# 強化植基於智慧卡之身分驗證暨秘密通訊檔案傳輸機制設計

作者／楊博元、陳毅恩、蘇品長

**提要**

一、國軍業務資訊化多年，包含電子公文、郵件及檔案交換等均仰賴網路執行，為確保授權存取之合法性，需透過有效的身分驗證機制，其中智慧卡因其輕便與高效能，廣泛應用於各類場景。

二、軍事應用中常需在不安全的通訊環境下傳輸機敏資料。本研究修正既有驗證架構，提出不經網路即可同步生成會議金鑰之方法，使檔案得以加密後再傳輸，有效防止金鑰外洩，保障資訊機密。

三、本研究具體貢獻為：（一）強化金鑰不可預測性；（二）提升參數選擇彈性；（三）實現離線同步加解密；（四）改善人工交換密碼機制，並可應用於智慧卡加密檔案傳輸，強化國軍通訊安全。

**關鍵詞：智慧卡、身分驗證、會議金鑰、檔案傳輸。**

## 前言

全球軍事力量現代化，資訊戰在現代戰爭中的地位日益重要，特別是烏俄戰爭中，雙方皆展現出利用網路攻擊癱瘓對方指揮通信系統的能力，[1]使得保護敏感軍事資訊成為重中之重。隨著網路傳輸速度不斷提升，越來越多服務及應用透過網路而完成，國軍的內部網路也不例外，舉凡人事資料查詢、後勤補保作業、公文電子交換、薪餉服務平台等各項系統，以提升工作效率或服務官兵為目的，陸續上線執行，網路環境使用者眾多，為了確保網路中的使用者能依據其授權範圍合法存取服務，身分驗證機制在通信協議中扮演著重要角色。

日常業務執行過程中，部門之間常需要共享訊息而進行檔案傳輸交換，實務上原仰賴內部網路通訊軟體交換功能或是國軍電子郵件夾帶檔案等方式完成，然因上述機制均無須經第三者針對檔案內容進行審核，機敏資訊未經審核流落無關人等手中，進而造成洩密等情事。為避免重蹈覆轍，現行檔案傳輸作業已建置專屬平台，並建立機制定期由第三方人員(單位保密軍官)針對被傳輸檔案進行審核，同時滿足業務間的需求及安全上的目的；然而，非營利組織OWASP(

1 舒孝煌，〈俄烏戰場上的網路戰與宣傳戰〉《國防安全研究院即時評析》，https://indsr.org.tw/focus?typeid=31&uid=11&pid=586，2023/02/23.

Open Web Application Security Project)，提出OWASP Top 10研究成果中，[2]公布網路中最具風險的十項安全議題中，認證及驗證機制失效（Identification and Authentication Failures）在風險項目中排名第七，是指應用程式未能正確執行使用者身份驗證(Identify Authentication)和會話管理(Session Management)，導致攻擊者能夠冒充其他用戶或繞過服務的身份驗證機制，微軟威脅情報中心（MSTIC）在其「俄烏網路戰爭早期經驗報告」中建議，政府機構、企業及其供應商應密切監控遠端存取基礎設施的所有身份驗證活動，尤其要檢查是否存在異常的遠端存取行為，並在發現問題時及時通報。報告特別強調，單因素身分驗證的帳戶系統存在較高風險，需特別注意並加強安全防護措施，[3]顯見在現代網路攻擊事件中，利用身分驗證弱點的手法仍層出不窮。

考量國軍在各項訊息傳遞時的重要性及機敏性，必須於現行檔案傳輸系統架構下建置更安全的資料交換機制(如圖1)，本研究期以現有硬體設施及資源狀況下，設計可同步加密之檔案傳輸系統，使得已獲得會議金鑰的雙方可於離線狀態下同步對該金鑰進行擾亂，並於完成後獲取同一把金鑰，減少會議金鑰在不安全的網路環境中傳遞之機會，以避免遭攔截，有效提升檔案傳輸之安全性。


圖 1 國軍檔案傳輸示意圖
資料來源：作者繪製。

## 文獻探討

### 一、身分驗證架構

Lamport首先提出了基於密碼的身分驗證架構，[4]以應對不安全網路環境的挑

2 OWASP, *Owasp Top 10 - 2021*, https://owasp.org/Top10, 2024/10/4.
3 施立成，〈網路戰爭無國界，以俄烏網路戰為鏡提升全民資安防護意識〉《數位時代》，*https://www.bnext.com.tw/article/71389/hacker%EF%BC%8Dinformation-security-mstic*, 2022/08/26.
4 Lamport, L. "Password Authentication with Insecure Communication." *Communications of the ACM*, vol. 24, no. 11(1981), pp. 770-772.

戰。隨後研究者們相繼發展多種身分驗證方案，Hwang和Li推出基於智慧卡的遠端使用者身分驗證方法，[5]採用了ElGamal離散對數加密技術，[6]避免密碼表使用及其可能之安全風險。

Liao和Wang則設計一種適用於多伺服器環境的身分驗證架構，[7]雖宣稱能防禦多種攻擊，但Hsiang和Shih指出其在抵禦內部攻擊(Insider Attack)、偽造攻擊(Masquerade Attack)和提供交互認證方面存在不足，並提出了修正版架構。[8]然而，Sood等學者發現此修正版架構仍易受到重送攻擊(Replay Attack)、偽冒攻擊(Impersonation Attack)及智慧卡失竊攻擊(Stolen Smart Card Attack)影響。[9]

此外，Lee等人也指出伺服器欺騙攻擊(Server Spoofing Attack)等問題，[10]儘管提出改進建議，但該架構仍未能完全解決其弱點。Xue等人進一步指出，[11]Li等學者的方案在應對重送攻擊、阻斷服務攻擊(Denial-of-Service Attack, DoS)、智慧卡偽造攻擊(Smart Card Forgery Attack)及竊聽攻擊(Eavesdropping Attack)上存在挑戰，[12]並建議在架構中引入時戳(Timestamp)以提升安全性。

## 二、智慧卡應用

智慧卡(Smart Card)廣泛的應用於生活之中，不論在交通、醫療、商務及居家生活等處均能夠享受其輕巧的便利性，智慧卡又稱作IC卡(Integrated Circuit Card, IC Card)，在與信用卡一般大小的塑膠製卡片上嵌入具有計算能力的晶片，使其具有基本運算及儲存能力，相關標準規範於ISO 7816、ISO 14443及ISO 18092之中，依照其使用方式可區分為接觸式、非接觸式及混合式卡片(如表1)，接觸式卡片必須透過讀卡機等載具實體接觸後才能進行讀寫，有著穩定的資料傳輸過程，一般用於要求傳輸穩定性及安全需求較高之服務，非接觸式卡片只需要將

5 Hwang, M. S., 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.

6 Elgamal, T. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." *IEEE Transactions on Information Theory*, Vol. 31, no. 4(1985), pp. 469-472.

7 Liao, Y. P., and S. S. Wang. "A Secure Dynamic Id Based Remote User Authentication Scheme for Multi-Server Environment." *Computer Standards & Interfaces*, Vol. 31, no. 1(2009), pp. 24-29.

8 Hsiang, H. C., and W. K. Shih. "Improvement of the Secure Dynamic Id Based Remote User Authentication Scheme for Multi-Server Environment." *Computer Standards & Interfaces*, Vol. 31, no. 6(2009), pp. 1118-1123.

9 Sood, S. K., A. K. Sarje, and K. Singh. "A Secure Dynamic Identity Based Authentication Protocol for Multi-Server Architecture." *Journal of Network and Computer Applications*, Vol. 34, no. 2(2011), pp. 609-618.

10 Lee, C. C., T. H. Lin, and R. X. Chang. "A Secure Dynamic Id Based Remote User Authentication Schemefor Multi-Server Environment Using Smart Cards." *Expert Systems with Applications*, Vol. 38, no. 11(2011), pp. 13863-13870.

11 Xue, K., P. Hong, and C. Ma. "A Lightweight Dynamic Pseudonym Identity Based Authentication and Key Agreement Protocol without Verification Tables for Multi-Server Architecture." *Journal of Computer and System Sciences*, Vol. 80, no. 1(2014), pp. 195-206.

12 Li, X., Y. Xiong, J. Ma, and W. Wang. "An Efficient and Security Dynamic Identity Based Authentication Protocol for Multi-Server Architecture Using Smart Cards." *Journal of Network and Computer Applications*, Vol. 35, no. 2(2012), pp. 763-769.

卡片放置於讀卡設備可感應之範圍之內，其採用線圈感應並以無線電波進行資料的讀寫，適用於要求速度及方便性的服務，而混合式卡片則同時具有接觸式及非接觸式之設計。

表 1 智慧卡分類比較表

| 區分 | 接觸式 | 非接觸式 | 混合式 |
|---|---|---|---|
| **適用環境** | 要求傳輸穩定及安全需求較高之環境 | 要求速度及方便性之環境 | 多功能應用環境 |
| **優點** | 資料傳輸過程較穩定 | 減少因接觸而導致之晶片磨損 | 可結合接觸式及非接觸式卡片之優點 |
| **缺點** | 晶片因接觸容易磨損 | 傳輸距離受限制 | 製作成本較高 |
| **應用** | IC 金融卡、健保 IC 卡 | 悠遊卡、一卡通 | 結合電子交通票券之金融卡 |

資料來源：作者整理。

## 三、串流加密

密碼系統亦可以對明文的加解密方式區分為區塊加密(Block Cipher)及串流加密(Stream Cipher)，區塊加密的概念是將明文區分為數個區塊，並分別對各個區塊實施加密處理，串流加密的特點是在不對文件進行分段的情況下，逐位元對其進行加密操作。然而，當金鑰長度不足時，設計者需開發一種可延伸金鑰的機制，生成足夠覆蓋整份文件之金鑰串流（Keystream）。該金鑰串流與明文結合運算後生成密文。此外，為確保加解密雙方使用相同模式對文件進行處理，系統必須具備高度同步性，以避免因不同步而影響加解密的準確性(流程如圖2)。

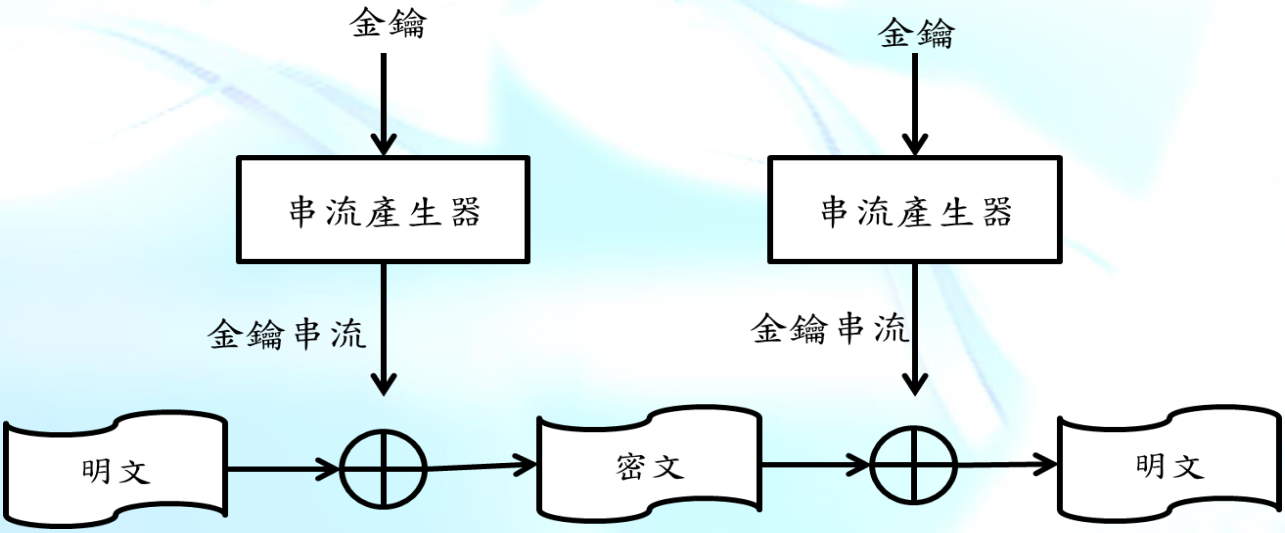


圖 2 串流加密流程示意圖

資料來源：作者繪製。

## 基於智慧卡之身分驗證暨秘密通訊檔案傳輸機制

本研究設計一種金鑰流產生器，能在會議金鑰生成後以離線方式運行，並確保雙方金鑰同步，解決Li等學者架構中會議金鑰需透過網路分享的問題。[13]其次，基於無理數小數點後數字不重複且無限長的特性，選擇將無理數集合引入系統，以生成具高度不可預測性之金鑰串流，克服了羅國良提出以單一圓周率（π）參數易遭測試的問題。[14]此設計使系統在參數選擇上更具彈性，並保證計算結果的不可預測性。通過註冊、登入、驗證、會議金鑰生成、擾亂與增長，以及加解密等階段，有效增強身分驗證的安全性與可靠性。以下對各階段方法進行詳細說明(研究設計架構符號意涵說明如附表)：

### 一、註冊階段

在此階段，系統中所有角色均需向管理伺服器$CS$完成註冊。檔案接收者$U_j$將其識別碼$ID_j$傳送至管理伺服器$CS$作為註冊請求。伺服器隨後選擇兩個隨機參數$x$和$y$，並執行兩次單向雜湊函數運算，將計算結果回傳給檔案接收者$U_j$。

另一方面，傳輸者選擇其識別碼$ID_i$、密碼$P_i$、隨機參數$b$與指定的接收對象，並將$ID_i$與計算結果$A_i = h(b||P_i)$一併傳送至管理伺服器進行註冊。伺服器在接收到$ID_i$和$A_i$後，依據傳輸者指定的接收者進行運算(流程如圖3)。

完成上述運算後，伺服器將$(C_i, D_i, E_i, W_{ij}, h(y), h(.))$存入智慧卡中。使用者取得智慧卡後，將隨機參數$b$存入卡片中，最終智慧卡中保存的資料包括$(C_i, D_i, E_i, W_{ij}, h(y), h(.), b)$。

### 二、登入階段

傳輸者$U_i$輸入其識別碼$ID_i$、密碼 $P_i$以及接收者$ID_j$，由智慧卡利用內部儲存的參數進行合法性驗證。首先智慧卡透過$b$和$P_i$的運算計算出$A_i$，接著將$A_i$、使用者輸入之$ID_i$以及智慧卡內儲存的$h(y)$進行運算，得出$C_i'$，並將其與原本儲存的$C_i$比對驗證是否一致，以確認使用者是否合法。

若驗證結果為合法，智慧卡將隨機生成參數$N_{i1}$，並進一步計算出$B_i, F_i, P_{ij}, CID_i, G_i$等參數。最後，智慧卡將這些參數組合為$(F_i, G_i, P_{ij}, W_{ij}, CID_i)$，通過安全的通道傳送至管理伺服器$CS$進行後續驗證（流程如圖4）。

---

13 Li, X., Y. Xiong, J. Ma, and W. Wang. "An Efficient and Security Dynamic Identity Based Authentication Protocol for Multi-Server Architecture Using Smart Cards." *Journal of Network and Computer Applications*, Vol. 35, no. 2(2012), pp. 763-769.

14 羅國良，〈適用於網站身分驗證及秘密通訊機制探討〉，國防大學管理學院資訊管理研究所碩士論文，2014年

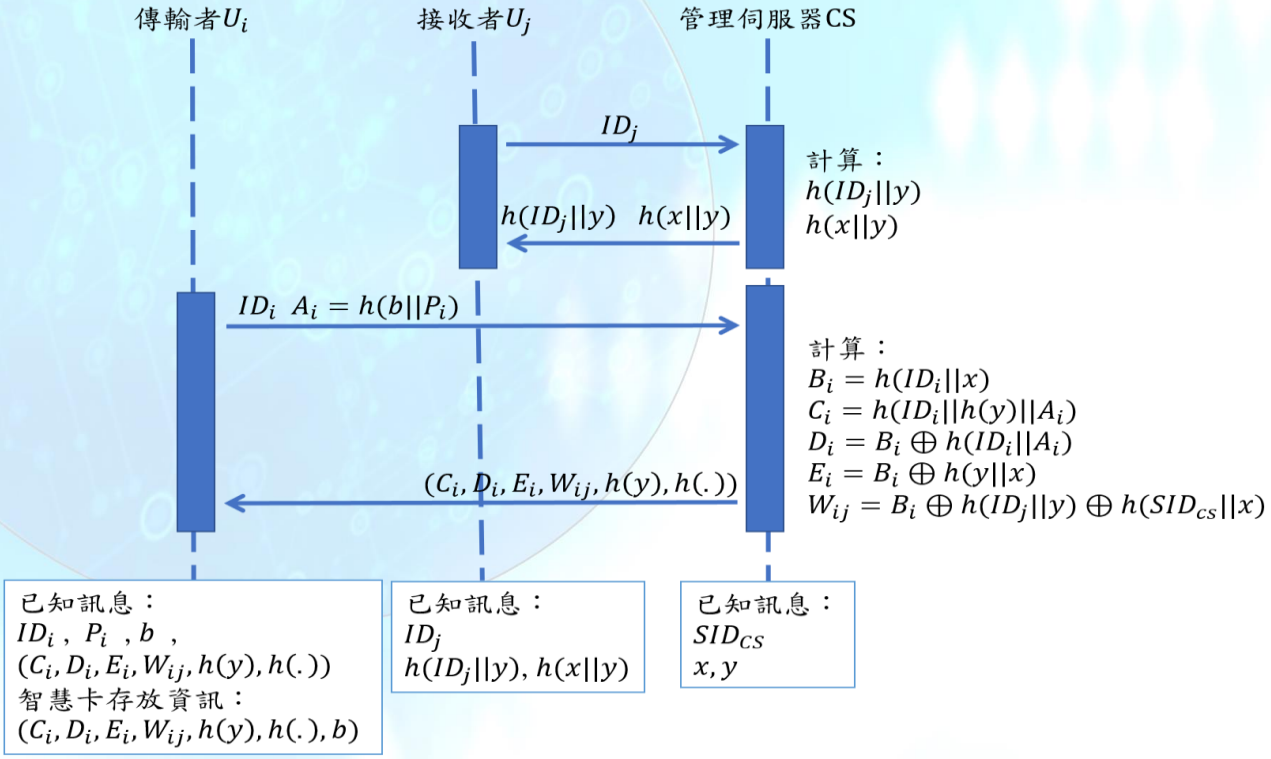


圖 3 系統註冊階段流程圖

資料來源：作者繪製。

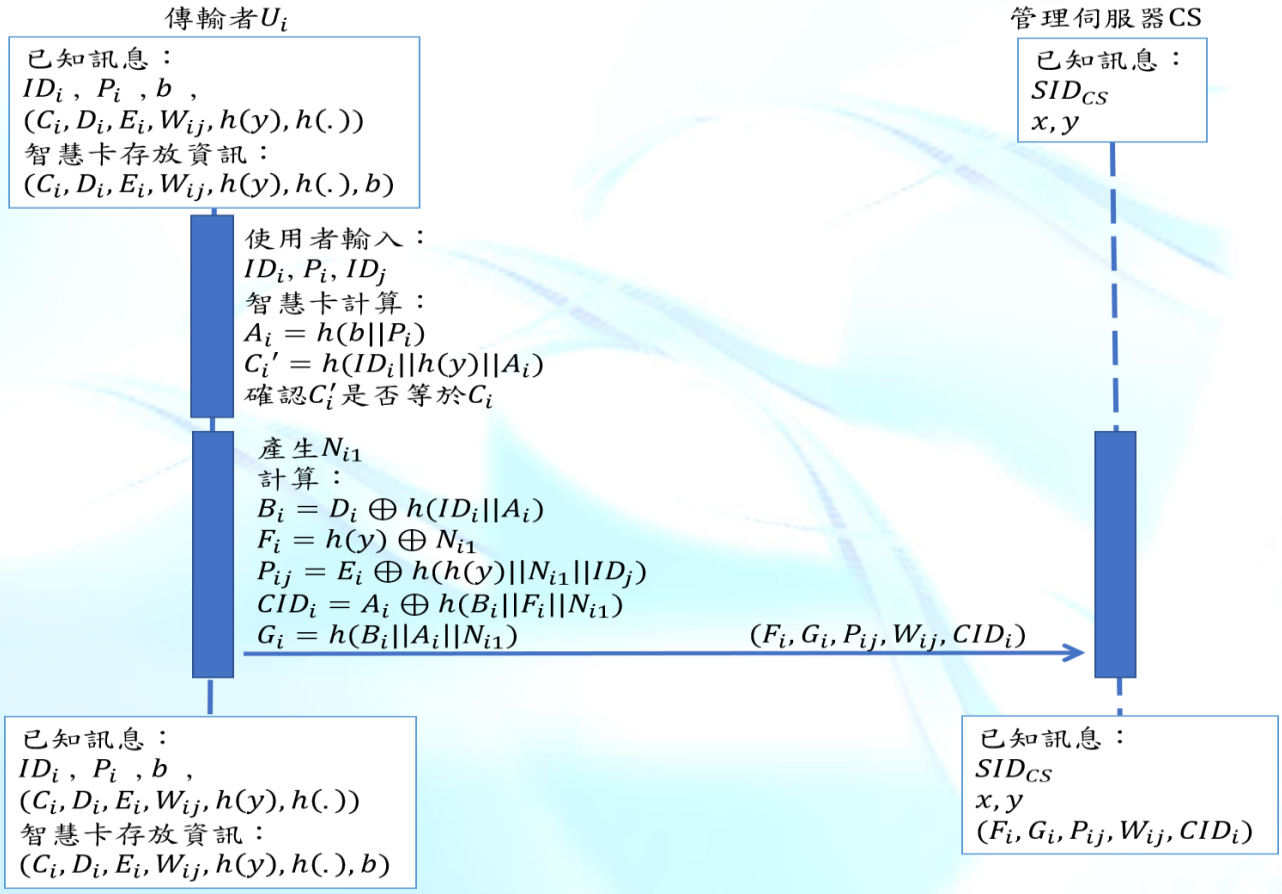


圖 4 系統登入階段流程圖

資料來源：作者繪製。

## 三、驗證及產生會議金鑰階段

當管理伺服器$CS$收到前一步傳輸的資料$(F_i, G_i, P_{ij}, W_{ij}, CID_i)$後，將進行一系列運算以完成驗證並生成會議金鑰。驗證過程是透過計算所得的$G_i'$與接收到的$G_i$進行比對，若兩者一致則驗證成功，否則驗證失敗。

驗證成功後，管理伺服器$CS$將票證$W_{ij}$傳送至接收者$U_j$，接收者$U_j$隨後隨機生成亂數$N_{i2}$並計算出$K_i$及$M_i$，接收者$U_j$將$(K_i, M_i)$傳回管理伺服器$CS$，管理伺服器再驗證計算所得的$M_i'$及$W_{ij}'$是否與$M_i$及$W_{ij}$相符。若相符，則接收者$U_j$通過了合法性驗證。

在確認接收者$U_j$合法後，管理伺服器$CS$將自行生成隨機亂數$N_{i3}$，並運算出$(Q_i, R_i, V_i, T_i)$，將結果傳送給接收者$U_j$用於驗證伺服器的合法性。接收者$U_j$驗證計算所得的$V_i'$是否與$V_i$一致，若一致則判定伺服器$CS$合法。隨後，接收者$U_j$將$V_i, T_i$傳回給傳輸者$U_i$，傳輸者進一步驗證$V_i'$是否等於$V_i$，以確認接收者$U_j$和伺服器$CS$的合法性。

上述所有驗證均通過，則本次會話的會議金鑰$SK$成功建立（流程如圖5）。

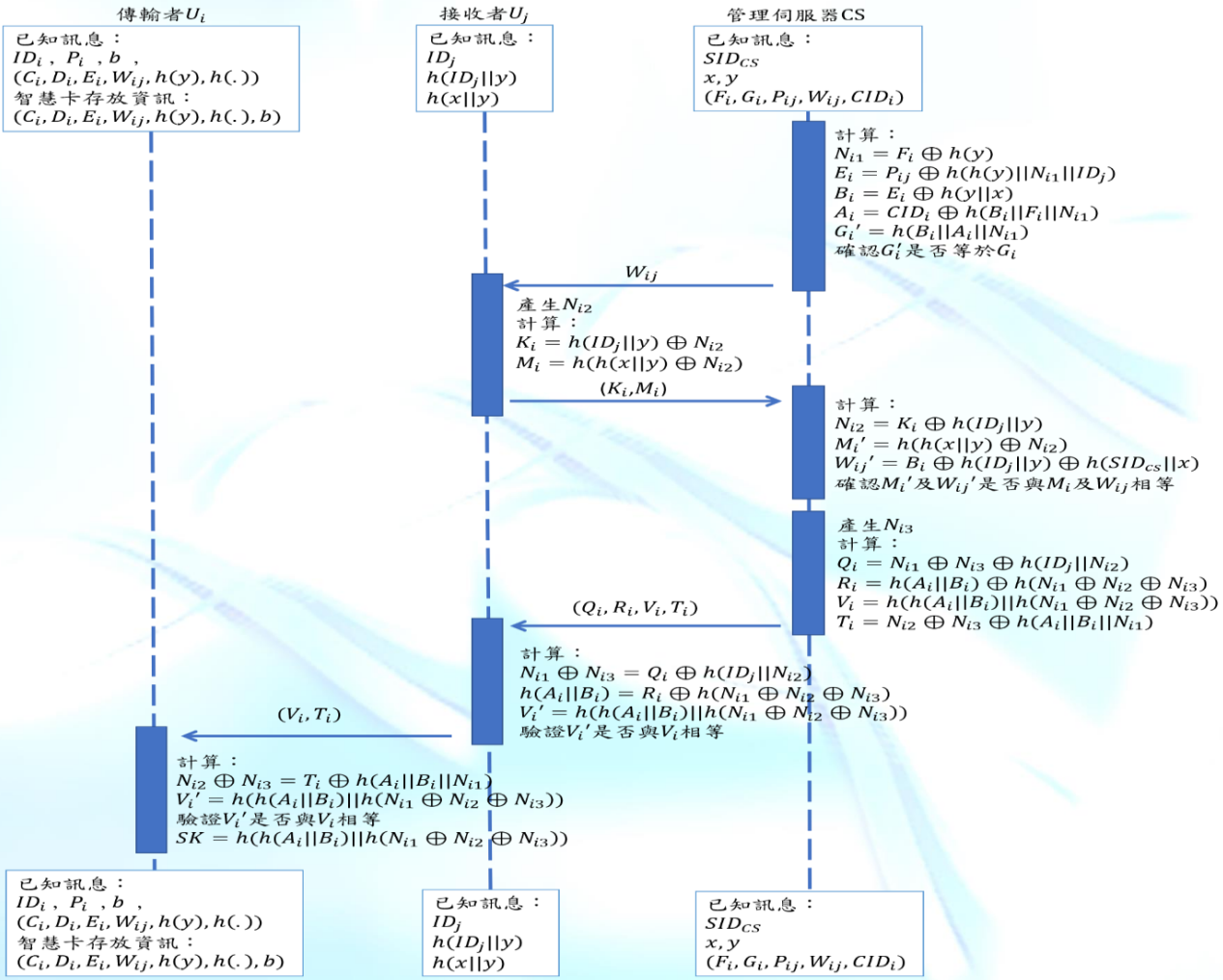


圖 5 驗證及產生會議金鑰流程圖

資料來源：作者繪製。

## 四、會議金鑰擾亂、增長及加解密

在獲取會議金鑰後，仍需設計一套機制以有效防止非法使用者合法存取系統服務。本研究應用環境適用於加解密不限長度的串流資料，因此需要對會議金鑰進行延伸處理，以支持後續之加密運行。為此本研究設計了一種多重選擇性的秘密通訊機制，其核心是引入多樣化之取位參數，並選擇具無限長度且位數不重複特性的無理數作為參數。在擾亂階段，系統引入多項無理數，使其具備高度的選擇性與不可預測性，從而進一步增強身分驗證安全性。

該機制初始設計由系統提供$P_n$項無理數參數作為選擇，整體運作流程分為三個主要階段：取位與擾亂、金鑰增長以及加解密。以下將分別對這三個階段進行詳細說明。

(一)取位與擾亂

在每次取位操作之前，系統會進行初始化，將提供的參數集合中之每個參數分別賦予編號，然後按照以下步驟運算，最終生成亂數長度需與會議金鑰$SK$等長，並通過XOR運算完成擾亂處理（流程如圖6）：

1.會議金鑰十進位化：

首先，將會議金鑰$SK$轉換為十進位數字表示形式。

2.決定使用參數的個數：

將前一步中生成之十進位數字$n$與系統提供的參數數量$P_n$進行模運算，其餘數即為本次加解密階段需要使用之參數個數$n'$。

3.選擇參數：

在參數集合$P_n$中，依續選取編號從1到$n'$的參數值，組成取位參數集合$INum$。

4.決定取位值：

將會議金鑰$SK$的每個數字進行相加運算後，再與$P_n$進行模運算，得到取位之起始位置$tb$。

5.取位：

在取位參數集合$INum$中，從每個參數的第$INum$位開始，按順序取出$SK_{len}/\mathrm{n}'$個位數，並將這些位數依序組合成亂數$p$。

6.擾亂：

將生成的亂數$p'$與會議金鑰$SK$進行XOR運算，以完成對會議金鑰之擾亂處理。

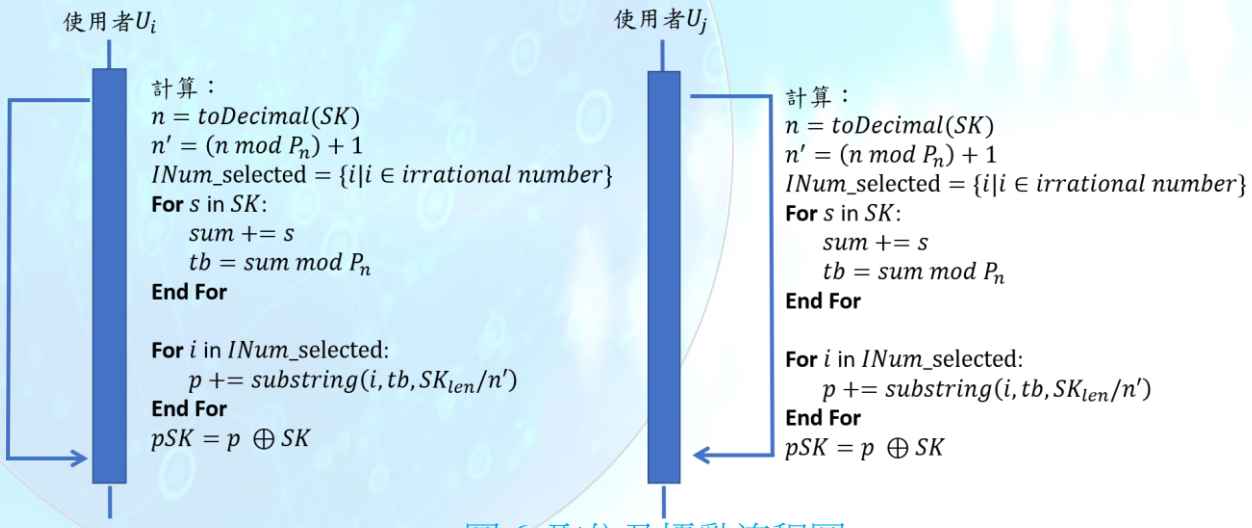


圖 6 取位及擾亂流程圖

資料來源：作者繪製。

(二)金鑰增長

本研究設計的架構採用串流加密機制，有別於區塊加密，在不切割文件前提下，針對明文檔案各位元逐一進行加密計算，以獲得密文。因此，會議金鑰的長度必須大於或等於文件大小，為滿足上述需求，會議金鑰在經過擾亂處理後，需進一步進行延展，以適應文件之加密運算。

本研究將擾亂後的會議金鑰$pSK$導入線性反饋移位暫存器（LFSR），並明確設定其線性函數之最高次方$m$滿足$m \geq pSK$。此設計確保LFSR產生的金鑰流長度足以覆蓋整個明文，避免因長度不足而影響加密完整性。若 $m$ 過小，可能導致金鑰流過短，無法有效對整個文件進行加密，或產生重複金鑰序列，降低加密強度，進而產生遭受攻擊之風險。因此，選擇合適的$m$值對於確保加密安全性至關重要(流程如圖7)。

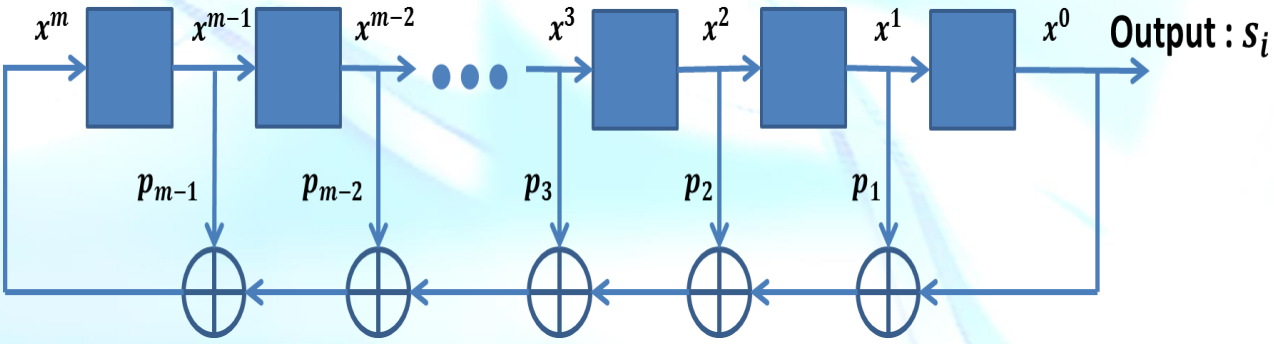


圖 7 金鑰增長流程圖

資料來源：作者繪製。

(三)加解密

在加密階段，訊息中每個位元會依次與金鑰串流進行XOR運算，產生加密後的密文，運算過程簡潔且具備良好的運行性能(流程如圖8)。

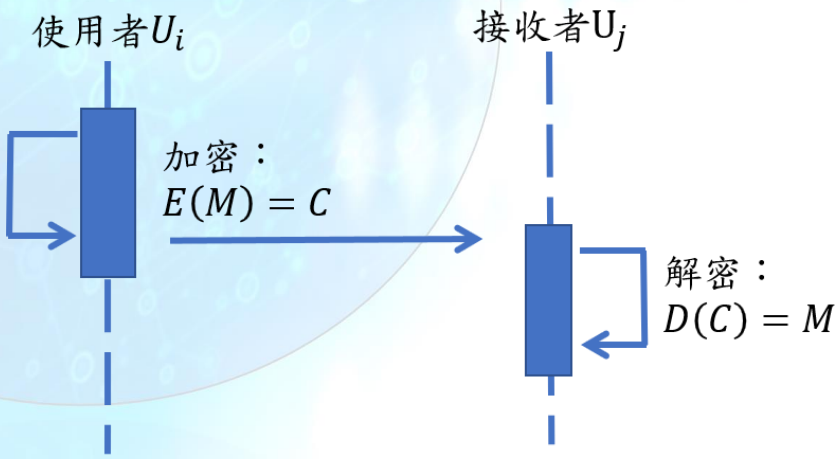


圖 8 加解密流程圖

資料來源：作者繪製。

## 安全性及效益分析

為確保本研究提出架構的安全性，我們將遵循國際標準ISO所訂定之資訊安全管理要求，包括存取控制安全性、服務可用性、資料機密性以及前向保密性（Forward Secrecy）等實施分析。此外將重點聚焦於串流加密機制的三大核心特徵，深入探討其在安全性與實用性方面的優勢，藉以證明本架構能符合國際標準，並說明其作為加密機制之可用性與可靠性。最後針對應用環境進行適用分析，以進一步驗證設計架構的可行性與實際效益。

### 一、安全性分析

(一)存取控制(Access Control)

存取控制的目標是確保組織所提供或使用網路服務免受未經授權之存取，並在系統中負責資源分配與存取權限管理。其核心在於通過認證機制，判斷使用系統資源的合法性，從而保障系統安全性。

本研究提出的架構透過驗證票券$W_{ij}$實現了存取控制概念，在此機制中，管理伺服器$CS$根據傳輸者$U_i$登入成功後所指定之檔案接收對象$U_j$，生成對應的票券$W_{ij}$，該票券由$U_i$傳遞至$CS$，並最終交付給接收者$U_j$。接收者$U_j$透過計算與回傳$W_{ij}'$進行驗證，檢查是否與$W_{ij}$相符，以確認傳輸者$U_i$與接收者$U_j$合法性。

此架構中，管理伺服器$CS$能根據傳輸者指定的接收者，生成針對不同對象的票券，並將其分配至對應之使用者。只有經授權的對象才能接收檔案，從而

有效實現存取控制之目標，並提升系統安全性與管理效能。

(二)服務可用性(Service Availability)

本架構設計理念與 Kerberos 系統類似，用戶在傳輸檔案前，必須經過管理伺服器的認證與授權，確保其合法性後才能進入伺服器。在註冊階段，傳輸者$U_i$從管理伺服器$CS$獲取票據$W_{ij}$，該票據生成公式為：

$$W_{ij} = B_i \oplus h(ID_j||y) \oplus h(SID_{cs}||x)$$

登入階段中，由智慧卡進一步計算授權碼$P_{ij}$，其公式為：

$$P_{ij} = E_i \oplus h(h(y)||N_{i1}||ID_j)$$

透過上述設計，確保用戶在完成註冊與登入流程後，能夠安全且受控的進行檔案傳輸操作，有效提高整體系統之安全性與管理效率。

在使用服務之前，用戶須將上述兩個參數傳送到$CS$進行驗證，若$CS$接收到的封包未包含前述兩個參數，則認為是非法請求，而攻擊者因無法得知$CS$隨機產生之$x$及$y$，無法計算票據$W_{ij}$，欲計算授權碼$P_{ij}$時，因無法得知$E_i = B_i \oplus h(y||x)$，將會導致授權失敗，因此上述機制可以有效抵禦阻斷服務攻擊(DoS)並保持系統可用性。

(三)機密性(Confidentiality)

本研究使用無理數集合$INum$作為生成隨機亂數的基礎，透過對會議金鑰進行轉置與擾亂操作，同時延長其長度，有效提高對金鑰進行猜測之難度。經過處理的會議金鑰可用於資料加解密，不僅確保雙方能獲取相同資料，還能使檔案在不安全之網路中以密文形式傳輸，保障系統機密性。此外，由於現行檔案傳輸系統針對檔案大小設有限制，反饋多項式設計雖未必達到質多項式標準，但已能滿足實際加密需求。

若網路傳輸中的密文遭攻擊者截獲，其將面對必須獲取會議金鑰之難題，惟本系統架構設計以雙方離線方式進行會議金鑰的同步處理，因此，攻擊者無法得知處理後之會議金鑰$pSK$，儘管密文遭截獲，仍無法利用會議金鑰將其解密，故本研究提出的方案可達系統機密性之要求。

(四)前向保密(Forward Secrecy)分析

前向保密(Forward Secrecy)即在攻擊者獲取當前會議金鑰的情況下，仍無法解密過去傳輸之加密內容。本架構中，會議金鑰由雙方在每次傳輸開始前生

成，且金鑰僅在當次檔案傳輸中有效，完成後即被銷毀，不在系統中保存。

此外會議金鑰生成過程依賴於隨機數與一次性參數（如無理數擾亂參數）共同運算完成，本研究所採用的金鑰擾亂與延長機制，以及動態參數之引入，使任何過去的金鑰對未來檔案傳輸之金鑰生成毫無影響，因此，即使攻擊者成功攔截當前金鑰，過去的傳輸內容仍然受到完整保護，進一步降低攻擊成功後之潛在損失，並能有效確保國軍檔案傳輸系統在長期運行中的數據安全。

## 二、串流加密主要特徵

(一)高彈性

本研究引入無理數集合$INum$，並於該集合中添加多種無理數參數，生成擾亂後之會議金鑰$pSK$。該機制運算均於溝通雙方的單機內完成，避免任何敏感資訊在不安全的網路環境中傳遞。透過此高彈性設計，系統在取位與擾亂階段能增加一道有效的防護屏障，進一步強化安全性。

(二)不可預測性

為實現不可預測性，本研究在取位與擾亂階段中，隨機為無理數集合中的參數賦予編號，並通過會議金鑰之十進位化運算，計算取位用參數的個數$n'$。系統依據$n'$從無理數集合中選取參數，使取位過程充滿隨機性與不可預測性，有效提高整體架構的安全性。

(三)同步性

本研究所設計的會議金鑰機制，無需通過網路傳遞即可實現雙方同步。發送方與接收方利用該機制進行文件的加解密後，能夠產生相同結果，保證通信過程之完整性與一致性。此同步性設計亦通過國際標準的檢驗，證明本研究架構符合身分驗證機制之安全要求，並具備實際應用的可行性。

## 三、應用環境適用分析

本研究設計架構以國軍檔案傳輸系統為應用環境，針對單一檔案大小不超過10MB的限制，提出基於串流加密之會議金鑰擾亂與同步機制。本架構利用單向雜湊函數建構的加密需求，僅需額外存取256bits(32Bytes)之會議金鑰與相關加密參數，國軍現行已廣泛使用晶片IC卡進行身分驗證，常見接觸式IC卡容量從16KB到512KB不等，非接觸式IC卡容量則在4KB至8KB之間。現行智慧卡不僅具備足夠記憶體容量以支援本研究所提出的加密需求，還能有效整合現有硬體設施，毋須考量後續增購硬體之預算。

綜上所述，本研究提出的加密架構與國軍現行系統具有高度適用性，能有效提升檔案傳輸過程中之安全性，並滿足實際應用的需求。

## 結論

本研究基於智慧卡應用環境，設計一套可提升國軍檔案傳輸安全性與效能的驗證暨加密架構，透過擾亂參數與串流加密機制，有效提升系統對惡意攻擊之抵抗能力，並兼顧實務作業中對低運算資源、高同步效率的需求。智慧卡目前已廣泛應用於各級公務機關與企業身分驗證作業，藉由導入本研究設計架構，能進一步提升既有身分驗證卡片的應用價值，亦可延伸至其他機敏資料處理場景，本研究於政策與技術整合上，具備四項具體貢獻：

**一、提升金鑰生成之不可預測性**

本研究導入無理數集合與動態選擇機制，使每次金鑰生成過程具備極高的不確定性與非重複性，避免使用固定參數或重複運算造成之潛在風險。此設計有效防止攻擊者透過金鑰模式推導、預測或重建出原始金鑰，強化整體機密性，對於國軍機敏資料保護尤為關鍵，特別適用於跨地、跨層級傳遞需避免關鍵資訊重複特徵的情境。

**二、建置具彈性之參數配置機制**

為因應不同任務、環境與使用者需求，本研究設計可動態選擇或自動調整參數組合的機制，使系統在不同條件下皆能維持穩定運作與加密強度。彈性配置亦有助於未來政策部署時，依任務等級、使用單位資源條件或資訊敏感程度進行差異化設定，有助於實施分級資安防護策略，並兼顧安全性與系統效能。

**三、實現可離線同步之加密作業模式**

在軍事通訊、突發事件處理或災害應變等場域中，網路連線可能受限甚至完全中斷。本研究提出之機制可於離線情況下雙方分別產生一致之金鑰，實現「網路不通、資料同步」的目標。此功能除降低金鑰傳輸風險外，更具備災難韌性與實務操作價值，為國軍執行備援通訊與緊急調度提供加密保障。

**四、簡化並強化密碼交換之安全性流程**

現行檔案加密作業仍多仰賴人工設定密碼，易造成使用錯誤、記憶負擔或密碼外洩風險。本研究提出自動建構金鑰及驗證機制，能在無需用戶干預的情況下完成安全交換與驗證流程，不僅提高操作便利性，也有效減少人為因素造成的資安缺口。

針對現行機制與本設計方案進行對照（如表2），顯示本架構可於智慧卡硬體規格內有效實施，勿須增購設備，降低導入成本。綜上本研究提出之加密架構除具備高度政策可行性外，亦可在有限資源下達到高安全性、高效率之檔案傳輸目標，為國軍戰備能量與資訊保護作業提供實質助益。

表 2 現行機制與本研究比較表

| 區分 | 現行機制 | 本研究提出架構 |
|---|---|---|
| 不可預測性 | △ | ○ |
| 彈性之參數配置 | ╳ | ○ |
| 離線同步之加密 | ╳ | ○ |
| 簡化並強化密碼交換 | ╳ | ○ |
| 符號說明：<br>○：符合，△：部分符合，╳：不符合 | | |

資料來源：作者整理。

## 未來發展建議

本研究主要應用於智慧卡為基礎之檔案傳輸服務架構中，然而隨著科技進步及人們不同的使用需求，智慧卡已不再是單一的身分驗證媒介。近年來熱門的生物特徵就是最好例子，不論是指紋或臉部辨識，利用生物特徵取代智慧卡為基礎之應用環境，減少帳號密碼記憶的負擔，應可適用於許多不同架構，諸如電腦資料交換之實體隔離機制、人事文件保存與驗證等應用，因此未來可針對不同的身分驗證因子所使用的環境進行研究。

另本研究設計的應用環境為國軍檔案傳輸機制，針對單一檔案大小限制在10MB的情境進行加密，透過實驗已證明現行基於LFSR加密架構能滿足既定之安全需求。然而LFSR作為核心加密結構在高風險應用中可能面臨代數攻擊的挑戰，因此未來的研究可進一步結合非線性處理、多LFSR結構或混淆層等技術，增強對代數攻擊之防護能力，同時透過動態反饋與隨機性設計，提升內部熵值（Entropy），以進一步減少潛在攻擊威脅，並拓展本研究架構在更高安全性需求環境中的應用可能性。

## 參考文獻

### 一、書籍(中文)

(一)蘇品長，〈植基於LSK和ECC技術之公開金鑰密碼系統〉，長庚大學電機工程研究所博士論文，2007年。

(二)葉昱宗，〈新型態之電子投票機制〉，國防大學管理學院資訊管理研究所碩士論文，2015年。

(三)羅國良，〈適用於網站身分驗證及秘密通訊機制探討〉，國防大學管理學

院資訊管理研究所碩士論文，2014年。

(四)蘇品長、賴怡聖、陳岳霖，「電腦資料交換之實體隔離機制探討—植基於身分驗證之USB存取管控研究」，資訊管理學報(Journal of Information Management), Vol. 31, No.1., 2024, pp. 93-121. (TSSCI)

(五)蘇品長、王永志，「區塊鏈技術於國防人事文件保存與驗證可行性研究-以國軍軍士官任官令為例」，國防管理學報(Journal of National Defense Management). ，Vol. 45, No.1, May,, 2024, pp. 1-20.

二、書籍(英文)

(一)Elgamal, T. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." *IEEE Transactions on Information Theory*, Vol. 31, no. 4(1985), pp. 469-472.

(二)Hsiang, H. C., and W. K. Shih. "Improvement of the Secure Dynamic Id Based Remote User Authentication Scheme for Multi-Server Environment." *Computer Standards & Interfaces*, Vol. 31, no. 6(2009), pp. 1118-1123.

(三)Hwang, M. S., 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.

(四)Lamport, L. "Password Authentication with Insecure Communication." Communications of the ACM, vol. 24, no. 11(1981), pp. 770-772.

(五)Lee, C. C., T. H. Lin, and R. X. Chang. "A Secure Dynamic Id Based Remote User Authentication Scheme for Multi-Server Environment Using Smart Cards." *Expert Systems with Applications*, Vol. 38, no. 11(2011), pp. 13863-13870.

(六)Liao, Y. P., and S. S. Wang. " A Secure Dynamic Id Based Remote User Authentication Scheme for Multi-Server Environment." *Computer Standards & Interfaces*, Vol. 31, no. 1(2009), pp. 24-29.

(七)Li, X., Y. Xiong, J. Ma, and W. Wang. "An Efficient and Security Dynamic Identity Based Authentication Protocol for Multi-Server Architecture Using Smart Cards." *Journal of Network and Computer Applications*, Vol. 35, no. 2(2012), pp. 763-769.

(八)Li, X., J. Ma, W. Wang, Y. Xiong, and J. Zhang. "A Novel Smart Card and Dynamic Id Based Remote User Authentication Scheme for Multi-Server Environments." *Mathematical and Computer Modelling*, Vol. 58, no. 1(2013)

, pp. 85-95.

(九)Sood, S. K., A. K. Sarje, and K. Singh. "A Secure Dynamic Identity Based Authentication Protocol for Multi-Server Architecture." *Journal of Network and Computer Applications*, Vol. 34, no. 2(2011), pp. 609-618.

(十)Xue, K., P. Hong, and C. Ma. "A Lightweight Dynamic Pseudonym Identity Based Authentication and Key Agreement Protocol without Verification Tables for Multi-Server Architecture." *Journal of Computer and System Sciences*, Vol. 80, no. 1(2014), pp. 195-206.

三、網路

OWASP, 〈Owasp Top 10 - 2021〉《OWASP》, https://owasp.org/Top10, 2024/10/7.

## 作者簡介

楊博元少校，國防大學管理學院資訊管理研究所108年班，曾任排長、人事官、人事參謀官，現任陸軍司令部計畫處系統分析官。

陳毅恩少校，國防大學管理學院資訊管理系101年班，曾任分隊長、修護組長、通信官，現任國防大學管理學院資訊管理學系碩士班研究生。

蘇品長教授，長庚大學電機工程博士，曾任預算財務官、程式設計官、資訊督導官，現任國防大學管理學院資訊管理學系教授。

附表

| 研究設計架構符號意涵說明表 | | | |
|---|---|---|---|
| 項次 | 區分 | 符號 | 說明 |
| 1 | 角色 | $U_i$ | 傳輸者 |
| 2 | | $U_j$ | 接收者 |
| 3 | | $CS$ | 管理伺服器 |
| 4 | 使用者資訊 | $ID_i$ | 傳輸者識別碼 |
| 5 | | $ID_j$ | 接收者識別碼 |
| 6 | | $CID_i$ | 傳輸者認證時動態產生之識別碼 |
| 7 | | $P_i$ | 傳輸者密碼 |
| 8 | 伺服器資訊 | $SID_{CS}$ | 管理伺服器識別碼 |
| 9 | 隨機參數 | $b$ | 傳輸者隨機參數(存於智慧卡中) |
| 10 | | $N_{i1}$ | 傳輸者智慧卡隨機產生之參數 |
| 11 | | $N_{i2}$ | 接收者智慧卡隨機產生之參數 |
| 12 | | $N_{i3}$ | 管理伺服器隨機產生之參數 |
| 13 | | $x$ 、$y$ | 管理伺服器隨機產生之參數 |
| 14 | 金鑰 | $SK$ | 會議金鑰 |
| 15 | | $SK_{len}$ | 會議金鑰長度 |
| 16 | 取位 | $P_n$ | 系統提供取位用參數之數量 |
| 17 | | $i$ | 無理數 |
| 18 | 其他 | $h(.)$ | 單向雜湊函數 |
| 19 | | $\oplus$ | 互斥或閘運算 |
| 20 | | $\|\|$ | 連接訊息 |