^{hLen}, H : \{0,1\}^* \rightarrow \{0,1\}^{hLen}$

$$\mathrm{Adv}(k)_{\Phi,A} = \left| \begin{matrix} \Pr[A(g, g^{a_1}, g^{a_2}, R)] = 1 \\ -\Pr[A(g, g^{a_1}, g^{a_2}, H(g^{a_1 a_2}))] = 1 \end{matrix} \right| \geq \varepsilon(k)$$

hash decision Diffie-Hellman assumption：

adversary A 的 advantage 是可以忽略的。

3． Decision Bilinear Diffie-Hellman (DBDH) assumption

decision bilinear Diffie-Hellman problem：

Φ : DBDH parameter generator
k : a sufficiently large input
A : polynomial time adversary

$$\left\langle q, G_1, G_2, P, \hat{e} \right\rangle \leftarrow \Phi(k)$$

$$P \in G_1; a_1, a_2, a_3, a_4 \in Z_q^*$$

$$\mathrm{Adv}(k)_{\Phi,A} = \left| \begin{array}{l} \Pr[(P, a_1P, a_2P, a_3P, \hat{e}(P,P)^{a_4})] = 1 \\ -\Pr[P, a_1P, a_2P, a_3P, \hat{e}(P,P)^{a_1a_2a_3}] = 1 \end{array} \right| \geq \varepsilon(k)$$

decision bilinear Diffie-Hellman assumption：

adversary A 的 advantage 是可以忽略的。

4． Decision Hash Bilinear Diffie-Hellman (DHBDH) assumption

decision hash bilinear Diffie-Hellman problem：

Φ : DHBDH parameter generator
k : a sufficiently large input
A : polynomial time adversary

$$\left\langle q, G_1, G_2, P, \hat{e} \right\rangle \leftarrow \Phi(k)$$

$$P \in G_1; a_1, a_2, a_3, a_4 \in Z_q^*, H_1 : G_2 \to Z_q^*$$

$$\mathrm{Adv}(k)_{\Phi,A} = \left| \begin{array}{l} \Pr[(P, a_1P, a_2P, a_3P, a_4)] = 1 \\ -\Pr[P, a_1P, a_2P, a_3P, H_1(\hat{e}(P,P)^{a_1a_2a_3})] = 1 \end{array} \right| \geq \varepsilon(k)$$

decision hash bilinear Diffie-Hellman assumption：

adversary A 的 advantage 是可以忽略的。

在非對稱潛隱通道系統的證明過程中，可以依據系統的環境去選擇適合的 assumption。

4.2.3 正規模型

在正規模型中有下列三個角色(如圖 14)。

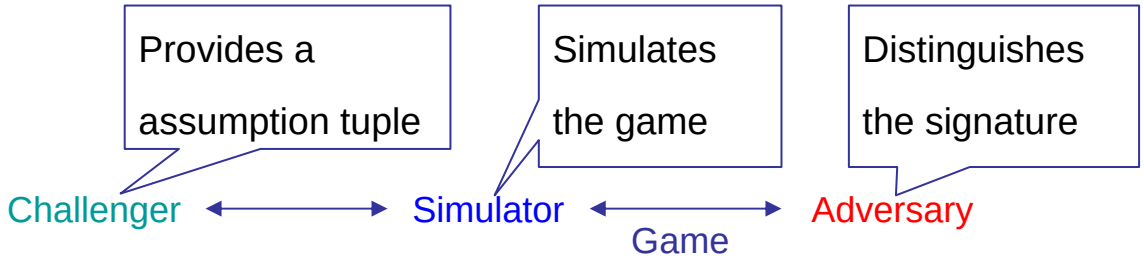


圖 14、正規模型示意圖

Challenger C：提供 assumption tuple 及所需參數。

Simulator B：模擬一個 game 並利用 adversary 去破解 problem。

Adversary A：試圖去破解非對稱潛隱通道系統。

在正規模型中，我們會假設 adversary 擁有 advantage 去破解系統。接著 challenger C 會選擇一亂數值 $c \in_R \{0,1\}$ 來決定是否給予 adversary A 一個 random tuple 或一個 assumption tuple。接著 simulator B 和 adversary A 進行遊戲。如圖 15 所示。

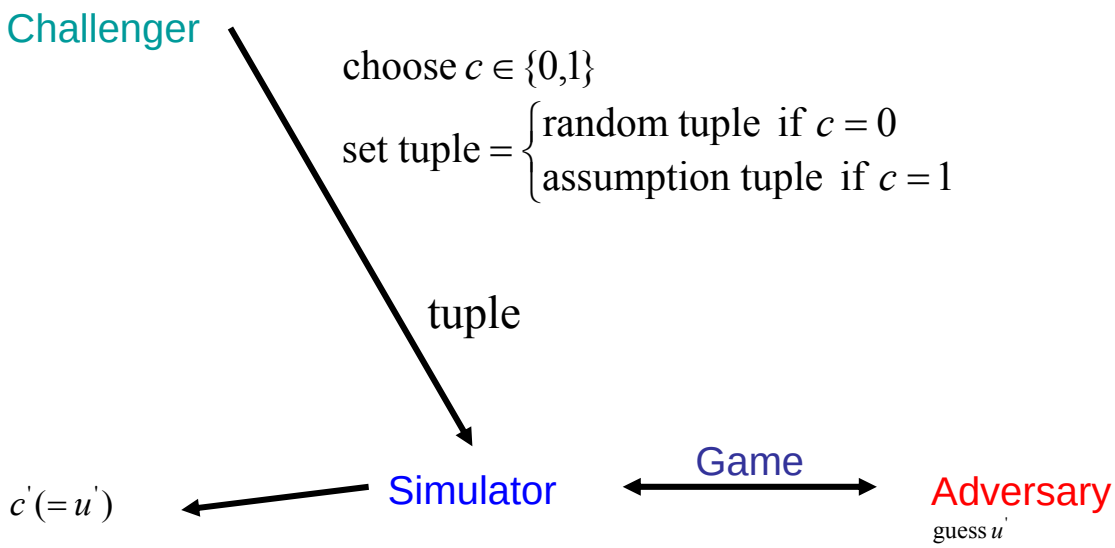


圖 15、 Challenger，simulator 與 adversary 運行示意圖

Simulator B 與 adversary A 進行的 game 如圖 16 所示，共有 5 個步驟。在 setup 步驟，simulator B 會將所需的參數傳送給 adversary A。接著在 phase 1，A 會向 B 要求簽章，B 由建構法則中選擇適合的作法配合原簽章系統的 sign algorithm 產生有可能藏有潛隱訊息的簽章並回應給 A。 在 challenge 時，adversary A 會向 simulator B 送出一個潛隱訊息及明文，simulator B 會以一個亂數值來決定是否藏匿潛隱訊息於此明文的簽章中，再將簽章回應給 adversary A。接著的 phase 2 進行與 phase 1 同樣的動作。最後的 response，adversary A 會回應一個猜測簽章是否藏有潛隱訊息的猜測值 u'，simulator B 以 u' 作為它自己的猜測值 c'。

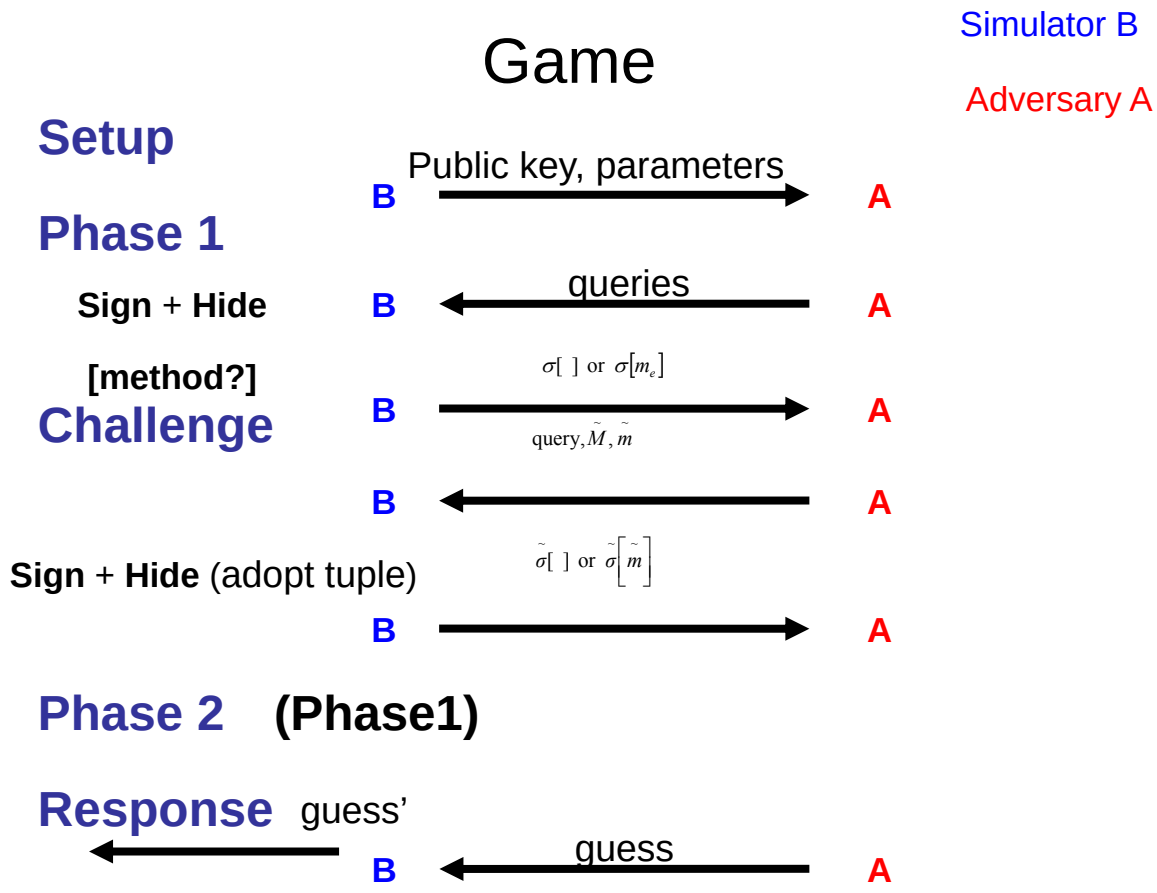


圖 16、game 示意圖

4.2.4 advantage 分析

在證明的最後步驟，我們會分析出 simulator 利用 adversary 去破解 DHBDH problem 的 advantage，其分析的來源為圖 17 所示幾個部分。

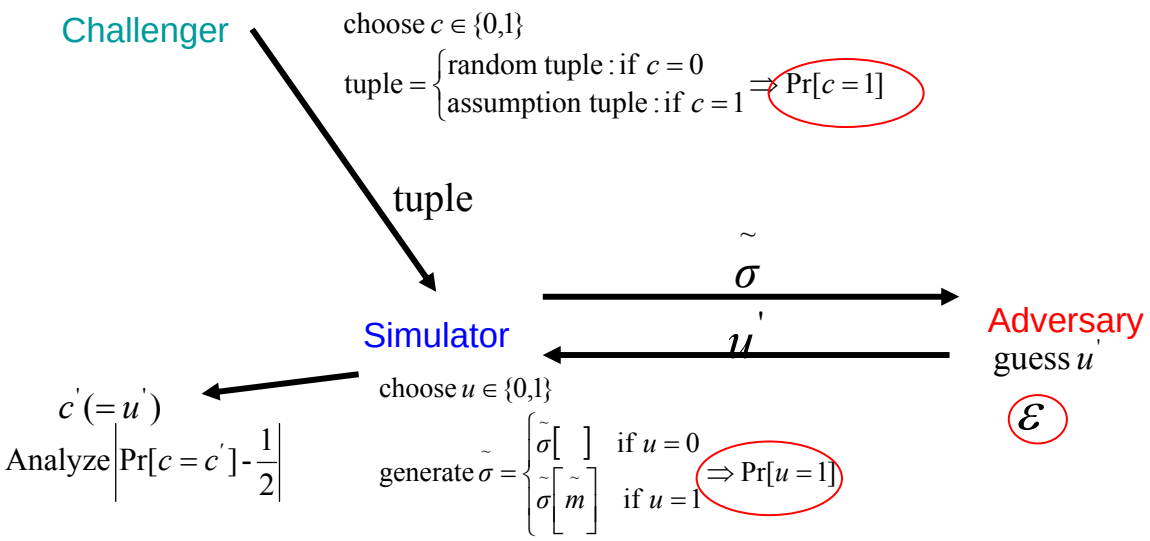


圖 17、 advantage 分析示意圖

遊戲結束後我們以下列三種可能發生的案例去分析 B 的 advantage：

Case 1.

若 $c=0$，則 challenger 給的是個隨機的 tuple，因此 A 無法獲得任何有關 μ 的資訊。因此機率 $\Pr[c'=c \mid c=0]=\frac{1}{2}$。

Case 2.

若 $c=1$ 且 $\mu=0$，則 challenger 給的是個有意義的 tuple，但 B 並無真正使用此去藏匿潛隱訊息 tuple。故 $\Pr[c'=c \mid c=1,\mu=0]\Pr[\mu=0]=\frac{1}{2}\frac{1}{2}=\frac{1}{4}$。

Case 3.

若 $c=1$ 且 $\mu=1$，則 $<P_1,P_2,P_3,P_4>$ 是個有意義的 tuple，且 B 真正使用此 tuple 去藏匿潛隱訊息。故 $\Pr[c'=c \mid c=1,\mu=1]\Pr[\mu=1]=(\frac{1}{2}+\varepsilon)\frac{1}{2}=\frac{1}{4}+\frac{\varepsilon}{2}$。

由以上三個 case 可得知 B 的 advantage 為：

$$\frac{1}{2}\Pr[c' = c \mid c = 0] + \frac{1}{2}\Pr[c' = c \mid c = 1] - \frac{1}{2}$$
$$= \frac{1}{2}\Pr[c' = c \mid c = 0] + \frac{1}{2}(\Pr[c' = c \mid c = 1, \mu = 0]\Pr[\mu = 0] + \Pr[c' = c \mid c = 1, \mu = 1]\Pr[\mu = 1]) - \frac{1}{2}$$
$$= \frac{1}{2}\frac{1}{2} + \frac{1}{2}(\frac{1}{4} + \frac{1}{4} + \frac{\varepsilon}{2}) - \frac{1}{2}$$
$$= \frac{\varepsilon}{4}$$

。

由 adversary 去破解非對稱潛隱通道系統的 advantage 及可分析機率的部分去推得 simulator 猜中 c' 的 advantage，即解決 problem 的 advantage 為 $\frac{\varepsilon}{4}$。因為 assumption 的定義得知此系統是安全的。

由證明的結果得知對於 adversary 而言，去分辨一個非對稱潛隱通道系統簽章是否藏有潛隱訊息是不可能的，因此也隱含著萃取出潛隱訊息是不可能的。此外若一個非對稱潛隱通道系統簽章無藏匿潛隱訊息，其簽章產生的流程與原始的簽章系統流程是完全一樣的，因此推得 adversary 無法判斷一個非對稱潛隱通道系統簽章是由非對稱潛隱通道系統產生或是由原始的簽章系統產生。可見非對稱潛隱通道系統擁有原始的簽章系統的安全特性。

第五章、計畫成果自評

預期完成之工作項目:

(1) 研究非對稱式潛隱通道之正規化證明分析邏輯。

(2) 利用正規模型定義非對稱式潛隱通道系統的安全性定義。

(3) 研究、綜整常用於數位簽章協定正規化證明的難題假設。

(4) 研究、分析非對稱式潛隱通道安全性之證明流程。

(5) 分析、證明第一年所設計之非對稱式潛隱通道協定是否符合期望之安全需求。並據以驗證第二年所提出非對稱式潛隱通道建構法則之正確性。

在這一年的計畫執行中，我們已經完成以下的工作：

簽署者可根據本報告提出的非對稱潛隱通道的建構法則，去判斷其使用的數位簽章是否可建立非對稱潛隱通道，並可依數位簽章的類型及欲達到的功能去決定要使用那種作法來建立非對稱潛隱通道系統。此外可根據本報告所提出的正規模型去證明非對稱潛隱通道系統的安全性。故已完成工作項目(1)、(2)、(3)。

基本上，正規證明的分析方法已廣為傳統密碼學的研究者所接受與應用，且公認為目前較為嚴謹之安全分析方式，但卻尚未被應用在非對稱式潛隱通道協定上。過去許多對稱式潛隱通道協定的安全證明都是採「說明式」的分析，而誠如先前所述，這類「說明式」的分析方法，未必周延，因此，若能提出非對稱式潛隱通道的正規證明模式，除可更嚴謹地驗證非對稱潛隱通道的安全性

外，更可謂是此類潛隱通道在安全分析上的一大進展。

因此我們提出一套利用亂數神諭(Random Oracle)之證明模組，說明攻擊者無法判斷一個非對稱潛隱通道系統簽章是由非對稱潛隱通道系統產生或是由原始的簽章系統產生，可見非對稱潛隱通道系統擁有原始的簽章系統的安全特性，且以此正規化之證明模組，證明第二年所設計非對稱潛隱通道系統的安全性，不僅可更嚴謹地驗證非對稱潛隱通道系統的安全性外，而且更可謂是此類非對稱潛隱通道系統在安全分析上的一大進展，故已完成工作項目(4)與(5)。最後，將研究成果撰寫成英文論文準備投稿，故以成果而言，我們已達成了本階段之研究目標。另外，在本計畫執行期間，我們也利用所獲得之非對稱潛隱通道相關知識結合環簽章技術，提出另一個有效率的非對稱潛隱通道系統[23]已發表於 International Journal of Computer Mathematics 期刊，此外，已將其他研究成果撰寫成三篇論文 [24-26]，準備投稿至國際期刊。

對於非對稱潛隱通道安全性分析中，如何去設計出一個通用的法則，讓證明者可以很容易地選擇適合證明的 assumption，並將之應用於證明過程中，這點是未來可以再深入研究的方向。

團隊收穫：

A. 收集許多關鍵性及代表性之相關論文。

B. 吸引有興趣的老師及學生共同參與，使得完成此目標後，大家都習得

相關知識。

C. 發揮參與人員們的團隊精神，集思廣益，找出可行之方案。

D. 學習非對稱潛隱通道的正規化安全證明模式。

E. 學習研究報告及論文之撰寫。

F. 奠定未來從事非對稱潛隱通道研究深厚之基礎。

參考文獻

[1] G. J. Simmons, “The Prisoner’s Problem And The Subliminal Channel”, Proc. CRYPTO’83, pp. 51-67, 1984.

[2] G. J. Simmons, “Subliminal Communication is Easy Using the DSA”, Eurocrypt’ 93, pp. 218-232, 1994.

[3] Bruce Schneier “Applied Cryptography”, Second Edition, 1996.

[4] D. Pointcheval, J. Stern, “Security Arguments for Digital Signatures and Blind Signatures”, Journal of Cryptology, pp. 361-396, 2000.

[5] R. Rivest, A. Shamir and L. Adleman, “A Method for Sbtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.

[6] T ElGamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, IEEE Transaction on Information Theory, Vol.IT-31, No. 4, pp. 469-472, 1985.

[7] C.P. Schnorr, “Efficient Signature Generation by Smart Cards”, Journal of Cryptology, Vol. 4, pp. 161-174, 1991.

[8] F. Zhang, B. Lee and K. Kim, “Exploring Signature Schemes with Subliminal Channel”, SCIS 2003, Itaya, Japan, Vol. 1/2, pp.245-250, Jan. 26-29, 2003.

[9] H. KUWAKADO, H. TANAKA, “New Subliminal Channel Embedded in ESIGN”,
Vol.E82-A No.10 p.2167-2171, 1999.

[10] J.K. Jan and Y.M. Tseng, “New Digital Signature with Subliminal Channel Based on the Discrete Logarithm Problem”, Proceedings of the 1999 International Workshops on Parallel Processing, pp. 198-203, 1999.

[11] L. Harn and G. Gong, “Digital Signature with a Subliminal Channel”, IEE Proc. Computer. Digit. Tech., Vol. 144, No. 6, pp. 387-389, 1997.

[12] N.Y. Lee and D.R. Lin, “Robust Digital Signature Scheme with Subliminal Channels”, IEICE Trans. Fundamentals, Vol.E86-A, No.1, pp.187-188, 2003.

[13] N. P. Smart, "An Identity Authenticated Key Agreement Based on the Weil Pairing," Electronics Letters 38 (2002), pp. 630-632.

[14] T. Okamoto, “Provably secure and practical identification schemes and correspon- ding signature schemes.” , in: Proc. CRYPTO’92, 1993, pp. 31-53.

[15] M. Michels, H. Petersen, P. Horster, *“Breaking and Repairing a Convertible Undeniable Signature Scheme“,* ACM Computer and Communications Security, pp. 148-152, 1996.

[16] J. K. Liu and D. S. Wong, *“Linkable Ring Signature: Security Models and New Schemes”,* ICCSA 2005.

[17] C. M. Li, C. C. Hung and T. Hwang, *“Multiple Subliminal Channels in the Ring Signature”*, , Master Thesis, NCKU, 2005.

[18] C. F Chang, T. Hwang and C. M. Li, *“Asymmetric Subliminal Channel Signature Scheme”*, Master Thesis, NCKU, 2004.

[19] Javier Herranz and German Saez, *“Forking Lemmas for Ring Signature Schemes”*, Progress in Cryptology - INDOCRYPT 2003: 4th International Conference on Cryptology, December 8-10, pp. 266-279, 2003.

[20] M. Bellare, P. Rogaway, “Provably secure session key distribution: The three party case”, Proc. 27th ACM Symp. on Theory of Computing (1995) 57-66.

[21] M. Bellare, P.Rogaway, “Random oracles are pratical: A paradigm for designing efficient protocols”, First ACM Conference on Computer and Communications Security (1993) 62-73.

[22] M. Bellare, D. Pointcheval, P. Rogaway, Authenticated key exchange secure against dictionary attack, Proceedings of Advances in Cryptology – EUROCRYPT 2000, LNCS 1807, Springer-Verlag (2000) 122-138.

[23] C.L. Yang, C.M. Li and Tzonelih Hwang, “Subliminal Channels in the ID-based Threshold Ring Signature”, International Journal of Computer Mathematics, Vol. 86, pp. 753-770, 2009.

[24] Chao-Lin Yang, Chuan-Ming Li and Tzonelih Hwang, “Subliminal Channels in the ID-based Threshold Ring Signature with Multiple Senders”.

[25] Tzonelih Hwang, Chao-Lin Yang and Chuan-Ming Li, “Asymmetric Subliminal Channels with Digital Signatures”.

[26] Chuan-Ming Li1, Chia-Chung Hung2 and Tzonelih Hwang2_, “Construction of Anonymous Subliminal Channels in Ring Signature Scheme”.

無衍生研發成果推廣資料

96 年度專題研究計畫研究成果彙整表

計畫主持人：黃宗立	計畫編號：96-2221-E-006-199-MY3
計畫名稱：數位簽章之非對稱式潛隱通道之研究	

成果項目			量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）
			實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比		
國內	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%		
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（本國籍）	碩士生	2	2	100%	人次	
		博士生	1	1	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
國外	論文著作	期刊論文	1	1	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%	章/本	
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力（外國籍）	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		

其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)	無

	成果項目	量化	名稱或內容性質簡述
科教處計畫加填項目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與（閱聽）人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

■達成目標

□未達成目標（請說明，以 100 字為限）

□實驗失敗

□因故實驗中斷

□其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文：■已發表 □未發表之文稿 □撰寫中 □無

專利：□已獲得 □申請中 ■無

技轉：□已技轉 □洽談中 ■無

其他：（以 100 字為限）

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）（以 500 字為限）

簽署者可根據本報告提出的非對稱潛隱通道之建構法則，判斷其使用的數位簽章是否可建立非對稱潛隱通道，並可依數位簽章的類型及欲達到的功能決定要使用那種作法建立非對稱潛隱通道系統。此外可根據本報告所提出的正規模型證明非對稱潛隱通道系統的安全性。基本上，正規證明的分析方法已被傳統密碼學的研究者所接受，且公認為目前較嚴謹之安全分析方式，但卻尚未被應用於非對稱式潛隱通道協定。過去許多對稱式潛隱通道協定的安全證明都是「說明式」的分析。因此，本報告提出非對稱式潛隱通道的正規證明模式。

本研究報告提出一套利用亂數神諭之證明模組，說明攻擊者無法判斷一個非對稱潛隱通道系統簽章是由非對稱潛隱通道系統產生或由原始的簽章系統產生，可見非對稱潛隱通道系統擁有原始的簽章系統的安全特性，且以此正規化之證明模組，證明本研究所設計非對稱潛隱通道系統的安全性，不僅可更嚴謹地驗證非對稱潛隱通道系統的安全性外，而且更是此類非對稱潛隱通道系統在安全分析上的一大進展。對於非對稱潛隱通道安全性分析，如何設計一個通用的法則，讓證明者可以容易選擇適合證明的假設，並將其應用於證明過程中，這點是未來可以再深入研究的方向。