Liu 等人遠端認證機制之安全漏洞

The Flaws in Liu et al.’s Remote Authentication Scheme

黃詳嘉
Hsiang-Chia Huang
中國文化大學
資訊管理學系
研究生
banana800908@hotmail.com

余平
Yu Ping
中國文化大學
資訊管理學系
助理教授
yp@faculty.pccu.edu.tw

摘　要

現今電腦普及和資訊科技蓬勃發展，使得資訊安全成為重要的研究議題之一，使用智慧卡結合密碼進行認證廣泛運用於網路上，例如金融卡及信用卡，其功能及安全性應用在資訊安全的研究，具有相當的重要性。

在 2016 年 Liu 等人指出 Li 等人之認證機制，機制上有許多缺失，如中間人攻擊、內部攻擊等，且有計算效能等問題，並提出改進認證機制，但本研究發現 Liu 等人之機制仍有許多安全漏洞，如中間人攻擊的安全漏洞、無法抵抗離線猜密碼攻擊且不具有完美前向私密性等問題，本研究針對 Liu 等人機制進行安全性分析，說明其弱點以於未來提出更具安全性的認證機制。

關鍵詞：智慧卡、認證、離線猜密碼攻擊、中間人攻擊、完美前向私密性。

Abstract

Nowadays, with the popularity of computer and the rapid development of information technology, information security has become one of the most important research issue. The use of smart cards combined with password authentication is widely used on the Internet, such as financial cards and credit cards. Its function and security in the application of information security research, has a considerable importance.

In 2016, Liu et al. proposed that Li et al. authentication scheme has many secure flaws, like man in the middle attack, insider attacks, and the problem computational inefficiency. Liu et al. proposed a new scheme to improve security. However, in this study, we find that their scheme still has many weakness, such as man in the middle attack, off-line password guessing attack and failure to achieve perfect forward secrecy. We also explain the point of weaknesses and prepare to propose a more secure authentication scheme in the future.

Keywords: Smart Card, Authentication, Off-line password guessing attack, Man in the middle attack, Perfect Forward Secrecy

1. 緒論

近年廣泛的運用智慧卡進行認證，許多學者提出不同的認證機制，希望能提升智慧卡的安全性，2012 年 Chen 等人[1]指出 Xu 等人[2]、Sood 等人[3]及 Song 等人[4]所提出的機制有許多的安全漏洞及計算效能低下。

2013 年 Li 等人[5]提出一個改良 Chen 等人[1]的認證機制，指出它具有完美前向私密性，可以抵抗重送攻擊、偽裝攻擊，可以互相認證等好處。Liu 等人[6]指出 Li 等人[5]之認證機制，無法抵抗中間人攻擊、內部攻擊，進而提出一個改良的認證機制以修正這些安全漏洞。

但本研究發現 Liu 等人的改良認證機制依舊無法抵抗中間人攻擊，及其他安全漏洞，如無法抵抗離線猜密碼攻擊、偽裝攻擊及完美前向私密性有問題；我們將在本研究中探討 Liu 等人之認證機制，解析其安全性。

本文其餘章節內容如下：第2節簡述Liu等人之遠端認證機制，第3節分析Liu等人認證機制安全漏洞，第4節為本文之結論。

2. Liu 等人所提之認證機制

Liu 等人提出一個改良 Li 等人的遠端認證機制，以增加其安全性，此認證機制由註冊、登入、認證、更改密碼四個階段組成。本研究所使用的各項符號如下表 1。

表 1：本研究使用的符號註解

代號	說明
U_i	使用者 i。
S	伺服器。
ID_i	使用者 i 的身分識別。
PW_i	使用者 i 的密碼。
SC_i	使用者 i 的智慧卡。
x	伺服器的私密金鑰。
r	隨機亂數
N_i	使用者 i 產生的隨機亂數。
N_s	伺服器 S 產生的隨機亂數。
$h(\cdot)$	單向雜湊函數。
$\|$	串聯運算子。
$\oplus$	互斥或運算子。
T_i	使用者 i 的時間戳記。
T_s	伺服器 S 的時間戳記。
ΔT	最大的傳輸延遲時間。
⋯⋯▶	秘密通道
——▶	公開通道

2.1 註冊階段

此階段使用者 U_i 向伺服器 S 註冊，以取得智慧卡。

(1) 使用者 U_i 選擇自己的身分識別 ID_i 和密碼 PW_i，還有一個隨機亂數 r，計算 $h(r \| PW_i)$，經安全通道傳送註冊資訊$\{ID_i, h(r \| PW_i)\}$給伺服器 S。

(2) 伺服器收到註冊資訊$\{ID_i, h(r \| PW_i)\}$後，計算 $A_i = h(ID_i \oplus x) \| h(x)$、$B_i = A_i \oplus h(r \| PW_i)$及 $C_i = h(A_i \| ID_i \| h(r \| PW_i))$。

(3) 伺服器儲存資料 B_i、C_i 及 $h(\cdot)$到智慧卡 SC_i 中，現 $SC_i = \{B_i, C_i, h(\cdot)\}$，經過安全通道把智慧卡交給使用者 U_i。

(4) 收到智慧卡後使用者儲存隨機亂數 r 到智慧卡 SC_i 中，故現 $SC_i = \{B_i, C_i, h(\cdot), r\}$。

註冊階段圖可參考附件 1 中的圖 1。

2.2 登入階段

(1) 使用者 U_i 將 SC_i 插入讀卡機，然後輸入身分識別 ID_i 及密碼 PW_i。

(2) SC_i 計算 $A_i' = B_i \oplus h(r \| PW_i)$及 $C_i' = h(A_i' \| ID_i \| h(r \| PW_i))$，並檢查是否 $C_i' = C_i$，如果相同進入下個步驟，若不同則終止登入階段。

(3) SC_i 選擇一個隨機亂數 N_i，計算 $D_i = h(ID_i \oplus N_i)$及 $E_i = A_i' \oplus N_i \oplus T_i$，其中 T_i 是使用者 U_i 目前的時間戳記。

(4) SC_i 傳送登入訊息$\{ID_i, D_i, E_i, T_i\}$經公開通道給伺服器 S。

2.3 認證階段

(1) 伺服器檢查 ID_i 的正確性及是否$(T_i' - T_i) \le \Delta T$，其中 T_i'為伺服器接收到 U_i 傳送登入訊息的時間戳記，ΔT 為最大的傳輸延遲時間，如果不符表示傳輸時間超過最大延遲時間，超過將終止此階段，若符合則進入下個步驟

(2) 伺服器計算 $A_i = h(ID_i \oplus x) \| h(x)$、$N_i' = E_i \oplus A_i \oplus T_i$ 及 $D_i' = h(ID_i \oplus N_i')$，其中 x 為伺服器的私密金鑰，檢查是否 $D_i' = D_i$，如果不符終止此階段，若符合則接受 U_i 的登入並進入下個步驟。

(3) 伺服器選擇一個隨機亂數 N_s，計算 $F_i = h(ID_i \oplus N_s)$及 $G_i = A_i \oplus N_s \oplus T_s$，其中 T_s 是伺服器 S 目前的時間戳記。

(4) 伺服器經公開通道傳送認證訊息$\{F_i, G_i, T_s\}$給使用者。

(5) 收到認證訊息$\{F_i, G_i, T_s\}$後，使用者檢查$(T_s' - T_s) \le \Delta T$，其中 T_s'為使用者接收到 S 傳送認證訊息的時間，如果不符終止此階段，若符合則接受 S 的驗證並進入下個步驟。

(6) 使用者計算 $N_s' = G_i \oplus A_i' \oplus T_s$ 及 $F_i' = h(ID_i \oplus N_s')$，檢查是否 $F_i' = F_i$，如果不符終止此階段，若符合則進入下個步驟。

(7) 使用者 U_i 和伺服器 S 各自利用計算結果建構一個共享的會期金鑰 $SKey_i = h(N_i \| N_s' \| h(A_i' \oplus ID_i))$及 $SKey_s = (N_i' \| N_s \| h(A_i \oplus ID_i))$確保秘密通訊。

登入及認證階段圖可參考附件 1 中的圖 2。

2.4 更換密碼階段

(1) 使用者 U_i 將智慧卡插入讀卡機，然後輸入 ID_i 及 PW_i，要求更換密碼。

(2) 智慧卡計算 $A_i^* = B_i \oplus h(r \| PW_i)$、$C_i^* = h(A_i^* \| ID_i \| h(r \| PW_i))$，檢查是否 $C_i^* = C_i$，如果不相同終止此階段，若相同使用者可輸入新密碼 PW_i^{new}。

(3) 智慧卡 SC_i 計算 $B_i^{new} = A_i^* \oplus h(r \| PW_i^{new})$及 $C_i^{new} = h(A_i^* \| ID_i \| h(r \| PW_i^{new}))$，智慧卡將 B_i^{new} 及 C_i^{new} 取代舊值 B_i 及 C_i，並儲存進智慧卡 $SC_i = \{B_i^{new}, C_i^{new}, h(\cdot), r\}$。

更換密碼階段圖可參考附件 2 中的圖 3。

3. Liu 等人遠端認證機制之安全性分析

本研究發現 Liu 等人提出的認證機制具有幾個缺失，包括無法抵抗離線猜密碼攻擊、偽裝攻擊及不具有完美前向私密性，還有跟 Li 等人所提出的認證機制一樣無法抵抗中間人攻擊，以下介紹我們所提出的攻擊方式。

3.1 離線猜密碼攻擊

Liu 等人的機制在註冊時並未檢驗 ID 是否被註冊過，如攻擊者重複註冊同樣 ID_i 即可得知使用者 U_i 之智慧卡中的共享秘密，其步驟如下。

(1) 攻擊者 U_A 選擇密碼 PW_A 和一個隨機亂數 r_A 還有跟使用者 U_i 一樣的 ID_i，ID_i 可由 U_i 的登入訊息取得，計算 $h(r_A \| PW_A)$，傳送$\{ID_i, h(r_A \| PW_A)\}$給伺服器。

(2) 伺服器收到註冊資訊$\{ID_i, h(r_A \| PW_A)\}$後，計算 $A_i = h(ID_i \oplus x) \| h(x)$、$B_A = A_i \oplus h(r_A \| PW_A)$ 及 $C_A = h(A_i \| ID_i \| h(r \| PW_A))$。

(3) 伺服器儲存資料 B_A、C_A 及 $h(\cdot)$到智慧卡 $SC_A = \{B_A, C_A, h(\cdot)\}$，經過安全通道把智慧卡交給攻擊者 U_A。

(4) 攻擊者知道 B_A 及 $h(r_A \| PWA)$， U_A 計算 $A_i = B_A \oplus h(r_A \| PW_A)$，算出 A_i。

(5) $A_i = h(ID_i \oplus x) \| h(x)$，因為 ID_i 相同且 x 為 S 的秘密金鑰所以 A_i 是一樣的，在取得使用者智慧卡 SC_i 後，解出 $SC_i = \{B_i, C_i, h(\cdot), r\}$的內容，其中 $B_i = A_i \oplus h(r \| PW_i)$，已知 B_i、A_i、$h(\cdot)$及 r，首先猜一個密碼 PW_i'，計算 $B_i' = A_i \oplus h(r \| PW_i')$，如 $B_i' = B_i$ 表示 $PW_i' = PW_i$，如不同則重新猜一個 PW_i'，重複上述步驟直到猜出正確 PW_i'。

3.2 使用者偽裝攻擊

Liu 指出攻擊者無法從登入訊息中得知 A_i 及 N_i，攻擊者會產生錯誤的 E_i 給伺服器，伺服器檢查時 $D_i' \neq D_i$，故攻擊者無法偽裝成使用者 U_i。

由 3.1 離線猜密碼攻擊中得知使用者 U_i 的密碼 PW_i 及共享秘密 A_i，可進一步進行使用者偽裝攻擊。

(1) 登入階段時攻擊者 U_A 產生隨機亂數 N_A，計算 $D_A = h(ID_i \oplus N_A)$及 $E_A = A_i \oplus N_A \oplus T_A$，其中 T_A 是攻擊者 U_A 目前的時間戳記。

(2) 傳送登入訊息$\{ID_i, D_A, E_A, T_A\}$經公開通道給伺服器 S。

(3) 伺服器檢查 ID_i 及是否$(T_A' - T_A) \leq \Delta T$，其中 T_A'為 S 接收到攻擊者傳送登入訊息的時間戳記，伺服器計算 $A_i = h(ID_i \oplus x) \| h(x)$、$N_A' = E_A \oplus A_i \oplus T_A$ 及 $D_A = h(ID_A \oplus N_A')$，檢查是否 $D_A' = D_A$，因 A_i 為正確的共享秘密，D_A 將符合伺服器的計算結果並接受攻擊者 U_A 的登入。

3.3 伺服器偽裝攻擊

Liu 指出攻擊者無法從認證訊息中得知 A_i 及 N_s，攻擊者產生錯誤的 F_i 給伺服器，伺服器檢查時 $F_i' \neq F_i$，故攻擊者無法偽裝成伺服器 S。

由 3.1 離線猜密碼攻擊中得知使用者 U_i 的共享秘密 A_i，於認證階段時，攻擊者 U_A 攔截 U_i 的登入及認證訊息進行伺服器偽裝攻擊。

(1) 驗證階段時伺服器選擇一個隨機亂數 N_s，計算 $F_i = h(ID_i \oplus N_s)$及 $G_i = A_i \oplus N_s \oplus T_s$。

(2) 伺服器 S 傳送認證訊息$\{F_i, G_i, T_s\}$經公開通道給 U_i。

(3) 攻擊者 U_A 從中攔截認證訊息$\{F_i, G_i, T_s\}$後，攻擊者選擇一個隨機亂數 N_a，計算 $F_a = h(ID_i \oplus N_a)$及 $G_a = A_i \oplus N_a \oplus T_a$，其中 T_a 是攻擊者 U_A 目前的時間戳記，再將認證訊息$\{F_a, G_a, T_a\}$傳送給 U_i。

(4) U_i 收到認證訊息$\{F_a, G_a, T_a\}$後，檢查是否$(T_a' - T_a) \leq \Delta T$，其中 T_a'為 U_i 接收到攻擊者傳送認證訊息的時間戳記，如果不符終止此階段，若符合則進入下個步驟。

(5) 使用者計算 $N_a' = G_a \oplus A_i' \oplus T_a$ 及 $F_a' = h(ID_i \oplus N_a')$，檢查是否 $F_a' = F_a$，如果不符表示使用者 U_i 不相信攻擊者 U_A 為伺服器 S，若符合則 U_i 把攻擊者 U_A 當作為伺服器 S。

3.4 中間人攻擊

Liu 宣稱他們的機制可以抵抗中間人攻擊，指出攻擊者無法從登入訊息中得知 A_i 及 N_i，所以攻擊者會產生錯誤的 E_i 給伺服器，伺服器檢查時 $D_i' \neq D_i$；Liu 指出攻擊者無法從認證訊息中得知 A_i 及 N_s，攻擊者產生錯誤的 F_i 給伺服器，伺服器檢查時 $F_i' \neq F_i$，故可以抵抗中間人攻擊。

但本研究 3.1 離線猜密碼攻擊中可得知使用者的共享秘密 A_i，攔截登入訊息$\{ID_i, D_i, E_i, T_i\}$得知 E_i 及 T_i，其中 $E_i = A_i \oplus N_i \oplus T_i$，故 $N_i = A_i \oplus E_i \oplus T_i$，即可算出 N_i；攔截認證訊息$\{F_i, G_i, T_s\}$得知 G_i 及 T_s，其中因為 $G_i = A_i \oplus N_s \oplus T_s$，故 $N_s = A_i \oplus G_i \oplus T_s$，即可算出 N_s，因此 Liu 等人的機制無法抵抗中間人攻擊。

承接上面 3.2 及 3.3 的偽裝攻擊，攻擊者同時偽裝使用者及伺服器。

(1) 使用者 U_i 登入時，SC_i 選擇一個隨機亂數 N_i，

計算 $D_i = h(ID_i \oplus N_i)$及 $E_i = A_i' \oplus N_i \oplus T_i$，其中 T_i 是使用者 U_i 目前的時間戳記。

(2) 傳送登入訊息$\{ID_i, D_i, E_i, T_i\}$經公開通道給伺服器 S。

(3) 攻擊者 U_A 從中攔截登入訊息，產生隨機亂數 N_A，計算 $D_A = h(ID_i \oplus N_A)$及 $E_A = A_i \oplus N_A \oplus T_A$，其中 T_A 是攻擊者 U_A 目前的時間戳記。

(4) 傳送登入訊息$\{ID_i, D_A, E_A, T_A\}$經公開通道給伺服器 S。

(5) 伺服器檢查 ID_i 及是否$(T_A' - T_A) \leq \Delta T$，其中 T_A'為 S 接收到攻擊者傳送登入訊息的時間戳記，伺服器計算 $A_i = h(ID_i \oplus x) \| h(x)$、$N_A' = E_A \oplus A_i \oplus T_A$ 及 $D_A = h(ID_A \oplus N_A')$，檢查是否 $D_A' = D_A$，因 A_i 為正確的共享秘密，D_A 將符合伺服器的計算結果並接受攻擊者 U_A 的登入。

(6) 伺服器選擇一個隨機亂數 N_s，計算 $F_i = h(ID_i \oplus N_s)$及 $G_i = A_i \oplus N_s \oplus T_s$，其中 T_s 是伺服器 S 目前的時間戳記。

(7) 伺服器 S 傳送認證訊息$\{F_i, G_i, T_s\}$經公開通道給 U_i。

(8) 攻擊者 U_A 從中攔截認證訊息$\{F_i, G_i, T_s\}$後，攻擊者選擇一個隨機亂數 N_a，計算 $F_a = h(ID_i \oplus N_a)$及 $G_a = A_i \oplus N_a \oplus T_a$，其中 T_a 是攻擊者 U_A 目前的時間戳記，再將認證訊息$\{F_a, G_a, T_a\}$傳送給 U_i。

(9) 使用者 U_i 收到認證訊息$\{F_a, G_a, T_a\}$後，檢查是否$(T_a' - T_a) \leq \Delta T$，其中 T_a'為 U_i 接收到攻擊者傳送認證訊息的時間戳記，如果不符終止此階段，若符合則進入下個步驟。

(10) 使用者 U_i 計算 $N_a' = G_a \oplus A_i' \oplus T_a$ 及 $F_a' = h(ID_i \oplus N_a')$，檢查是否 $F_a' = F_a$，如果不符表示使用者 U_i 不相信攻擊者 U_A 為伺服器 S，若符合則 U_i 把攻擊者 U_A 當作為伺服器 S。

3.4 不具完美前向私密性

Liu 指出他們所提出的認證機制提供完美前向私密性，指出攻擊者必須知道 N_i、N_s 才可得到會期金鑰 $SKey_i = h(N_i \| N_s' \| h(A_i' \oplus ID_i))$及 $SKey_s = (N_i' \| N_s \| h(A_i \oplus ID_i))$。

在完美前向私密性下，伺服器的私密金鑰 x 暴露了。

(1) 攔截登入訊息得知 ID_i，由 $A_i = h(ID_i \oplus x) \| h(x)$ 算式中可算出 A_i。

(2) 攔截登入訊息$\{ID_i, D_i, E_i, T_i\}$，由 $E_i = A_i \oplus N_i \oplus T_i$ 算式中算出 N_i。

(3) 攔截驗證訊息$\{F_i, G_i, T_s\}$，由 $G_i = A_i \oplus N_s \oplus T_s$ 算式中算出 N_s。

(4) 伺服器的私密金鑰 x 被得知後，可算出會期金鑰 $SKey_i = h(N_i \| N_s' \| h(A_i' \oplus ID_i))$及 $SKey_s = (N_i' \| N_s \| h(A_i \oplus ID_i))$，故 Liu 等人提出的機制沒有完美前向私密性。

4. 結論

現今認證機制是資訊安全中重要的研究之一，需要完備的認證機制以應付目前的智慧卡安全需求。

Liu 等人之認證機制，抵抗離線猜密碼攻擊的簡易改進方法可於註冊時檢驗 ID 是否被註冊過，以避免受到惡意使用者重複註冊相同 ID 進行離線猜密碼攻擊，進而進行偽裝及中間人攻擊；在完美前向私密性下，由於 A_i 僅使用 ID_i 與 x 進行互斥或和雜湊函數的保護，過於簡單即可算出，導致會期金鑰因 x 暴露了也跟著被計算出來，以至於不具有完美前向私密性。

且 Liu 等人的機制並沒有提供匿名，因此未來研究方向如果可以提出具有匿名性的認證機制，可使安全機制更加完善及安全。

參考文獻

[1] Chen, B. L., Kuo, W. C., & Wuu, L. C. (2014). Robust smart-card-based remote user password authentication scheme. *International Journal of Communication Systems*, 27(2), 377-389.

[2] Xu J, Zhu WT, Feng DG. An improved smart card based password authentication scheme with provable security.*Computer Standards & Interfaces* 2009; 31(4):723–728.

[3] Sood SK, Sarje AK, Singh K. An improvement of Xu *et al.*'s authentication scheme using smart cards. *Proceedings of The Third Annual ACM Bangalore Conference*, Bangalore, Karnataka, India, 2010; 1–5.

[4] Song R. Advanced smart card based password authentication protocol. *Computer Standards & Interfaces* 2010;32(5):321–325.

[5] Li, X., Niu, J., Khan, M. K., & Liao, J. (2013). An enhanced smart card based remote user password authentication scheme. *Journal of Network and Computer Applications*, 36(5), 1365-1371.

[6] Liu, Y. J., Chang, C. C., & Chang, S. C. (2016). An Efficient and Secure Smart Card Based Password Authentication Scheme. *International Journal of Network Security*.

附件 1

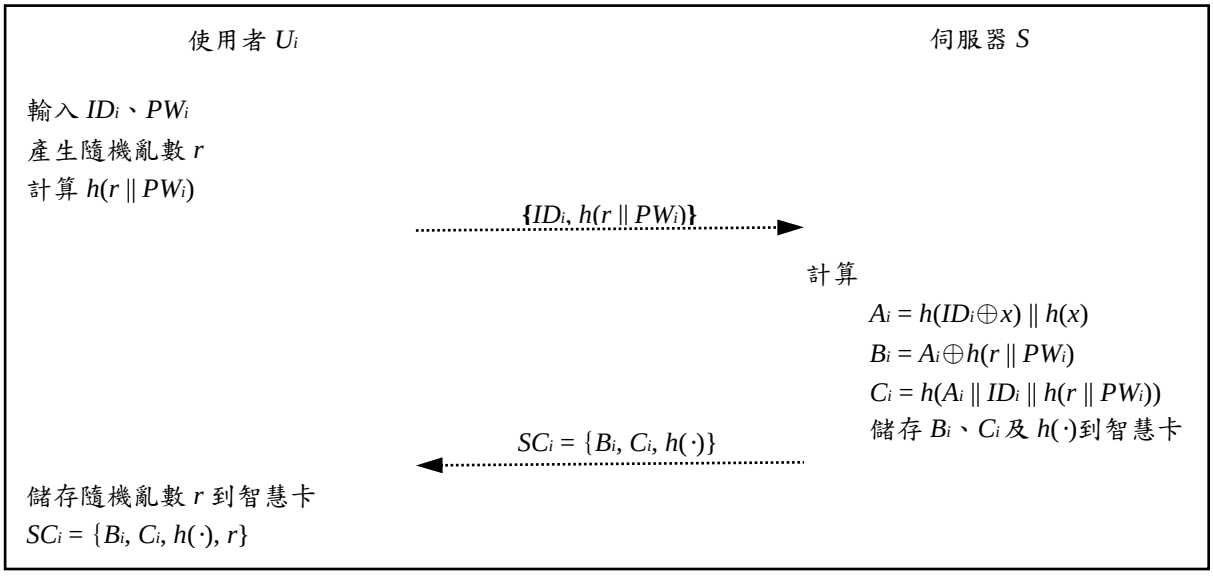

圖 1 Liu 等人註冊階段

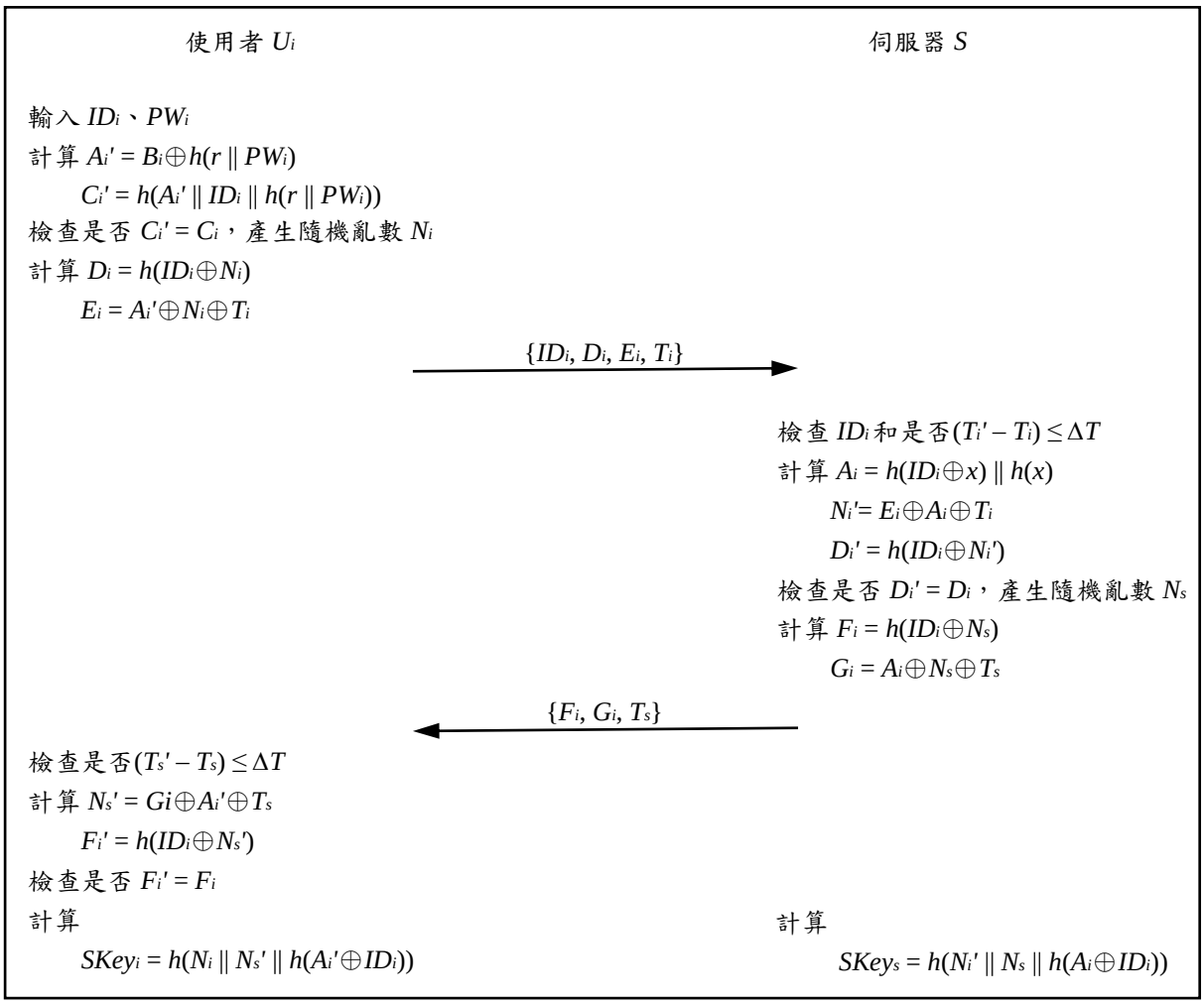

圖 2 Liu 等人登入及認證階段

附件 2

使用者 U_i

輸入 ID_i、PW_i

計算 $A_i^* = B_i \oplus h(r \| PW_i)$

$C_i^* = h(A_i^* \| ID_i \| h(r \| PW_i))$

檢查是否 $C_i^* = C_i$

選擇新密碼 PW_i^{new}

計算 $B_i^{new} = A_i^* \oplus h(r \| PW_i^{new})$

$C_i^{new} = h(A_i^* \| ID_i \| h(r \| PW_i^{new}))$

$SC_i = \{B_i^{new}, C_i^{new}, h(\cdot), r\}$

圖 3 Liu 等人更換密碼階段