遠端用戶隱私保護認證方案之安全漏洞探討
Security analysis of privacy preserving remote user authentication scheme

龔建丞
Jian-cheng Gong
中國文化大學
資訊管理研究所
學生
a0939797269@gmail.com

余 平
Ping Yu
中國文化大學
資訊管理研究所
助理教授
yp@faculty.pccu.edu.tw

摘要

隨著網路與科技的演變，智慧卡的發明使得人們在生活上更加的便利，例如在交通上，除了投幣的方式也多了悠遊卡的付費方式。透過卡片的方式省去許多人力與時間上不必要的浪費。其中遠端用戶與伺服器，常倚賴智慧卡進行認證，如何確保認證過程安全無虞是資訊安全研究一直努力的目標。其中在 2015 年 Chaudhry 等人認為 Kumari 提出的密碼認證方案有安全漏洞，並提出一套機制，可防止相關攻擊等特性。但經過本研究後發現 Chaudhry 等人提出的機制仍有重大的安全疏失，例如無法阻止離線猜弱密碼，偽裝攻擊及阻絕服務等。本文將詳述 Chaudhry 等人的機制所具有的安全漏洞，並探討可能的問題，以於後續研究中提出更具有安全性的機制。

關鍵字: 遠端認證、智慧卡、離線猜密碼、阻絕服務攻擊、偽裝攻擊

Abstract

With the conversion of Internet and Information technology, the smart card makes us more convenience in daily life. For example, in bus or MRT, except coin we can use smart card that save a lot of labor and time. The remote user and server are often using smart cards for authentication, that the security and privacy are important issue. In 2015, Chaudhry et al. proposed that Kumari et al.'s scheme has security weaknesses, and proposed an improved scheme.They indicate that the scheme can against many attack. However, we find that the Chaudhry et al.'s scheme is still with security problem, such as offline password guessing attack etc. In this paper, we will analyze that weaknesses of Chaudhry et al.'s scheme, point out the problem, and prepare to propose a more safe scheme in the future.

Keywords: *smart card*; *offline password guessing attack*; *remote authentication*

1. 緒論

資訊與網路通訊在日新月異的發展下，人與人之間交易已經不僅僅限制於面對面的金錢交易，取代的是更加便利的智慧卡。智慧卡是一種可攜式塑膠卡片，卡片上鑲著一塊含有積體電路的晶片。包含了微處理器、I/O 介面及記憶體，提供資料的運算、存取控制及儲存功能。由法國人羅蘭莫雷諾於 1974 年發明，利用具有存儲加密及資料處理能力的積體電路晶片模組封裝於和信用卡尺寸一樣大小的塑膠片基中，製成 *IC* 卡，並經常應用在身分辨識上。而智慧卡的認證一般都會將重要的資料儲存在卡片中保護，外界無法直接讀取。每當遇到需要進行驗證時，由使用者輸入驗證請求的資料，在晶片裡面與儲存的密碼進行運算及驗證。

智慧卡的認證機制多採用遠端認證方式，由使用者與遠端伺服器相互認證。認證過程是透過一個公開的網路通訊環境中傳遞使用者訊息至伺服器，並驗證登入之要求，及進行後續的交易或重要訊息交換。儘管智慧卡提供驗證的便利性與安全性，但因公開通道潛藏漏洞危機，攻擊者可以輕易地攔截訊息，進行離線猜密碼、重送攻擊、阻絕服務等的攻擊。

在 2009 年 Wang[1]等人提出一個以動態 *ID* 為基礎的認證機制，並聲稱他們的方法可以抵抗已知的攻擊，但在 2012 年 Wen[2]等人證明 Wang 等人的機制是無法防禦偽裝與離線猜密碼攻擊，並提出一套新的認證機制但也被 Chung[3]等人提出具有相同弱點。在 2014 年 Chung[3]等人同時對 Wang[1]等人的機制提出質疑，指出 Wang[1]的機制有登錄不正確與密碼更改階段的錯誤，並提出一個修正的機制。但 Kumari[4]等人在 2015 年 6 月發現 Chung[3]的機制還是具有偽冒攻擊和猜密碼等系統弱點。並提出具有使用者匿名等特點的改善機制。Chaudhry[5]等人於 2015 年發表研究指出 Kumari[4]的機制在使用者匿名與智慧卡失竊方面仍然存在弱點。並提出新的機制，該機制具備以下的優點:(1)在註冊階段使用單向雜湊函數與多項是雜湊函數防止內部攻擊;(2)智慧卡失竊的攻擊;(3)可抵抗匿名攻擊;(4)可抵抗偽冒攻擊;(5)可利用智慧卡防止登錄錯誤次數避免線上猜密碼攻擊;(6)可避免離線猜弱密碼;(7)利用時間戳記防止重送攻擊;(8)可防止 *DOS* 攻擊;(9)具有前推私密性及(10)可防止盜取驗證攻擊。但在本研究發現此驗證機制還是存有會遭受到阻絕服務攻擊以及離線猜弱密碼攻擊的弱點。

主要因在 Chaudhry 等人的機制中，於登錄與認證階段，伺服器端發送回給使用者端的密文並未妥善保護，可被截取與竄改，進而進行離線猜密碼的攻擊。我們將在第二節說明 Chaudhry 等人的機制，第三節說明本研究對 Chaudhry 等人機制的安全性分析與探討，並在最後一節做出本研究的結論。

2. Chaudhry 等人的遠端用戶隱私保護認證協定機制

Chaudhry 之遠端用戶隱私保護認證協定機制主要目的是為了增強 Kumari 等人提出的認證機制。以避免各項攻擊，由三個階段所構成，依序為(1)使用者註冊階段，(2)使用者登入階段及(3)伺服器驗證階段。Chaudhry 之機制個階段說明如下。本研究所使用各項符號的定義如附件 1 中之表 1。

2.1 註冊階段

當使用者 U_i 想向伺服器 S 註冊成為合法使用者時，雙方依照以下步驟完成註冊:

Step 1: 使用者自行選擇 ID_i 及 PW_i 並產生一個隨機亂數 c，接著計算 $RP_i = h(c||PW_i)$，最後使用者通過安全通道將 $\{ID_i, RP_i\}$ 傳遞給伺服器 S 進行註冊。

Step 2: 伺服器 S 收到使用者 U_i 所傳的的註冊訊息後，計算 $PID_i = E_{ks2}(ID_i||T_{s0})$、$G_i = h(ID_i||k_{s1})$

$\oplus RP_i$、$K_i = k_i \oplus RP_i$、$H_i = h(ID_i \| k_i \| RP_i)$與 $J_i = k_i \oplus h(k_{s2}\|ID_i)$，其中 k_{s1}、k_{s2} 為伺服器秘密金鑰。伺服器將{K_i,H_i,J_i,PID_i,$h()$}存入智慧卡 SC_i，然後將 SC_i 與 G_i 通過安全通道傳回給使用者。

Step 3:使用者收到{SC_i,G_i}，並計算 $R_i = (ID_i \|PW_i)\oplus c$ 與 $L_i = G_i \oplus c$，其中 c 為隨機亂數，並將兩者存入智慧卡 SC_i。最後，智慧卡包含了{ K_i,H_i, J_i,PID_i, $h()$,R_i,L_i }。並完成註冊。註冊階段如附件 2 之圖一所示。

2.2 登入階段

當使用者 U_i 想登入遠端伺服器 S 時，使用者先將智慧卡 SC_i 插入讀卡機，並輸入使用者之 ID_i 與 PW_i。智慧卡 SC_i 依照以下步驟進行登入作業:

Step 1: 智慧卡 SC_i 計算 $c = R_i \oplus (ID_i\|PW_i)$、$RP_i = h(c\|PW_i)$、$h(ID_i\|k_{s1}) = L_i \oplus RP_i \oplus c$、$k_i = K_i \oplus h(c\|PW_i)$與 $H_i^* = h(ID_i\|k_i\|RP_i)$。

Step 2: 智慧卡 SC_i 檢查 H_i 是否等於儲存 H_i^*，若不相等，則智慧卡終止登入作業，若相等則進行下一步驟。

Step 3: 智慧卡計算 $h(k_{s2}\|ID_i) = k_i \oplus J_i$、$G_i = L_i \oplus c$、$G_i' = G_i \oplus h(k_i \| T_{ui})$、$Q_i = h(G_i\|k_i\| P_i\|T_{ui})$、$P_i = G_i \oplus RP_i$ 與 $S_i = k_i \oplus (h(k_{s2}\|ID_i) \|T_{ui})$。然後智慧卡傳送驗證要求之訊息{ PID_i, G_i', Q_i, S_i,T_{ui}}給伺服器 S。其中 T_{ui} 為使用者 U_i 的時間戳記。

登入階段如附件 2 之圖二所示。

2.3 驗證階段

延續上述的 2.2 節登入階段，伺服器收到使用者之訊息後，依照以下步驟進行驗證作業:

Step 1:首先伺服器先確認 T_{ui} 的合法性，即 $(T_{s1}-T_{ui}) \leqq \triangle T$，其中 T_{s1} 為伺服器收到訊息之時間，ΔT 為合理之網路傳輸延遲時差。然計算$(ID_i\|T_{s0}) = D_{ks2}(PID_i)$、$k_i = S_i(h(k_{s2}\|ID_i)T_{ui})$、$G_i = G_i' \oplus h(k_i \| T_{ui})$、$P_i^* = h(ID_i \| k_{s1})$，$Q_i^* = h(G_i\|k_i\|P_i^*\|T_{ui})$。

Step 2:伺服器檢查 Q_i 是否等於 Q_i^*若相等使用

Step 3:伺服器計算 $a = h(P_i^*\|k_i\|T_{s2})$，$Z_i = P_i \oplus E_{ks2}(ID_i\|T_{s1})$。伺服器更進一步將{$a$,$T_{s2}$,$Z_i$}傳回給使用者 U_i。

Step 4:使用者接收到伺服器傳回之訊息{a,T_{s2},Z_i}，先確認 T_{s2} 合法性，即$(T_u - T_{s2}) \leqq \triangle T$，其中 T_u 為使用者收到訊息之時間，然後計算 $a^* = h(P_i\|k_i\|T_{s2})$並與伺服器之認證碼 a 是否相同，若兩者相同，使用者確認伺服器為合法正確的。

Step 5:伺服器 S 與使用者 U_i 共同計算共享秘密金鑰 $SK = h(P_i\|k_i\|T_{ui}\|T_{s2}\|h(k_{s2}\|ID_i))$。

驗證階段如附件 2 之圖三所示。

3. 探討 Chaudhry 隱私保護認證協定之安全漏洞

3.1 無法對抗阻絕服務攻擊(*Denial Of Server Attack*)

Chaudhry 的機制在使用者輸入帳號和密碼後，智慧卡會驗證其正確性，若兩者都正確才能通過驗證請求並傳送至伺服器，若有一者錯誤就會在提出驗證請求階段終止對話，達到抵抗阻絕服務的攻擊。但我們發現在驗證階段，會造成阻絕服務的問題。因在驗證階段，伺服器 S 傳回 Z_i 給使用者 U_i，但 Z_i 並未放在認證碼 a 裡面保護，並且使用者 U_i 檢查時只檢查 a 是否等於 a^*，所以如果 Z_i 在網路上傳遞時被攻擊者擷取竄改，使用者無法發現。由 $Z_i = P_i \oplus E_{ks2}(ID_i\|T_{s1})$可知，$Z_i$ 是 $E_{ks2}(ID_i\|T_{s1})$與 P_i 互斥或後的密文，而 $E_{ks2}(ID_i\|T_{s1})$就是新的 PID_i。Z_i 被竄改為 Z_i'後，U_i 在計算並儲存新的 $PID_i = P_i \oplus Z_i$ 就會發生錯誤，造成使用者 U_i 下次登入傳送錯誤 PID_i'給伺服器 S。伺服器 S 在$(ID_i\|T_{s0}) = D_{ks2}(PID_i')$將 PID_i'解密後得到$(ID_i\|T_{s0})$，這個 ID_i 會是錯誤的 ID_i。隨後由 $P_i^{*\prime} = h(ID_i' \|k_{s1})$我

們知道 $P_i^{*}{}'$會使用到錯誤的 ID_i，而 $Q_i^{*}{}' = h(G_i||k_i||P_i^{*}||T_{ui})$的 $Q_i^{*}{}'$包含了 $P_i^{*}{}'$，以至於在伺服器 S 檢查 Q_i 是否等於 $Q_i^{*}{}'$時失敗，將拒絕使用者登入。而使用者被拒絕登入，將導致使用者端儲存之錯誤的 PID_i 無法更正，使用者將無法登入伺服器，造成阻絕服務。

3.2 推算部份密碼之漏洞

從 Chaudhry 的協定機制中，我們發現可以使用機制中給的資訊來推算部份密碼。詳細的推導方式如下:

Step 1.從 SC_i 取得 R_i、L_i 及 K_i 做互斥或運算，即 $R_i \oplus L_i \oplus K_i = (ID_i||PW_i) \oplus c \oplus h(ID_i||k_{s1}) \oplus RP_i \oplus c \oplus S_i \oplus (h(k_{s2}||ID_i)||T_{ui}) \oplus RP_i$。

Step 2.化簡後可得:$R_i \oplus L_i \oplus K_i = (ID_i||PW_i) \oplus P_i \oplus S_i \oplus (h(k_{s2}||ID_i)||T_{ui})$。其中 $P_i = h(ID_i||k_{s1})$。

Step 3.P_i 可利用 $P_i = PID_i \oplus Z_i$ 計算得到。我們可用兩種方式取得資料計算 P_i:

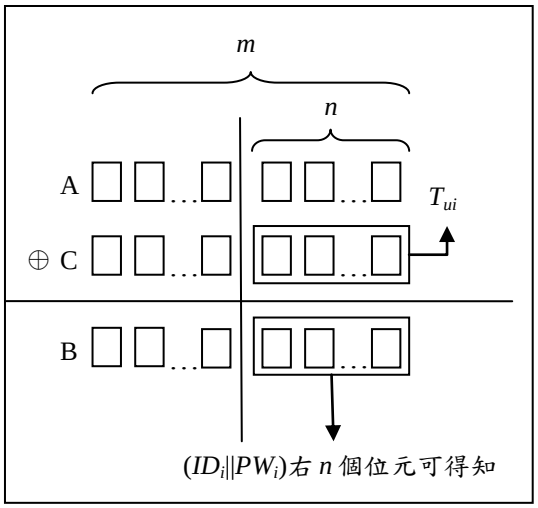
A. 攻擊者注意目標使用者,在使用者登入時的驗證階段側錄伺服器 S 傳回的密文 Z_i。請注意,使用者的 SC_i 會使用該 Z_i 來更新 $PID_i = P_i \oplus Z_i$。接著，在使用者結束登入後找機會竊取該使用者之 SC_i，取出其中儲存之新的 PID_i，利用前次回傳的訊息及 SC_i 計算 $P_i = PID_i \oplus Z_i$ 得到 P_i。

B. 在目標使用者的辦公室外的網路節點側錄該使用者連續兩次登入時的網路訊息。取得前次回傳時的 Z_i 及本次登入時的 PID_i 後，計算 $P_i = PID_i \oplus Z_i$ 得到 P_i。此處要需要注意的是,攻擊者取得的 Z_i 及 PID_i，必須是屬於使用者一前一後連續兩次登入時的網路訊息才有效。

Step 4.由登入訊息可得 T_{ui} 假設$|T_{ui}| = n$，則我們可計算出$(ID_i||PW_i)$的最右邊 n 個位元，若 $|PW_i| < n$，則部分 ID 也可以被算出，如$|PW_i| = n$ 則可得到 U_i 的密碼。其中$|T_{ui}|$及$|PW_i|$為 T_{ui} 及 PW_i 的長度。計算說明如下

A. 我們將 $R_i \oplus L_i \oplus K_i = (ID_i||PW_i) \oplus P_i \oplus S_i \oplus (h(k_{s2}||ID_i)||T_{ui})$移項，可得出 $R_i \oplus L_i \oplus K_i \oplus P_i \oplus S_i \oplus (ID_i||PW_i) = (h(k_{s2}||ID_i)||T_{ui})$。

B. 假設 $R_i \oplus L_i \oplus K_i \oplus P_i \oplus S_i$ 值為 A 且全部為已知、$(ID_i||PW_i)$ 值為 B 且為未知，$(h(k_{s2}||ID_i)||T_{ui})$值為 C 且$|T_{ui}| = n$，為已知。且 A、B 及 C 三者長度相同，假設三者長度為 m，以及右邊為 n 個位元，可將 $A \oplus C = B$ 的運算表示成下列圖示，即可得知 B 右邊 n 個位元值。如下圖圖四示。



圖四:推算密碼之圖示

3.3 離線猜密碼攻擊

在 Chaudhry 的安全分析中提到智慧卡失竊，攻擊者可取得裡面的參數$\{K_i, H_i, J_i, PID_i, h(), R_i, L_i\}$,其中只有 R_i ,K_i, H_i 包含使用者的密碼,但要從這三個參數計算出密碼至少要猜三個未知數，所以是不會被猜出密碼的。但是利用 3.2 節之推算部分密碼結果我們根據 Chaudhry 等人的協定機制,可進行離線猜密碼攻擊。攻擊者可先利用使用者的個人資訊，如身分證字號等，建立使用者的帳號密碼資料庫，再利用其組合進行帳號及密碼的推導。演算步驟如下:

Step 1. 攻擊者猜一組 ID_i'及 PW_i'。其中依 3.2 節 $ID_i' \,||\, PW_i'$中最右邊 n 個位元已算出，故實際只需猜 $ID_i' \,||\, PW_i'$當中左邊剩下 m-n 的部分。

Step 2. 計算 $c' = R_i \oplus (ID_i' \| PW_i')$。其中 R_i 取自 SC_i。

Step 3. 計算 $RP_i' = h(c' \| PW_i')$。

Step 4. 計算 $k_i' = K_i \oplus h(c' \| PW_i')$。其中 K_i 取自 SC_i。

Step 5. 計算 $H_i' = h(ID_i' \| (K_i \oplus RP_i') \| RP_i')$

Step 6. 若 $(H_i' = H_i)$ 其中 H_i 取自 SC_i。

則輸出正確的 ID_i'及 PW_i'並結束否則再回到 Step1 重新執行各 Step。因利用已知 n 個位元的 $ID_i \| PW_i$ 即是先建立的帳密資料庫，如使用者使用較弱的帳號及密碼，攻擊者將可猜得正確的 ID_i 與 PW_i。

3.4 假冒伺服器攻擊

Chaudhry 聲稱該機制能抵抗假冒伺服器攻擊，是因為攻擊者必須有辦法製造出伺服器數位簽章 a，而 a 裡的 P_i 與 k_i 需要 k_{s1} 和 k_{s2} 兩個秘密金鑰才能得到，因此攻擊者無法假冒，且我們發現在 Chaudhry 的協定機制中，驗證階段伺服器傳回 a、T_{s2} 及 Z_i。使用者收到傳回訊息後，只利用計算的 a 與 a^*使否相等來確認使否為真正的伺服器。雖然 Chaudhry 聲稱攻擊者無法製造出認證碼 a，但我們是可以製作出一樣的認證碼 a 傳給使用者，進而假冒伺服器。攻擊的步驟如下:

Step 1.取得 U_i 登入訊息$\{PID_i, G_i', Q_i, S_i, T_{ui}\}$及 SC_i 卡。

Step 2.利用 3.2 節取得 P_i^{*}'值，及 3.3 節計算出的 k_i'值。

Step 3.攻擊者自行產生一個 T_{s2}'。

Step 4.計算 $a' = h(P_i^{*}' \| k_i' \| T_{s2}')$

Step 5.再產生一個 Z_i'，傳送$\{ a', T_{s2}', Z_i' \}$給使用者成功。

Step 6.使用者計算 $a^* = h(P_i \| k_i \| T_{ui})$，並驗證 $a^* = a'$，攻擊者偽裝伺服器成功，因使用者只驗證 a 不驗證 Z_i。

值得一提的是，Z_i 因為使用者不會檢查，所以攻擊者可傳回一個無用的任意訊息給使用者，而使用者也不會發現，還如同 3.1 節阻絕服務攻擊所述將造成使用者下次登入時被拒絕登入。

3.5 計算會期金鑰 *SK*

經過前面的安全性分析，我們還發現能算出會期金鑰 *SK* 裡所有的參數。Chaudhry 協定機制中的會期金鑰 $SK = h(P_i \| k_i \| T_{ui} \| T_{s2} \| h(k_{s2} \| ID_i))$。其中 P_i 與 k_i 可利用 3.2 節與 3.3 節的方法取得。T_{ui} 與 T_{s2} 都是在公開網路上傳遞可以攔截取得。$(h(k_{s2}\|ID_i)\|T_{ui}) = S_i \oplus k_i$ 再去除串接的 T_{ui} 即刻得到$(h(k_{s2}\|ID_i)$。所以會期金鑰 *SK* 的訊息全部都可以被算出。也因此 Chaudhry 所稱因 *SK* 無法被算出，而具有前向私密性是不成立的。

4. 結論

近年來，科技日益進步，技術更新的速度不斷加快，生活上使用到智慧卡也越來越頻繁，例如我們每天搭乘交通工具會用到的悠遊卡，提領現金用到的提款卡，這些都與我們的生活密不可分，因此智慧卡認證的安全性也就更加重要。本文 Chaudhry 等人的機制存在無法抵抗阻絕服務攻擊、推算密碼漏洞、離線猜密碼、假冒伺服器及不具前向私密性等弱點，因此我們認為 Chaudhry 等人的機制並不適用於智慧卡遠端認證機制上。探討的此篇論文讓我們更加瞭解，雖然科技進步，我們也一直在改善各種智慧卡機制上的問題，但相對的，攻擊的方法與技術也是會日新月異的，如何設計出更安全的機制有其必要性也是未來研究的方向。

參考文獻

[1] Wang Y., Liu J., Xiao F., Dan J.,“A more efficientand secure dynamic ID-based remote user authentication scheme”. *Computer Communications*, 32(4):583–585, 2009.

[2] Wen F, Li X. , “An improved dynamic ID-based remote user authentication with key agreement scheme”. *Computers & Electrical Engineering*, 38(2): 381–387, 2012.

[3] Chung YF, Tai WL, Chang HC., “Untraceable dynamicidentity-based remot -e user authentication scheme with verifiable password update”. *International Journal of Communication Systems*, 27(11):3430–3440, 2014

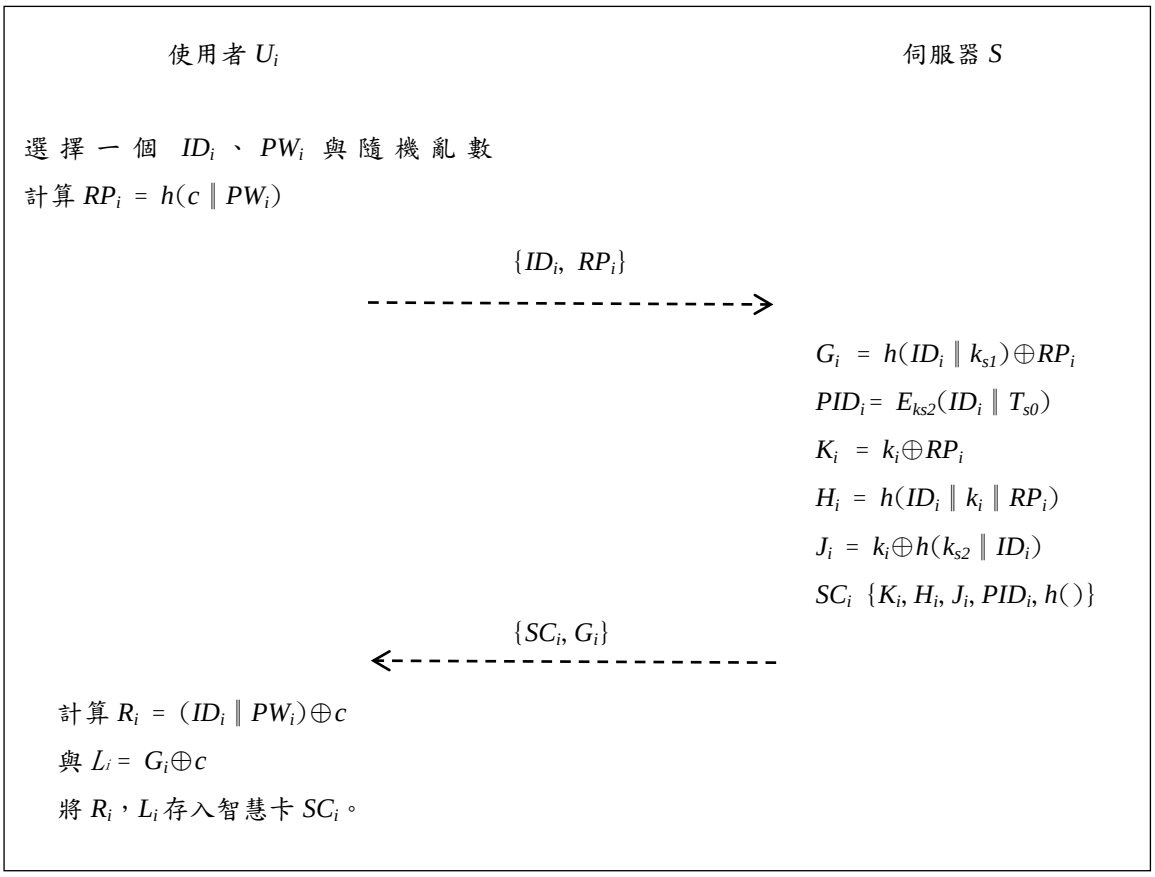
[4] Kumari S, Gupta MK, Khan MK, Li X., “An improved timestamp-based password authentication scheme: comments, crypt -analysis, and improvement. ”*Security and Communication Networks*, 7(11): 1921-19 32, 2014.

[5] Shehzad Ashraf Chaudhry, Mohammad Sabzinejad Farash,, Saru Kumari, Syed Husnain AbbasNaqvi, “An enhanced privacy preserving remote user authentication scheme with provable security”,*Security and Communication Networks*, 10.1002, 1-15, 2015.

附件1

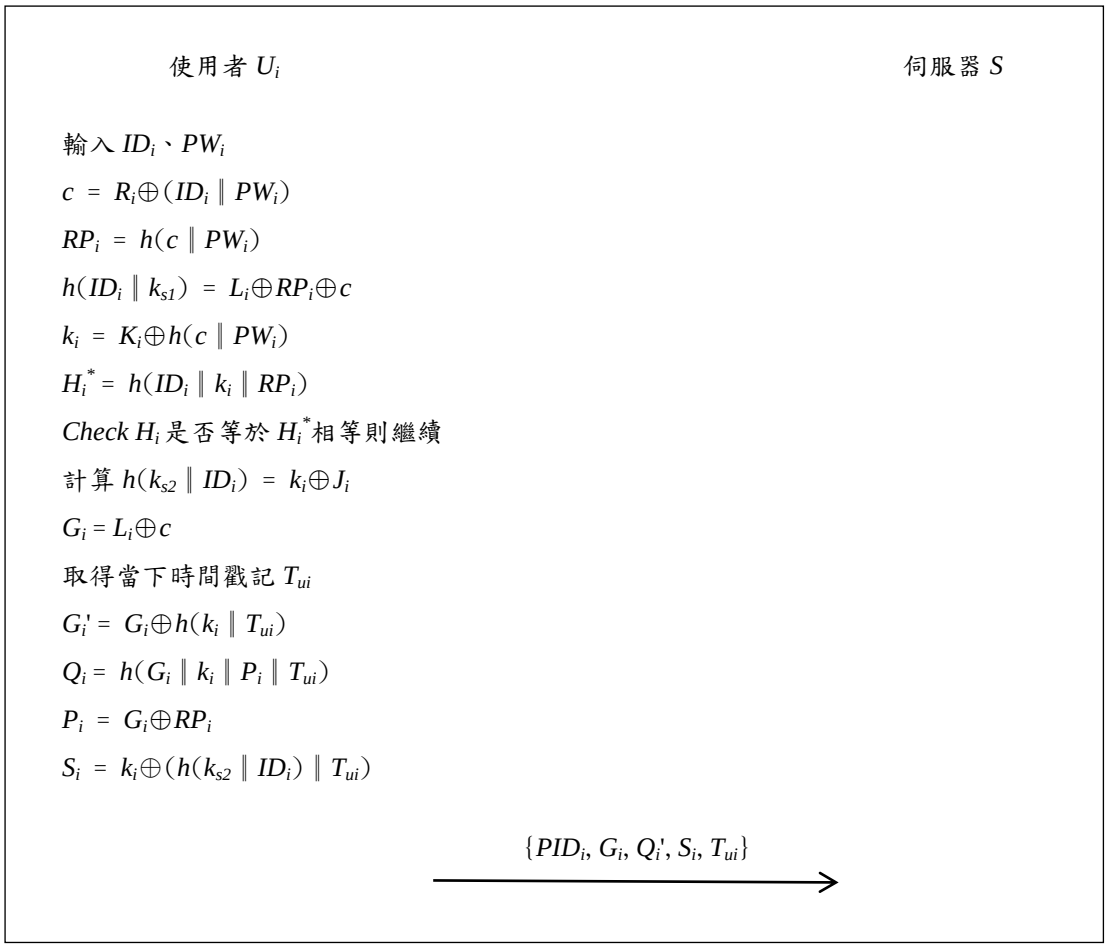
符號	說明	符號	說明
S	伺服器	U_i	使用者 i
ID_i	使用者 i 的帳號	A_i	攻擊者
PW_i	使用者 i 的密碼	k_i	獨特隨機數
k_{s1}, k_{s2}	伺服器秘密金鑰	$\|$	串聯運算子
T_u, T_{ui}	使用者時間戳記	T_{si}	伺服器第 i 次時間戳記
$\oplus$	互斥或運算子	$h()$	單向雜湊函數
PID_i	使用者 i 的虛擬帳號	SC_i	使用者 i 的智慧卡
$E_k()$	對稱加密函數	$D_k()$	對稱解密函數

附件 2



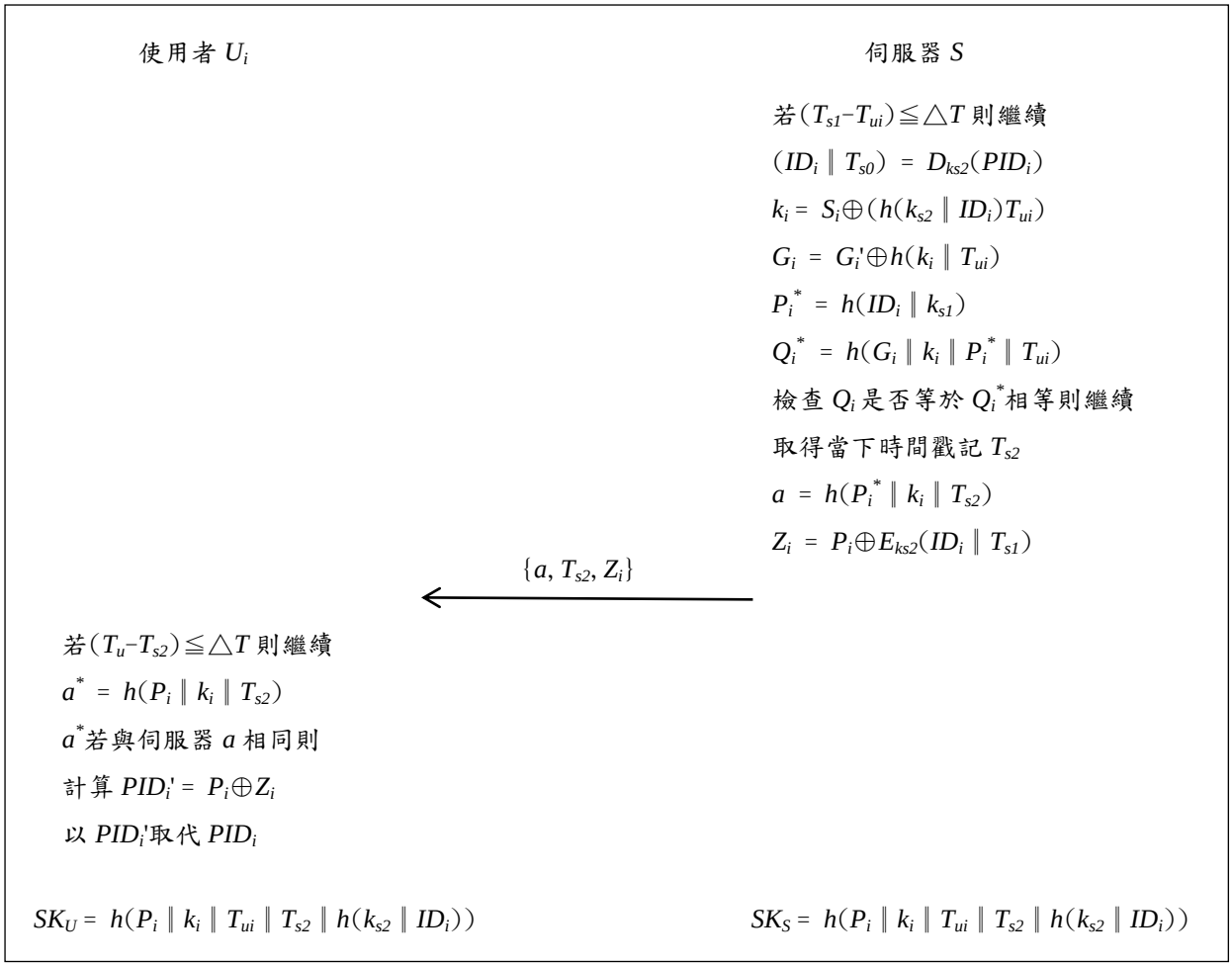
圖一: Chaudhry 等人機制的註冊階段

附件 2



圖二: Chaudhry 等人機制的登入階段

附件 2



圖三: Chaudhry 等人機制的驗證階段