具效率性之通行碼認證及金鑰交換機制

Efficient password authentication and key exchange protocol

吳宗杉
國立台灣海洋大學資訊工程學系
ilan543@gmail.com
陳益森
國立台灣海洋大學資訊工程學系
j1010958@trts.dorts.gov.tw
許令芷
佛光大學資訊學系
lisahsu@ncic.com.tw
黃世豪
佛光大學資訊學系
hao.430@gmail.com

摘要

網際網路提供的服務不勝枚舉，各種資訊安全的攻擊也接踵而至。使用者透過遠端伺服器存取電腦資源，先確認溝通雙方的身份，是網路安全考量的議題之一。本研究應用智慧卡儲存使用者資訊及微量運算的功能，提出通行碼認證與金鑰交換的方法，可達到使用者與伺服器之間雙向認證，產生互相通訊的交談金鑰，並做有效期限的控制。歸納具有以下特性：1.伺服器不需要儲存認證資料；2.使用者可自行選擇通行碼；3.達到雙向認證；4.產生交談金鑰；5.可控制使用期限；6.運算成本低且效率佳。

關鍵詞：智慧卡、交談金鑰、雙向認證、通行碼

ABSTRACT

Internet provides various services enabling the convenience of human life. However, it accompanies a verity of information security attacks. Before having access to the computer resources in remote site, it is one of the important issues in network security considerations to have a mutual authentication of the communicating entities. We proposed a new method of password authentication and key exchange protocol with smart card in this paper. The proposed scheme has the following characteristics: 1. it is not required for the server to store any authentication data for users; 2. users can freely choose their own passwords; 3. it meets the requirement of mutual authentication; 4. the communicating parties can exchange one common session key; 5. it provides the control expiration; 6. the computation complexity of the scheme is low as compared with other previously proposed ones and thus gain computing efficiency.

Keyword: Smart card, Session key, Mutual authentication, Password

1. 前言

資訊科技迅速的發展，許多資訊都透過共通的網路傳遞，使用者很容易取得網路上傳送的資訊，使得個人隱私遭受極大的威脅，使用資訊安全技術來防禦各式各樣的攻擊是刻不容緩的。在開放的網路環境下，遠端資源的所提供的服務及存取控制面臨著安全上的挑戰，網際網路的資源並非提供給所有使者任意使用，有些服務是必須付費或是經過註冊。目前遠端系統服務機制，提供使用者與伺服器之間相互驗證，使用的方法簡單、便利，因此廣受歡迎。

1981 年，Lamport [8] 提出通過不安全通道使用者遠端驗證機制後，即有相關研究被提出發表，Lamport 所提出的機制，需要在伺服器存放一個驗證表格，當使用者登入時，驗證是否為合法使用者，可以抵抗重送攻擊，但是存在密碼驗證表格遭受竊取的危機。在 1993 年 Chang and Wu [2] 提出智慧卡的應用，主要特色是可以任意選用密碼。於 2000 年，Hwang and Li [6] 提出一個利用智慧卡的使用者遠端確認機制，毋需在伺服器存放一個密碼驗證表，避免驗證表被竊取，針對 Lamport 所提出之機制的弱點加以改良。之後，Sun [12] 提出可以改善 Hwang and Li 效能的遠端使用者驗證機制，但是使用者無法任意選擇或是改變密碼。2002 年 Chien 等人 [4] 以及 2003 年 Wu 和 Chieu [14] 等指出 Sun 所提出機制的弱點：1.不能讓使用者自由選擇密碼。2.無法達到雙方認證。並根據上述弱點加以改良。但 Chien 等人的方法沒有產生交談金鑰，而 Wu 和 Chieu 的方法，容易遭受重送攻擊以及沒有達到雙向身份驗證在安全上仍然有些缺失。

2004 年 Juang [7] 提出可以達成雙向認證，使用對稱式加解密的方式，產生交談金鑰的機制，在安全上的缺點為：每次產生交談金鑰之前，皆使用同一把金鑰做加解密。2005 年 Chen-Yeh [3] 提出一個亂數基底 (nonce-based) 的身份認證協定，亦可提供雙向認證及會議密鑰協議 (session key agreement) 的功能，但於登入階段，使用者傳送訊息給伺服器時，伺服器無法立即確認是否為合法使用者，容易遭受阻斷服務 (Denial of Service, DOS) 攻擊。2006 年 Liaw 等人 [10] 提出的機制，可以達到 Chen-Yeh 的功能，但是在產生交談金鑰階段，使用公鑰加密的方法，效率不佳。本文保留 Juang 和 Chen-Yeh 機制的優點，改善他們在安全上的缺失，提出通行碼認證及金鑰交換機制，並且控制智慧卡的使用期限，讓使用者遠端認機制更安全且有效率。

在第 2 章節中，依序介紹 Juang、Chen 和 Yeh 及 Liaw 等人的身分認證機制。第 3 章節，提出一個具效率性身份認證及金鑰交換方法。在第 4 章節，為所提的機制，做安全上的分析及效率上的比較。最後章節針對本論文做一簡單的為結論。

2. 相關文獻

在近幾年，許多學者陸續提出各種使用智慧卡之使用者認證機制，本章將分 2.1~2.3 節來介紹三個認證機制，並分三個階段來討論，分為初始階段、註冊階段、登入階段。

2.1 Juang 認證機制

在 2004 年，Juang [7] 發表一個使用智慧卡的認證機制，它提供雙向認證與金鑰交換，而且伺服器不需要儲存任何驗證表格，在安全上的缺點為，同一個使用者，

在登錄階段，每次都使用同一把金鑰做加解密，之後產生交談金鑰。其方法詳述如下：

[初始階段]

在此階段，系統需先設定以下參數：

U_i：第 i 位使用者並擁有自己的識別碼 ID_i 和通行碼 PW_i。

S：伺服器

x：伺服器的秘密金鑰。

$E_k(m)$：表示使用秘密金鑰 k，對訊息 m 做加密。

$D_k(m)$：表示使用秘密金鑰 k，對訊息 m 做解密。

$h(\,)$：為單向雜湊函數。

[註冊階段]

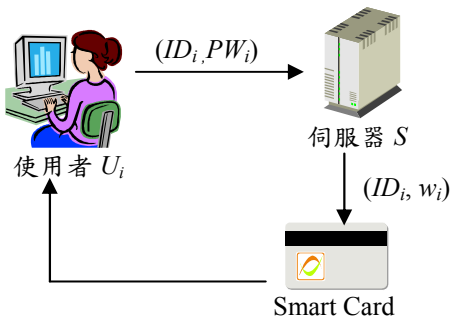
當使用者 U_i 要向伺服器 S 註冊時，使用者 U_i 傳送自己的 ID_i 和 PW_i 給伺服器 S，若伺服器接受使用者的需求，將執行以下步驟 (如圖一所示)：

步驟一：計算使用者 U_i 的秘密資訊，其中

$$v_i = h(ID_i, x) \qquad (1)$$

$$w_i = v_i \oplus PW_i \qquad (2)$$

步驟二：伺服器 S 將 ID_i 和 w_i 儲存到智慧卡，並配發給使用者 U_i。



圖一　Juang 方法註冊階段

[登入階段]

此階段運作 (如圖二所示)，當使用者 U_i 要登入系統時，將智慧卡插入讀卡機，透過終端設備輸入 ID_i 和 PW_i。假設為第 j 次登入伺服器，於是智慧卡會進行以下步驟：

步驟一：首先利用使用者輸入的 PW_i 計算

$$v_i = w_i \oplus PW_i \qquad (3)$$

步驟二：隨機選取二個亂數分別為 ru_j 和 N_1，使用 v_i 為加密金鑰，加密訊息如下

$$E_{v_i}(ru_j, h(\mathrm{ID}_i \| N_1)) \qquad (4)$$

步驟三：$\{N_1, ID_i, E_{v_i}(ru_j, h(ID_i \| N_1))\}$ 訊息，傳送遠端伺服器。

遠端伺服器收到登入訊息時，驗證使用 U_i 是否為合法的使用者，執行以下的步驟：

步驟一：計算 v_i 如(1)，接著計算

$$D_{v_i}(E_{v_i}(ru_j, h(\mathrm{ID}_i \| N_1))) \qquad (5)$$

步驟二：檢查 $h(ID_i \| N_1)$ 和 N_1 是否合法，如果 N_1 不是新的，或者 $h(ID_i \| N_1)$ 不正確，則拒絕使用者登入。

步驟三：隨機選取一個亂數分別為 rs_j 使用 v_i 為加密金鑰，加密訊息，並將訊息傳給使用者 U_i

$$E_{v_i}(rs_j, N_1 + 1, N_2) \qquad (6)$$

步驟四：計算雙方第 j 次的交談金鑰

$$k_j = h(ru_j, rs_j, v_i) \qquad (7)$$

結束上述步驟，確認使用者 U_i 通過驗證後，遠端伺服器 S 與使用者 U_i，分別執行以下步驟：

步驟一：當使用者接收到伺服器 S 傳送的訊息，首先計算

$$D_{v_i}(E_{v_i}(rs_j, N_1+1, N_2)) \qquad (8)$$

步驟二：檢查 N_1+1 是否為正確，如果正確，則計算雙方第 j 次的交談金鑰 k_j 如(7)

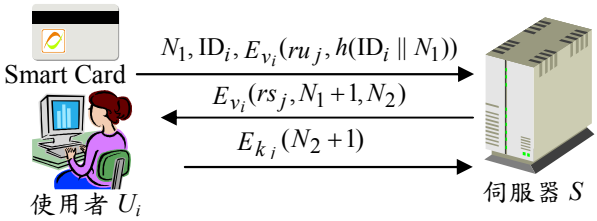
步驟三：使用 k_j 為加密金鑰，加密訊息，並將訊息傳給伺服器 S

$$E_{k_j}(N_2+1) \qquad (9)$$

步驟四：伺服器計算

$$D_{k_j}(E_{k_j}(N_2+1)) \qquad (10)$$

步驟五：檢查 N_2+1 是否正確，若正確雙方就建立起彼此溝通的交換金鑰 k_j。



圖二 Juang 方法登入階段

2.2. Chen-Yeh 認證機制

在 2005 年，Chen-Yeh [3] 提出一個高效率亂數基底 (nonce-based) 的身份認證協定，它保留 Juang 所提出方法的優點，但登入階段，使用者傳送訊息給伺服訊息時，伺服器無法確認使用者是否合法，所以遭受阻斷攻擊。其方法詳述如下：

[初始階段]

在此階段，先設定以下參數：

U_u：第 u 位使用者並擁有自己的識別碼 ID_u 和通行碼 PW_u。

S：伺服器。

x：伺服器的秘密金鑰。

$h(\,)$：為單向雜湊函數。

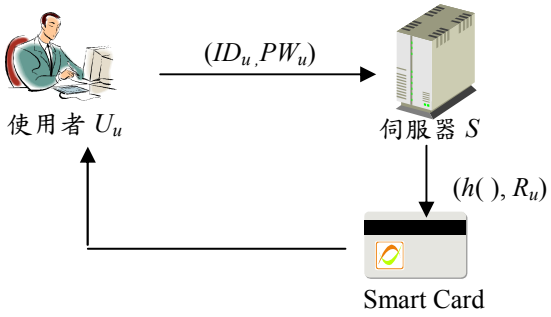
[註冊階段]

註冊階段是由伺服器來執行，在使用者註冊被接受後，伺服器將配發智慧卡給使用者。當一個新的使用者 U_u 要向伺服器 S 註冊為合法的使用者時，首先，使用者 U_u 必須傳送自己的 ID_u 和容易記憶的通行碼 PW_u 給伺服器 S，若伺服器接受使用者的需求，將執行以下步驟 (如圖三所示)：

步驟一：計算使用者 U_u 的秘密資訊，其中

$$R_u = h(ID_u \oplus x) \oplus PW_u \qquad (11)$$

步驟二：伺服器將 $h(\,)$ 和 R_u 儲存到智慧卡，並配發給使用者 U_u。



圖三 Chen-Yen 方法註冊階段

[登入階段]

此階段的運作 (如圖四所示)，當一個合法的使用者 U_u 要存取伺服器提供的服務時，將智慧卡插入讀卡機，透過終端設備輸入 ID_u 和 PW_u。於是智慧卡會進行以下步驟：

步驟一：首先利用使用者輸入的 PW_i 計算

$$h(ID_u \oplus x) \leftarrow R_u \oplus PW_u \qquad (12)$$

步驟二：讀卡機隨機選取一個亂數值為 N_c，計算 M_1

$$M_1 = h^2(ID_u \oplus x) \oplus N_c \quad (13)$$

步驟三：使用者 U_u，傳送訊息 (ID_u, M_1) 給遠端伺服器 S。

在交換認證訊息上，使用二個亂數值，一個亂數值是由讀卡機任選，產生在使用者登入時，另一個是由伺服器任選，因此，二個亂數值可以保護認證的訊息，和每個經過身份認證的參與者。在遠端伺服器收到登入訊息時，執行以下的步驟：

步驟一：收到登入訊息 (ID_u, M_1) 後，計算

$$h^2(ID_u \oplus x) \quad (14)$$

$$N_c \leftarrow M_1 \oplus h^2(ID_u \oplus x) \quad (15)$$

步驟二：伺服器產生一個新的亂數值 N_s，接著計算

$$M_2 = h(h(ID_u \oplus x) \oplus N_c) \oplus N_s \quad (16)$$

$$M_3 = h(h(ID_u \oplus x) \| N_c \| N_s) \quad (17)$$

步驟三：伺服器 S 將訊息 (M_2, M_3) 傳給使用者 U_u。

使用者 U_i 與遠端伺服器 S，分別執行以下步驟：

步驟一：當接收到伺服器 S 訊息 (M_2, M_3) 時，使用者 U_u 首先計算

$$h(h(ID_u \oplus x) \oplus N_c) \quad (18)$$

$$N_s \leftarrow M_2 \oplus h(h(ID_u \oplus x) \oplus N_c) \quad (19)$$

步驟二：驗證伺服器 S，是否確切的知道 N_c，使用者 U_u 更進一步檢查

$$M_3 \stackrel{?}{=} h(h(ID_u \oplus x) \| N_c \| N_s) \quad (20)$$

步驟三：若上述式子相等，則使用者 U_u 確認伺服器 S 是合法非冒充或偽裝，進一步計算 M_4，並傳送訊息給伺服器 S

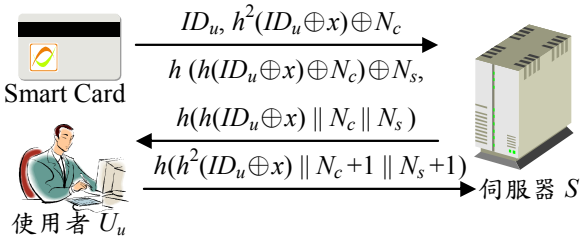
$$M_4 = h(h^2(ID_u \oplus x) \| N_c + 1 \| N_s + 1) \quad (21)$$

步驟四：伺服器驗證 M_4 是否正確，計算

$$M_4 \stackrel{?}{=} h(h^2(ID_u \oplus x) \| N_c + 1 \| N_s + 1) \quad (22)$$

步驟五：若步驟四驗證正確，則雙方分別計算彼溝通的交換金鑰 SK。

$$SK = h(h^3(ID_u \oplus x) \| N_c + 2 \| N_s + 2) \quad (23)$$



圖四 Chen-Yeh 方法登入階段

2.3. Liaw 等人認證機制

在 2006 年，Liaw [10] 提出使用智慧卡具效率性和完整性的通行碼認證方法，它的安全性是建構在單向雜湊函數和亂數基底 (nonce-based) 上。使用亂數基底的方法，因亂數值不會跟之前使用過的數值有重覆，可以避免重送攻擊，並且沒有時間同步的問題。但是 Liaw 等人所提出的方法，在產生交談金鑰時，使用公鑰加密的方法，比使用私鑰加密或是單向雜湊函數，需要更多的運算時間，效率較差，其方法詳述如下：

[初始階段]

在此階段，先設定以下參數：

U_i：第 i 位使用者並擁有自己的識別碼 ID_i 和通行碼 PW_i。

S：遠端系統

x：伺服器的秘密金鑰。

$h(\,)$：為單向雜湊函數。

q：大質數。

[註冊階段]

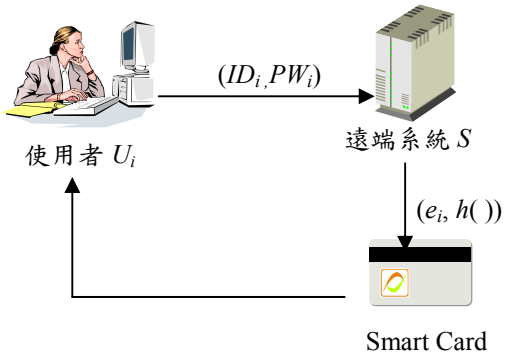
使用者 U_i 要向遠端系統 S 註冊時，使用者 U_i 傳送自己的 ID_i 和 PW_i 給遠端系統 S，當遠端系統接受到訊息之後，將執行以下步驟：

步驟一：計算使用者 U_i 的秘密資訊，其中

$$v_i = h(ID_i, x) \qquad (24)$$

$$e_i = v_i \oplus PW_i \qquad (25)$$

步驟二：遠端系統 S 將 e_i 和 $h(\,)$ 儲存到智慧卡，並配發給使用者 U_i。



圖五 Liaw 等人方法註冊階段

[登入階段]

當使用者 U_i 想要登入遠端系統 S 時，必須將智慧卡插入讀卡機，透過終端設備輸入 ID_i 和 PW_i。於是智慧卡會進行以下步驟：

步驟一：首先產生一個亂數 N_i。

步驟二：計算 C

$$C = h(e_i \oplus PW_i, N_i) \qquad (26)$$

步驟三：使用者 U_i，傳送訊息 (ID_i, C, N_i) 給遠端系統 S。

在遠端系統接收到認證需求的訊息 (ID_i, C, N_i) 之後，使用者 U_i 與遠端系統 S 進行相互認證，由遠端系統執行以下的步驟：

步驟一：檢查 ID_i 是否合法，如果不合法，則拒絕使用者 U_i 的需求。

步驟二：計算 v_i' 同(24)，檢查 C

$$C \stackrel{?}{=} h(v_i', N_i) \qquad (27)$$

如果不相等則拒絕需求，否則執行以下步驟。

步驟三：產生一個亂數 N_s。

步驟四：使用 v_i 為加密金鑰，加密訊息，並將訊息傳給智慧卡。

$$M = E_{v_i}(N_i, N_s) \qquad (28)$$

由智慧卡執行以下步驟：

步驟一：當接收到訊息 M 時，首先解開訊息 M，計算

$$(N_i', N_s') \leftarrow D_{v_i}(M) \qquad (29)$$

步驟二：檢查亂數是否相等

$$N_i' \stackrel{?}{=} N_i \qquad (30)$$

如果不相等則中斷連線，否則執行以下步驟。

步驟三：檢查亂數是否相等

$$N_s' \stackrel{?}{=} N_s \qquad (31)$$

如果相等，則完成雙向認證。

在完成雙向認證之後，運用 Diffie-Hellman 的金鑰交換技術，產生共同的交談金鑰，將執行以下步驟：

步驟一：遠端系統 S，計算 S_i，並將 S_i 傳送給智慧卡

$$S_i = \alpha^{N_s} \bmod q \qquad (32)$$

步驟二：同樣地，智慧卡計算 W_i，並傳送 W_i 給遠端系統 S

$$W_i = \alpha^{N_i} \bmod q \qquad (33)$$

步驟三：在接收到訊息後，遠端系統 S 計算 K_s，使用者計算 K_u，然後檢查 $K_s = K_u$ 是否成立，如果成立，則產生交談金鑰。

$$K_S = (W_i)^{N_S} \qquad (34)$$

$$K_u = (S_i)^{N_i} \qquad (35)$$

步驟四：如果遠端系統 S 要傳送訊息 M_s 給使用者 U_i 時，使用 K_s 做互或斥的運算，再用 e_i' 為加密金鑰，加密訊息，當使用者 U_i 收到訊息，利用智慧卡解開訊息，得到 M_s

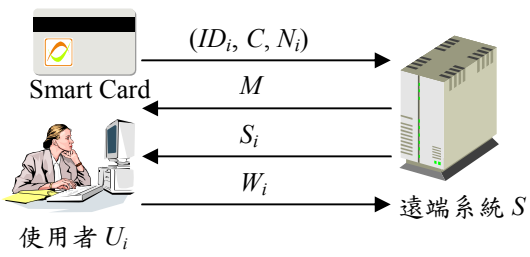
$$E_{ei'}(M_S \oplus K_S) \qquad (36)$$

$$M_s \leftarrow D_{ei'}(E_{ei'}(M_S \oplus K_S)) \oplus K_S \qquad (37)$$

步驟五：如果使用者 U_i 要傳送訊息 M_u 給遠端系統 S 時，使用 K_u 做互或斥的運算，再用 e_i 為加密金鑰，加密訊息，當遠端系統 S 收到訊息，做解密得到 M_u

$$E_{ei}(M_u \oplus K_u) \qquad (38)$$

$$M_u \leftarrow D_{ei}(E_{ei}(M_u \oplus K_u)) \oplus K_u \qquad (39)$$



圖六 Liaw 等人方法登入階段

3. 我們的方法

本文方法保留 Juang [7]、Chen-Yeh [3] 和 Liaw 等人 [10] 機制的優點，改善他們在安全上的缺失，提出使用智慧卡之通行碼認證及金鑰交換的方法 (如圖七所示)，達到雙向認證，產生交談金鑰，並且控制智慧卡的使用期限，讓遠端使用者與伺服器之間認證機制更安全且有效率。本文的方法分為三個階段：初始階段、註冊階段、登入階段最後產生交談金鑰，詳述方法如下：

[初始階段]

在此階段，先設定以下參數：

U_i：第 i 位使用者並擁有自己的識別碼 ID_i 和通行碼 PW_i

S：伺服器

x：伺服器的秘密金鑰。

$E_x(m)$：表示使用秘密金鑰 x，對訊息 m 做加密。

$D_x(m)$：表示使用秘密金鑰 x，對訊息 m 做解密。

$h(\,)$：為單向雜湊函數。

$date$：記錄使用限期相關資訊。

now：伺服器目前時間。

[註冊階段]

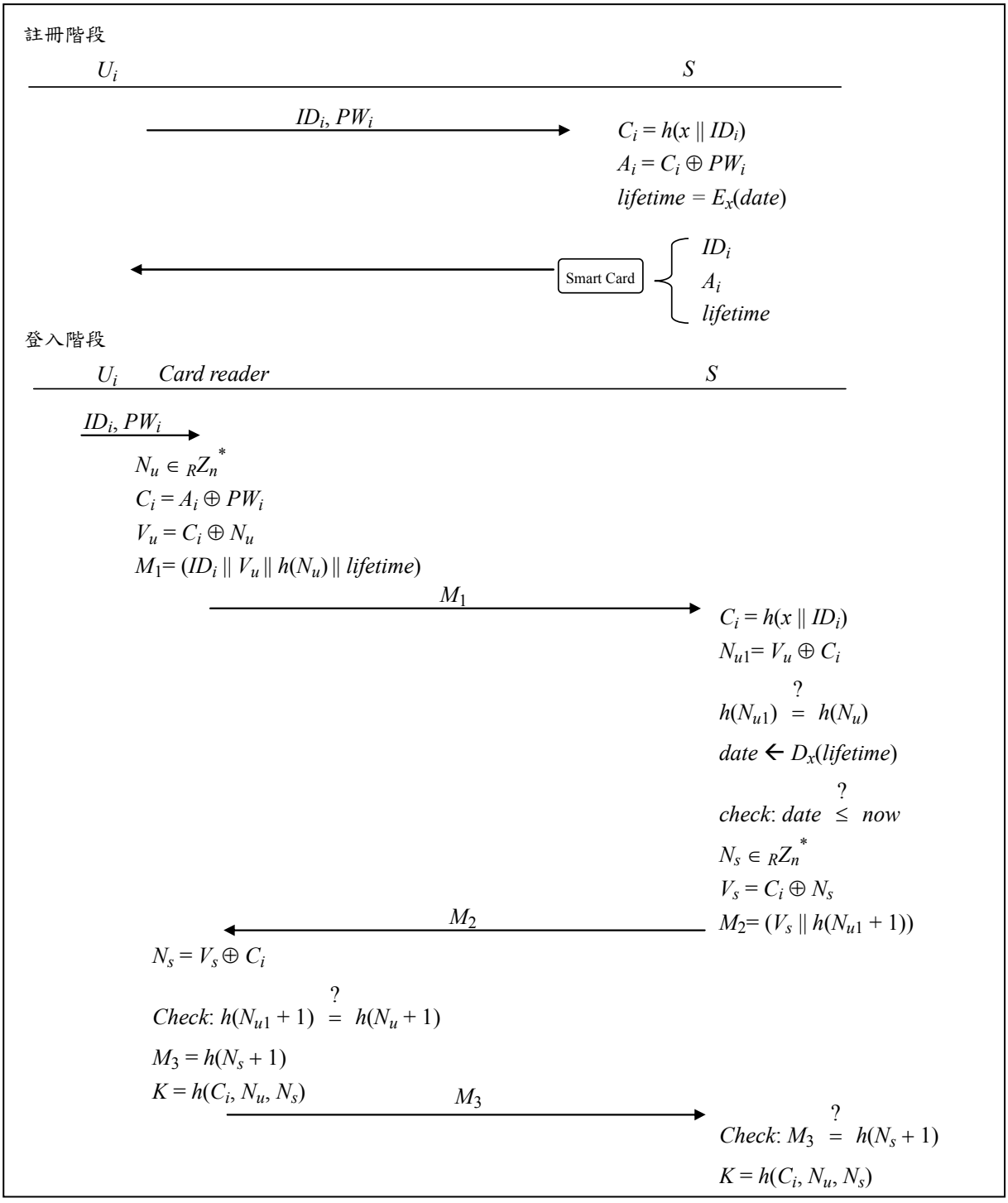
當使用者 U_i 要向伺服器 S 註冊時，使用者 U_i 傳送自己的 ID_i 和 PW_i 給伺服器 S，若伺服器接受使用者的需求，將執行以下步驟：

步驟一：計算使用者 U_i 的秘密資訊

$$C_i = h(x \| ID_i) \qquad (1)$$

$$A_i = C_i \oplus PW_i \qquad (2)$$

$$lifetime = E_x(date) \qquad (3)$$



圖七　通行碼認證及金鑰交換機制

步驟二：伺服器 S 將 $(ID_i, A_i, lifetime)$ 儲存到智慧卡，並配發給使用者 U_i。

[登入階段]

當使用者 U_i 要登入系統時，將智慧卡插入讀卡機，透過終端設備輸入 ID_i 和 PW_i。於是智慧卡會進行以下步驟：

步驟一：首先利用使用者 U_i 輸入的 PW_i 計算

$$C_i = A_i \oplus PW_i \qquad (4)$$

步驟二：隨機選取一個亂數 N_u，計算

$$V_u = C_i \oplus N_u \quad (5)$$

步驟三：將 M_1 傳送遠端伺服器 S

$$M_1 = (ID_i \| V_u \| h(N_u) \| lifetime) \quad (6)$$

遠端伺服器收到登入訊息 M_1 時，執行以下的步驟：

步驟一：計算 C_i 如(1)與 N_{u1}

$$N_{u1} = V_u \oplus C_i \quad (7)$$

步驟二：檢查 $h(N_{u1})$ 是否等於 $h(N_u)$，若相等，可以確認雙方所計算的 C_i 是相等的，亦可確認使用者 U_i 身份，若不相等，則拒絕提供使用者需求。

$$h(N_{u1}) \stackrel{?}{=} h(N_u) \quad (8)$$

步驟三：將 $lifetime$ 解密，取得使用期限相關資訊，檢查使用期限是否到期，若到期則拒絕提供服務，否則進行以下步驟。

$$Date \leftarrow D_x(lifetime) \quad (9)$$

$$Date \stackrel{?}{\leq} now \quad (10)$$

步驟四：隨機選取一個亂數 N_s，計算 V_s 和 M_2，並將 M_2 傳給使用者 U_i

$$V_s = C_i \oplus N_s \quad (11)$$

$$M_2 = (V_s \| h(N_u+1)) \quad (12)$$

結束上述步驟，確認使用者 U_i 通過驗證後，遠端伺服器 S 與使用者 U_i，分別執行以下步驟：

步驟一：當使用者接收到伺服器 S 傳送的訊息 M_2 ，首先計算

$$N_s = V_s \oplus C_i \quad (13)$$

步驟二：檢查 $h(N_{u1}+1)$ 是否為正確，若等於 $h(N_u+1)$，則繼續執行以下步驟，此動作在確認伺服器 S，是否能正確算出 N_u。

$$h(N_{u1}+1) \stackrel{?}{=} h(N_u+1) \quad (14)$$

步驟三：計算 M_3 與交談金鑰 K，將訊息 M_3 傳送給使用者 U_i

$$M_3 = h(N_s+1) \quad (15)$$

$$K = h(C_i, N_u, N_s) \quad (16)$$

步驟四：收到訊息 M_3，檢查 M_3 是否正確，此動作在確認使用者 U_i，是否能正確算出 N_s，並計算交談金鑰 K 如(16)

$$M_3 \stackrel{?}{=} h(N_s+1) \quad (17)$$

4. 效能分析

4.1 功能比較

遠端使用者確認機制不斷的被學者們提出，各有其優缺點，本章針對我們所提方法與近年來學者們所提使用者確認機制，做功能 (如表 1)、效率分析 (如表 2)、儲存與通訊成本 (如表 3) 的比較。

在表 1 中，列出使用智慧卡機制用來提供的功能，以及可以抵抗安全上的攻擊

法。其中，不需通行碼驗證表是意指伺服器不需要儲存驗證表；可自行選擇通行碼是意指使用者可以自由選擇容易記憶的通行碼，在 Lu-Cao 的方法中，不能讓使用者自行選擇通行碼並且也不能自行修改通行碼；雙向驗證意指使用者與伺服器，雙方皆有確認對方的身分，在 Lu-Cao 的方法中，並未達到雙向認證的功能；產生交談金鑰意指在每次登入系統之後，產生一把共同的金鑰，在 Lu-Cao、Change-Lee、Hsu 和 Liaw 等人的方法中，並未提供此功能；使用期限控制意指對智慧卡的使用效期做控制，僅本文方法提供此功能；在防制安全攻擊方面，大部分的機制皆可防範，只有 Chen-Yeh 的機制，當攻擊者侵入伺服器時，伺服器無法立即確認使用者是否合法，容易遭受阻斷服務攻擊。

4.2 效率分析比較

這一節將近年提出的使用者確認機制與我們提出的方法，做效率上的分析比較，彙整於表 2，整個機制包含註冊階段、登入階段與產生交談金鑰，並分成使用者 U_i 和伺服器 S 來比較。在此先定義一些參數：

T_m：乘法 (Multiplication) 運算時間。

T_s：平方根 (Square) 運算時間。

T_i：反轉 (Inverse) 運算時間。

T_e：指數 (Exponentiation) 運算時間。

T_h：雜湊 (Hash) 運算時間。

T_{sym}：對稱式加解密運算時間。

NA：表示未提供。

整理結果如表 2，從表 2 中可以發現，若加總註冊階段、登入階段、產生交談金鑰的效率做加總，本論文的總體效率比其它方法佳，若分別來比較，本文的方法，在註冊階段比 Liaw、Chen-Yeh 和 Juang 的方法，增加些許運算成本，註冊階段只有新使用者加入時才會用到，對系統執行效率影響不大；在產生交談金鑰時，使用者端和 Wang 等人的方法一樣，運算成本是最低的，而從伺服器端來看，較 Wang 等人的方法增加一些負擔，但於伺服器端運算效能高，使用者端運算效能低的不平衡系統下，伺服器增加微量的運算，不會影響系統整體效能。除上述所提的部分外，本文方法，皆小於其它方法所耗費的運算時間。

4.3 儲存與通訊成本比較

表 3 針對儲存與通訊的長度做比較，分成儲存訊息長度、通訊階段訊息長度、交換金鑰階息長度。就 Lu-Cao、Chang-Lee、Hsu、Liao 等人的方法來比較，因為未提供交談金鑰和有效期限的控制，若本文的方法扣除這二項功能所產生的訊息長度 $2|sym| + 3|h|$，在儲存訊息與通訊階段訊息長度總和來看，比 Lu-Cao、Chang-Lee、Hsu、Liao 等人的方法有較短的訊息長度。若與 Wang 等人、Liaw 等人、Chen-Yeh、Juang 的方法來比較，因為未提供有效期限控制的功能，若本文扣除這項功能所產生的訊息長度 $2|sym|$，就總和的長度的角度來看，與 Wang 等人、Liaw 等人、Chen-Yeh、Juang 的方法，此四種方法與本文所提的方法訊息長度不相上下，皆有較低的儲存與通訊成本的特性。

5. 結論

在 1981 年，Lamport 提出通過不安全通道的使用者遠端認證機制後，陸續有許多相關的方法被提出，在安全與效率上做改良。我們的方法提供雙方認證，並且產生交談金鑰，使用二個亂數值分別由雙方產生，攻擊者不能偽裝使用者或是伺服器。在完成雙向認證後，運用雙方產生的亂數值更進一步的建立交談金鑰。本文中所提之具效率性的通行碼認證及金鑰交換機制，改良 Juang、Chen-Yeh 和 Liaw 等人方法的缺點，保留其優點，並利用控制智慧卡的有效期限功能，讓伺服器提供使用者服務時，做效期的管理與控制。

表 1 功能比較表

	不需通行碼驗證表	可自行選擇通行碼	可修改通行碼	達到雙向驗證	產生交談金鑰	使用期限控制	可避免重送攻擊	可防制通行碼猜測攻擊	可防制偽裝攻擊	可防制阻斷服務攻擊
Wang 等人方法[13]	V	V	V	V	V	×	V	V	V	V
Liaw 等人方法[10]	V	V	V	V	V	×	V	V	V	V
Chen-Yeh 方法[3]	V	V	V	V	V	×	V	V	V	×
Juang 方法[7]	V	V	V	V	V	×	V	V	V	V
Lu-Cao 方法[11]	V	×	×	×	×	×	V	V	V	V
Chang-Lee 方法[1]	V	V	V	V	×	×	V	V	V	V
Hsu 方法[5]	V	V	V	V	×	×	V	V	V	V
Liao 等人方法[9]	V	V	V	V	×	×	V	V	V	V
本文方法	V	V	V	V	V	V	V	V	V	V

表 2 效率分析比較

	註冊階段		登入階段		產生交談金鑰	
	U_i	S	U_i	S	U_i	S
Wang 等人方法[13]	T_h	$3T_h$	$4T_h$	$3T_h$	$2T_h$	0
Liaw 等人方法[10]	0	T_h	$T_h + T_{sym}$	$2T_h + T_{sym}$	$2T_e$	$2T_e$
Chen-Yeh 方法[3]	0	T_h	$2T_h$	$4T_h$	$5T_h$	$3T_h$
Juang 方法[7]	0	T_h	$T_h + T_{sym}$	$2T_{sym}+T_h$	$2T_{sym}+T_h$	$T_{sym}+T_h$
Lu-Cao 方法[11]	0	$T_s + 2T_e + 3T_h$	$T_m + T_h$	$T_m + T_s + T_i + 2T_e + 4T_h$	NA	NA
Chang-Lee 方法[1]	0	$T_i + T_e + T_h$	$T_m + T_h$	$T_m + T_i + T_e + T_h$	T_h	$T_m + T_i + T_e + 2T_h$
Hsu 方法[5]	0	$T_m + T_i + T_e + 2T_h$	$T_e + 2T_h$	$T_e + 2T_h$	NA	NA
Liao 方法[9]	T_h	$T_e + 2T_h$	$2T_m + T_i + T_e + 3T_h$	$T_m + T_e + 2T_h$	NA	NA
本文方法	0	$T_h + T_{sym}$	T_h	0	$2T_h$	T_h

表 3 儲存與通訊成本比較

	儲存訊息長度	通訊階段訊息長度	交換金鑰階段訊息長度
Wang 等人方法[13]	$4\|h\|$	$\|ID\| + 2\|h\|$	$\|h\|$
Liaw 等人方法[10]	$2\|h\|$	$\|ID\| + \|h\| + \|sym\|$	$2\|p\|$
Chen-Yeh 方法[3]	$2\|h\|$	$\|ID\| + \|h\|$	$3\|h\|$
Juang 方法[7]	$\|ID\| + \|h\|$	$\|ID\| + \|sym\|$	$2\|sym\|$
Lu-Cao 方法 [11]	$\|h\| + \|p\|$	$\|ID\| + \|h\| + \|p\| + \|T\|$	*NA*
Chang-Lee 方法[1]	$2\|h\| + \|p\|$	$\|ID\| + \|h\| + 3\|p\|$	*NA*
Hsu 方法[5]	$\|ID\| + \|h\| + \|p\| + \|g\|$	$\|ID\| + \|h\| + \|T\|$	*NA*
Liao 等人方法[9]	$\|ID\| + \|h\| + \|p\| + \|g\|$	$\|ID\| + 2\|h\| + \|T\|$	*NA*
本文方法	$\|ID\| + \|h\| + \|sym\|$	$\|ID\| + 2\|h\| + \|sym\|$	$3\|h\|$

註：1. $|ID|, |p|, |g|$：分別表示參數長度
2. $|h|$：表示雜湊函數輸出長度
3. $|sym|$：表示對稱式加密金鑰長度
4. *NA*：表示未提供

參考文獻

[1] C. C. Chang and J. S. Lee, "An efficient and secure remote authentication scheme using smart cards", Information & Security, Vol. 18, pp. 122-133, 2006.

[2] C. C. Chang and T. C. Wu, "Remote password authentication with smart card", IEE Proceedings-E, Vol. 138, No. 3, pp. 165-168, 1993.

[3] Y. C. Chen and L. Y. Yeh, "An efficient nonce-based authentication scheme with key agreement", Applied Mathematics and Computation, Vol. 169, No. 2, pp. 982-994, 2005.

[4] 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, pp. 372-375, 2002.

[5] C. L. Hsu, "A user friendly remote authentication scheme with smart cards against impersonation attacks", Applied Mathematics and Computation, Vol. 170, No. 1, pp. 135-143, 2005.

[6] 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, pp. 28-30, 2000.

[7] W. S. Juang, "Efficient password authenticated key agreement using smart cards", Computer and Security, Vol. 23, No. 2, pp. 167-173, 2004.

[8] L. Lamport, "Password authentication with insecure communications", Communication of ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[9] I. E. Liao, C. C. Lee and M. S. Hwang, "A password authentication scheme over insecure networks", Journal of Computer and System Sciences, Vol. 72, No. 4, pp. 727-740, 2006.

[10] H. T. Liaw, W. F. Zhang and C. W. Wu, "An efficient and complete remote user authentication scheme using smart card", Mathematical and Computer Modelling, Vol. 44, No. 1-2, pp. 223-228, 2006.

[11] R. Lu and Z. Cao, "Efficient remote user authentication scheme using smart card", Computer Networks, Vol. 49, No. 6, pp.535-540, 2005.

[12] H. M. Sun, “An efficient remote use authentication scheme using smart cards”, IEEE Transactions on Consumer Electronics, Vol. 46, No. 4, pp. 958-961, 2004.

[13] X. M. Wang, W. F. Zhang, J. S. Zhang and M. K. Khan, “Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards”, Computer Standards & Interfaces, Vol. 29, No. 5, pp. 507-512, 2007.

[14] S. T. Wu and B. C. Chieu, “A user friendly remote authentication scheme with smart cards”, Computer & Security, Vol. 22, No. 6, pp. 547-550, 2003.