私立東海大學資訊工程與科學系研究所

碩士論文

指導教授：林祝興 博士、周志賢 博士

(Dr. Chu-Hsing Lin, Dr. Jue-Sam Chou)

遠端使用者身份驗證方法研究

A Study on Remote User Authentication Schemes

研 究 生：薛 家 羿

(Jia-Ie Shiue)

中　華　民　國　九　十　三　年　六　月

謝　誌

二年的研究生涯很快的就過去了，依稀還記得在暑假期間前往拜訪林祝興指導教授的場景。能夠在這很順利的完成研究所的學業，並且將所研究的論文發表於知名國際會議(ICICS)，能夠跨越這一步達成研究生涯的第一個目標，首要感謝我的指導教授林祝興博士與周志賢博士所給予的指導。使我在資訊安全領域，研究學問的方法及做人處事態度上有長遠的受益。我還要感謝東海大學資訊安全研究所的學長、同學及學弟妹在專業上的互相砥勵及研究討論，使我的研究視野更加寬廣。

另外我要特別感謝我所服務學校的電算中心系統發展組全體同仁。感謝他們對我在進修研究所期間，對於所給予的勉勵、關懷及協助。特別地，我要感謝這一路走來，所有給我協助及鼓勵的人。另外感謝張真誠老師、黃胤傅老師與李維斌老師，感謝您們對學生的指導，讓學生受益良多。

最後，我願將完成碩士論文的喜悅及收獲，獻給我的賢慧的內人鳳秋和可愛的兒子少凱，一路上有你們陪伴，真得好幸福。

目錄

圖表目錄

中文摘要

近幾年來，網路上提供的各種服務正迅速地融入於我們的日常生活中，因此屬於個人祕密資訊的安全與否便成為非常重要的考量，鑑於各種安全上的威脅(例如，總會有一些非法者想要從網路環境中去竊取一些不屬於他們的祕密資訊)，發展出一個安全且有效的機制將是刻不容緩的事。因此在本論文中，我們的目的是提出利用通行碼表與智慧卡等方式做一個具有可攜性、安全性、便利性的遠端系統認證服務機制，有效解決身份驗證問題與防範可能的惡意破壞。因此將提出一系列這方面相關研究的分析及探討，並加以改進，使其理論方法和架構更符合當下網路服務的應用環境。

關鍵字: 智慧卡、通行碼表、遠端系統認證、安全性、可攜性、便利性。

ABSTRACT

In recent years, various kinds of services offered on the internet are incorporated into our daily life rapidly, so the security which belongs to personal secret information becomes very important. Due to various kinds of threats exist on the Internet, for example, there might be an illegal person who wants to steal some secret information not belonging to him from the Internet, it is the very urgent to develop a safe and effective mechanism. Thus, in this thesis, we study and analyze a series of relevant researches in this aspect. Our goal is to propose an effective method to frustrate the various attacks and other malicious damages in the login and authentication phases between an user and a remote system. Our method of a password table and a smart card which make our mechanism portable, secure and convenient. Thus, we make a much more reliable circumstance on the Internet.

Keyword: Smart Card, Password table, Remote authentication, Portable, Secure, Convenient

第一章 序論

1.1 研究背景與動機

由於網際網路蓬勃發展，所有的資訊及資源都在共通的網路上傳遞，任何人都可以很容易取得網路上傳遞之動態資訊。在這樣一個開放的網路環境中，對使用者的個人權益及隱私等造成莫大的威脅，因此如何因應網路資訊安全技術來防範偽造、竊聽、修改與重送等攻擊的安全議題就成為現實環境下刻不容緩的重點。

就目前遠端系統服務機制而言，它提供了使用者與系統雙方所需的安全性和驗證；由於它使用方法非常簡單、方便因而長久以來廣受大眾歡迎。但是安全性一直是此方法的致命傷[27]。一般而言，遠端系統認證服務機制除必須要達到上述的安全需求外，還需本著科技始終來自人性化的訴求，使其使用方法非常簡單、便利並具可攜性，因此我們利用通行碼表與智慧卡合作的方式提出一有效的方法，原因有二，其一：利用通行碼表的方式可使系統建置成本降低且在便利性方面，使用者只須記憶通行碼即可。其二，以智慧卡方式，它的優點是在硬體技術方面提供唯一性、不可複制性且使用者須有智慧卡才能進行認證服務。因此在密碼系統中無需做金鑰交換和儲存通行碼表[1, 2, 21, 25]以及無需可信賴的第三者；基於以上的優點，所以長久以來普遍地被運用於各式各樣的系統中。

基於上述，本論文先對於近年來對遠端使用者身分認證相關的研究作一完整的介紹分析後提出我們設計的基於應用通行碼表與智慧卡[25]為基礎之遠端使用者身分認證機制，並且也針對我們的方法作一個完整的分析與特性介紹。此法亦符合下列幾種基本的需求:

(1).使用者能自由的選擇所喜愛或容易記憶之通行碼。

(2).它能抵禦任何強大的攻擊行為，例如猜測、重送、系統偽造、修改等攻擊。

(3).當系統與遠端使用者間做機密資料的傳輸時,它能夠提供所需的雙向身份認證。

1.2 研究目的

自 1981 年，從有身份認證觀念開始，Lamport [7]最初提出以單向赫序函數 (One way hash function) 為基礎的方法後，從 1985 年開始，Shamir [22]提出利用 RSA[24]公開金鑰密碼系統為基礎，結合智慧卡的應用，使得遠端使用者認證系統具有多項優點，達到遠端使用者身分認證的安全需求，隨後在 1985 年 ElGamal [23]則結合上述兩種方法優點；其一為：公開金鑰密碼系統之基礎，其二為，利用單向赫序函數觀念，設計出遠端使用者服務系統認證方法。由於相關的服務系統認證文獻非常多，在此，我們僅對近幾年，以通行碼表和智慧卡為基礎之系統認證方法作簡單的介紹與分析。

1.2.1 以通行碼表為基礎的通行碼身份認證協定

在 2000 年 Peyravian 和 Zunic [3]等學者所提通行碼傳送方法很容易遭受到各種攻擊，例如猜測攻擊、系統資訊竊取和系統偽造等等。在 2002 年，Hwang 和 Yeh [4]等學者改善 Peyravian 方法的缺點。之後在 2003 年，Yang [5] 等學者發現 Hwang-Yeh 的方法也有弱點；其一為：偽造者可攔截登入請求並且利用使用者登入資訊，成功的通過系統的驗證程序，其二，偽造者可以利用字典攻擊的方法去猜測出使用者的通行碼。依據以上所提出的安全上的漏洞，Yang 等學者提出了改善的方法。可是在我們對 Yang 所提的方法做研究分析後發現，它仍然會遭受到偽造者假冒攻擊。

1.2.2 以智慧卡為基礎的通行碼身份認證協定

自 1981 年，學者 Lamport [7]提出一個遠端使用者通行碼認證方法，此法具有防範重送攻擊 (Replay Attack) 的優點，但由於系統必須儲存驗證所用的通行碼表。一旦通行碼表被暴露或非法者入侵系統，則系統安全將產生嚴重威脅。其後在 2000 年，Hwang 和 Li [8]等學者，指出 Lamport 所提方法有其通行碼表遭受到修改的風險並且和維護也需成本，因此 Hwang 提出改善的方法但也同時產生無法防範重送攻擊的弱點，在此之後有許多學者便提出利用智慧卡的方法來改善此弱點。

2000 年， Sun [1]提出植基於單向赫序函數的遠端使用者認證方法。他所提出的方法可以改善智慧卡需負擔的計算量太大的問題。最後在 2002 Chien, Jan 和 Tseng [9]及 2003 年 Wu 和 Chieu [2]等學者分別指出 Sun 所提的方法還有弱點；其一為：無法讓使用者自由的選擇所喜愛或容易記憶之通行碼，其二，此方法無法達到雙方身份驗證的安全需求，並各自提出改善方法。但經過我們對 Wu 和 Chieu [2]方法作一分析後發現它仍然有弱點；其一為：偽造者可攔截登入請求並且利用使用者登入資訊，成功的通過系統的驗證程序，其二，此方法很容易遭受到重送攻擊以及無法達成雙向身份驗證的安全性。(雙方驗證，也就是說，除了系統可以驗證使用者是否為合法註冊者外，網路使用者亦可同時驗證系統身份的合法性。)

有鑑於上述二項系統認證技術分析中我們所發現的缺點，在本論文中，將加以改良，使其安全性大大地提高。此外本研究將會對我們所提方法做安全性分析，使我們所提出的方法更趨完備。

1.3 論文架構

本論文內容共分為六章，其組織架構如下：第一章為序論、研究背景與動機、研究目的與論文架構。第二章為文獻探討，主要介紹各種基本密碼學應用理論，第三章方法回顧，主要針對相關學者所提出的通行碼認證機制的方法做探討，在第四、五章，將會提出我們的改善方法並對我們的方法做安全性的分析，最後結論在第六章。

第二章 文獻探討

在論本文中，我們將對單向赫序函數理論及 RSA 公開金鑰密碼系統基本理論作簡介，之後的章節提出各學者所研究的身份認證協定並對各協定的安全性做分析，再針對我們所提的方法做深入的分析。在本文中所描述的協定均包含三個階段：註冊階段 (Registration Phase)、登入階段 (Login Phase) 和身份認證階段(Authentication Phase)；首先定義在本文中用到的參數符號。

2.1 符號定義

遠端認證系統定義以下參數：

(1). ID_i：使用者身份識別碼。

(2). pw_i：使用者通行碼。

(3). p,q：大質數p及q滿足$q \mid p-1$，$q \geqq 2^{160}$及$p \geqq 2^{512}$。

(4). g ：在乘法群Z_n^*中有最大序(order)的整數原根 。

(5). N ： $p \cdot q$。

(6). $\phi(N)$：$(p-1)\cdot(q-1)$。

(7).e, d ：遠端認證系統的公開金鑰 e 與祕密金鑰 d, 滿足

$$e \cdot d \bmod \phi(N) = 1。$$

(8). rc ：用戶端所產生的暫時亂數。

(9). rs ：遠端認證系統所產生的暫時亂數。

(10).rs_new：遠端認證系統所新產生的暫時亂數。

(11).$h(m)$：為單向赫序函數(One-way hash function)，諸如 MD5, SHA-1，輸入任意長度 m ，其輸出長度為分別為 128-bit, 160-*bits* 的摘要訊息長度。

(12).$MAC_K(m)$：用 secret key K 對 m 求訊息驗證碼。

2.2 單向赫序函數

所謂的單向赫序函數 (One-way hash function) 是一種可以將任意長度的明文 m ，經由 h 赫序函數產生出固定長度之輸出赫序值的數學函數或演算法。在驗證性與完成性的考量下，由於公開金鑰系統先天上的限制，直接用私密金鑰對明文加密很沒效率，因此一個明文的數位簽章機制必須引入單向赫序函數。先針對明文求其赫序函數值，並對以簽署者的私密金鑰來加密當成數位簽章 (digit signature)；由此可知，數位簽章的功能與印章或親筆簽名的功能相似。換言之，在簽章過程中，簽署者必須先透過單向

赫序函數將電子文件轉換成固定長度的位元資料， 稱之為 “摘要”（Digest）， 或是 “指紋” Fingerprint 。隨後再使用密鑰簽署該摘要以產生數位簽章；同樣地，驗證者亦需先使用此單向赫序函數，將電子文件轉換成固定長度的摘要再進行驗證動作。因此單向赫序函數必要滿足以下的條件：

(1). 是一種可以將任意長度的明文輸入，壓縮成固定長度的赫序值，並且無法從其輸出赫序值輸出去推算其輸入明文。

(2). 不可逆性是此方法的最大特點，也就是說要從任一赫序值找出原文，在計算上是不可能的。

(3). 如果從兩個不同明文中找出相同赫序值，在計算上也是不可行的。

2.3 RSA 公開金鑰密碼系統

1978 年，由美國麻省理工學院的三位教授 Rives, Shamir 和 Adleman [26] 三位學者利用分解非常大整數的困難度，此種演算法是一種基於因數分解困難度為基礎的演算法。其公開金鑰為(e, N)，若能因式分解N，則此法會被破解，其專利權至 2000 年為止。目前，VISA、MasterCard 等公司所協力制定的安全電子交易標準 (Secure Electronic Transactions) 也是採用 RSA 演算法機制。

雖然，目前還沒有學者能證明破解 RSA 系統等於分解因數，但是在使

用此系統時，對於公開參數$N=(p\cdot q)$的選擇是非常重要，即是無法從N中因式分解$\phi(N)=(p-1)\cdot(q-1)$，另外在公開金鑰 e，以及私密金鑰 d，的選定也相對重要。

第三章 方法回顧

在 2000 年，Peyravian 和 Zunic [3]及 Sun [1]等學者提出了一個有效率的遠端使用者認證方法。Peyravian 和 Sun 的方法植基於單向赫序函數的安全性。而在 2002 年，Hwang [24]、Chien [9]等學者亦利用單向赫序函數的方法來改善 Sun 遠端使用者認證的弱點，之後在 2003 年，Wu 和 Chieu [2]等學者亦利用植基於 RSA 公開金鑰演算法與單向赫序函數的安全性來改善 Sun 的方法。在 2002 年 Hwang-Yeh [4]等學者的方法是利用植基於 RSA 公開金鑰演算法與單向赫序函數的方法來改善 Peyravian-Zunic [3]弱點，同時在 2003 年 Yang, Chang, Li 和 Hwang [5]等學者亦針對 Hwang-Yeh [4]的弱點來改善。在本論文中我們提出了上述學者方法的缺點，進而改進其方法的安全性。接下來，我們將分別介紹他們的方法。

3.1 以應用通行碼表密碼學技術為基礎

3.1.1 Peyravian 和 Zunic 學者所提出的方法

在這章中，將描述 Peyravian 和 Zunic [3]學者所提出的方法，首先介紹 Peyravian 在 2000 年所提出植基於保護密碼傳遞方法 (Methods for Protecting Password Transmission)。在 Peyravian 等學者所提出的方法中，系統將使用者身份識別碼 ID_i 和針對 ID_i 對應的通行碼 pw_i 做單向赫序函數後的值 (即 $h(ID_i, pw_i)$) 兩者儲存在系統資料庫中。

遠端認證系統 (Remote Authentication System 以下簡稱 RS)之設定階段完成後，其將公佈公開參數 h ；系統可依使用者 (以下簡稱 U_i) 註冊、登入及系統驗證這三個階段來描述。

【本系統三階描述】

在註冊階段時，使用者將自己的身份相關資訊與通行碼傳給遠端系統；在登入階段時，使用者傳遞公開資訊及使用者通行碼以完成系統驗證階段所需的程序。以下就各階段詳細說明：

【註冊階段】

首先，U_i 會將自己的 ID_i 對應的 pw_i 透過安全管道(secure channel)傳送到 RS。RS 在收到使用者的 ID_i 對應的 pw_i 後，系統會依下列方程式計算出 v_pw_i：

$$v\_pw_i = h(ID_i, pw_i)$$

然後，RS 會儲存 v_pw_i 在系統資料庫中。最後，系統會將公開參數 h 送回給 U_i。結束註冊階段的程序。

【登入階段】

在註冊成為合法的使用者後，當 U_i 想要進入遠端系統時，首先 U_i 輸入自己的 ID_i 及 pw_i 後，終端機會執行下列步驟：

(1). 終端機會隨機產生一個亂數 rc。

(2).透過終端機傳送登入請求訊息$m_1\left(=\left(ID_i, rc\right)\right)$至遠端系統。

當遠端系統在收到U_i的請求登入訊息m_1，則會執行下列驗證步驟：

(3).檢查ID_i的合法性。若ID_i的格式不符，系統立刻拒絕U_i的登入請求。

(4).在通過上述的驗證後系統會隨機產生一個亂數rs，之後則傳送回應訊息$m_2(=rc)$給使用者。

【系統驗證階段】

當遠端系統在收到U_i的驗證請求訊息m_2，則會執行下列驗證步驟：

(1).終端機在收到系統傳送訊息m_2後，則會產生訊息$m_3\left(=(ID_i, C_1)\right)$至遠端系統，方程式$C_1$如下所示：

$$C_1 = h(h(ID_i, pw_i), rc, rs)$$

(2).系統會將資料庫中與使用者相對應之v_pw_i值取出，之後則會利用v_pw_i來計算下列方程式：

$$C^*_1 = h(v\_pw_i, rc, rs)$$

(3).然後，檢查其C^*_1與C_1是否相等，如果相等則接受U_i的登入請求，否則，拒絕登入請求。

綜合上述系統三個階段如圖 1 所示。

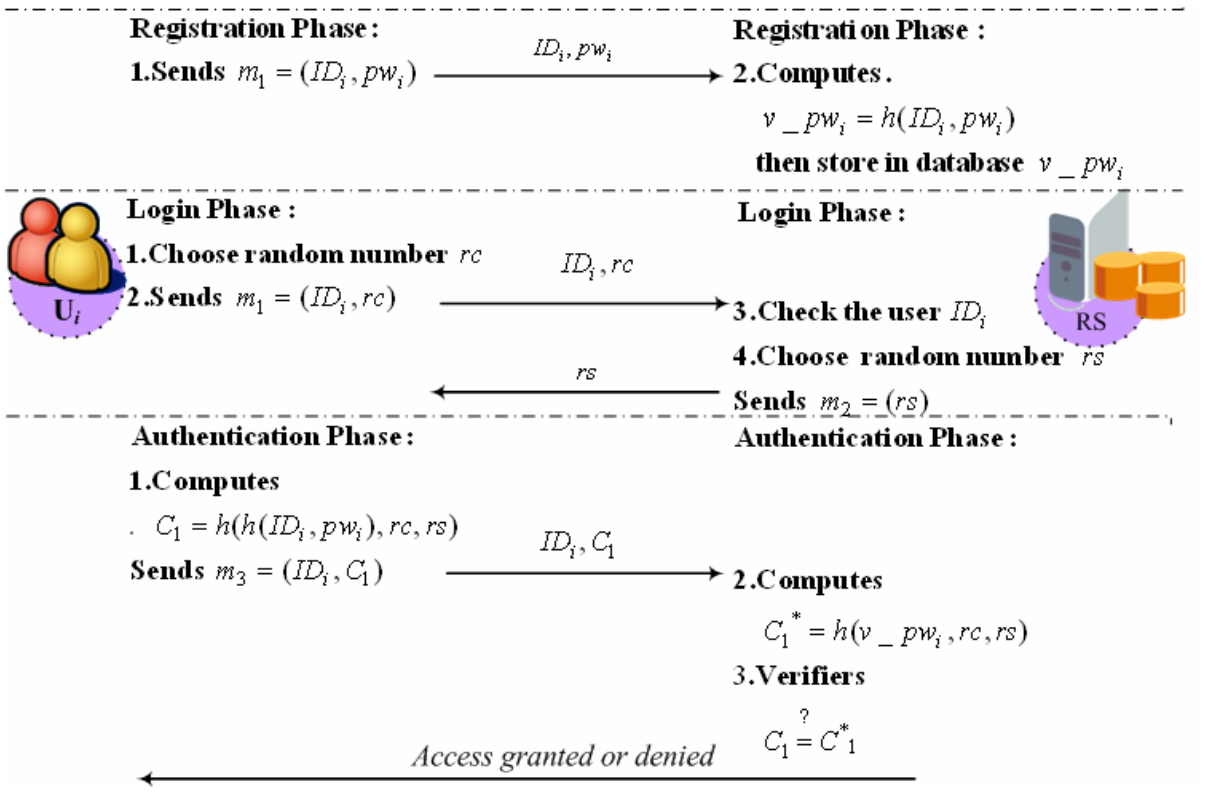

圖 1：Peyravian 和 Zunic[3]等學者的方法

【使用者改變通行碼程序】

在使用者想要交換通行碼時，使用者將自己的身份相關資訊與新的通行碼傳給遠端系統；在登入階段時，使用者傳遞公開資訊及使用者通行碼以完成系統驗證階段所需的程序。以下就各階段詳細說明：

【登入階段】

首先使用者需選擇新的通行碼，在登入階段時，傳送新的通行碼給系統完成交換通行碼程序，當U_i想要進入遠端系統時，首先U_i輸入自己的

ID_i、pw_i和new_pw_i後，終端機會執行下列步驟：

(1). 終端機會隨機產生一個亂數rc並傳送登入請求訊息$m_1\left(=\left(ID_i, rc\right)\right)$至遠端系統。

當遠端系統在收到U_i的登入請求訊息m_1，則會執行下列驗證步驟：

(2).檢查ID_i的合法性。若ID_i的格式不符，系統立刻拒絕U_i的登入請求。

(3).在通過上述的驗證後系統會隨機產生一個亂數 rs，之後則傳送回應訊息$m_2(=rc)$給使用者。

【系統驗證階段】

當遠端系統在收到U_i的驗證請求訊息m_2，則會執行下列驗證步驟：

(1). 終端機在收到系統傳送訊息m_2後，則會產生訊息$m_3\left(=(ID_i, C_1, C_2)\right)$至遠端系統，方程式$C_1, C_2$如下所示：

$$B_i = h(h(ID_i, pw_i), rc+1, rs)$$
$$C_1 = h(h(ID_i, pw_i), rc, rs)$$
$$C_2 = B_i \oplus h(ID_i, new\_pw_i)$$

(2).系統會將資料庫中與使用者相對應之v_pw_i值取出，之後則會利用v_pw_i來計算下列方程式：

$$C^*_1 = h(v\_pw_i, rc, rs)$$

(3).然後，檢查其C^*_1與C_1是否相等，如果相等則接受U_i的登入請求，否則，拒絕登入請求。然後，系統將會取出使用者新通行碼$v_pw^*_i$並且與資料庫中的通行碼v_pw_i進行交換其計算方法如下列方程式：

$$v\_pw^*_i = C_2 \oplus h(v\_pw_i, rc+1, rs)$$

綜合上述系統交換通行碼過程如圖 2 所示。

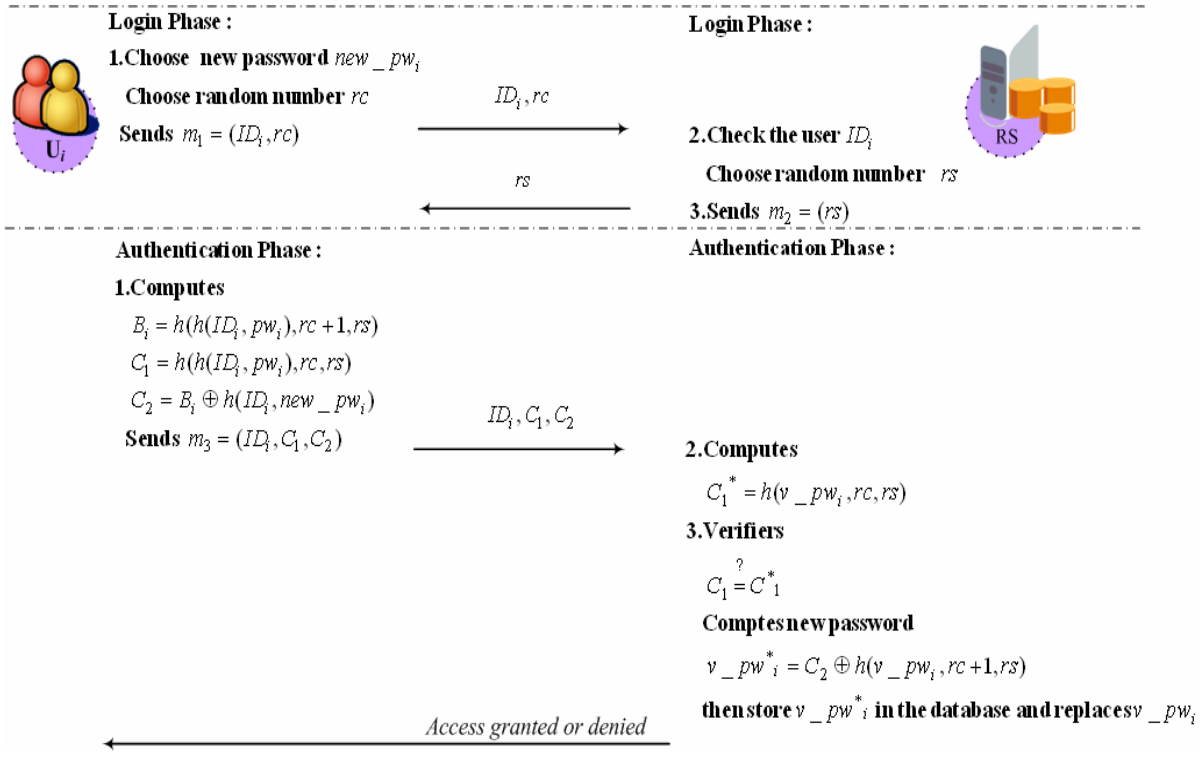

圖 2：Peyravian 和 Zunic[3]等學者的改變通行碼方法

3.1.2 Hwang 和 Yeh 等學者所提出的方法

在 2002，Hwang 和 Yeh[4]學者所提出的改善 Peyravian 和 Zunic[3]的遠端保護通行碼傳送認證系統方法 (Improvement on Peyravian-Zunic's password authentication schemes)，在 Hwang 和 Yeh 等學者所提出的方法中，系統將使用者身份識別碼 ID_i 和針對 ID_i 對應的通行碼 pw_i 做單向赫序函數後的值 (即 $h(pw_i)$) 兩者儲存在系統資料庫中。

遠端通行碼認證系統 RS 在設定階段時，系統首先會建立本身的基本參數，並將公開參數 N, e, g, h 公佈出來，而保留私密參數 $d, \phi(N)$ 之後；本系統可依使用者 U_i 註冊、登入及系統驗證這三個階段來描述。在註冊階段時，使用者將自己的身份相關資訊傳給遠端系統；在登入階段時，使用者透過傳遞公開資訊及使用者通行碼以讓系統完成驗證程序。以下就各階段詳細說明：

【註冊階段】

首先，U_i 會將自己的 ID_i 對應的 pw_i 透過安全管道(secure channel)傳送到 RS。RS 在收到使用者的 ID_i 對應的 pw_i 依下列方程式計算出 v_pw_i：

$$v\_pw_i = h(pw_i)$$

然後，RS 會儲存v_pw_i在系統資料庫中。最後，系統會將公開參數N, e, g, h送回給U_i。結束註冊階段的程序。

【登入階段】

在註冊成為合法的使用者後，當U_i想要進入遠端系統時，首先U_i輸入自己的ID_i及pw_i後，終端機會執行下列步驟：

當U_i輸入自己的ID_i及pw_i後，終端機會執行下列步驟：

(1).終端機會隨機產生一個亂數 rc。

(2).計算參數A_i的值，滿足$A_i = (rc, pw_i)^e$，透過終端機傳送登入請求訊息$m_1\left(=\left(ID_i, A_i\right)\right)$至遠端系統。

當遠端系統在收到U_i的登入請求訊息m_1，則會執行下列驗證步驟：

(3).檢查ID_i的合法性。若ID_i的格式不符，系統立刻拒絕U_i的登入請求。

(4).系統利用私密金鑰 d，解出m_1中的pw_i與rc的值，並且利用單向赫序函數h計算$v_pw_i^* = h(pw_i)$。然後取出與使用者相對應已存於系統資料庫中之參數$v_pw_i(=h(pw_i))$的值。檢查$v_pw_i^*$與v_pw_i是否相等，如果相等則接受U_i的登入請求，否則，拒絕登入請求。

(5).如果系統通過上述驗證程序，則會計算參數 B_i 的值，滿足 $B_i = rc \oplus rs$。其中遠端系統會計算當時請求登入系統時間之暫時亂數 rs；系統會傳送訊息 $m_2 \left(= (B_i, h(rs))\right)$ 至終端機。

【系統驗證階段】

當終端機在收到遠端系統訊息 m_2 後，則會執行下列驗證步驟：

(1).計算 $h(rs')$ 的值，滿足 $h(rs') = h(B_i \oplus rc)$。其中 rc 為當時終端機所請求登入系統時所產生的暫時亂數。

(2).然後驗證遠系統所傳過來的 m_2 中之 $h(rs)$ 與 $h(rs')$ 是否滿足下列方程式：

$$
\begin{aligned}
& h(rs') \\
& = h(B_i \oplus rc) \\
& = h(rc \oplus rs \oplus rc) \stackrel{?}{=} h(rs) \text{ the second half in } m_2
\end{aligned}
$$

若上述方程式等式成立，終端機則接受遠端系統的身份，否則，拒絕遠端系統之訊息。

(3).如果驗證為合法之遠端系統，終端機則會計算 $C_1 = h(rc, rs)$ 並且傳送訊息 $m_3 \left(= \left(ID_i, C_1\right)\right)$ 至遠端系統。

當遠端系統在收到 U_i 的驗證請求訊息 m_3，則會執行下列驗證步驟：

(4).計算 $C_1^* = h(rc, rs)$，驗證其 C_1^* 與 m_3 中的 C_1 是否相等，如果相等則

接受U_i的登入請求，否則，拒絕登入請求。

綜合上述系統的三個階段表示在圖 3 中。

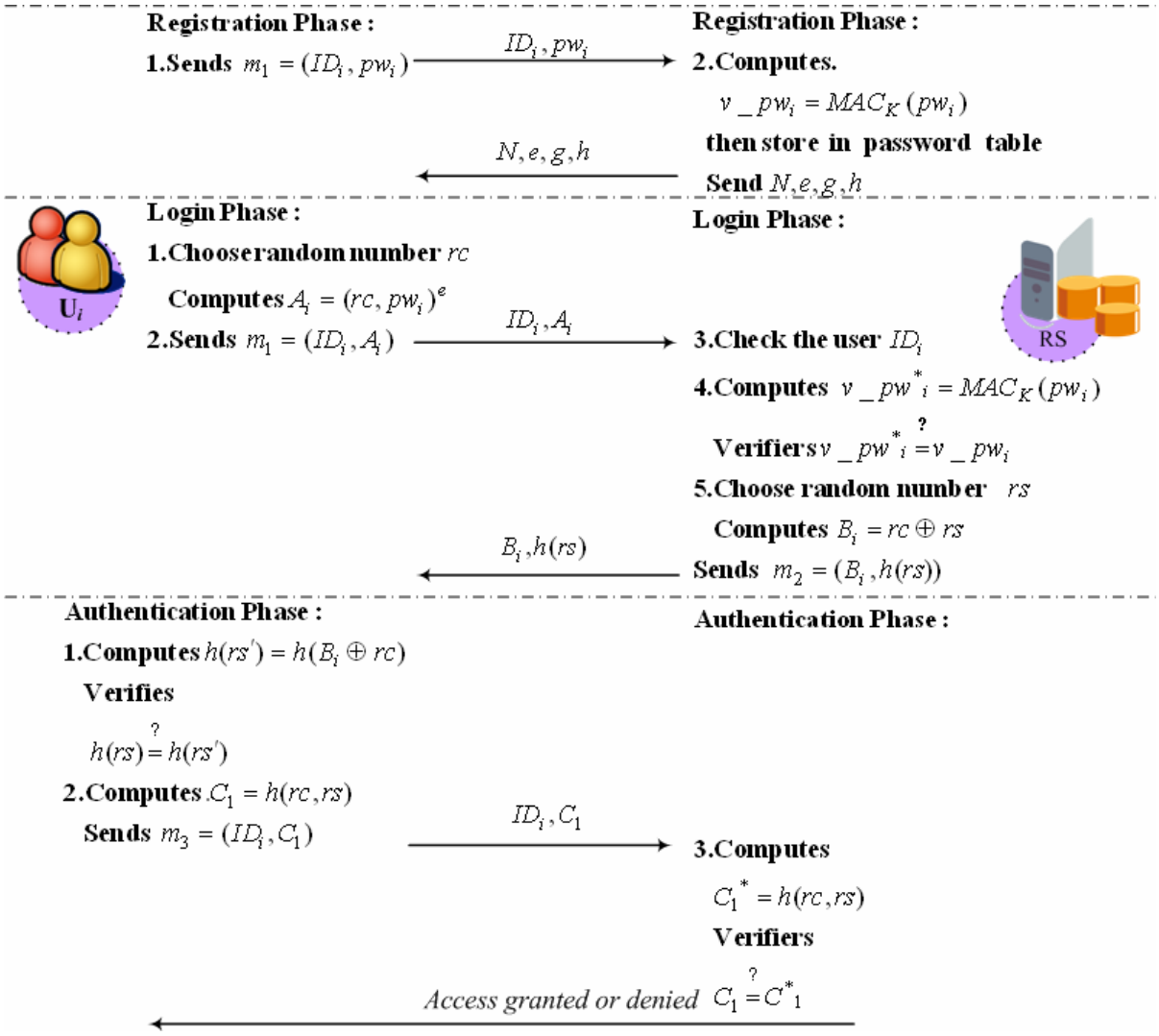

圖 3：Hwang 和 Yeh [4]等學者的方法

【使用者改變通行碼程序】

在使用者想要交換通行碼時，使用者將自己的身份相關資訊與新的通行碼傳給遠端系統；在登入階段時，使用者傳遞公開資訊及使用者通行碼

以完成系統驗證階段所需的程序。以下就各階段詳細說明：

【登入階段】

首先使用者需選擇新的通行碼，在登入階段時，傳送新的通行碼給系統完成交換通行碼程序，當U_i想要進入遠端系統時，首先U_i輸入自己的ID_i、pw_i和新通行碼new_pw_i後，終端機會執行下列步驟：

(1).終端機會傳送登入請求訊息$m_1\left(=\left(ID_i, A_i\right)\right)$至遠端系統。計算參數$A_i$的值，滿足$A_i=(rc, pw_i)^e$，其中$rc$是隨機產生一個亂數；透過終端機傳送登入請求訊息$m_1\left(=\left(ID_i, A_i\right)\right)$至遠端系統。

當遠端系統在收到U_i的登入請求訊息m_1，則會執行下列驗證步驟：

(2).檢查ID_i的合法性。若ID_i的格式不符，系統立刻拒絕U_i的登入請求。

(3).系統利用私密金鑰 d，解出m_1中的pw_i與rc 的值，並且利用單向赫序函數h 計算$v_pw_i^*=h(pw_i)$。然後取出與使用者相對應已存於系統資料庫中之參數$v_pw_i(=h(pw_i))$的值。檢查$v_pw_i^*$與v_pw_i是否相等，如果相等則接受U_i的登入請求，否則，拒絕登入請求。

(4).如果通過上述的驗證後系統會隨機產生一個亂數rs並且計算參數B_i

的值，滿足$B_i = rc \oplus rs$。其中遠端系統會計算當時請求登入系統時間之暫時亂數 rs；系統會傳送訊息$m_2\left(=(B_i, h(rs))\right)$至終端機。

【系統驗證階段】

當遠端系統在收到U_i的驗證請求訊息m_3，則會執行下列驗證步驟：

(1).計算$h(rs')$的值，滿足$h(rs') = h(B_i \oplus rc))$。其中$rc$為當時終端機所請求登入系統時所產生的暫時亂數。

(2).然後驗證遠系統所傳過來的m_2中之$h(rs)$與$h(rs')$是否滿足下列方程式：

$$h(rs')$$
$$= h(B_i \oplus rc)$$
$$= h(rc \oplus rs \oplus rc) \stackrel{?}{=} h(rs) \text{ the second half in } m_2$$

若上述方程式等式成立，終端機則接受遠端系統的身份，否則，拒絕遠端系統之訊息。

(3).如果驗證為合法之遠端系統，終端機計算C_1和C_2並且傳送訊息$m_3\left(=\left(ID_i, C_1, C_2\right)\right)$至遠端系統，方程式$C_1, C_2$如下所示：

$$C_1 = h(rc, rs)$$
$$C_2 = h(new\_pw_i) \oplus h(rc+1, rs)$$

當遠端系統在收到U_i的驗證請求訊息m_3，則會執行下列驗證步驟：

(4).計算$C_1^* = h(rc, rs)$，驗證其C_1^*與m_3中的C_1是否相等，如果相等則接受U_i的登入請求，否則，拒絕登入請求。

若上述方程式等式成立，終端機則接受遠端系統的身份，否則，拒絕遠端系統之訊息。

(5).如果驗證為合法之使用者，系統將會取出使用者新通行碼$v_pw^*_i$並且與資料庫中的通行碼v_pw_i進行交換其計算方法如下列方程式：

$$v\_pw^*_i = C_2 \oplus h(rc+1, rs)$$

綜合上述系統交換通行碼過程如圖 4 所示。

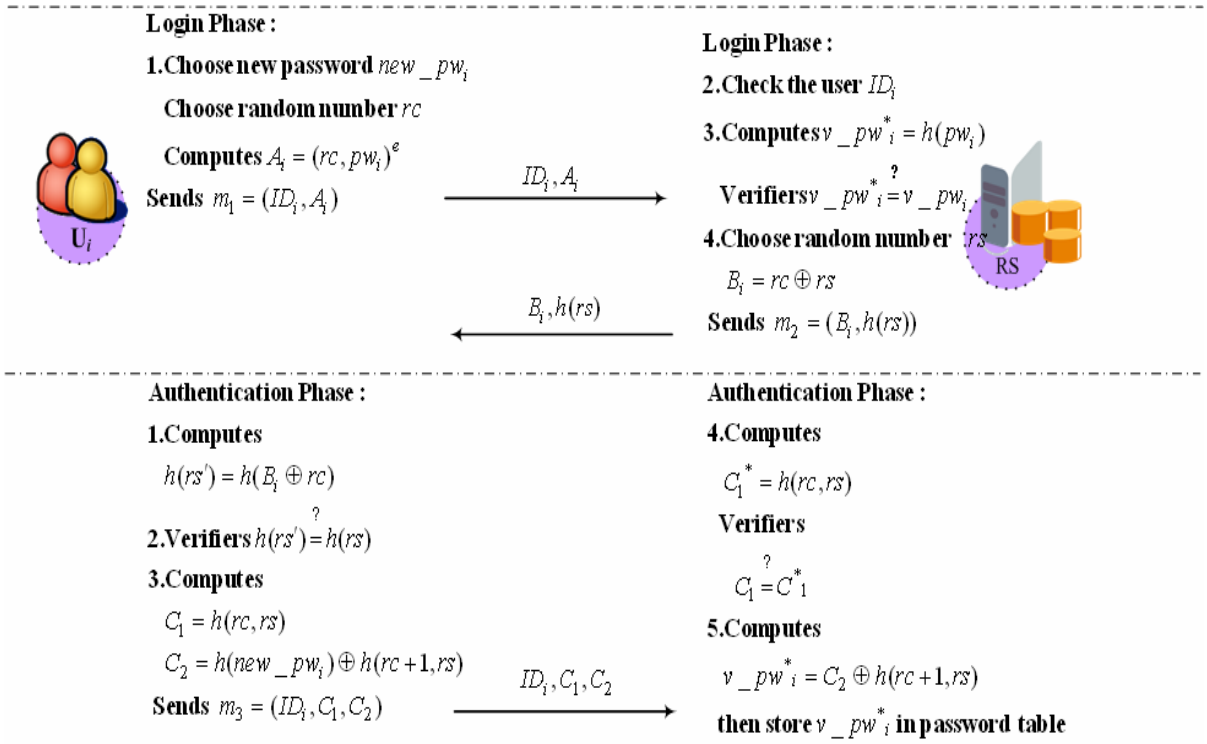

圖 4：Hwang 和 Yeh [4]等學者的改變通行碼方法

3.1.3 Yang, Chang, Li 和 Hwang 等學者所提出的方法

在 2003，Yang, Chang, Li 和 Hwang [5] 學者所提出的改善 Hwang 和 Yeh 學者的提升遠端保護通行碼傳送安全系統方法 (Security Enhancement for Protecting Password Transmission)，在 Yang 等學者所提出的方法中，系統將使用者身份識別碼 ID_i 和針對 ID_i 對應的通行碼 pw_i 做 MAC 後的值 (即 $\left(ID_i, MAC_K(pw_i)\right)$) 兩者儲存在系統資料庫中。遠端認證系統之基本參數設定完成後，其將公佈公開參數 N, e, g, h ，並保留私密參數 $K, d, \phi(N)$。

遠端認證系統 (Remote Authentication System 以下簡稱 RS) 在基本參數設定完成，並將公開參數公佈出來之後；系統可依使用者(以下簡稱 U_i) 註冊、登入及系統驗證這三個階段來描述。

【本系統三階描述】

在註冊階段時，使用者將自己的身份相關資訊與通行碼傳給遠端系統；在登入階段時，使用者傳遞公開資訊及使用者通行碼以完成系統驗證階段所需的程序。以下就各階段詳細說明：

【註冊階段】

首先，U_i 會將自己的 ID_i 對應的 pw_i 透過安全管道(secure channel)

傳送到 RS。RS 在收到使用者的ID_i對應的pw_i後，系統會利用其私密金鑰K依下列方程式計算出：

$$v\_pw_i = MAC_K(pw_i)$$

然後，RS 會儲存v_pw_i在系統資料庫中，並且保留私密金鑰K。最後，系統會將公開參數N, e, g, h送回給U_i。結束註冊階段的程序。

【登入階段】

當U_i輸入自己的ID_i及pw_i後，終端機會執行下列步驟：

(1).計算參數A_i的值，滿足$A_i = (rc, pw_i)^e$。其中rc為終端機以目前請求登入系統時間所產生的暫時亂數。

(2).透過終端機傳送登入請求訊息$m_1\left(=\left(ID_i, A_i\right)\right)$至遠端系統。

當遠端系統在收到U_i的登入請求訊息m_1，則會執行下列驗證步驟：

(3).檢查ID_i的合法性。若ID_i的格式不符，系統立刻拒絕U_i的登入請求。

(4).系統利用私密金鑰d，解出m_1中的pw_i與rc的值，並且利用私密金鑰K做為求MAC之 key, 計算$v_pw_i^* = MAC_K(pw_i)$。然後取出與使用者相對應已存於系統資料庫中之參數$v_pw_i(=MAC_K(pw_i))$的值。檢查$v_pw_i^*$與v_pw_i是否相等，如果相等則接受U_i的登入請求，否則，拒絕登入請求。

(5).如果系統通過上述驗證程序，則會計算參數 B_i 的值，滿足 $B_i = rc \oplus rs$。其中遠端系統會計算當時請求登入系統時間之暫時亂數 rs；系統會傳送訊息 $m_2 \left(= (B_i, h(rs))\right)$ 至終端機。

【系統驗證階段】

當終端機在收到遠端系統訊息 m_2 後，則會執行下列驗證步驟：

(1).計算 $h(rs')$ 的值，滿足 $h(rs') = h(B_i \oplus rc)$。其中 rc 為當時終端機所請求登入系統時所產生的暫時亂數。然後驗證遠系統所傳過來的 m_2 中之 $h(rs)$ 與 $h(rs')$ 是否滿足下列方程式：

$$
\begin{aligned}
& h(rs') \\
& = h(B_i \oplus rc) \\
& = h(rc \oplus rs \oplus rc) \stackrel{?}{=} h(rs) \text{ the second half in } m_2
\end{aligned}
$$

若上述方程式等式成立，終端機則接受遠端系統的身份，否則，拒絕遠端系統之訊息。

(2).如果驗證為合法之遠端系統，終端機則會計算 $C_1 = h(rc, rs)$ 並且傳送訊息 $m_3 \left(= \left(ID_i, C_1\right)\right)$ 至遠端系統。

當遠端系統在收到 U_i 的驗證請求訊息 m_3，則會執行下列驗證步驟：

(3).計算 $C_1^* = h(rc, rs)$，驗證其 C_1^* 與 m_3 中的 C_1 是否相等，如果相等則接受 U_i 的登入請求，否則，拒絕登入請求。

綜合上述系統的三個階段表示在圖 5 中。

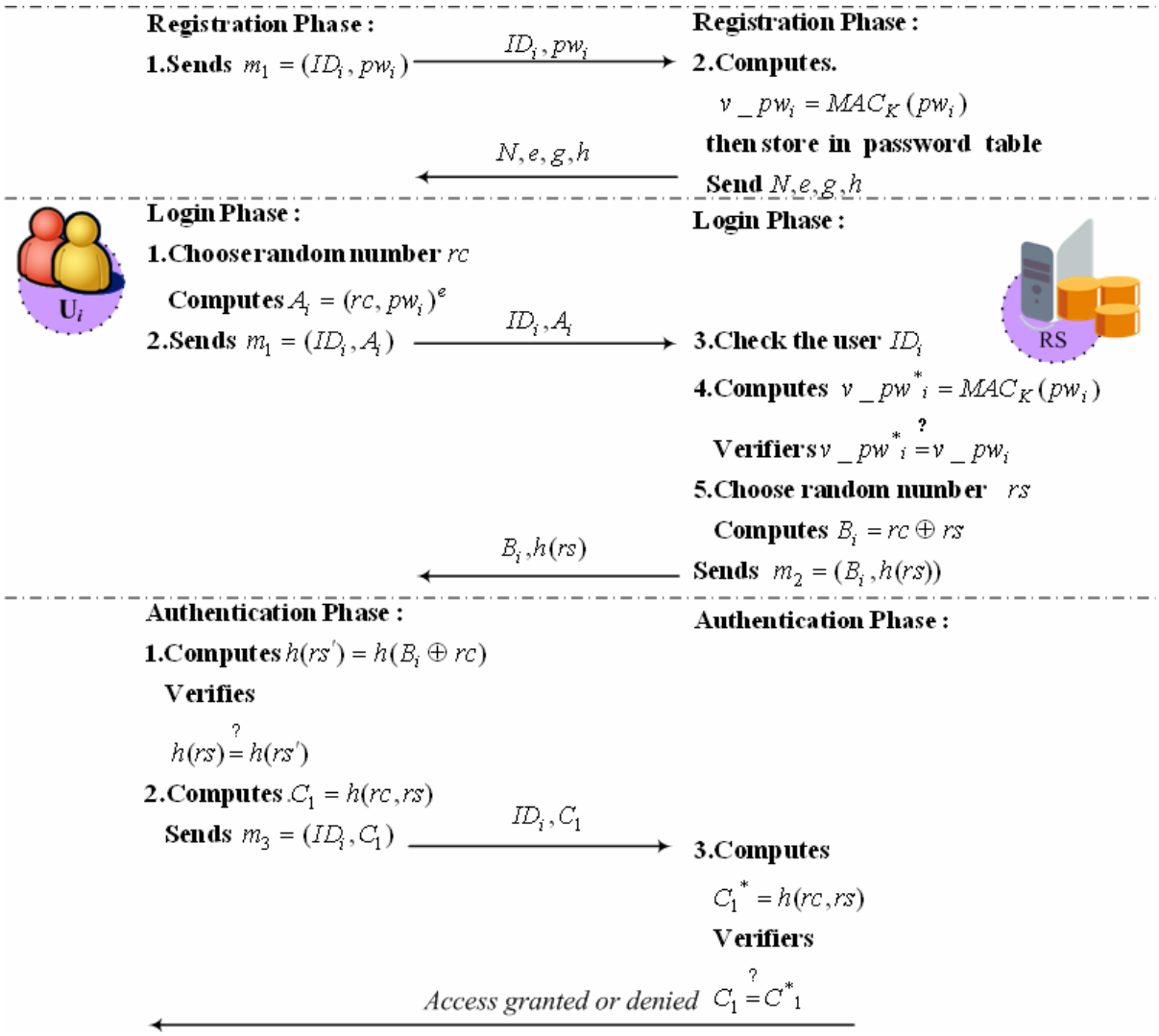

圖 5：Yang [5]等學者的方法

【使用者改變通行碼程序】

在使用者想要交換通行碼時，使用者將自己的身份相關資訊與新的通行碼傳給遠端系統；在登入階段時，使用者傳遞公開資訊及使用者通行碼以完成系統驗證階段所需的程序。以下就各階段詳細說明：

【登入階段】

首先使用者需選擇新的通行碼，在登入階段時，傳送新的通行碼給系統完成交換通行碼程序，當U_i想要進入遠端系統時，首先U_i輸入自己的ID_i、pw_i和新通行碼new_pw_i後，終端機會執行下列步驟：

(1).終端機會傳送登入請求訊息$m_1\left(=\left(ID_i, A_i\right)\right)$至遠端系統。計算參數$A_i$的值，滿足$A_i = (rc, pw_i, new_pw_i)^e$，其中$rc$是隨機產生一個亂數；透過終端機傳送登入請求訊息$m_1\left(=\left(ID_i, A_i\right)\right)$至遠端系統。

當遠端系統在收到U_i的登入請求訊息m_1，則會執行下列驗證步驟：

(2).檢查ID_i的合法性。若ID_i的格式不符，系統立刻拒絕U_i的登入請求。之後，系統利用私密金鑰d，解出m_1中的pw_i與rc的值，並且利用私密金鑰K做為求MAC之key, 計算$v_pw_i^* = MAC_K(pw_i)$。然後取出與使用者相對應已存於系統資料庫中之參數$v_pw_i(=MAC_K(pw_i))$的值。檢查$v_pw_i^*$與v_pw_i是否相等，如果相等則接受U_i的登入請求，否則，拒絕登入請求。

(3).如果系統通過上述驗證程序，則會計算參數B_i的值，滿足$B_i = rc \oplus rs$。其中遠端系統會計算當時請求登入系統時間之暫時亂數rs；系統會傳送訊息$m_2\left(=(B_i, h(rs))\right)$至終端機。

【系統驗證階段】

當終端機在收到遠端系統訊息m_2後，則會執行下列驗證步驟：

(1).計算$h(rs')$的值，滿足$h(rs') = h(B_i \oplus rc)$。其中$rc$為當時終端機所請求登入系統時所產生的暫時亂數。

(2).然後驗證遠系統所傳過來的m_2中之$h(rs)$與$h(rs')$是否滿足下列方程式：

$$h(rs')$$
$$= h(B_i \oplus rc)$$
$$= h(rc \oplus rs \oplus rc) \stackrel{?}{=} h(rs) \text{ the second half in } m_2$$

若上述方程式等式成立，終端機則接受遠端系統的身份，否則，拒絕遠端系統之訊息。

(3).如果驗證為合法之遠端系統，終端機則會計算$C_1 = h(rc, rs)$並且傳送訊息$m_3\left(=\left(ID_i, C_1\right)\right)$至遠端系統。

當遠端系統在收到U_i的驗證請求訊息m_3，則會執行下列驗證步驟：

(4).計算$C_1^* = h(rc, rs)$，驗證其C_1^*與m_3中的C_1是否相等，如果相等則接受U_i的登入請求，否則，拒絕登入請求。若上述方程式等式成立，終端機則接受遠端系統的身份，否則，拒絕遠端系統之訊息。

(5).如果驗證為合法之使用者，系統將會取出使用者新通行碼$v_pw^*_i$並且與資料庫中的通行碼v_pw_i進行交換其計算方法如下列方程式：

$$v\_pw^*_i = MAC_K(new\_pw_i)$$

綜合上述系統改變通行碼過程如圖 6 所示。

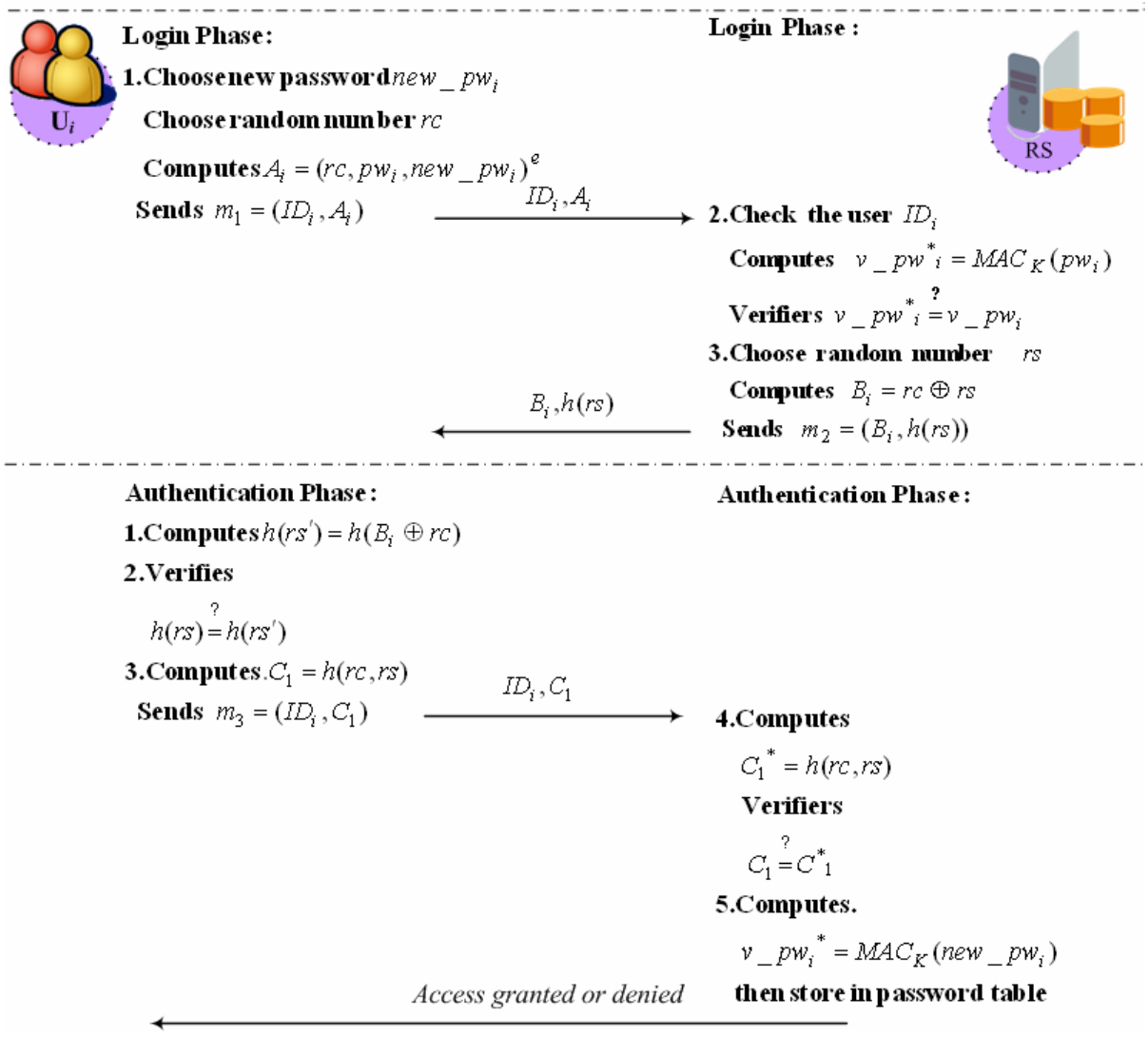

圖 6：Yang [5]等學者改變通行碼的方法

3.2 以應用智慧卡密碼學技術為基礎

3.2.1 Sun 學者所提出的方法

在這章中，將描述 Sun [1] 學者所提出的方法，首先介紹 Sun [1] 在 2000 年所提出植基於智慧卡的高效能遠端使用者認證系統 (An efficient remote use authentication scheme using smart card)。遠端認證系統之基本參數設定完成後，其將公佈公開參數 h ，並保留私密參數 x 。

遠端認證系統 (Remote Authentication System 以下簡稱 RS) 在基本參數設定完成，並將公開參數公佈出來之後；系統可依使用者(以下簡稱 U_i) 註冊、登入及系統驗證這三個階段來描述。

【本系統三階描述】

在註冊階段時，使用者將自己的身份相關資訊與通行碼傳給遠端系統；在登入階段時，使用者傳遞公開資訊及使用者通行碼以完成系統驗證階段所需的程序。以下就各階段詳細說明：

【註冊階段】

首先，U_i 會將自己的 ID_i 傳送到 RS。RS 在收到使用者的 ID_i 後，系統會利用其私密金鑰 x 依下列方程式計算出：

$$pw_i = h(ID_i, x)$$

然後 RS 會核發給使用者一張智慧卡，智慧卡儲存 pw_i 以及公開的 h 參數儲存在智慧卡的記憶體中。最後，系統會將智慧卡送回給 U_i。結束註冊階段的程序。

【登入階段】

當 U_i 將智慧卡插入終端機，並輸入自己的 ID_i 及 pw_i 後，智慧卡會執行下列步驟：

(1).計算參數 C_1 的值，滿足 $C_1 = h(pw_i \oplus T)$。其中 T 為目前請求登入系統的時間戳記。

(2).透過終端機傳送含有參數 (ID_i, C_1, T) 的登入請求訊息 m_1 至遠端系統。

【系統驗證階段】

當遠端系統在時間戳記 T' 時收到 U_i 的登入請求訊息 m_1，則會執行下列驗證步驟：

(1).檢查 ID_i 的合法性。若 ID_i 的格式不符，系統立刻拒絕 U_i 的登入請求。

(2).檢查時間戳記 T' 及 T 的差距是否在一個合理的時間延遲範圍內，亦即若 $T' - T \geq \Delta T$ (ΔT 為系統所設定的合理時間延遲參數)，則系統將拒絕 U_i 的登入請求。

(3).計算 pw^*_i 的值，滿足 $pw^*_i = h(ID_i, x)$。然後利用 pw^*_i 來計算 C^*_1 的值，使滿足 $C^*_1 = h(pw^*_i \oplus T)$。最後檢查 C^*_1 與 C_1 是否相等，如果相等則接受 U_i 的登入請求，否則，拒絕登入請求。

綜合上述系統三個階段如圖 7 所示。

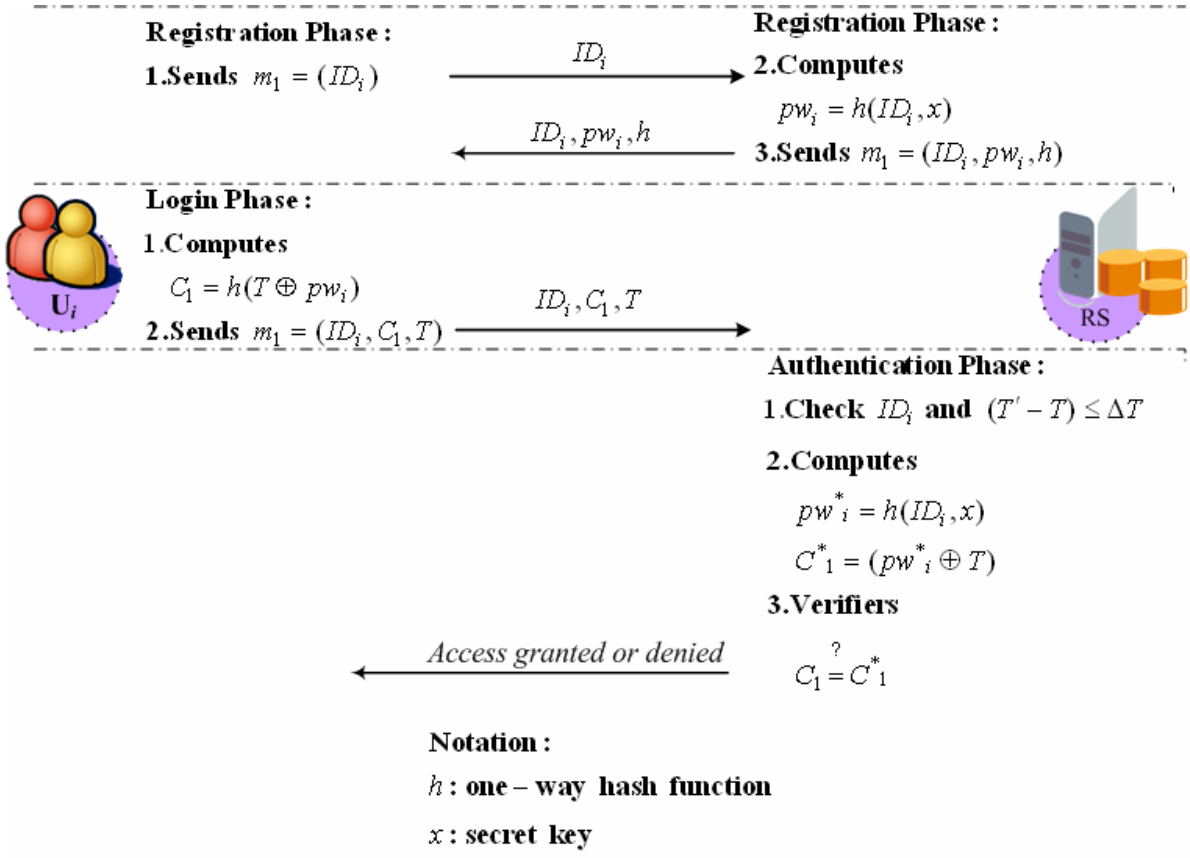

圖 7：Sun [1]等學者的方法

3.2.2 Wu 和 Chieu 等學者所提出的方法

首先我們先介紹 Wu 和 Chieu [2] 學者在 2003 所提出人性化智慧卡遠端認證系統 (A user friendly remote authentication scheme with smart cards) ，其架構詳細說明如下。

遠端通行碼認證系統 RS 在設定階段時，系統首先會建立本身的基本參數，並將公開參數 p, g, h 公佈出來，而保留私密參數 x 之後；系統可依使用者(以下簡稱U_i)註冊、登入及系統驗證這三個階段來描述。

【本系統三階描述】

在註冊階段時，使用者將自己的身份相關資訊與通行碼傳給遠端系統；在登入階段時，使用者傳遞公開資訊及使用者通行碼以完成系統驗證階段所需的程序。以下就各階段詳細說明：

【註冊階段】

當U_i將自己的ID_i與相對應的通行碼pw_i透過一個安全的通道傳送到 RS。在收到使用者的ID_i後，系統會利用下列方程式計算出對應的A_i, B_i：

$$A_i = h(ID_i \oplus x)$$
$$B_i = g^{A_i \cdot h(pw_i)}$$

然後，RS 會核發給使用者一張智慧卡，智慧卡中所預先儲存的參數 $(ID_i, A_i, B_i, p, g, h)$。最後，結束註冊階段的程序。

【登入階段】

當 U_i 將智慧卡插入終端機，並輸入自己的 ID_i 及 pw_i 後，智慧卡會執行下列步驟：

(1).計算參數 B^*_i 的值，滿足 $B^*_i = g^{A_i \cdot h(pw_i)}$。並且計算參數 C_1 的值，滿足 $C_1 = (B^*_i \oplus T)$。其中 T 為目前請求登入系統的時間。

(2).透過終端機傳送 $\left(ID_i, C_1, B^*_i, T\right)$ 的登入請求訊息 m_1 至遠端系統。

【系統驗證階段】

當遠端系統在時間戳記 T' 時收到 U_i 的登入請求訊息 m_1，則會執行下列驗證步驟：

(1).檢查 ID_i 的合法性。若 ID_i 的格式不符，系統立刻拒絕 U_i 的登入請求。然後，檢查時間戳記 T' 及 T 的差距是否在一個合理的時間延遲範圍內，亦即若 $T' - T \geq \Delta T$ (ΔT 為系統所設定的合理時間延遲參數)，則系統將拒絕 U_i 的登入請求。

(2).計算 C^*_1 的值，滿足 $C^*_1 = (B^*_i \oplus T)$。最後檢查 C^*_1 與 C_1 是否相等，則接受 U_i 的登入請求，否則，拒絕登入請求。

綜合上述系統三個階段如圖 8 所示。

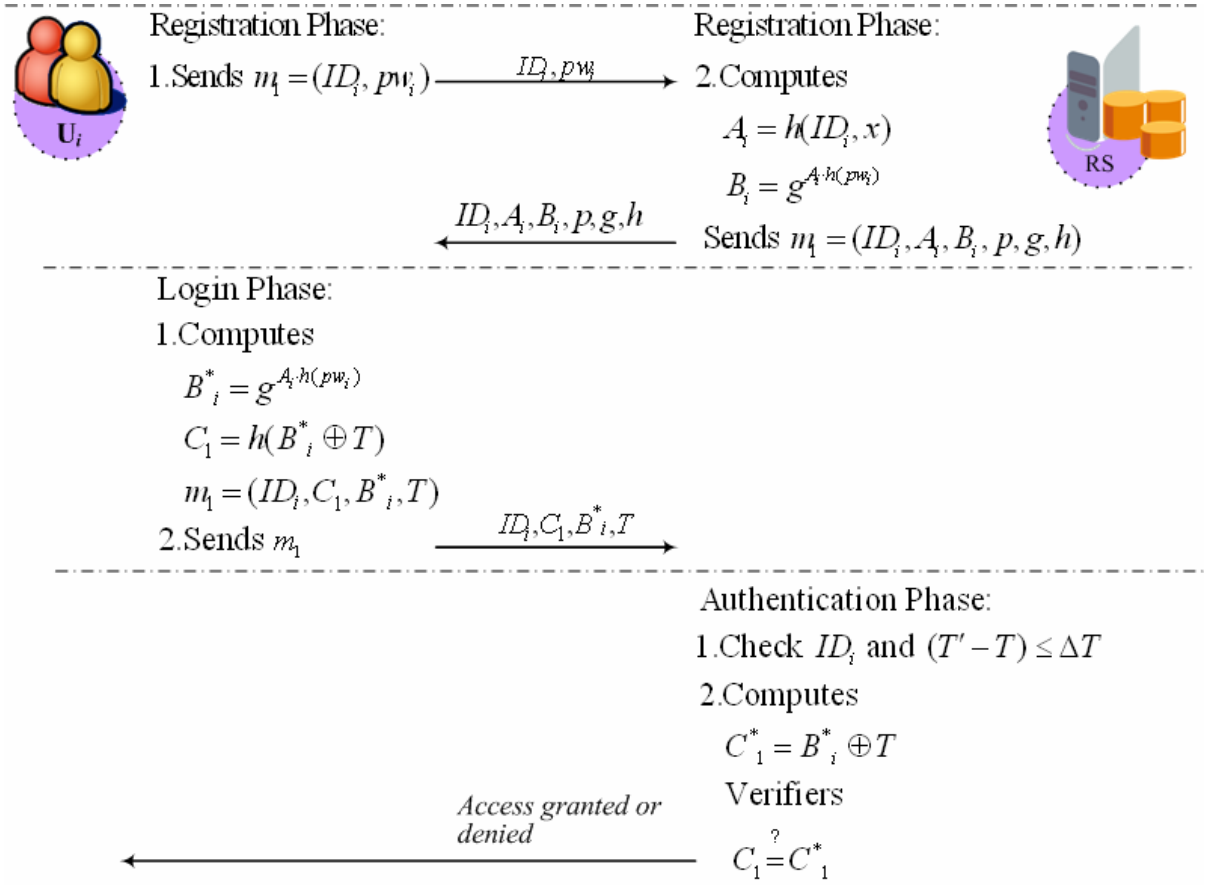

圖 8：Wu 和Chieu[2] 等學者方法

【使用者改變通行碼程序】

在這裡，我們將會討論改變通行碼認證的協定，在這裡也有如上所定義之系統參數。首先，U_i 會將智慧卡插入終端機，並輸入自己的 ID_i、pw_i 和使用者自行所選擇的新通行碼 new_pw_i，之後終端機會從儲存在智慧卡記憶體中 B^*_i 的值以 B'_i 替代，執行下列步驟：

(1).計算參數 B'_i 的值，滿足 $B'_i = g^{A_i \cdot h(new\_pw_i)}$ 。

在完成上述改變通行碼交換程序之後使用者就可以新通行碼去登入系統。

第四章 現有方法安全性分析

4.1 以通行碼表為設計基礎的安全性分析

4.1.1 Yang 等學者所提之方法的弱點

在 2003 年 Yang 等學者所提出的改善方法中，我們發現仍然有些弱點。因為根據 2003 年 Ku [6]等學者所提出的重送攻擊方法，我們可以有效的攻擊 Yang 所提出的方法。以下我們展示一個有效的攻擊如下圖 9 所示：

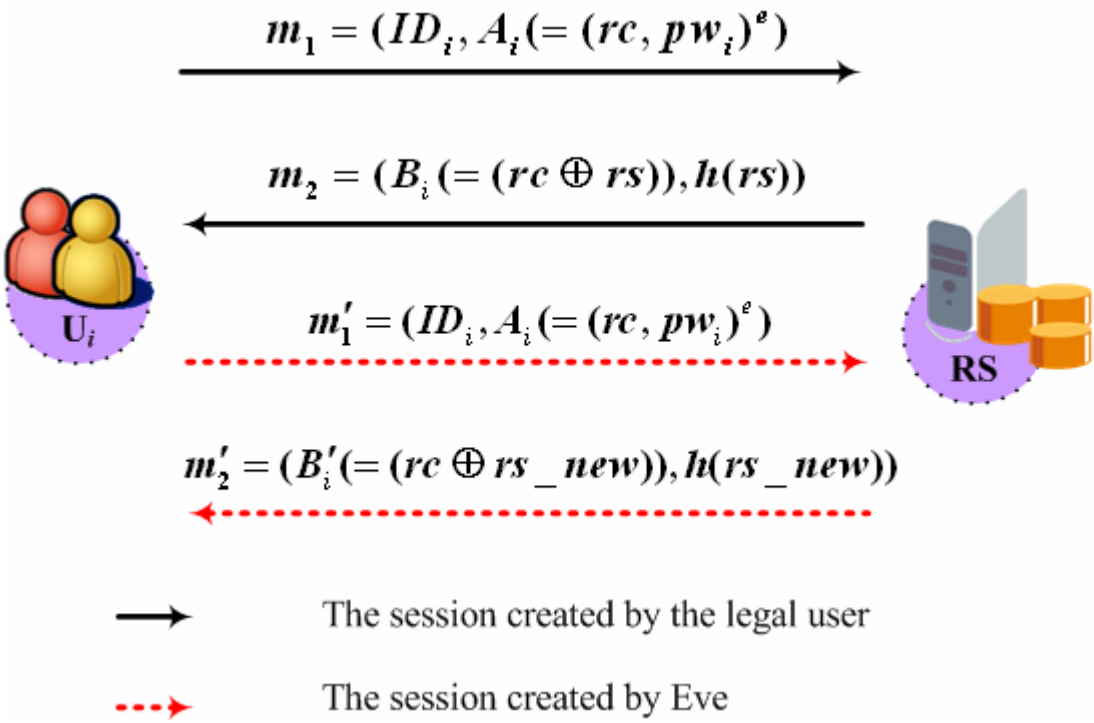

圖 9：Yang 等學者方法的弱點

使用者於第 n 次身份認證過程中，攻擊者竊聽並記錄使用者與遠端系統之間傳遞的資料：$m_1\left(=\left(ID_i,(A_i=(rc,pw_i)^e)\right)\right)$ 與

$m_2\left(=\left((B_i = rc \oplus rs), h(rs)\right)\right)$。攻擊者可將攔截取得之訊息$m_1$做重送攻擊 (以$m_1'$表示) 傳送至遠端系統

$$m_1'\left(=\left(ID_i, (A_i = (rc, pw_i)^e)\right)\right)$$

並利用先前所記錄的$m_2\left(=\left((B_i = rc \oplus rs), h(rs)\right)\right)$對$rc$進行破解，因為攻擊者會驗證由 RS 所送過來的訊息m_2中之$h(rs)$與自己所猜算的$h(rs')$是否相等，若相等則攻擊者知$rc'(=rc)$。其破解動作如下：

Step1. Guesses a random number rc'
Step2. Computes $rs' = B_i \oplus rc'$
Step3. Computes $X = h(rs')$
Step4. Checks to see whether $X = h(rs)$,
if the equation holds, then $rc' = rc$,
where $h(rs)$is the second half in message m_2.

由於攻擊者可以在離線的情況下,輕易的進行驗證所獲破解資料之正確性，故當攻擊者猜得正確之$rc'(=rc)$值時，攻擊者可成功地偽裝成合法的使用者通過身份認證，而以假冒身份登入遠端系統。以下分別就攻擊者如何成功地登入系統與成功地通過遠端系統驗證二階段做說明：

【登入階段】

攻擊者將先前攔截到的訊息m_1 (由U_i傳到 RS) 與 m_2 (由 RS 傳到U_i)，做 replay attack，透過終端機做m_1的重送攻擊，傳送訊息m_1' (以m_1'表示重送的m_1)至遠端系統。

當遠端系統在收到攻擊者的登入請求訊息m_1'，則會執行下列初步驗證：

(1).檢查ID_i的合法性。若ID_i的格式不符，系統立刻拒絕攻擊者的登入請求。否則系統視攻擊者為合法使用者。

(2).一旦系統讓攻擊者成功通過驗證程序，則系統將會計算參數B_i'的值，滿足$B_i' = rc \oplus rs_new$。其中rs_new為遠端系統依目前系統時間(即收到 Eve 所傳m_1'後的系統時間) 所產生新的暫時亂數。

(3).系統傳送訊息$m_2'\left(=(B_i', h(rs_new))\right)$至攻擊者的終端機。

【系統驗證階段】

當攻擊者在收到遠端系統訊息m_2'，則會執行下列步驟：

(1).攻擊者會計算$C_1' = h(rc', rs_new)$(攻擊者在離線下可以成功地破解$rc'(=rc)$，故亦可成功地自m_2'中的B_i'取出rs_new)並且傳送訊息$m'_3\left(=(ID_i, C_1')\right)$至遠端系統。

當遠端系統在收到攻擊者的驗證請求訊息m'_3，則會執行下列驗證步驟：

(2).計算$C_1^* = h(rc, rs_new)$，驗證其C_1^*是否與m'_3中的C_1'相等，如果相等則接受攻擊者的登入請求，否則，拒絕登入請求。

4.2 以智慧卡為設計基礎的安全性分析

4.2.1 Wu 和 Chieu 等學者所提之方法的弱點

在 2003 年 Wu 和 Chieu [2]等學者所提出的改善方法中，我們發現仍然有些弱點。根據我們所提出的重送攻擊方法，我們可以有效的攻擊 Wu 所提出的方法。以下我們展示一個有效的攻擊如下圖 10 所示：

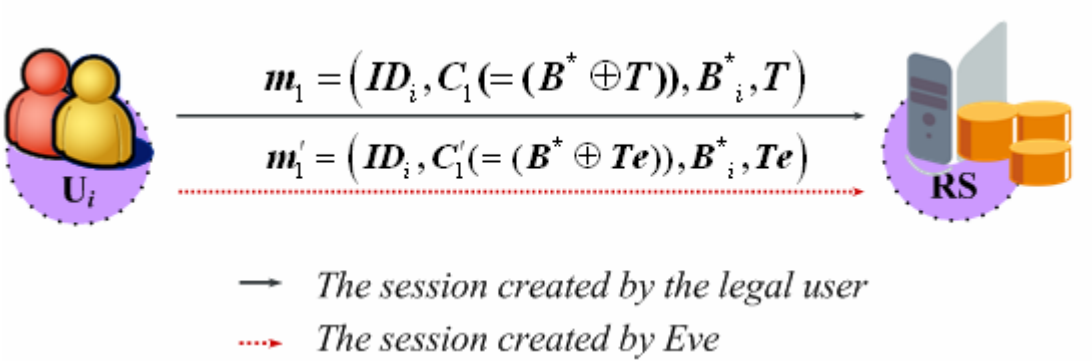

圖 10：Wu 和 Chieu 等學者方法的弱點

使用者於第 n 次身份認證過程中，攻擊者竊聽並記錄使用者與遠端系統之間傳遞的資料：$\boldsymbol{m_1}\left(=\left(\boldsymbol{ID_i}, \boldsymbol{C_1}, \boldsymbol{B^*_i}, \boldsymbol{T}\right)\right)$。攻擊者可將攔截取得之訊息 $\boldsymbol{m_1}$ 做重送攻擊 (以 $\boldsymbol{m_1'}$ 表示) 傳送至遠端系統

$$\boldsymbol{m_1'}\left(=\left(\boldsymbol{ID_i}, \boldsymbol{C_1'}, \boldsymbol{B^*_i}, \boldsymbol{Te}\right)\right)$$

Eve 利用先前所記錄的 $\boldsymbol{m_1}\left(=\left(\boldsymbol{ID_i}, \boldsymbol{C_1}, \boldsymbol{B^*_i}, \boldsymbol{T}\right)\right)$ 對 $\boldsymbol{C_1}$ 進行偽造。其偽造破解動作如下：

(1).計算參數 $\boldsymbol{C_1'}$ 的值，滿足 $\boldsymbol{C_1'} = (\boldsymbol{B^*_i} \oplus \boldsymbol{Te})$。其中 $\boldsymbol{Te}$ 為目前請求登入系

統的時間。

由於攻擊者可以在離線的情況下，輕易的進行驗證資訊的偽造，攻擊者可成功地偽裝成合法的使用者通過身份認證，而以假冒身份登入遠端系統。以下分別就攻擊者如何成功地登入系統與成功地通過遠端系統驗證二階段做說明：

【登入階段】

攻擊者將先前攔截到的訊息$\boldsymbol{m}_1$ (由$\boldsymbol{U}_i$傳到 RS)，做 replay attack，透過終端機做$\boldsymbol{m}_1$的重送攻擊，傳送訊息$\boldsymbol{m}_1'$ (以$\boldsymbol{m}_1'$表示重送的$\boldsymbol{m}_1$)至遠端系統。

當攻擊者在收到遠端系統訊息m_1，則會執行下列步驟：

(1).攻擊者會將攔截到的訊息$\boldsymbol{m}_1\left(=\left(\boldsymbol{ID}_i,\boldsymbol{C}_1,\boldsymbol{B}^*_i,\boldsymbol{T}\right)\right)$ (攻擊者在離線下可以成功地偽造破解$\boldsymbol{C}_1'=(\boldsymbol{B}^*_i\oplus\boldsymbol{Te})$，故亦可成功地自$m_1$中的取出$\boldsymbol{C}_1$，$\boldsymbol{T}$並以$\boldsymbol{C}_1'$，$\boldsymbol{Te}$取代)並且傳送訊息偽造訊息$\boldsymbol{m}_1'\left(=\left(\boldsymbol{ID}_i,\boldsymbol{C}_1',\boldsymbol{B}^*_i,\boldsymbol{Te}\right)\right)$至遠端系統。

【系統驗證階段】

當遠端系統在收到攻擊者的驗證請求訊息$\boldsymbol{m}'_1$，則會執行下列驗證步驟：

(1).計算$\boldsymbol{C}^*_1$的值，滿足$\boldsymbol{C}^*_1=(\boldsymbol{B}^*_i\oplus\boldsymbol{Te})$。此訊息將會成功的通過系統驗

證程序，因為其中C_1'中之B^*_i是從先前攔截到的訊息m_1中取出，而Te為當時所登入時間戳記，因此攻擊者可成功的假冒合法使用者通過系統驗證程序。

第五章 我們所提的改善的方法

5.1 以通行碼表為設計基礎的改善方法

5.1.1 改善 Yang 等學者的方法

在這章節，我們將會改善 Yang 等學者的方法，而成功的防止重送攻擊。由於根據我們的安全性分析，得知訊息 m_2 會產生弱點。因此改善的方法如下圖 11 所示，並分述如下：

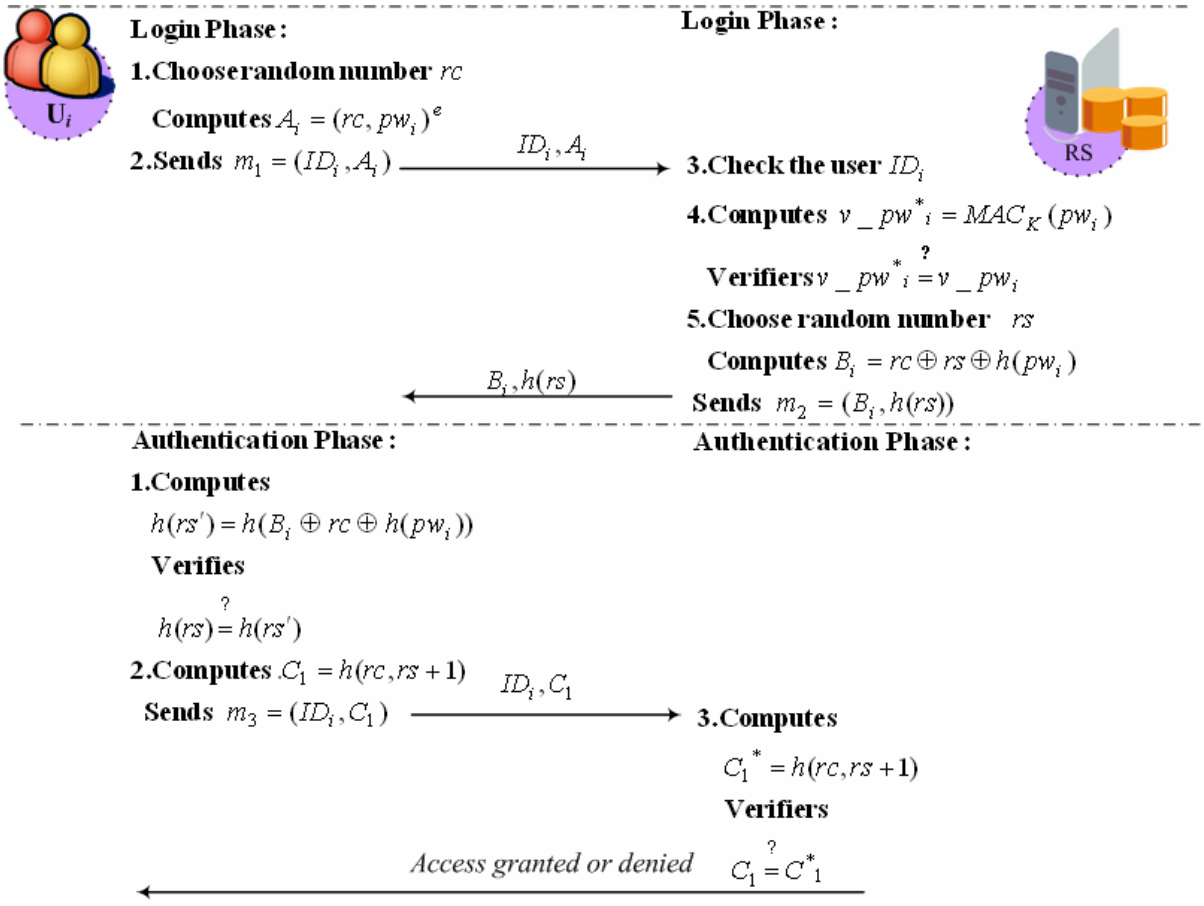

圖 11：我們改善 Yang 等學者的方法

【登入階段】

當U_i輸入自己的ID_i及pw_i後，終端機會執行下列步驟：

(1).計算參數A_i的值，滿足$A_i = (rc, pw_i)^e$。其中rc為終端機以目前請求登入系統時間所產生的暫時亂數。

(2).透過終端機傳登入請求訊息$m_1\left(=\left(ID_i, A_i\right)\right)$至遠端系統。

當遠端系統在收到U_i的登入請求訊息m_1後，則會執行下列驗證步驟：

(3).檢查ID_i的合法性。若ID_i的格式不符，系統立刻拒絕U_i的登入請求。

(4).系統利用私密金鑰 d，解出 pw_i 與 rc 的值，並且利用私密金鑰K做為求MAC之 key, 計算$v_pw_i^* = MAC_K(pw_i)$。然後取出與使用者相對應已存於系統資料庫中之參數$v_pw_i\left(=MAC_K(pw_i)\right)$的值。檢查$v_pw_i^*$與$v_pw_i$是否相等，如果相等則接受$U_i$的登入請求，否則，拒絕登入請求。

(5).如果系統通過上述驗證程序，則會產生參數B_i的值，$B_i = rc \oplus rs \oplus h(pw_i)$。其中遠端系統會計算當時請求登入系統時間之暫時亂數rs；然後，遠端系統傳送訊息$m_2\left(=(B_i, h(rs))\right)$至終端機。

【遠端系統驗證階段】

當終端機在收到遠端系統訊息m_2，則會執行下列驗證步驟：

(1).計算$h(rs')$的值，$h(rs')=h(B_i \oplus rc \oplus h(pw_i))$。其中$rc$為當時終端機所請求登入系統時間而產生的暫時亂數，$B_i$為 RS 所送來之訊息$m_2$中之$B_i$。然後，驗證遠端系統送來訊息$m_2$中之$h(rs)$是否與$h(rs')$相等，如下述：

$$h(rs')$$
$$= h(B_i \oplus rc \oplus h(pw_i))$$
$$= h(rc \oplus h(pw_i) \oplus rs \oplus rc \oplus h(pw_i)) \stackrel{?}{=} h(rs) \text{ (the second half in } m_2)$$

(2).若上述方程式等式成立，則終端機接受遠端系統的身份，否則，拒絕遠端系統之訊息。如果驗證為合法之遠端系統，終端機則會計算$C_1 = h(rc, rs+1)$並且傳送訊息$m_3 \left(= (ID_i, C_1)\right)$至遠端系統。

當遠端系統在收到U_i的驗證請求訊息m_3後，則會執行下列驗證步驟：

(3).計算$C^*_1 = h(rc, rs+1)$，驗證其C^*_1與U_i所送來m_3中之C_1是否相等，如果相等則接受U_i的登入請求，否則，拒絕登入請求。

5.1.2 所提改善 Yang 法的安全性分析

以下針對我們所提的方法用 Ku [6] 學者所提的重送攻擊法去做使用者登入與遠端系統驗證的攻擊分析。(攻擊者 Eve 在截取訊息m_1下，做重送攻擊時，以m_1'表示原來的訊息m_1)

5.1.2.1 使用者登入分析

在登入階段，系統會利用它的私密金鑰解開m_1' 並且取出rc 和pw_i。系統會計算出$MAC_K(pw_i)$並且去核對是否為v_pw_i值。他將會驗證成功因為m_1'是之前合法使用者的登入訊息。

之後，系統會選擇新的亂數new_rs並且計算出$m_2'\left(=(B_i', h(rs_new)\right)$，其中$B_i'\left(=rc \oplus rs_new \oplus h(pw_i)\right)$。系統將會傳送此訊息$m_2'$給攻擊者 Eve。Eve 可以由訊息$m_2'$中的$B_i'$依下述步驟取出亂數$rs_new$值。

Step 1. Guesses a random number r

/*

Eve wants to guess the right r , such that $r = rc \oplus h(pw_i)$, to cancel out the $rc \oplus h(pw_i)$ portion in $B_i \left(= rs \oplus rc \oplus h(pw_i)\right)$ of m_2 sent by RS to a legal user. Put it in another way, under Eve guessing and canceling the right r in B_i, $h(B_i)$ should be equal to $h(rs)$.

*/

Step 2. Computes $r' = B_i \oplus r$

Step 3. Computes $X = h(r')$

Step 4. Checks to see whether $X = h(rs)$,

if the equation holds then he knows $r = rc \oplus h(pw_i)$.

/*

Eve can use $r(= rc \oplus h(pw_i))$ to extract the rs_new value in $B_i' \left(= rc \oplus h(pw_i) \oplus rs\_new\right)$

*/

else go to Step 1: go on guessing

在猜出 r ，和取出 rs_new 後接下來 Eve 將想辦法產生 $C_1' = h(rc, rs\_new + 1)$。

【遠端系統驗證的分析】

攻擊者會傳送這結果 C_1' 和使用者 ID_i 去給系統完成驗證程序。但在這裡，攻擊者想要通過系統驗證 $h(rc, rs\_new + 1)$ 是不可能的，因為縱使 Eve 萃取出 rs_new 但 Eve 只猜到 $rc \oplus (pw_i)$ 並不知道 rc 的值。因此攻擊者的 replay attack 不可能成功。

另外附加說明各種所提的方法是否能有效的抵擋各種攻擊法，列出如下表

1 所示。

表 1：各種所提的方法是否能有效的抵擋各種攻擊法

	Peyravian and Zunic[3]	Hwang and Yeh[4]	Yang[5]	Our scheme
可防範重送攻擊	No	No	No	Yes
可防範修改攻擊	No	No	Yes	Yes
可防範系統假冒攻擊	No	No	Yes	Yes
可防範系統資料竊聽攻擊	No	No	Yes	Yes
可防範猜測攻擊	No	Yes	Yes	Yes
雙向身份驗證	No	Yes	Yes	Yes

5.2 以智慧卡為設計基礎的改善方法

5.2.1 改善 Wu 和 Chieu 等學者的方法

在這章節將介紹我們所提出人性化智慧卡遠端認證系統 [25] (A New Scheme for Remote User Authentication with Smart Cards) ，其架構詳細說明如下。

遠端通行碼認證系統 RS 在設定階段時，系統首先會建立本身的基本參數，並將公開參數 N, e, g, h 公佈出來，而保留私密參數 $d, \phi(N)$ 之後；系統可依使用者(以下簡稱 U_i)註冊、登入及系統驗證這三個階段來描述。

【本系統三階描述】

在註冊階段時，使用者將自己的身份相關資訊與通行碼傳給遠端系統；在登入階段時，使用者傳遞公開資訊及使用者通行碼以完成系統驗證階段所需的程序。以下就各階段詳細說明：

【註冊階段】

當 U_i 將自己的 ID_i 與相對應的通行碼 pw_i 透過一個安全的通道傳送到 RS。在收到使用者的 ID_i 後，系統會利用下列方程式計算出對應的 S_i：

$$S_i = (h(ID_i \oplus pw_i) \oplus h(d))^d$$

然後，RS 會核發給使用者一張智慧卡，智慧卡中所預先儲存的參數 (ID_i, S_i, e, h, N, g)。最後，結束註冊階段的程序。

【登入階段】

當U_i將智慧卡插入終端機，並輸入自己的ID_i及pw_i後，智慧卡會執行下列步驟：

(1).首先，透過終端機傳送使用者身份ID_i至系統。

當遠端系統在收到U_i的登入請求訊息$m_1 (= ID_i)$後，則會執行下列驗證步驟：

(2).檢查ID_i的合法性。若ID_i的格式不符，系統立刻拒絕U_i的登入請求。

(3).上述驗證通過後，系統則選擇目前的系統時間T與使用者身份識別碼ID_i並利用系統私密金鑰d，簽合出參數R值，滿足$R = (ID_i \| T)^d$。之後則傳送訊息$m_2 = (R, T)$至終端機。

【系統驗證階段】

當終端機在收到 RS 訊息m_2後，則會執行下列驗證步驟：

(1)終端機首先會檢查時間戳記T是否在一個合理的時間延遲範圍內，亦即若$T' - T \geq \Delta T$ (ΔT 為系統所設定的合理時間延遲參數)。最後

檢查 $R^e = (ID_i \| T)$ 與 $(ID_i \| T)$ 是否相等，若方程式等式成立，則終端機接受遠端系統的身份，否則，拒絕遠端系統之訊息。

(2).如果以上驗證通過後，則透過終端機傳送 (X_i, S_i) 的登入請求訊息 m_3 至遠端系統，其 X_i 的方程式如下：

$$X_i = h(ID_i \oplus pw_i)^R$$

當遠端系統在收到 U_i 的登入請求訊息 $m_3 (= (X_i, S_i))$ 後，則會執行下列驗證步驟：

(3).計算 S^*_i 的值，滿足 $((S_i)^e \oplus h(d))^R$。最後檢查 S^*_i 與 X_i 是否相等，則接受 U_i 的登入請求，否則，拒絕登入請求，以下為系統驗證方程式。

$$\begin{aligned} & S_i^* \\ &= ((S_i)^e \oplus h(d))^R \\ &= ((h(ID_i \oplus pw_i) \oplus h(d))^d)^e \oplus h(d))^R \\ &= h(ID_i \oplus pw_i)^{(ID_i \| T)^d} \end{aligned}$$

and

$$\begin{aligned} & X_i \\ &= h(ID_i \oplus pw_i)^R \\ &= h(ID_i \oplus pw_i)^{(ID_i \| T)^d} \end{aligned}$$

綜合上述系統三個階段如圖 12 所示。

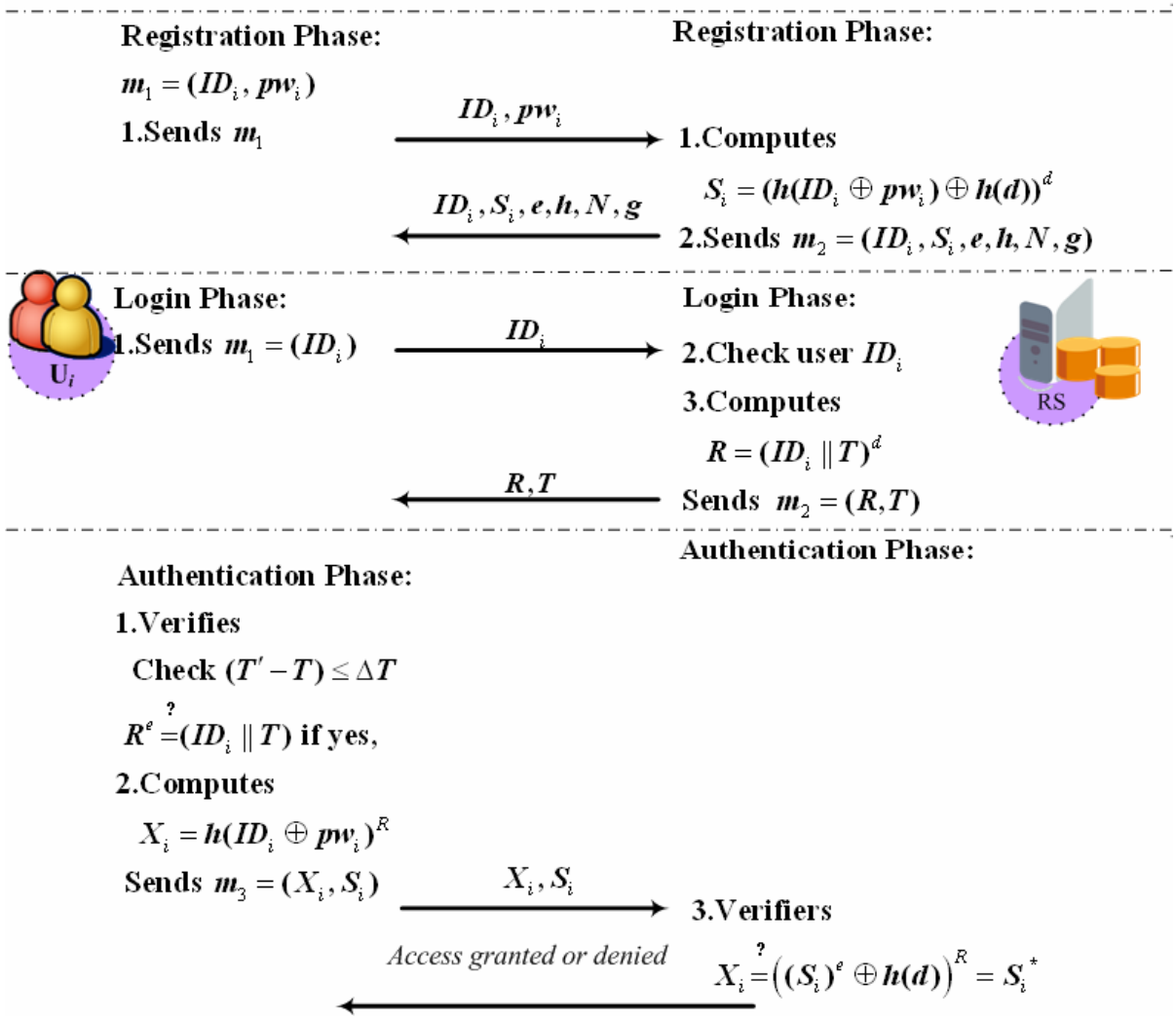

圖 12：我們所提的新方法[25]

【使用者改變通行碼程序】

在這裡，我們將會討論改變通行碼認證的協定，在這裡也有如上所定義之系統參數。首先，U_i 會將自己的 ID_i 對應的 new_pw_i 透過安全管道(secure channel)傳送到 RS。RS 在收到使用者的 ID_i 對應的 new_pw_i 後，系統會利用其私密金鑰 d 依下列方程式計算出 S_i'：

(1).計算參數S_i'的值，滿足$S_i' = (h(ID_i \oplus new_pw_i) \oplus h(d))^d$。

(2).之後使用者就可以完成下次登入遠端通行碼認證系統驗證程序。

然後，RS 會儲存S_i'在智慧卡中，並且保留私密金鑰 d 。最後，系統會將公開參數(ID_i, S_i', e, h, N, g)送回給U_i。結束改變通行碼階段的程序。

5.2.2 所提改善 Wu 和 Chieu 法的安全性分析

在這個章節，我們將審查所提方法的安全性分析，分析方法如下所示：

分析 1：攻擊者無法假冒合法的系統偽造出 $\boldsymbol{m}_2\left(=\boldsymbol{(R,T)}\right)$ 訊息是不可行的，因為，此訊息將會受到時間戳記和系統的私密金鑰以及使用者身分識別碼所保護。如果偽造者想要以重送訊息的方法重送此訊息，他將會在認證階段步驟(1)中被檢驗出來。

分析 2：當偽造者想要假冒合法的使用者，重送訊息 $\boldsymbol{m}_3$ 的資訊，以重送攻擊的方式在登入階段登入系統，他將會失敗。因為 $\boldsymbol{X_i}=\left(\boldsymbol{h(ID_i \oplus pw_i)}\right)^{\boldsymbol{R}}$ 他仍然受到系統之私密金鑰 $\boldsymbol{d}$ 和當時系統時間戳記 T 以及 $\boldsymbol{ID_i}$ 所保護，並且在認證階段步驟(3)被檢驗出來。

分析 3：任何的偽造者不能夠偽造出 $\boldsymbol{X_i}=\left(\boldsymbol{h(ID_i \oplus pw_i)}\right)^{\boldsymbol{R}}$ 和 $\boldsymbol{S_i}\left(=\boldsymbol{(ID_i \oplus pw_i)} \oplus \boldsymbol{h(d)^d}\right)$ 的值，事實上由於 $\boldsymbol{X_i}, \boldsymbol{S_i}$ 受到單向赫序函數不可逆性以及質因數分解問題的困難度上的安全性保護。

另外附加說明各種所提的方法是否能達成下列優勢及有效的抵擋各種攻擊法，列出如下表 2 所示。

表 2：各種所提的方法是否能達成下列優勢及有效的抵擋各種攻擊法

	Sun[1]	Wu-Chieu[2]	Our scheme[25]
可防範重送攻擊	Yes	No	Yes
可自由選擇通行碼	Yes	Yes	Yes
可雙向身份驗證	No	No	Yes
可防範修改攻擊	Yes	Yes	Yes
可防範系統假冒攻擊	No	No	Yes
可防範系統資料竊聽攻擊	Yes	Yes	Yes
可防範猜測攻擊	Yes	Yes	Yes

第六章 結論與建議

在現今分散式電腦網路普遍的時代，傳統的通行碼認證系統已無法提供使用者與遠端系統之間資料通訊的安全性。如何提供一個有效且安全的使用者與遠端系統之間的身份認證機制，則是遠端使用者身份認證所要討論的議題。而由近年的各種相關的研究中，我們知道，以智慧卡為驗證基礎之遠端使用者確認方法，除了具有不需儲存通行碼、可防範重送攻擊的功能之優勢外，更合乎人性化的考量；基於此，在本篇論文中，我們針對幾種已提出的方法加以分析、發現其缺點，且改良補強提出我們改善的方法，並加以分析；為了提升實用性與方便性，在未來的研究我們將會探討如何利用智慧卡的技術結合二次剩餘的理論以設計出更具安全性及降低運算量的身分認證系統，此一議題仍有待吾人進一步的研究。

參考文獻

[1] H. M. Sun, “An efficient remote use authentication scheme using smart card, ” IEEE Transactions on Consumer Electronics, Vol. 46, November, 2000, pp.958-961.

[2] S. T. Wu and B. C. Chieu, “A user friendly remote authentication scheme with smart cards, ” Computers & Security 22 (6) 2003, pp. 547-550.

[3] M. Peyravian and N. Zunic, “Methods for Protecting Password Transmission, ” Computers and Security Vol.19, no.5, pp. 466-469, July 1 2000.

[4] J. J. Hwang and T. C. Yeh, “Improvement on Peyravian-Zunic’s password authentication schemes, ” IEICE Transactions on Communications., vol.E85-B, no.4, pp.823-825, April 2002.

[5] C. C. Yang, T. Y. Chang, J. W. Li and M. S. Hwang, “Security Enhancement for Protecting Password Transmission, ” IEICE Transactions on Communications., vol.E86-B, no.7, pp.2178-2181, JULY 2003.

[6] W. C. Ku, C. M. Chen and H. L. Lee, “Cryptanalysis of a Variant of Peyravian-Zunic’s password authentication schemes, ” IEICE Transactions on Communications., vol.E86-B, no.5, pp.1682-1684, MAY 2003.

[7] L. Lamport, “Password authentication with insecure communication, ”Communications of the ACM, Vol. 24, No. 11, 1981, pp. 770-772.

[8] M. S. Hwang and L. H. Li, “A new remote user authentication scheme using smart cards, ” IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, 2000, pp. 28-30.

[9] H. Y. Chien, J. K. Jan, and Y. M. Tseng, “An efficient and practical solution to remote authentication: Smart Card, ” Computers and Security, Vol. 21, No. 4, 2002, pp. 372-375.

[10] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, ” Communications of the ACM, January. 1983, Vol. 26, No. 1, pp. 96-99

[20] The RSA Challenge Numbers, http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html.

[21] G. Horng, “Password authentication without using password table,” Inf. Process. Lett., vol.55, pp.247–250, 1995.

[22] A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” Proceedings of CRYPTO’84, pp. 47-53, 1985.

[23] T. ElGamal, “A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms, ” IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985.

[24] M. S. Hwang, C. C. Lee and Y. L. Tang, “A Simple Remote User Authentication Scheme, ” Mathematical and Computer Modeling, vol. 36, pp. 103-107, 2002.

[25] J. S. Chou, C. H. Lin and J. I. Shiue “A New Scheme for Remote User Authentication with Smart Cards, ” Proceedings of International Conference on Informatics, Cybernetics, and Systems 2003, pp.1353~1358.

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

[27] 吳育展，「以智慧卡為基礎的密碼驗證架構之研究與其應用」，逢甲大學資訊工程學系碩士論文(2002)。