適用於多重伺服器環境之點對點可鑑別金鑰交換協定

許建隆[1]、畢仕誠[2]、呂崇富[3*]
[1,2]長庚大學 資訊管理學系、[3]致理科技大學 資訊管理學系
[1]clhsu@mail.cgu.edu.tw、[2]psc0128@hotmail.com、[3]peter61@mail.chihlee.edu.tw

摘要

隨著網路服務的快速發展及多元化，使用者可以透過網際網路向多重不同的網路應用服務提供者取得資源及服務。為了確保經授權的使用者才能存取資源及服務，網路應用服務提供者通常會提供使用者身分鑑別協定，甚至網路通訊安全保護。對於使用者而言，其通常透過使用者通行碼來進行身分鑑別動作。然而，當使用者面對多重伺服器時，雖然仍可透過各別原有的使用者鑑別協定來達到所宣稱的安全性，但卻可能引發潛在的安全性及通行碼管理的問題。我們提出一個適用於多重伺服器環境下，結合智慧卡與通行碼的雙因子身分鑑別協定，除了可以滿足鑑別金鑰交換協定特性（人性化需求、雙因子身份鑑別、雙向鑑別、低計算與通訊成本、建立交談金鑰、前推安全性、防止智慧卡遺失遭冒用、可動態修改通行碼、抵擋所有現存的攻擊法攻擊）外，並允許使用者使用單一且具可記憶之通行碼註冊並登錄不同伺服器，以達到跨網域（inter-domain）的四方通訊。

關鍵詞：多重伺服器、通行碼、雙因子鑑別、雙向鑑別、金鑰交換協定

End-to-End Authenticated Key Exchange Protocols in Multi-Server Environments

Chien-Lung Hsu[1], Shih-Cheng Pi,[2], Chung-Fu Lu[3*]
[1,2] Department of Information Management, Chang Gung University
[3]Department of Information Management, Chihlee University of Technology
[1]clhsu@mail.cgu.edu.tw、[2]psc0128@hotmail.com、[3]peter61@mail.chihlee.edu.tw

Abstract

With rapid development of varied internet services, users can access resources and services from different internet service providers via internet. Such internet service providers

* 通訊作者 (Corresponding author.)

generally provide user authentication protocols to ensure only the authorized users can access resources and services, and further provide secure communication protocols. Hence, users generally use their passwords to login servers for authenticating their legitimacy. However, such solutions might face password management problems and some potential attacks. For multi-server environments, we propose a password-based authentication protocol using smart cards for the cross domains. The proposed protocol not only solve password management problems, but also withstand some potential passive and active attacks, and achieve three-party and four party end-to-end user authentication and key agreement for the same domain and the cross domains without the assistance of a trusted registration center.

Keywords：Multi-server、Password、Two-factor authentication、Mutual authentication、Key exchange protocol

壹、前言

綜觀近年來電信業者的蓬勃發展，從原本的有線電話演進到無線電話，進而發展到行動通訊；從原本單一電信業者的網內聯繫，進展到跨越不同的電信公司的網外通話，僅僅單憑一組門號，不需其他繁雜的手續即可與所有電信公司的使用者達成通話，這種簡單跨越其他電信公司的作法，在現今發展快速的網際網路上卻未能如預期中達到相同的功能。截至目前為止，網際網路上大部份的 ISP（Internet Service Provider）僅提供使用者個別申請使用，例如：YAHOO、Google 等知名 ISP 都有提供相同類以的服務功能，讓使用者依據自己的需求及喜好申請，但只能使用個別申請的帳號、密碼登入，才能與相同伺服器中的其他使用者溝通，如果使用者需要跨越使用其他伺服器時，就必須重新申請其他伺服器的帳號、密碼，才能登入使用，而無法像行動通訊一樣，僅憑一組帳號、密碼即可登入不同的伺服器，當使用者申請愈多，所必須記憶的帳號、密碼將愈多，造成使用者在使用上的困擾及不便。

因此，要安全的在網路上傳遞各種訊息，就必須運用諸多適當的保護機制來達成，而訊息傳遞時常見的安全保護機制包括加密金鑰交換協定（encryption key exchange protocol）、KDC 金鑰分配協定（key distribution center key distribution protocol）、通行碼驗證金鑰交換協定（password-based authentication key agreement）、多重伺服器的通行碼鑑別機制等不同方法。而現今的三方金鑰交換協定都必須透過單一具信任的遠端伺服器來驗證，如此就出現下列幾個問題：

- 假設使用者要登入多個伺服器時，就必須記住多個通行碼，對使用者而言是相當不方便的。

- 僅能透過單一且具信任性的遠端伺服器來做驗證，無法進行不同伺服器的四方通訊。另在具驗證者（verifier）的金鑰交換協定中，雖然已提出適用於多重伺服器環境的機制，但是僅適用於單一使用者，並無法進行三方或四方通訊。

為有效解決上述所面臨的問題，我們設計出一個可適用於多重伺服器環境之點對點可鑑別金鑰交換協定，在多重伺服器環境下，並結合智慧卡與單一且具可記憶之通行碼的雙因子身分鑑別技術，以達到同網域（intra-domain）及跨網域（inter-domain）的三方及四方驗證之目的。我們提出的方法除了滿足一般鑑別金鑰交換協定之特性外（抵擋現存攻擊法攻擊、人性化需求、雙因子身份鑑別、雙向鑑別、低計算與通訊成本、建立交談金鑰、前推安全性、防止重送攻擊、防止智慧卡遺失遭冒用、可動態修改通行碼、提供明確金鑰鑑別等），亦可允許使用者使用單一且具可記憶之通行碼註冊並登錄不同伺服器，以達成同網域（intra-domain）的三方通訊及跨網域（inter-domain）的四方通訊，當其中一台伺服器遭受攻擊、破解時，並不會因為被攻擊者得知其相關參數資訊，而影響其他伺服器或使用者的正常運作，大幅降低整體的損失。我們的方法除了能抵擋目前現有的相關攻擊外，並可滿足下列的特性：

1. 多重伺服器環境驗證，不用透過 RC 向伺服器註冊。
2. 遠端伺服器不用儲存鑑別表（no password table）。
3. 建立雙方的交談金鑰，以達到私密通訊的目的。
4. 雙向鑑別機制，可分別確認雙方身分。
5. 雙因子鑑別技術，可以選擇簡單、容易記憶的通行碼。
6. 通行碼可依照使用者需求任意選擇或變更。
7. 使用者可以在遠端伺服器上動態新增註冊或註銷服務。
8. 允許使用者點對點傳送訊息。

貳、文獻探討

一、加密金鑰交換協定（encryption key exchange protocol）

為維護訊息在傳遞過程中的安全性與私密性，最常見的方式就是利用金鑰交換技術使欲通訊的使用者雙方產生共同的金鑰，或是運用公開金鑰密碼系統（public key cryptosystem）來解決訊息傳遞時的金鑰交換問題。

- Diffie-Hellman [4] 於 1976 年首先提出的金鑰交換協定（key exchange protocol），其是運用模指數的運算來建立雙方相同的交談金鑰（session key）。但如果欲通訊的使用者雙方沒有針對彼此所交換的訊息進行鑑別時，攻擊者可以很容易從中間假冒雙方的身分，再分別與雙方建立交談金鑰，此攻擊法稱為中間者攻擊法（man-in-the-middle attack）。

- 另一種方式是先運用接收者的公鑰將金鑰加密成為密文後再傳送給接收者，然後接收者運用自己的私鑰解密所接收的密文後，即可獲得雙方可以共用的秘密金鑰。但是如果接收者無法對所接收的密文進行鑑別時，則很容易遭受到假冒攻擊（impersonation attack）。

二、KDC 金鑰分配協定（key distribution center key distribution protocol）

雖然金鑰交換技術可以讓任意兩方建立秘密的通訊，但如果有攻擊者假冒欲通訊的使用者雙方身分時，任何一方的使用者很難驗證判斷，而解決此問題的方式可以在使用者雙方進行訊息傳遞時，先經由一個公正可信任的第三方實施驗證，該第三方一般稱為憑證中心 CA（certificate authority）或金鑰配發中心 KDC（key distribution center）。Popek 與 Kline[16]於 1979 提出 KDC 金鑰分配協定的觀念，就是讓欲通訊的使用者雙方能夠透過金鑰中心的分配協定，產生雙方可秘密通訊的交談金鑰，但前提必須是雙方必須經由金鑰中心註冊認證，才能確保訊息傳遞時的安全。當欲通訊的使用者雙方進行秘密通訊時，傳送者必須先向金鑰中心取得接收者的相關資訊，在過程中是以秘密通訊方式進行，以免遭受其他攻擊者攔截或阻斷。要達成此一目的，欲通訊的使用者雙方在與金鑰中心完成請求與認證後，金鑰中心就會將接收者的相關資訊提供給傳送者，而通訊雙方即可分享短暫性的私密金鑰（secret key），傳送者就可以與接收者進行通訊。假設欲通訊的使用者任何一方遺失相關資訊或金鑰中心伺服器遭攻擊者破解時，則將成為攻擊者入侵的最佳時機。

三、通行碼驗證金鑰交換協定（password-based authentication key agreement）

如果以三方通訊而言，要達成通訊傳遞時的安全並非不可能，首先必須保證欲通訊的使用者雙方與金鑰中心伺服器進行通訊時的安全，其次，與金鑰伺服器的通訊內容必須愈簡單愈好，因為在真實的網路環境中，雙方的通訊次數或通訊量愈多，愈容易成為攻擊者覬覦鎖定的對象。因此，Bellovin 與 Merritt[1]於 1992 年提出以通行碼為基底（password-based）的概念，稱為通行碼驗證金鑰交換協定（password-based authentication key agreement），就是透過欲通訊的使用者雙方以簡易的共享密碼，進行金鑰交換及驗證的程序，簡化傳遞時的通訊量及金鑰儲存問題。而此概念真正延伸運用到三方通訊則是由 Steiner 等人[21]於 1995 年提出植基於通行碼基礎的三方通訊金鑰共同協定（three-party protocol for password-based key agreement），但 Ding 與 Horster [5]即於 1995 年指出上述協定容易受到不可探測的線上密碼猜測攻擊（undetectable on-line password guessing attack），雖然有諸多專家學者陸續針對此協定會面臨到的各項攻擊問題提出可能的改善方案 [12][14]，但是仍以 Sun 等人[17]於 2003 年提出以通行碼為基礎的三方通訊金鑰交換方法最具代表性，他們運用不同的網路架構，提出讓欲通訊的使用者雙方使用金鑰伺

服器的公鑰加密訊息，然後金鑰伺服器分別計算雙方不同的短暫金鑰，讓雙方分別計算出同一把交談金鑰，並利用此金鑰進行秘密通訊，但是 Nam 等人[15] 於 2004 年指出此方法仍然容易受到中間攻擊法攻擊，於是 Lee 等人[11]於 2005 年時提出不使用金鑰伺服器的公鑰加密方法，此方法能增強原有通行碼的基礎，改用驗證值基礎（verifier-based）的三方通訊金鑰交換協定。

通行碼驗證金鑰交換協定的主要作用是為了讓欲通訊的使用者雙方能擁有相同的交談金鑰，然後讓雙方達到身分驗證（mutual authentication）的目的，而進行通訊的對象通常可以分為兩類：

1. 使用者與伺服器：使用者向伺服器註冊時必須提供一組自選的通行碼，而伺服器則必須儲存每位使用者註冊的通行碼，然後，使用者與伺服器運用通行碼驗證金鑰交換協定進行交談金鑰的分配與身分驗證。由於在此階段參與通行碼驗證金鑰交換協定的對象僅有使用者與伺服器兩方，因此，稱為二方通訊（two-party）通行碼驗證金鑰交換協定。
2. 使用者與使用者：當使用者彼此之間進行通訊時，都必須分享一組秘密的通行碼，如果對象數量過多時，則會讓使用者記憶過多的通行碼，因此，在此模式中，每位使用者只和同一個被信任的伺服器秘密分享通行碼，當使用者雙方需要進行通訊時，則透過此一伺服器的通行碼驗證交換協定，來進行雙方的交談金鑰分配及身分驗證。由於在此階段參與通行碼驗證金鑰交換協定的對象有兩個使用者與一個伺服器，因此，稱為三方通訊（three-party）通行碼驗證金鑰交換協定。

通行碼鑑別機制中，當使用者（user）向遠端任一伺服器（server）註冊後，即可成為此伺服器的合法用戶，並依據使用者申請的需求，給予可識別使用者身分的識別碼（identifier，簡稱 ID）以及通行碼（password，簡稱 PW）。遠端伺服器的鑑別表（verification table）中同時也儲存相同資訊，所以，當合法用戶想要向已註冊的遠端伺服器取用資源或服務時，必須先輸入給予的 ID 和 PW，透過網路將 ID 和 PW 傳至遠端伺服器，伺服器先確認傳送的 ID 是否已存在於鑑別表內，此一過程稱為身分識別（identification）；當 ID 確認後，會將傳送的 PW 比對鑑別表內 ID 所對應的 PW 是否相同，此一過程稱為身分鑑別（authentication）。看似簡單的架構卻有許多安全上的問題存在，例如：透過網路傳輸 ID 和 PW，如果遭受攻擊者竊聽，則可以假冒合法用戶取得伺服器的資源或服務。[30]

Lamport[10]於 1981 年提出以單向雜湊函數為基礎的身分鑑別機制來解決上述問題，他將使用者的 PW 先利用一次雜湊函數運算後，再儲存於鑑別表中，以避免 PW 被攻擊者得知。Shimizu[18]於 1990 年提出動態通行碼（dynamic password/one-time password）概念，他將通行碼分為二個部份，一個提供使用者記憶的通行碼稱作使用者通行碼，另一個則是儲存在鑑別表內的通行碼稱為鑑別通行碼，使用者可運用使用者通行碼產生鑑別通行碼後登入遠端伺服器。但是上述的這些機制均使用弱通行碼（weak password）[20] [25] [26][27]，無法抵擋離線通行碼的猜測攻擊（off-line password guessing attack）。因此，

Sandirigama–Shimizu–Noda [19]於 2000 年提出使用強通行碼（strong password）的身分鑑別機制後，陸續有許多專家學者指出此類機制仍有安全上的漏洞[2][9][13][23][24]，並進而提出相關改進機制。

而上述的機制仍然需要在伺服器上建立及維護鑑別表，依然會有安全上的威脅，因此，Sun[22]於 2000 年提出無鑑別表的通行碼鑑別機制，他是將使用者 ID 與遠端伺服器的秘密參數當成身分鑑別的方式，但此機制的缺點是不讓使用者有選擇通行碼的權利。而以人性化的角度，機制本身應符合使用者個人的需求任意選擇或變更通行碼，所以，文獻[6]將針對此方向做深入的研究，並提出改進機制。

另外，在國內研究方面，2006 年張國義曾提出可驗證的三方通訊金鑰交換協定[28]，使用者雙方分別預先與伺服器建立秘密分享的通行碼，使用者雙方不需儲存伺服器的相關資訊，然後再利用公鑰加密的方法，將使用者的 ID 與計算後的通行碼加密成為秘密資訊。而當使用者雙方向伺服器請求通訊時，伺服器可利用本身的儲存資料，進行驗證並計算雙方需交換的訊息，以扼制其他惡意的各種攻擊。但此方法不適用於多重伺服器環境，使用者也無法動態加入或註銷伺服器，且伺服器可以得知通訊雙方的交談金鑰。

四、多重伺服器的通行碼鑑別機制

以往的通行碼鑑別機制通常只運用於單一的遠端伺服器，但近年來，網路發展愈來愈迅速普及，單一伺服器已無法滿足使用者的需求，因此，使用者紛紛向其他伺服器進行註冊，以取得所需要的服務與功能，然而，當註冊的伺服器愈多，使用者就會必須去記憶愈多的 ID 與 PW 來登錄使用不同的伺服器，相對的，就會產生使用者的不方便性。假設使用者以相同的通行碼去註冊不同的伺服器時，則會面臨伺服器內部的不法管理者利用使用者的通行碼，假冒使用者身分去登錄其他伺服器。

為考量使用者的便利性及通行碼的安全性，陸續有專家學者提出適用於多重伺服器架構的研究機制[3][7][8]，探討多重伺服器的使用者身份鑑別機制，讓使用者能運用單一通行碼來登錄不同的伺服器，例如 Juang[8]運用對稱式加解密技術來保護認證資訊，Chang 與 Kuo[3]則是利用中國的餘數定理來鑑別資訊及保護存取控制權限，還有 Hwang 與 Sheng[7]也運用對稱式加解密技術來保護鑑別資訊並改進 Juang [8]所提出的機制。而以上的鑑別機制仍然存在著需要儲存鑑別碼、無法動態加入或退出伺服器、鑑別機制必須經過註冊中心完成及系統執行效能較差等問題，這些都是目前多重伺服器架構中身分鑑別機制所會遇到的困難。

但是，通行碼鑑別機制還是有其他多樣化的設計方式，除了探討遠端伺服器可以鑑別合法使用者的身分，同時也必須讓使用者能鑑別合法的遠端伺服器，確實達到雙向鑑別的目的。因此，除了身分鑑別可以確保資料傳輸時的機密性與完整性，還必須同時產生一把交談金鑰來驗證所收到的訊息是否確實為對方所傳送，以防止他人偽冒，上述這種機制稱為「通行碼鑑別與金鑰交換協定」[30]。

另外，在 2008 年陳建仁提出適用於多重伺服器環境之可鑑別金鑰交換協定[29]，目的在於確保使用者與數個遠端伺服器能夠相互鑑別彼此身分的合法性，同時建立共享金鑰，作為確保後續的秘密通訊。其方法是使用者可運用單一通行碼登錄數個伺服器，假設其中一台伺服器遭到破解、駭客入侵或監守自盜等情事，依然不會危害使用者登錄其他伺服器的安全性，但此方法伺服器仍可以得知通訊雙方的交談金鑰。

參、一個適用於多重伺服器環境之點對點可鑑別金鑰交換協定

為了在多重伺服器環境下進行多方秘密通訊時，可以有效解決原本註冊中心（RC）在多重伺服器架構中讓使用者和遠端伺服器面臨安全威脅的問題，並使遠端伺服器不須儲存鑑別表以減少管理風險，而使用者也可隨時動態加入伺服器得到所提供服務，並能隨時修改密碼，也能讓使用者間建立交談金鑰以達到三方或四方的私密通訊目的，我們提出一個適用於多重伺服器環境下之點對點可鑑別金鑰交換協定，不但可以結合多方通訊與多重伺服器的優點，亦能解決兩者所面臨的問題，以提供使用者安全且便利的網路環境。

在系統初始階段，先任選兩台經 CA 合法驗證的遠端伺服器，使用者雙方各自領取智慧卡後，個別輸入身分碼與通行碼並分別登入，然後被登入的伺服器會個別產生系統參數 p, q 和 g。在註冊階段時，使用者雙方和不同的兩台遠端伺服器建立彼此共享的秘密，並將這個秘密加以保護後分別儲存在使用者雙方的隨身碟中。在登入暨金鑰交換階段，使用者雙方首先透過各自隨身碟上的秘密值，啟動智慧卡，並輸入本身的通行碼，智慧卡透過加密金鑰交換技術計算建立使用者雙方與兩台遠端伺服器彼此的共享金鑰，，兩台遠端伺服器個別確認使用者雙方身份後，利用電子商務認證授權機構（certificate authority,簡稱 CA）所提供的簽章對共享金鑰加密後，兩台遠端伺服器互相傳送，經驗證正確後，兩台遠端伺服器利用傳送的共享金鑰再重新計算共享金鑰後，傳送給個別的使用者計算屬於使用者雙方各自的私有金鑰。最後，如果使用者雙方擁有相同的私有金鑰時，就可以建立僅屬於雙方的私有通道，以達到四方通訊。有關我們提出協定中所使用的符號意義如表一所示。

一、系統初始階段

在系統初始階段，使用者親自到智慧卡的發卡中心領取智慧卡後，並於現場立即輸入身分碼與通行碼。在此一階段，預設兩台遠端伺服器依據數位簽章演算法 DSA（Digital Signature Algorithm，簡稱 DSA）產生值 p 、q 和 g ，其參數的定義如下：

p ：一個很大的質數。

q ：一個很大的質數，$q|(p-1)$。

g ：一個秩（order）為 q 的生成數（generator）g ，即 g 滿足 $(g^q = 1 \bmod p)$ 且 $g \neq 1$。

我們設定兩台遠端伺服器均向電子商務認證授權機構(certificate authority,簡稱 CA)註冊，並取得各自的憑證、簽章及公私鑰對，且兩台遠端伺服器不可為同一台($m \neq n$)，

表一：符號意義表

符號	說明
$ID_{U_{i,m}}$	使用者U_i登入遠端伺服器S_m的 ID
$ID_{U_{j,n}}$	使用者U_j登入遠端伺服器S_n的 ID
ID_{S_m}	遠端伺服器S_m的 ID
ID_{S_n}	遠端伺服器S_n的 ID
$PW_{U_{i,m}}$	使用者U_i登入遠端伺服器S_m通行碼
$PW_{U_{j,n}}$	使用者U_j登入遠端伺服器S_n通行碼
$r_{i,m}$	智慧卡對使用者U_i登入遠端伺服器S_m產生的隨機亂數
$r_{j,n}$	智慧卡對使用者U_j登入遠端伺服器S_n產生的隨機亂數
x_m	遠端伺服器S_m的秘密值
x_n	遠端伺服器S_n的秘密值
$a_{i,m}$	使用者$U_{i,m}$智慧卡產生的隨機亂數
$a_{j,n}$	使用者$U_{j,n}$智慧卡產生的隨機亂數
b_m	遠端伺服器S_m產生的隨機亂數
b_n	遠端伺服器S_n產生的隨機亂數
$R_{i,m}$	使用者$U_{i,m}$的加解密金鑰
$R_{j,n}$	使用者$U_{j,n}$的加解密金鑰
$E_{R_{i,m}}()$	使用者$U_{i,m}$運用加解密金鑰$R_{i,m}$的對稱式加密演算法
$D_{R_{i,m}}()$	使用者$U_{i,m}$運用加解密金鑰$R_{i,m}$的對稱式解密演算法
$E_{R_{j,n}}()$	使用者$U_{j,n}$運用加解密金鑰$R_{j,n}$的對稱式加密演算法
$D_{R_{j,n}}()$	使用者$U_{j,n}$運用加解密金鑰$R_{j,n}$的對稱式解密演算法
$T_{i,m}$	使用者U_i登入遠端伺服器S_m註冊時的時間戳記
$T_{j,n}$	使用者U_j登入遠端伺服器S_n註冊時的時間戳記
$\oplus$	互斥或運算元
$H()$	單向雜湊函數
$Cert_m$	遠端伺服器S_m取得的 CA 憑證
$Cert_n$	遠端伺服器S_n取得的 CA 憑證
Sig_m	遠端伺服器S_m取得的 CA 簽章
Sig_n	遠端伺服器S_n取得的 CA 簽章
p,q,g	數位簽章演算法 DSA 所需之參數

其參數的定義如下：

α_i：為U_i所註冊的 server 集合

α_j：為U_i所註冊的 server 集合

α_i：其中 $m \in \alpha_i$
$U_{j,n}$：其中 $n \in \alpha_j$ $\Big\}$ $m \neq n$

$Cert_{S_m}$、Sig_{S_m}：為 CA 發送給遠端伺服器S_m的憑證及簽章

$Cert_{S_n}$、Sig_{S_n}：為 CA 發送給遠端伺服器S_n的憑證及簽章

二、註冊階段

在註冊階段時，使用者雙方與兩台遠端伺服器共同執行下列步驟，讓使用者雙方至兩台遠端伺服器完成註冊程序。

步驟 1：使用者$U_{i,m}$將註冊資訊傳送給遠端的伺服器S_m，使用者$U_{i,m}$執行下列步驟：

步驟 1-1：輸入身分碼$ID_{U_{i,m}}$和通行碼$PW_{U_{i,m}}$。

步驟 1-2：智慧卡產生隨機亂數$r_{i,m}$。

步驟 1-3：智慧卡計算$A_{i,m} = H(PW_{U_{i,m}}) \oplus H(r_{i,m} \| ID_{S_m})$。

步驟 1-4：將身分碼$ID_{U_{i,m}}$和計算出的值$A_{i,m}$傳給遠端伺服器S_m。

步驟 2：使用者$U_{j,n}$將註冊資訊傳送給遠端的伺服器S_n，使用者$U_{j,n}$執行下列步驟：

步驟 2-1：輸入身分碼$ID_{U_{j,n}}$和通行碼$PW_{U_{j,n}}$。

步驟 2-2：智慧卡產生隨機亂數$r_{j,n}$。

步驟 2-3：智慧卡計算$A_{j,n} = H(PW_{U_{j,n}}) \oplus H(r_{j,n} \| ID_{S_n})$。

步驟 2-4：將身分碼$ID_{U_{j,n}}$和計算出的值$A_{j,n}$傳給遠端伺服器S_n。

步驟 3：遠端伺服器S_m計算與使用者$U_{i,m}$共同的秘密，遠端伺服器S_m執行下列步驟：

步驟 3-1：計算$u_{m,i} = H(ID_{U_{i,m}} \| x_m)$。

步驟 3-2：計算$B_{m,i} = u_{m,i} \oplus A_{i,k}$。

步驟 3-3：將計算出的值$B_{m,i}$回傳給使用者$U_{i,m}$。

步驟 4：遠端伺服器S_n計算與使用者$U_{j,n}$共同的秘密，遠端伺服器S_n執行下列步驟：

步驟 4-1：計算$u_{n,j} = H(ID_{U_{j,n}} \| x_n)$。

步驟 4-2：計算$B_{n,j} = u_{n,j} \oplus A_{i,m}$。

步驟 4-3：將計算出的值 $B_{n,j}$ 回傳給使用者 $U_{j,n}$ 。

步驟 5：使用者 $U_{i,m}$ 及 $U_{j,n}$ 在收到遠端伺服器 S_m 和 S_n 分別傳送的值 $B_{m,i}$ 和 $B_{n,j}$ 後，將值分別儲存在個別的隨身碟內。

三、登錄暨金鑰交換階段

登錄暨金鑰交換階段中，使用者雙方與二台遠端伺服器共同執行下列步驟，讓使用者雙方可以分別向各自的遠端伺服器登錄取得服務。

步驟 1：使用者 $U_{i,m}$ 登錄到遠端的伺服器 S_m ，使用者、智慧卡和遠端伺服器會共同執行下列步驟：

步驟 1-1：使用者 $U_{i,m}$ 註冊完畢後，當插入智慧卡，輸入通行 $PW_{U_{i,m}}$ 時，智慧卡中所儲存的亂數 $r_{i,m}$ 與伺服器 S_m 身分碼 ID_{S_m} 及使用者 $U_{i,m}$ 輸入通行碼 $PW_{U_{i,m}}$ 進行運算得到值 $A_{i,m}$ 。

步驟 1-2：使用者 $U_{i,m}$ 插入隨身碟，會將隨身碟內的秘密值 $B_{m,i}$ 和智慧卡中所計算出的值 $A_{i,k}$ 進行互斥或運算得到共享的秘密值 $u_{i,m}$ 。

步驟 1-3：使用者 $U_{i,m}$ 的智慧卡計算 $V_{i,m} = g^{u_{i,m}} \bmod p$ 。

步驟 1-4：使用者 $U_{i,m}$ 的智慧卡選取隨機亂數 $a_{i,m} \in_R Z_p^*$ 。

步驟 1-5：使用者 $U_{i,m}$ 的智慧卡計算 $R_{i,m} = g^{a_{i,m}} \bmod p$ 。

步驟 1-6：使用者 $U_{i,m}$ 的智慧卡計算 $M_{i,m} = R_{i,m} \| ID_{U_{i,m}}$ 。

步驟 1-7：使用者 $U_{i,m}$ 的智慧卡計算 $MAC_{i,m} = H(M_{i,m} \| T_{i,m})$ 。

步驟 1-8：使用者 $U_{i,m}$ 的智慧卡計算 $X_{i,m} = (R_{i,m} \| MAC_{i,m}) \oplus V_{i,m}$ 。

步驟 1-9：使用者 $U_{i,m}$ 將 $X_{i,m}$ 、 $ID_{U_{i,m}}$ 和 $T_{i,m}$ 傳送給遠端的伺服器 S_m 。

步驟 2：使用者 $U_{j,n}$ 登錄到遠端的伺服器 S_n ，使用者、智慧卡和遠端伺服器會共同執行下列步驟：

步驟 2-1：使用者 $U_{j,n}$ 註冊完畢後，當插入智慧卡，輸入通行 $PW_{U_{j,n}}$ 時，智慧卡中所儲存的亂數 $r_{j,n}$ 與伺服器 S_n 身分碼 ID_{S_n} 及使用者 $U_{j,n}$ 輸入通行碼 $PW_{U_{j,n}}$ 進行運算得到值 $A_{j,n}$ 。

步驟 2-2：使用者 $U_{j,n}$ 插入隨身碟，會將隨身碟內的秘密值 $B_{n,j}$ 和智慧卡中所計算出的值 $A_{j,n}$ 進行互斥或運算得到共享的秘密值 $u_{j,n}$ 。

步驟 2-3：使用者 $U_{j,n}$ 的智慧卡計算 $V_{j,n} = g^{u_{j,n}} \bmod p$ 。

步驟 2-4：使用者 $U_{j,n}$ 的智慧卡選取隨機亂數 $a_{j,n} \in_R Z_p^*$ 。

步驟 2-5：使用者$U_{j,n}$的智慧卡計算$R_{j,n} = g^{a_{j,n}} \bmod p$。

步驟 2-6：使用者$U_{j,n}$的智慧卡計算$M_{j,n} = R_{j,n} \| ID_{U_{j,n}}$。

步驟 2-7：使用者$U_{j,n}$的智慧卡計算$MAC_{j,n} = H(M_{j,n} \| T_{j,n})$。

步驟 2-8：使用者$U_{j,n}$的智慧卡計算$X_{j,n} = (R_{j,n} \| MAC_{j,n}) \oplus V_{j,n}$。

步驟 2-9：使用者$U_{j,n}$將$X_{j,n}$、$ID_{U_{j,n}}$和$T_{j,n}$傳送給遠端的伺服器S_n

步驟 3：遠端伺服器S_m鑑別使用者$U_{i,m}$身分的合法性，此時遠端伺服器S_m會執行下列步驟：

步驟 3-1：先利用$u_{m,i}$計算$V_{m,i} = g^{u_{m,i}} \bmod p$。

步驟 3-2：利用$V_{m,i}$將傳送的$X_{i,m}$做互斥或運算後得到$R_{i,m} \| MAC_{i,m} = X_{i,m} \oplus V_{m,i}$。

步驟 3-3：將$R_{i,m}$擷取出來與使用者$U_{i,m}$所傳送過來的$ID_{U_{i,m}}$計算$M_{m,i} = R_{i,m} \| ID_{U_{i,m}}$。

步驟 3-4：將$R_{i,m}$擷取出來與$M_{m,i}$計算$MAC_{m,i} = H(M_{m,i} \| T_{i,m})$。

步驟 3-5：比對計算值$MAC_{m,i}$和所接收擷取出來的值$MAC_{i,m}$是否相等，若相等則可以確認使用者$U_{i,m}$身分的合法性。

步驟 4：遠端伺服器S_n鑑別使用者$U_{j,n}$身分的合法性，此時遠端伺服器S_n會執行下列步驟：

步驟 4-1：先利用$u_{n,j}$計算$V_{n,j} = g^{u_{n,j}} \bmod p$。

步驟 4-2：利用$V_{n,j}$將傳送的$X_{j,n}$做互斥或運算後得到$R_{j,n} \| MAC_{j,n} = X_{j,n} \oplus V_{n,j}$。

步驟 4-3：將$R_{j,n}$擷取出來與使用者$U_{j,n}$所傳送過來的$ID_{U_{j,n}}$計算$M_{n,j} = R_{j,n} \| ID_{U_{j,n}}$。

步驟 4-4：將$R_{j,n}$擷取出來與$M_{n,j}$計算$MAC_{n,j} = H(M_{n,j} \| T_{j,n})$。

步驟 4-5：比對計算值$MAC_{n,j}$和所接收擷取出來的值$MAC_{j,n}$是否相等，若相等則可以確認使用者$U_{j,n}$身分的合法性。

步驟 5：遠端伺服器S_m確認使用者$U_{i,m}$身分的合法性後，會產生對使用者$U_{i,m}$的共享金鑰，此時遠端伺服器S_m會執行下列步驟：

步驟 5-1：選取隨機亂數$b_{m,i} \in_R Z_p^*$。

步驟 5-2：計算$V_{m,i} = g^{b_{m,i}} \bmod p$。

步驟 5-3：對使用者$U_{i,m}$計算共享金鑰$K_{m,i} = (R_{i,m})^{b_{m,i}} = (g^{a_{i,m}} \bmod p)^{b_{m,i}} = g^{a_{i,m}b_{m,i}} \bmod p$

步驟 5-4：利用 CA 給遠端伺服器S_m的簽章計算$\partial_m = Sig_{S_m}(K_{m,i})$

步驟 5-5：將∂_m和$Cert_{S_m}$傳送給遠端伺服器S_n進行驗證。

步驟 6：遠端伺服器S_n確認使用者$U_{j,n}$身分的合法性後，會產生對使用者$U_{j,n}$的共享金鑰，此時遠端伺服器S_n會執行下列步驟

步驟 6-1：選取隨機亂數$b_{n,j} \in_R Z_p^*$。

步驟 6-2：計算$V_{n,j} = g^{b_{n,j}} \bmod p$。

步驟 6-3：對使用者$U_{j,n}$計算共享金鑰$K_{n,j}=(R_{j,n})^{b_{n,j}}=(g^{a_{j,n}} \bmod p)^{b_{n,j}}=g^{a_{j,n}b_{n,j}} \bmod p$

步驟 6-4：利用 CA 給遠端伺服器S_n的簽章計算$\partial_n=Sig_{S_n}(K_{n,j})$

步驟 6-5：將∂_n和$Cert_{S_n}$傳送給遠端伺服器S_m進行驗證。

步驟 7：遠端伺服器S_m先驗證遠端伺服器S_n所傳送的∂_n和$Cert_{S_n}$，確認遠端伺服器S_n身分後，利用所傳送的值計算共享金鑰，此時遠端伺服器S_m會執行下列步驟：

步驟 7-1：遠端伺服器S_m利用 CA 的公開金鑰驗證遠端伺服器S_n所傳送的∂_n和$Cert_{S_n}$，以確認遠端伺服器S_n的身分。

步驟 7-2：利用遠端伺服器S_n傳送的值對使用者$U_{i,m}$計算公開金鑰
$Y_{m,i}=(K_{n,j})^{b_{m,i}}=(g^{a_{j,n}b_{n,j}} \bmod p)^{b_{m,i}}=g^{a_{j,n}b_{m,i}b_{n,j}} \bmod p$

步驟 7-3：對使用者$U_{i,m}$計算：$\beta_{m,i}=H(K_{m,i} \| Y_{m,i} \| ID_{U_{i,m}} \| ID_{S_m})$

步驟 7-4：對使用者$U_{i,m}$計算：$\theta_{m,i}=E_{R_{i,m}}(V_{m,i},Y_{m,i},\beta_{m,i})$

步驟 7-5：將值$\theta_{m,i}$傳送給使用者$U_{i,m}$。

步驟 8：遠端伺服器S_n先驗證遠端伺服器S_m所傳送的∂_m和$Cert_{S_m}$，確認遠端伺服器S_m身分後，利用所傳送的值計算共享金鑰，此時遠端伺服器S_n會執行下列步驟：

步驟 8-1：遠端伺服器S_n利用 CA 的公開金鑰驗證遠端伺服器S_m所傳送的∂_m和$Cert_{S_m}$，以確認遠端伺服器S_m的身分。

步驟 8-2：利用遠端伺服器S_m傳送的值對使用者$U_{j,n}$計算公開金鑰：
$Y_{n,j}=(K_{m,i})^{b_{n,j}}=(g^{a_{i,m}b_{m,i}} \bmod p)^{b_{n,j}}=g^{a_{i,m}b_{m,i}b_{n,j}} \bmod p$

步驟 8-3：對使用者$U_{j,n}$計算：$\beta_{n,j}=H(K_{n,j} \| Y_{n,j} \| ID_{U_{j,n}} \| ID_{S_n})$

步驟 8-4：對使用者$U_{j,n}$計算：$\theta_{n,j}=E_{R_{j,n}}(V_{n,j},Y_{n,j},\beta_{n,j})$

步驟 8-5：將值$\theta_{n,j}$傳送給使用者$U_{j,n}$。

步驟 9：使用者$U_{i,m}$鑑別遠端伺服器S_m的身分並驗證彼此的共享金鑰，此時智慧卡會執行下列步驟：

步驟 9-1：使用者$U_{i,m}$的智慧卡在收到遠端伺服器S_m回傳的值$\theta_{m,i}$後，以$R_{i,m}$解密得到值$(V_{m,i},Y_{m,i},\beta_{m,i})$。

步驟 9-2：使用者$U_{i,m}$的智慧卡計算與遠端伺服器S_m的共享金鑰
$K_{i,m}=(V_{m,i})^{a_{i,m}}=(g^{b_{m,i}} \bmod p)^{a_{i,m}}=g^{a_{i,m}b_{m,i}} \bmod p$。

步驟 9-3：使用者$U_{i,k}$的智慧卡計算$\beta_{i,m}=H(K_{i,m} \| Y_{m,i} \| ID_{U_{i,m}} \| ID_{S_m})$

步驟 9-4：使用者$U_{i,m}$的智慧卡驗證計算值$\beta_{i,m}$和所接收擷取出來的值$\beta_{m,i}$是否相等，若相等則可以確認使用者$U_{i,m}$和遠端伺服器S_m擁有相同的共享金鑰。

步驟 9-5：使用者$U_{i,m}$的智慧卡將遠端伺服器S_m傳送的$K_{m,i}$擷取出來，計算屬於使用者$U_{i,m}$的私密金鑰$Y_i=(Y_{m,i})^{a_{i,m}}=(g^{a_{j,n}b_{n,j}b_{m,i}} \bmod p)^{a_{i,m}}=g^{a_{i,m}a_{j,n}b_{m,i}b_{n,j}} \bmod p$

步驟 10：使用者$U_{j,n}$鑑別遠端伺服器S_n的身分並驗證彼此的共享金鑰，此時智慧卡會執行下列步驟：

步驟 10-1：使用者$U_{j,n}$的智慧卡在收到遠端伺服器S_n回傳的值$\theta_{n,j}$後，以$R_{j,n}$解密得到值$(V_{n,j},Y_{n,j},\beta_{n,j})$。

步驟 10-2：使用者$U_{j,n}$的智慧卡計算與遠端伺服器S_n的共享金鑰$K_{j,n}=(V_{n,j})^{a_{j,n}}=(g^{b_{n,j}} \bmod p)^{a_{j,n}}=g^{a_{j,n}b_{n,j}} \bmod p$。

步驟 10-3：使用者$U_{j,n}$的智慧卡計算$\beta_{j,n}=H(K_{j,n} \| Y_{n,j} \| ID_{U_{j,n}} \| ID_{S_n})$

步驟 10-4：使用者$U_{j,n}$的智慧卡驗證計算值$\beta_{j,n}$和所接收擷取出來的值$\beta_{n,j}$是否相等，若相等則可以確認使用者$U_{j,n}$和遠端伺服器S_n擁有相同的共享金鑰。

步驟 10-5：使用者$U_{j,n}$的智慧卡將遠端伺服器S_n傳送的$K_{n,j}$擷取出來，計算屬於使用者$U_{j,n}$的私密金鑰$Y_j=(Y_{n,j})^{a_{j,n}}=(g^{a_{i,m}b_{m,i}b_{n,j}} \bmod p)^{a_{j,n}}=g^{a_{i,m}a_{j,n}b_{m,i}b_{n,j}} \bmod p$

步驟 11：驗證使用者$U_{i,m}$的私密金鑰Y_i與使用者$U_{j,n}$的私密金鑰Y_j是否相等，若相等則使用者$U_{i,m}$與使用者$U_{j,n}$可建立專屬於雙方的私有通道傳達訊息。

四、通行碼變更階段

在通行碼變更階段，使用者$U_{i,m}$、$U_{j,n}$和智慧卡$SC_{i,m}$、$SC_{j,n}$會執行下列步驟，完成變更使用者通行碼程序，由於不同使用者和智慧卡的變更程序步驟均相同，在此僅以使用者$U_{i,m}$和智慧卡$SC_{i,m}$的變更程序步驟為例加以說明。

步驟 1：使用者$U_{i,m}$將智慧卡$SC_{i,m}$插入，輸入 PIN 碼啟動智慧卡$SC_{i,m}$，將智慧卡中的隨機亂數$r_{i,m}$和$A_{i,m}$取出。

步驟 2：使用者將$A_{i,m}$值內的原通行碼$PW_{U_{i,m}}$變更成新的通行碼$PW'_{U_{i,m}}$，並利用單向雜湊函數重新計算成為$A'_{i,m}$值。

步驟 3：將更新通行碼後的$A'_{i,m}$值回存智慧卡內。

肆、安全性暨功能性分析

本節將探討與分析我們提出方法的安全性與功能性，並與多重伺服器環境下達到安全性的相關研究加以分析比較，以驗證我們提出方法確實可改進面臨註冊中心擁有不合理權限的安全性等問題。我們所提出的可鑑別金鑰交換協定是植基於離散對數問題（discrete logarithm problem，簡稱 DLP）與單向雜湊函數 （one-way hash function，簡稱 OWHF）的密碼假設，除可以滿足金鑰交換之機密性、鑑別性與完整性三項安全要求，

將針對通行碼安全性、交談金鑰安全性、使用者身分鑑別性、伺服器身分鑑別性、多重伺服器通行碼的安全性、不同伺服器之間身分的鑑別性等進行分析及探討。

一、通行碼安全性分析

1.通行碼猜測攻擊（password guessing attack）

假設遠端伺服器 S_k 內部某管理者為攻擊者 U_{att}，其利用本身權限取得使用者 $U_{i,k}$ 在註冊階段的 $A_{i,k}$ 值，欲猜測其通行碼 $PW_{U_{i,k}}$，則攻擊者 U_{att} 如果想要得到 $U_{i,k}$ 的通行碼 $PW_{U_{i,k}}$，最簡單的方法就是利用使用者在註冊階段所傳送的 $A_{i,k}=H(PW_{U_{i,k}})\oplus H(r_{i,k}\|ID_{S_k})$ 值進行猜測推算，但當進行猜測通行碼 $PW_{U_{i,k}}$ 時，攻擊者將面臨 OWHF 問題，無法猜測逆推得到通行碼。

2.通行碼破解攻擊

假設遠端伺服器 S_k 內部某管理者為攻擊者 U_{att}，當攻擊者 U_{att} 利用已知的 ID_{S_j} 及登入階段的 $X_{i,k}$ 值、$ID_{U_{i,k}}$ 和 $T_{i,k}$ 值，欲破解其通行碼 $PW_{U_{i,k}}$，則攻擊者 U_{att} 必須利用使用者在登入階段所傳送的 $X_{i,k}=(R_{i,k}\|MAC_{i,k})\oplus V_{i,k}$ 值進行通行碼 $PW_{U_{i,k}}$ 破解，但欲破解通行碼時，攻擊者必須先推導出 $V_{i,k}$ 值，此時會面臨到互斥或運算問題。假設攻擊者想破解得知 $V_{i,k}$ 值，仍須將 $u_{k,i}$ 值推導出來，此時攻擊者就必須面臨 $V_{i,k}=g^{u_{k,i}} \bmod p$ 的 DLP 問題。

二、交談金鑰安全性分析

1.交談金鑰安全性

當使用者 $U_{i,k}$ 或遠端伺服器 S_k 不小心洩漏彼此的密文 $\theta_{k,i}$ 時，攻擊者 U_{att} 有機會截取獲得密文 $\theta_{k,i}$，攻擊者若欲利用此一訊息破解雙方的交談金鑰，由於交談金鑰之密文 $\theta_{k,i}=E_{R_{i,k}}(V_k,K_{k,j},\beta_{k,i})$ 是利用 $R_{i,k}$ 將交談金鑰 $K_{k,j}$ 等資訊加密傳送，因此，攻擊者欲取得交談金鑰 $K_{k,j}$ 時，其必須先得到 $R_{i,k}$ 再從 $\theta_{k,i}$ 得到 $K_{k,j}$。然而，攻擊者欲得到 $R_{i,k}$ 時，須先得 $V_{i,k}$，欲得到 $V_{i,k}$ 必須先得到 $u_{k,i}$，欲得到 $u_{k,i}$ 則須得到 $B_{k,i}$ 及 $A_{i,k}$，此安全性乃基於通行碼安全性，有關通行碼安全性已於前述討論分析過，已證明攻擊無法成功。

2.前推安全性

假設使用者$U_{i,k}$或遠端伺服器S_k不小心洩漏彼此的密文$\theta_{k,i}$及交談金鑰$K_{k,j}$，攻擊者U_{att}截獲取得$\theta_{k,i}$及$K_{k,j}$後，攻擊者欲利用此訊息去推導出之前的交談金鑰，則因$K_{k,j}=(R_{j,k})^{b_k}=g^{a_{j,k}b_k} \bmod p$，而每次的交談金鑰是由使用者與遠端伺服器各自產生的隨機亂數$a_{j,k}$與b_k所組成，而亂數與亂數之間是各自獨立且無關連性的，因此所計算出來的交談金鑰彼此之間也無任何關連，所以攻擊者想利用此一方式去推算其他交談金鑰是不可行的。攻擊者如果仍想要破解交談金鑰$K_{k,j}$時，就必須得分別破解隨機亂數，當攻擊者要破解隨機亂數$a_{j,k}$與b_k時，又得面臨到 DLP 問題。

三、使用者身分鑑別性分析

攻擊者若想發動假冒使用者身分攻擊，企圖假冒使用者登入遠端伺服器後，並與其他使用者進行通訊或資料交換，則攻擊者必須從使用者與遠端伺服器所交談的訊息中截取相關資訊，並藉此推算出$PW_{U_{i,k}}$，此種方式屬於通行碼猜測攻擊，經由前述討論已知此種攻擊將面臨 OWHF 問題。另一種方式則是攻擊者直接破解使用者的$PW_{U_{i,k}}$，以取得使用者的合法身份，但此種方式屬於通行碼破解攻擊，經由前述討論已知此種攻擊將面臨 DLP 問題。而無論是那種攻擊方式，攻擊者都會面臨到通行碼的安全性而無法進行，這些方式已於之前討論分析過，已證明攻擊無法成功。

四、伺服器身分鑑別性分析

攻擊者若想發動假冒伺服器身分攻擊，攻擊者U_{att}企圖假冒遠端伺服器S_j的身份，與其他使用者進行通訊或資料交換，則攻擊者必須通過身分驗證式$\beta_{j,k}=H(K_{j,k}\|K_{k,i}\|ID_{U_{j,k}}\|ID_{S_k})$，因為$\beta_{j,k}$主要由二把交談金鑰所組成，即$K_{i,k}$及$K_{k,j}$，其意指安全性將基於交談金鑰的安全性，有關交談金鑰安全性已於前述討論分析過，已證明攻擊無法成功。

五、不同伺服器通行碼的安全性分析

假設攻擊者U_{att}為不同伺服器的其中一台遠端伺服器S_m內部的某管理者，其欲利用另一台遠端伺服器S_n傳送的已知資訊，來猜測或破解使用者$U_{j,n}$的通行碼，而不同的遠端伺服器S_m和S_n之間所傳遞的訊息為$\partial_n = Sig_{S_n}(K_{n,j})$，其訊息內容與使用者通行碼無關，因此其通行碼的安全性乃基於相同伺服器的通行碼安全性分析，有關通行碼安全性已於前述討論分析過，已證明攻擊無法成功。

六、不同伺服器交談金鑰的安全性分析

我們所提出方法之交談金鑰乃基於 Diffie-Hellman 金鑰交換協定，有關交談金鑰安全性已於前述討論分析過，已證明相關攻擊無法成功。

七、不同伺服器間的身分鑑別性分析

我們所提出方法為不同伺服器間的身分鑑別，主要基於公開金鑰基礎架構（Public Key Infrastructure, PKI）之數位簽章，所以其安全性乃植基為 PKI 之數位簽章的安全性，本文不再贅述。

伍、結論

如何讓合法使用者僅需記憶一組簡單的通行碼即可向不同的遠端伺服器註冊與登錄，以取得資源或服務，採用以通行碼為基底之可鑑別金鑰交換方式是一種相當普遍的作法。我們提出一個適用於多重伺服器環境下，結合智慧卡與通行碼的雙因子身分鑑別協定，除了可以滿足鑑別金鑰交換協定特性外，並允許使用者使用單一且具可記憶之通行碼註冊並登錄不同伺服器，以達到同網域（intra-domain）的三方通訊及跨網域（inter-domain）的四方通訊知目的。

我們所提出適用於多重伺服器架構之可鑑別金鑰交換機制兼具安全性與完整性觀點，未來則可納入使用者權限管控與伺服器資源管理等相關議題，探討何種身份的使用者可以取得多大的權限去存取伺服器的資源及服務，而且為避免使用者長期佔用資源，造成其他人無法取得服務，在伺服器資源管理運用方面也是可以列入研究考量的議題。

參考文獻

[1] S.M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," *Proceedings of the IEEE Computer Society Conference*, pp. 72-84, 1992.

[2] C.M. Chen and W.C. Ku, "Stolen-Verifier Attack on Two New Strong-Password Authentication Protocols," *IEICE Transaction on Communication*, Vol. E85-B, No. 11, pp. 2519-2521, 2004.

[3] C.C. Chang and J.Y. Kuo, "An Efficient Multi-Server Password Authenticated Key Agreement Scheme Using Smart Cards with Access Control," *IEEE International Conference on Advanced Information Networking and Applications (AINA 2005)*, Vol. 2, No. 56, pp. 257-260 , 2005.

[4] W. Diffie, and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 644-654, 1976.

[5] Y. Ding and P. Horster, "Undetectable on-line password guessing attacks," *ACM Operating System Review*, Vol. 29, No. 4, pp. 77-86,1995.

[6] M.S. Hwang and L.H. Li, "A New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactons on Comsumer Electronics*, Vol. 46, No. 1, pp. 28-30, 2000.

[7] R.J. Hwang and S.H. Shiau, "Provably Efficient Authenticated Key Agreement Protocol for Multi-Servers," *The Computer Journal*, Vol. 50, No. 5, pp. 602-615, 2007.

[8] W.S. Juang, "Efficient Multi-Server Password Authentication Key Agreement Using Smart Cards," *IEEE Transaction on Consumer Electronics*, Vol.50, No. 1, pp. 251-255, 2004.

[9] W.C. Ku, H.C. Tsai and S.M. Chen, "Two Simple Attack on Lin-Shen-Hwang's Strong-Password Authentication Protocol," *ACM Operating Systems Review*, Vol. b37, No. 4, pp. 26-31, 2003.

[10] L. Lamport, "Password Authentication with Insecure Communication," *Communications of the ACM*, Vol. 24, No. 11, pp. 770-772, 1981.

[11] S.W. Lee, H.S. Kim and K.Y. Yoo, "Efficient verifier-based key agreement protocol for three parties without server's public key," *Applied Mathematics and Computation*, Vol. 167, No. 1, pp. 996-1003,2005.

[12] C.L. Lin, H.M. Sun and T. Hwang, "Three-party encrypted key exchange: attacks and a solution," A*CM Operating Systems Review*, Vol. 34, No. 4, pp. 12-20,2000.

[13] C.W. Lin, J.J. Shen and M.S. Hwang, "Security Enhancement for Optimal Strong-Password Authentication Protocol," *ACM Operating Systems Review*, Vol. 37, No. 2, pp. 7-12, 2003.

[14] C.L. Lin, H.M. Sun, M. Steiner and T. Hwang, "Three-party encrypted key exchange without server public-keys," *Publisher Item Identifier S11072*, pp. 1089-7798, 2001.

[15] J. Nam, S. Kim and D. Won, "A weakness in Sun-Chen-Hwang three-party key agreement protocols using passwords," *The Journal of Systems and Software*, Vol. 75, pp. 63-68, 2004.

[16] G. Popek and C. Kline, "Encryption and secure computer networks," *ACM Computing Surveys*, Vol. 11, No. 4, 1979.

[17] H.M. Sun, B.C. Chen and T. Hwang, "Secure key agreement protocols for three-party against guessing attack," *The Journal of Systems and Software*, Vol. 75, No. 1-2, pp. 63-68, 2003.

[18] A. Shimizu, "A Dynamic Password Authentication Method by One-way Function," *IEICE Transactions on Communications*, Vol. J73-D-I, No. 7, pp. 630-636, 1990.

[19] M. Sandirigama, A. Shimizu and M.T Noda, "Simple and Secure Password Authentication Protocol（SAS）," *IEICE Transaction on Communications*, Vol. 83, No. 6, pp. 1363-1365, 2000.

[20] W. Stallings, *Cryptography and Network Security: Principles and Practices*, Pearson Education International, Third Edition, 2000.

[21] M. Steiner, G. Tsudik and M. Waidner, "Refinement and extension of encrypted key exchange," *ACM Operating Systems Review*, Vol. 29, No. 3, pp. 22-30,1995.

[22] H.M. Sun, "An Efficient Remote Use Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, Vol. 46, No. 4, pp. 958-961, 2000.

[23] T. Tsuji, T. Kamioka and A. Shimizu, "Simple and Secure Password Authentication Protocol, Ver2.（SAS-2）," *IEICE Technical Report*, OIS2002-30, 2002.

[24] T. Tsuji and A. Shimizu, "An Impersonation Attack on One-Time Password Authentication Protocol OSPA," *IEICE Transaction on Communication*, Vol. E86-B, No. 7, pp. 2182-2185, 2004.

[25] K. Tan and H. Zhu, "Remote User Authentication Scheme Using Smart Cards," *Computer Communications*, Vol. 46, No. 4, pp. 390-393, 1999.

[26] S.J. Wang, and J.F. Chang, "Smart Card Based Secure Password Authentication Scheme," *Computers and Security*,Vol. 15, No. 3, pp. 231-237, 1996.

[27] W.H. Yang and S.P. Shieh, "Password Authentication Schemes with Smart Cards," *Computers and Security*, Vol. 18, No. 8, pp. 727-733, 1999.

[28] 張國義，"可驗證的三方通訊金鑰交換協定之研究"，*佛光大學資訊管理學系碩士學位論文*，2005年。

[29] 陳建仁，"適用於多重伺服器環境之可鑑別金鑰交換協定"，*長庚大學資訊管理研究所碩士學位論文*，2008年。

[30] 許沁如，"結合智慧卡之通行碼認證機制研究"，*世新大學資訊管理學系碩士學位論文*，2004年。