# 設計身分認證及混和式公開金鑰之空軍空情前遞系統機制

蘇品長　阮于哲　王泰豐*

國防大學管理學院資訊管理學系

論文編號：4201-5
來稿2020年9月25日→第一次修訂2021年10月15日→第二次修訂2021年6月28日→
同意刊登2021年7月12日

## 摘要

國防部運用國軍大型營區結合重大慶典、抗戰勝利來舉辦營區開放，以增進全民之國防知識及提升國軍正面形象，營區開放其表演項目又以我國戰機操演最受人矚目;在其飛行操演中地面指揮官能透過空情前遞系統提供之空情圖來及時掌握飛機動態，進而預知飛行動態與數據，以期達到運籌帷幄及提前部屬；用戶端因任務特性，需於戶外建立相關設備故其連線品質及效能較為受限，且僅使用單一帳號及密碼的認證方式來登入本系統，若其帳密遭竊將有機敏洩漏疑慮；本研究將基於橢圓曲線加密、隨機背包密碼系統及結合智慧卡，利用橢圓曲線密鑰小的優點與隨機背包密碼系統運算效能快，來強化空軍空情前遞系統的資訊安全及處理速度，加上國軍內部所使用的智慧卡建立更安全的身分認證，避免遭敵竊取重要資訊，並使空情前遞系統能達到機密性、完整性及不可否認性等安全標準。

**關鍵字：身分認證、混合式金鑰系統、空情前遞系統**

* 聯絡作者:王泰豐 email:alex0951402@gmail.com

# Design of the User Authentication and Hybrid-Mode Public-Key Cryptosystem Based on Air Picture Forward System

**Su, Pin-Chang　Juan, Yu-Che　Wang, Tai-Feng***

**Department of Information Management, National Defense University, Taiwan, R.O.C.**

## Abstract

The Ministry of National Defense combine with the grandest festivals and the Victory over Japan by visiting important base of military to promote knowledges of the public's defense and raise the positive image for the national armed forces. The most popular performance of the base visiting is fighter jet drills. During the flight performance, the ground commander is able to grasp real-time aircraft dynamics from air plots provided by Air Picture Forward System, and predict flight dynamics and data to strategize and guide advanced deployment. Due to the task characteristics at the user end where relevant equipment has to be set up outdoors, its connection quality and performance are relatively limited, and only the authentication method of a single account and password can be allowed to login to the system. If the account be stolen, the confidential data may be leaked. This study is based on elliptic curve cryptography, random knapsack cryptosystem, and smart card. By using the advantages of the small elliptic curve key and fast computing performance of random knapsack cryptosystem enhances System's information security and processing speed, also with the smart card used internally in the national armed forces, it will establishe a more secure identity authentication, prevent the theft of important information from an enemy, and enabling Air Picture Forward System to attain safety standards including confidentiality, completeness, non-repudiation, etc.

**Keywords**: Identity Authentication, Hybrid Cryptosystem System, Air Picture Forward System.

## 一、前言

現今資訊科技時代中，數位資訊就是資產，在這自由與開放的網際網路中，人們的生活與習慣都與網路連結一起，相對的資訊安全問題也必須更加重視，所以世界各國目前針對網路的管理與研究不遺餘力，並延伸至各國與各國間彼此協助；而我國也因地緣位置，經常遭受到網路攻擊，面對此資安事件，我國也訂定相關策略，而其主軸為以三大資安政策執行(國家安全會議 2018):將資安提升至國安層級、打造國家級資安機制與團隊、推動國防資安自主研發。依據國軍資訊安全政策，國軍各式「指管」、「戰情」、「資訊管理」及其他專用系統，不論其為獨立運作之封閉系統，或經由軍、民網提供服務之開放架構，應列入資安防護目標(國防部，2012)。在我軍資訊戰(Information Warfare)中防護作業是以保護我方的資訊資產避免遭敵方破壞或降低效能，確保資訊具機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，有效發揮資訊戰力(國防部空軍司令部，2012)。

空軍空情前遞系統為運用於飛行演訓任務管帶及各飛行駐地共同戰情圖像(Common Tatical Picture)資料提供，格外需要針對使用者及設備執行管制，避免被有心人士竊取相關資料，其主體架構為虛擬機器(Virtual Machine, VM)，並運用虛擬桌面連線方

式，用戶端僅須運用簡易電腦及安裝可支援之瀏覽器，便可在遠端透過虛擬私有網路(Virtual Private Network, VPN)方式連至虛擬服務器，再透過入口網站(Web Portal)輸入使用者帳號密碼登入，即可接收其相關戰情圖像，但也因用戶端屬靜態認證無法自行更改密碼，安全性較低，假設其帳號密碼若不慎被竊取，或用戶端電腦被入侵，則系統將有可能遭受情資外流導致洩密之行為。以空情前遞系統來說，為了設計提高原系統之加密安全性、高效率及強化用戶端身分認證，因應瞬息萬變的演習情況或真實環境下，若能針對用戶端綁定所使用虛擬設備(虛擬機器)，除了避免讓其他用戶端窺見其相關設定或佔用，主要因線路中斷導致須重新連線時，避免分配到初始值虛擬設備(原系統為隨機分配) 。

本研究主要探討空軍空情前遞系統的安全問題，運用虛擬桌面基礎架構（Virtual Desktop Infrastructure, VDI），基於伺服器虛擬化誕生出的一種技術，透過多個環境中共用單一電腦的資源，讓單一電腦資源可以完成多部電腦的作業，除了提升硬體資源的使用效率並可降低資本支出外，還可以有效管理桌面平台、增加安全性，以及改善災難復原程序，其將所有桌面電腦所需的作業系統軟體、應用程式軟體、用戶數據全部存放到後台伺服器中，通過專門的管理系統賦予給特定用戶，用戶通過專用的網絡傳輸協議連接到後端伺服器分配的桌面資源，連接後，用戶可在連接本地終端上直接使用後台運行的桌面系統，使用體驗基本與實體電腦一致，在使用虛擬桌面時，電腦作業系統在後台伺服器端運行，本地終端僅用於連接顯示作用。本研究將運用於橢圓曲線密碼系統演算法(Elliptic Curve Cryptosystem, ECC)加上改良式隨機背包密碼系統(Random Knapsacks Cryptosystem, RKC)強化本系統身分認證及訊息傳遞方式，並結合國軍自行研發智慧卡(Smart Card)來強化用戶端安全，以防止間諜攻擊及偽冒身分等資安攻擊手段。並期望達成下列目的：

一、 使空情系前遞系統於身分認證上能配合多因子認證，將具備有更高的安全性，能防止用戶端偽冒、敵攻擊及抵禦竊聽。

二、 本系統設計架構將植基於橢圓曲線密碼系統，故在相同的安全強度下，其金鑰長度遠較 RSA 短且處理速度較快，加解密應用效率較佳。

三、 運用自我認證使在有限環境資源下，除能完善系統安全性及執行效益外，且功能正常運作並達機密性、完整性、可用性之各項標準。

## 二、 文獻探討

本章節首先介紹空軍空情前遞系統，再分類整理、歸納分析相關文獻，並針對身分認證機制加以說明後，提出與本研究相關密碼學應用技術，加以彙整作為本研究基礎。

### 2.1 空情前遞系統概述

空情前遞系統的目標為有效提升國軍各項空中戰演訓任務支援，可透過本系統接收空中航跡動態之情資來產生共同戰場圖像，以輔助戰場指揮官建立有效、可靠及實用的指揮管制作為，提早了解敵軍所在位置之威脅，機動性掌握敵進襲目標動態，採用桌面

虛擬化基礎架構，可將航跡動態圖像及相關戰情圖資透過遠端桌面技術方式傳遞給使用者，而使用者僅需使用瀏覽器、精簡型電腦透過專線連線至虛擬伺服器上的入口網站，並輸入個人帳號及密碼，即可使用所分配的虛擬桌面，這不僅可節省個人電腦安裝，期能符合機動性設置，但也因客戶端僅需要具備有瀏覽器功能的電腦，在申請服務時無法判定是否具有合法性，若用戶端帳密遭敵竊取，敵方便可從中非法竊取相關機敏情資。本系統主要運用為各飛行演訓任務的管帶及提供各飛行駐地其共同戰情圖像資料顯示，架構包含系統伺服器中心、工作站、防火牆、用戶端終端機及保密器等，系統說明如后：

一、 系統伺服器中心：具高可用性(High Availability, HA)，採複式配置，主要為用戶端認證後提供遠端虛擬機器桌面派送，網路管理系統，資訊安全系統及資料庫系統。

二、 工作站：為管理及監控各虛擬機器運作情況，維護及建立各用戶端帳號密碼。

三、 防火牆：是一個架設在網際網路與企業內網之間的資安系統，可於兩個或多個網路實行網路間存取或控制。

四、 用戶端終端機：建置於網路末端，須安裝支援超文本標記語言 5.0 版(HyperText Markup Language, HTML)瀏覽器之電腦及相對應網頁安全通訊端層(Secure Socket Layer, SSL)憑證。

五、 保密器：具加解密功能之裝置，使用對稱式加密演算法。

空情前遞系統架構示意圖 1：

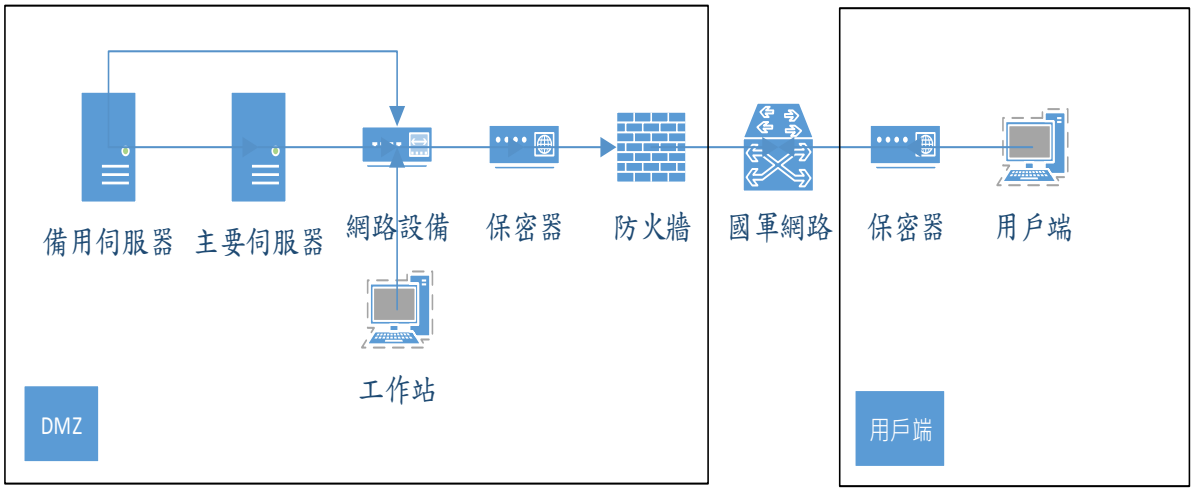


圖 1　系統架構示意圖

資料來源：本研究整理

空情前遞系統的目標為有效提升國軍各項空中戰演訓任務支援，可透過本系統接收空中航跡動態之情資來產生共同戰場圖像，以輔助戰場指揮官建立有效、可靠及實用的指揮管制作為，提早了解敵軍所在位置之威脅，機動性掌握敵進襲目標動態，空軍前遞系統採用桌面虛擬化基礎架構，可將航跡動態圖像及相關戰情圖資透過遠端桌面技術方式傳遞給使用者，而使用者僅需使用瀏覽器、精簡型電腦透過專線連線至虛擬伺服器上的入口網站，並輸入個人帳號及密碼，即可使用所分配的虛擬桌面，這不僅可節省個人電腦安裝，期能符合機動性設置，但也因客戶端僅需要具備有瀏覽器功能的電腦，在申請服務時無法判定是否具有合法性，若用戶端帳密遭敵竊取，敵方便可從中非法竊取相關機敏情資。

## 2.2 身分認證機制與應用

隨著人們使用網路習慣越來越多頻繁，衍生出網路登入時所使用者帳號 、密碼也越

多也越難以管理，惟目前所會面對的困境。多年來，以輸入帳號密碼為使用者其驗證身分的方式，也漸漸浮現出密碼管理的問題，不僅是易於暴力破解的弱密碼，同一組帳密用在多個網站平臺的問題更是嚴重，今年已有多家資安公司指出，自動化的帳號密碼填充攻擊（俗稱撞庫）手法，就是使用大量外流的電子郵件與密碼來嘗試入侵。 (羅正漢，2019)；有鑑於前無效身分認證，主因是因為網路應用程式必須進行身分認證和工作階段管理，此時若導入方式不正確，就有可能會讓攻擊者取得密碼、金鑰、工作階段存取控制、…等暫時或永久取得使用者的身分資訊。所以建議在可能的情況下落實多因素的身分驗證機制 (Burr et al., 2006)，以利避免無效身分認證的攻擊成功。

隨著資訊科技的演進，人們所運用的電子設備也多樣化發展，現行電子設備大致區分智慧型手機、平板電腦、筆記型電腦、智慧手環等產品，所具備功能亦不盡相同，且對於身分鑑別所面臨的資訊安全問題，只用單一驗證方法，在安全考量上並不夠嚴謹，倘若身分認證機制如結合上述二種以上方法，可有效提升系統使用安全，此種方法亦為多因子認證方式(Tsai & Su，2021)，用戶認證途徑可看作存取控制(Access Control)為最需重視的一環，用戶端必須先與認證伺服器證明自己的身分，來獲得授權(Authorization)，才有讀寫、執行及刪除等權限。身分認證通常具有三種要素(Factors)分別是所知之事（如帳號密碼）、所持之物（如智慧卡及一次性密碼）及所具之形（如生物辨識）。基本上，可能有下列幾種途徑：

一、 使用者帳號／密碼(Account Password)：利用使用者帳號與密碼辨識身分是最普遍的方法，但必須事先在系統上建立帳戶才行，因為密碼是靜態的數據，身分認證機制在使用方面都非常簡單，且驗證過程中很容易被攔截及破解，從安全性上來講，已經無法滿足網際網路對於身分認證安全性的需求(黃建衛，2011)。為提升安全性通常會採取下列措施：

·針對密碼的長度與複雜度有須遵守原則。
- 密碼若輸入錯誤達一定次數時，帳號將被鎖定。
- 明確訂定其用戶帳號使用時間與權限。
- 設定密碼使用的有時效，到期須立即更換密碼。
- 配合系統額外增加問題詢答與驗證。

二、 智慧卡(Smart Card)：近年來智慧卡已經漸漸融入我們的日常生活中，智慧卡是一張嵌入微晶片的塑膠卡片，其具運算能力、儲存功能及自我保護的硬體，使用時為證明持有人確實為該卡的授權使用者，必須鍵入預先設定的密碼，並與卡片內儲存的密碼驗證無誤後方能運作，例如政府積極推動的「自然人憑證」（或稱「電子身分證 IC 卡」、「網路上的身分證」），提倡國人只要透過一張智慧卡一台讀卡機就可以透過個人電腦連結至政府機關進行戶政網路申辦服務、個人所得稅結算申報繳稅、中華電信帳單查詢等多項的便民措施(林政宏，2011)。國軍第一代電子憑證系統於 2001 年誕生，當時只運用 IC 卡(後續稱作智慧卡)進行電子公文交換，至 2011 年因應網路架構由初始主從式架構演進成三層式架構，並由國防部本部運用智慧卡針對公文系統試行線上簽核機制，2012 年逐步推廣至各軍種，但當時僅是在席位辨認上使用，隔年才開始正式發放個人用智慧卡、並啟用於迄今（陳柏諭，2014）；依據智慧卡與讀卡機的傳輸資料方式來區分，可分為接觸式(Contact Card)、非接觸式(Contact less Card)與混合式(Hybrid-Card 或 Combi -Card)三種說明如下:

(1)接觸式：藉由卡片與讀卡機接觸執行讀取或寫入資料。

(2)非接觸式：運用 RFID、電流感應、紅外線等來驅動其運作，無需卡片與讀卡機做接觸。

(3)混合式：同時擁有接觸與非接觸介面。

三、 一次性密碼(One Time Password, OTP)：動態密碼(Dynamic-Password)，又稱一次性動態密碼(One Time Password, OTP)，主要產生的原理是採用特定的數學運算函式，因為每次產生的密碼都不會相同，故稱為動態密碼(方俊斌，2012)。另所產生的密碼都不相同，而且每組密碼只能使用一次，與傳統的固定式密碼相比，具有「不可預測性」、「不可重複性」及「使用一次」，讓攻擊者即使得到一組密碼也無法繼續使用。動態密碼的產生可分為兩種形式，分別為同步(Synchronous)演算法與非同步(Asynchronous)演算法，而同步演算法包括兩種技術為事件同步(Event-Based)、時間同步(Time-Based)為主；非同步演算法則以挑戰與應答(Challenge&Response)為主，其分類與比較如表 1。

表1 一次性性密碼分類與比較

| 分析項目 / 種類 | 運用方式 | 安全性 | 常見程度 | 抵禦重送攻擊 |
|---|---|---|---|---|
| 事件同步 | 登入次數 | 低 | 低 | 可 |
| 時間同步 | 時間 | 中 | 中 | 可 |
| 挑戰與應答 | 金鑰、亂數 | 高 | 高 | 可 |

資料來源：方俊斌(2012)

四、 基於智慧卡動態身分認證：Das 等人提出使用智慧卡與動態身分的認證機制，能防止身分盜用、內部攻擊，可抵抗重送攻擊並且具匿名性(Das et al., 2007)。但 Wang 等人在 2009 年指出，聲稱 Das 等人的機制未能達到雙方身分認證，也無法防禦偽冒伺服器攻擊。所以提出強化其密碼認證方案。同年，Chang 等人針對 Wang 等人所提出之方案，指出其執行效率較差，且無具匿名性，不能抵禦偽冒攻擊等(Chang et al., 2009)。並於 2014 年 Chang 等人又提出運用智慧卡相互認證的一種新機制，其不需要驗證表，便可完成彼此認證，且聲稱改善後因每次認證其參數均重新產生，故能具備不可追蹤性及認證後用戶能便利的更換密碼(Chang et al., 2014)。在 2014 年，Kumari 等人提出一種改進用戶認證方案及會議密鑰協定的機制，並指出 Chang 等人的機制違反動態身分認證的目的，假使其某用戶的智慧卡若被竊取將造成其他用戶面臨被偽冒的危機，並且不能抵抗離線猜密碼攻擊及內部攻擊等。而 Kumari 等人聲稱其新方案可以抵抗智慧卡竊取、偽冒攻擊等(Kumari et al., 2014)。在 2015 年 Shi 等人指出 Kumari 等人的機制仍不安全，且不能提供適當的相互認證。並提出一套改善機制，且證明該機制能抵抗如離線猜密碼攻擊及偽裝攻擊等(Shi et al., 2015)。另於同年 Chaudhry 等人發表研究指出 Kumari 等人的機制仍然存在智慧卡失竊與使用者匿名等方面弱點。並提出新的改善方案 (Chaudhry et al., 2015)。在 2016 年，Gong 發現 Chaudhry 等人的其研究方案還是存有會遭受到阻絕服務攻擊以及離線猜弱密碼攻擊等弱點。另外在 Shi 等人的發表的機制 Gong 發現仍有安全漏洞。並提出一個增強智慧卡遠端認證機制，提供使用者匿名及抵抗相關攻擊，使機制更具安全性(龔建丞，2018)。

五、 生物辨識技術：生物辨識技術是運用人體的生物特徵(Physiological Characteristics)和行為特徵(Behavioral Characteristics)，經過數位運算過程，以做為比對驗證依據的技術。美國麻省理工學院( Massachusetts Institute of Technology, MIT)將「生物鑑定科學」(Biometrics)，視為最具有發展潛力的十大科技之一，在未來生物特徵的應

用越來越廣泛。生物特徵的分類大致可區分為生理特徵與行為特徵。生理上的特徵有虹膜、聲紋、指紋、掌紋、臉型、掌型、靜脈、體型及 DNA 等，又稱為靜態的特徵，行為上的特徵則有聲紋、心跳、步態及簽名等，則屬於動態的特徵。以下簡介幾種的生物辨識技術應用(謝定芳，2017)：

- 人臉辨識(Face Identification)：人臉辨識技術是目前各辨識技術中不需要特殊裝置，只要有一個高解析度的影像攝影裝置即可使用。人臉辨識技術注重於影像處理為基礎的演算法作為辨識準確度的依據，其運用之演算法主要分為，由統計測量方法取得由臉部特徵向量集合為臉部型態的相關特徵和關係；另一種方法是以樣版為基礎，當結構預知，可變形樣版對找出臉部特徵型態是一種有效技術。
- 指紋辨識(Fingerprint Identification)：指紋辨識技術是將個人指紋先行採樣，並擷取其中重要的特徵作為特徵值，再比對特徵值以鑑別身分，而指紋特徵值只有 250 位元組到 1K 位元組，指紋辨識技術的穩定性高及設備價格低廉，使指紋辨識系統成為目前最受歡迎的設備。
- 虹膜辨識(Iris Identification)：虹膜位於眼球角膜與水晶體之間，每個虹膜都是獨一無二的構造，虹膜基於像冠、水晶體、細絲、斑點、結構、凹點、射線、皺紋和條紋等特徵，虹膜辨識是利用每個人的虹膜特徵都是獨一無二的特性、不會發生變化，且不像指紋容易因為受傷或污染而無法辨識，因此漸漸被用來做身分辨識。
- 掌形辨識(Hand-geometry Identification)：掌形辨識技術是利用每個人的手掌形狀彼此不同，來進行辨識，利用影像裝置，擷取手掌的形狀及特徵，來鑑別身分，有些掌型辨識系統只紀錄中指及食指的形狀及特徵，因此特徵檔案很小幾乎低於 100 個位元組。

### 2.3 密碼學技術

密碼學(Crptography)既指秘密書寫、加密訊息、隱藏訊息內容的科學，同時也泛指與密碼有關的科學；要談到當代密碼學核心，我們就無可避免地要了解當代密碼系統的運作機制；當代密碼系統應對資訊安全提供以下四大功能(鄧安文，2018)：

一、 機密性(Confidentiality)：Cathy 無法破譯解讀 Alice 傳給 Bob 的密文，而其主要工具就是該密碼系統的加密、解密演算法。

二、 完整性(Integrity)：Bob 想要確定 Alice 所傳訊之訊息未被竄改，(但在傳訊上可能會出錯，此時就要考慮具偵錯功能的編碼理論(Coding Theory)，而密碼 Hash 函數，提供了可偵測資料是否遭竄改的方法。

三、 身分認證(Authentication):Bob 希望能確定傳訊之訊息「應該」是由 Alice 本人所發送的，而非他人所偽造。

四、 不可否認性(Non-Repudiation):Alice 不能否認這是他所發送的訊息。

密碼系統主要可分為對稱式金鑰系統(Symmetric Key Cryptosystem)以及公開鑰密碼系統(Public Key Cryptosystem)亦也是非對稱式金鑰密碼系統(Asymmeric Key Cryptosystem)兩類(張志義，2004)。而密碼系統的使用，其安全性就在於金鑰的保密，如何強化金鑰的保密，密碼系統的演算法的強度就至關重要，在幾經許多密碼學家與研究學者的努力下，越來越多的加密演算法也漸漸被提出，像是知名的 RSA 即為目前被公認為最安全的加密演算法。事實上，在眾多的演算法中，每一個演算法具有其不同的安

全程級，若是能夠在眾多的演算法之中，選擇足以保障網路安全的演算法，如此一來，不僅讓這些演算法發揮其效益，更可以讓用戶用較少的成本，達到最大的安全防護（資策會，2006）。密碼學核心仰賴於數學理論，即表示有些事情比破壞更加容易。就像粉碎一張圖畫比將所有碎片粘合在一起更容易一樣，將兩個質數相乘以獲得一個大的數字比把這個大數字再分解成兩個質數要容易得多。這種不對稱單向函數和陷阱門單向函數一是所有密碼學的基礎。

### 2.3.1 對稱式金鑰系統

過去在為對稱式金鑰密碼(Symmrtric Encryption)主流的年代，一般而言，對稱式金鑰密碼系統保密性不如公開金鑰密碼系統，但由於其計算速度快速，再傳送大筆資料的加密上，在沒有好的替代品出現之前，仍有其必要性。其運作方式是服務端與用戶端雙方在交換訊息前，彼此先持有一分共同的金鑰；當服務端傳輸前，先以共同金鑰對明文編碼成密文。這分密文看起來就跟一堆亂碼無異，因此在通道上傳送，既使有心人從中竊聽或截取，也不易解讀明文內容，以保障其機密性。用戶端收到後，再以同一把金鑰將密文解碼回明文，如圖 2 所示。目前較著名的對稱式密碼系統則有：DES、IDEA、AES、RC2、RC4、RC5 等（邱英捷，2006）。

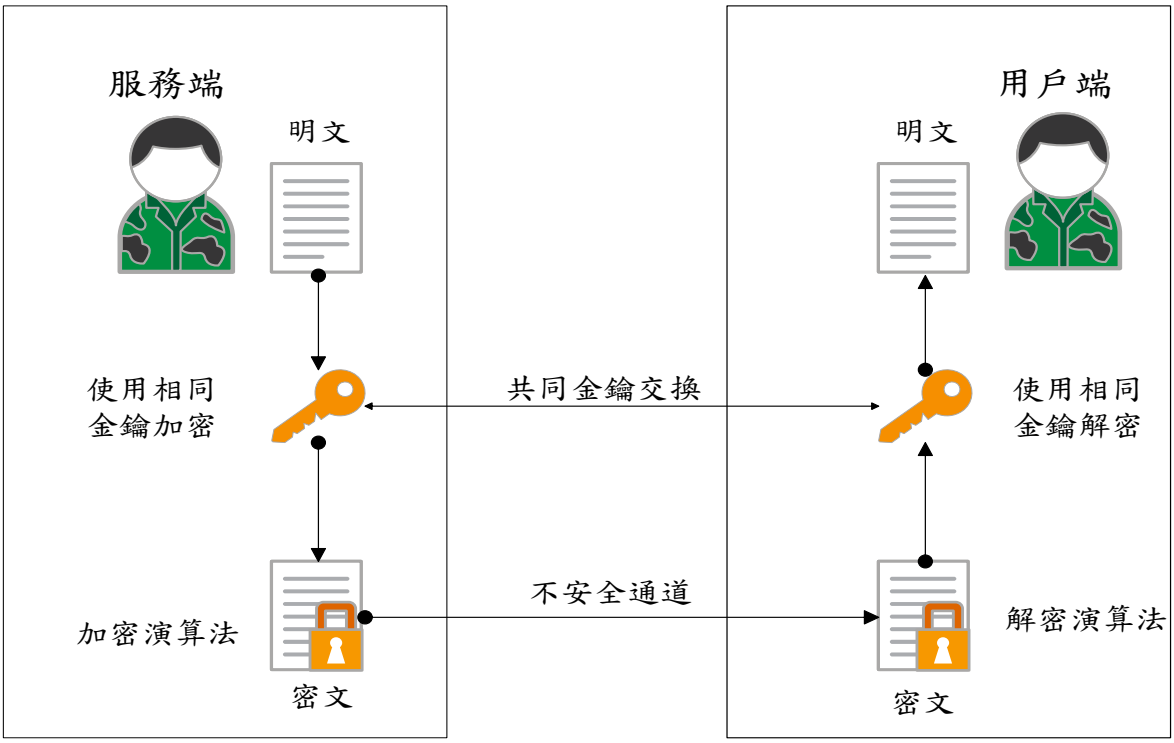


圖 2　對稱式密碼系統示意圖
資料來源：本研究整理

### 2.3.2 非對稱式金鑰系統

非對稱式金鑰系統即為公開金鑰加密系統，意指加密與解密時，分別採用不同的金鑰進行演算。如圖 3 為常見的公開金鑰加密系統示意圖，當伺服端將資料傳送給用戶端

時，必須先使用用戶端的公開金鑰將文件予以加密產生相對應的密文(Ciphertext)。當用戶端接收到的資料之後，即可使用自己的私密金鑰將密文解開求出明文。公開金鑰加密方法與對稱式金鑰加密最大的不同即為金鑰的使用。公開金鑰加解密時是採用不同的金鑰，而私密金鑰加解密時，則是採用相同的金鑰。目前較著名的非對稱式密碼系統有 RSA、ElGamal、背包演算法及 ECC 等。

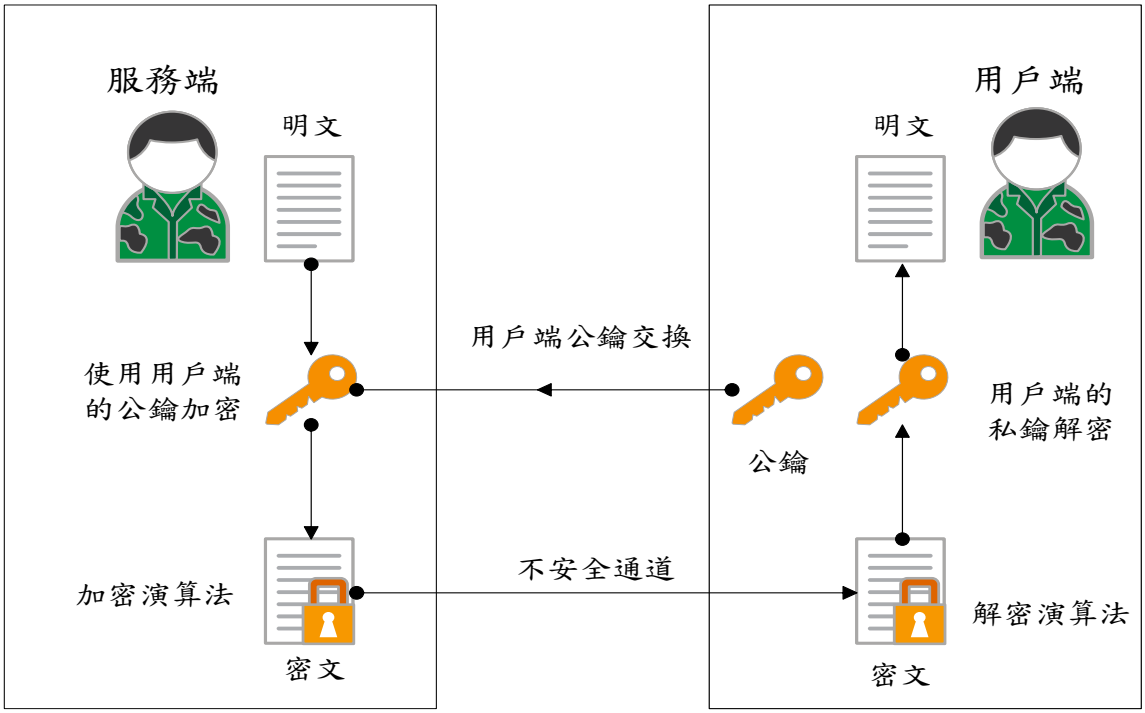


圖 3　公開金鑰加密系統示意圖

資料來源：本研究整理

一、 RSA 加密演算法：RSA 加密演算法，在 1977 年在麻省理工學院工作之 Ron Rivest, Adi Shamir 與 Leonard Adleman 由三人一起提出來，並從其名字首字母第一個字命名之（維基百科，2018）。其演算法如圖 4，我們令伺服端欲將明文$m$用 RSA 演算法加密成密文$c$傳給用戶端，用戶端將密文$c$還原成明文$m$。

- (金鑰產生)用戶端取相異質數$p.q$(保密)，計算 RSA 模數$n = pq$ 將其公開，取$e$為加密鑰將其公開，其中$e$必需與$\varphi(n)$互質

$$\varphi(n) = (p-1)(q-1)\text{(保密)}。$$

- 用戶端之公開金鑰$(n, e)$；用戶端計算$d$為解密鑰（保密），$(n, d)$為用戶端的私鑰(Private Key)，其中

$$ed \equiv 1 \pmod{\varphi(n)}$$

- (加密)伺服端取得用戶端的公開金鑰$(n, e)$，用加密函數計算

$$c = \mathrm{E}(m) \equiv m^e \pmod{n}$$，將密文傳給用戶端。

- (解密)用戶端用解密函數計算

$$m = \mathrm{D}(c) \equiv c^d \pmod{n}$$，解密還原成明文。

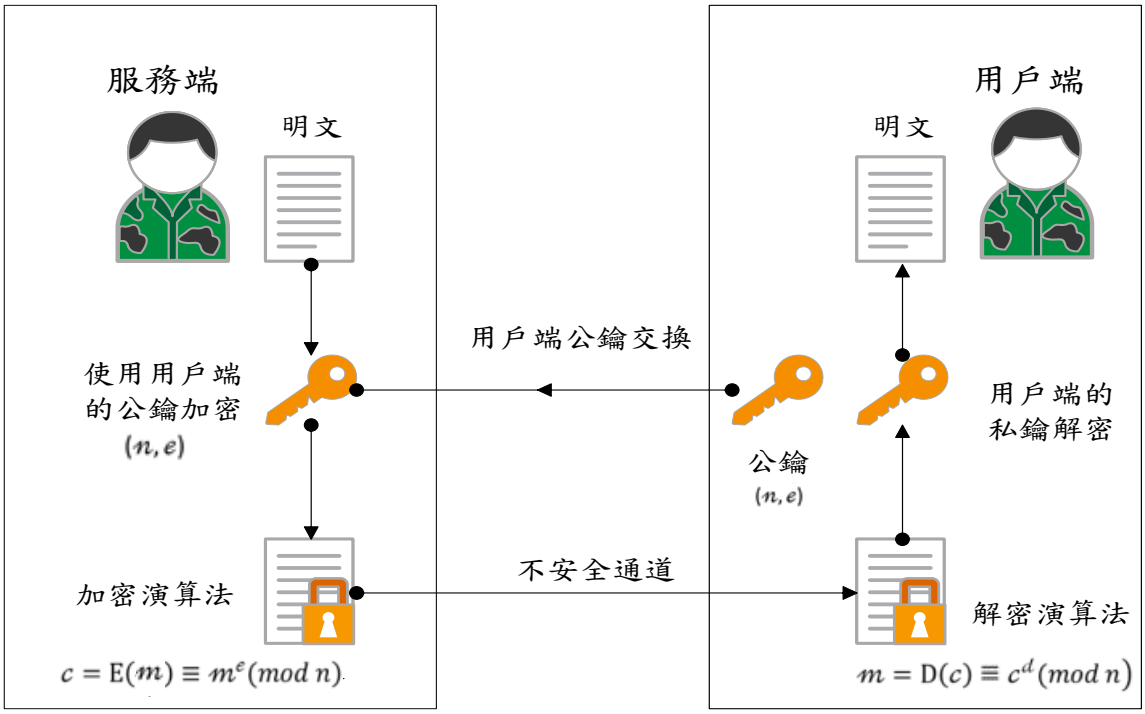


圖4　RSA加密演算法示意圖

資料來源：本研究整理

二、 橢圓曲線密碼系統：在 150 年前數學家針對橢圓曲線(Elliptic Curve)的已有相關文獻研究，但在當時是僅限於在數論以及代數幾何所研究的課題，沒人認為橢圓曲線有何實值用途；但自從 Koblitz 發表如何將橢圓曲線引入密碼學的文章(Kkoblitz, 1987)，橢圓曲線開始在密碼學開始受到重視，橢圓曲線密碼(Elliptic Curve Cryptography, ECC)與傳統的基於大質數因數分解的加密方法不同，ECC 所產生 164 位元的密鑰安全性，相當於 RSA 1024 位元密鑰提供保密強度，而且 ECC 運算量相比 RSA 較小，相對處理速度較快(Elaine, 2016)，如表 2。

表2 RSA與ECC同樣安全性密碼長度比較

| ECC | 112-bit | 163-bit | 224-bit | 256-bit | 384-bit | 512-bit |
|---|---|---|---|---|---|---|
| RSA | 512-bit | 1024-bit | 2048-bit | 3072-bit | 7680-bit | 15360-bit |
| 金鑰長度比 | 1:5 | 1:6 | 1:9 | 1:12 | 1:20 | 1:30 |

資料來源：Elaine(2016)

- 橢圓曲線方程式

  一條橢圓曲線是在射影平面上滿足 Weieerstrass 方程式所有點的集合：

  $$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

- 橢圓曲線是一個齊次函數
- 橢圓曲線即三次平滑代數平面曲線(Smooth Algebraic Plane Curve)
- 橢圓曲線加法律

在橢圓曲線 $E: y^2 = x^3 + ax + b$ (判別式$\Delta = -16(4a^3 + 27b^2 \neq 0)$ 定義加法如下

$E$包含無限遠點$\mathcal{O}$，並代表為加法單位元素，點P的加法反元素即點−P，定義為點P對x軸之鏡射；一般而言，三次曲線與直線截交於 3 點(需計算重數(Multiplicity)若相切時，重數為 2)，P、Q、$-(\mathrm{P}+\mathrm{Q})$共線，點$\mathrm{P}+\mathrm{Q}$即$-(\mathrm{P}+\mathrm{Q})$對x軸之鏡射，依此定義加法。

- 加法座標計算：令$\mathrm{P} = (\mathrm{x}(\mathrm{P}), \mathrm{y}(\mathrm{P}))$、$Q = (x(Q), y(Q))$，欲求$R = P + Q = (x(R), y(R))$，其中可分 3 種情形:
- $\mathrm{x}(\mathrm{P}) \neq \mathrm{x}(\mathrm{Q})$：取通過P、Q截線之斜率$\mathrm{m} = \frac{y(Q)-y(P)}{x(Q)-x(P)}$。
- $\mathrm{x}(\mathrm{P}) = \mathrm{x}(\mathrm{Q})$、$\mathrm{y}(\mathrm{P}) = \mathrm{y}(\mathrm{Q})$ ：即$\mathrm{P} = \mathrm{Q}$，取通過P切線之斜率 $\mathrm{m} = \frac{3X(P)^2+a}{2y(P)}$。
- $\mathrm{x}(\mathrm{P}) = \mathrm{x}(\mathrm{Q})$、$\mathrm{y}(\mathrm{P}) = -\mathrm{y}(\mathrm{Q})$：此時$\mathrm{R} = \mathrm{P} + \mathrm{Q} = \mathcal{O}$

## 三、研究方法與研究架構

本研究將基於橢圓曲線密碼系統之解離散對數之難度及國軍智慧卡的身分認證技術並結合改良式隨機背包密碼系統，藉以強化空軍空情前遞系統之身分驗證機制管控之安全性。區分初始階段、註冊及獲取金鑰階段、登入與驗證階段、再次連線階段等四個階段。

### 3.1 系統架構及說明

本研究將設計一個認證伺服器，為了能夠提供用戶端及虛擬伺服器公開金鑰產生，用戶端及虛擬伺服器在與認證伺服器完成註冊後，能藉此驗證用戶端及虛擬伺服器是否具有合法性，另外，在用戶端與虛擬伺服器完成建立連線後，能針對虛擬機器分配提供綁定用戶。系統流程架構圖（如圖 5），系統符號說明表（如表 3）。

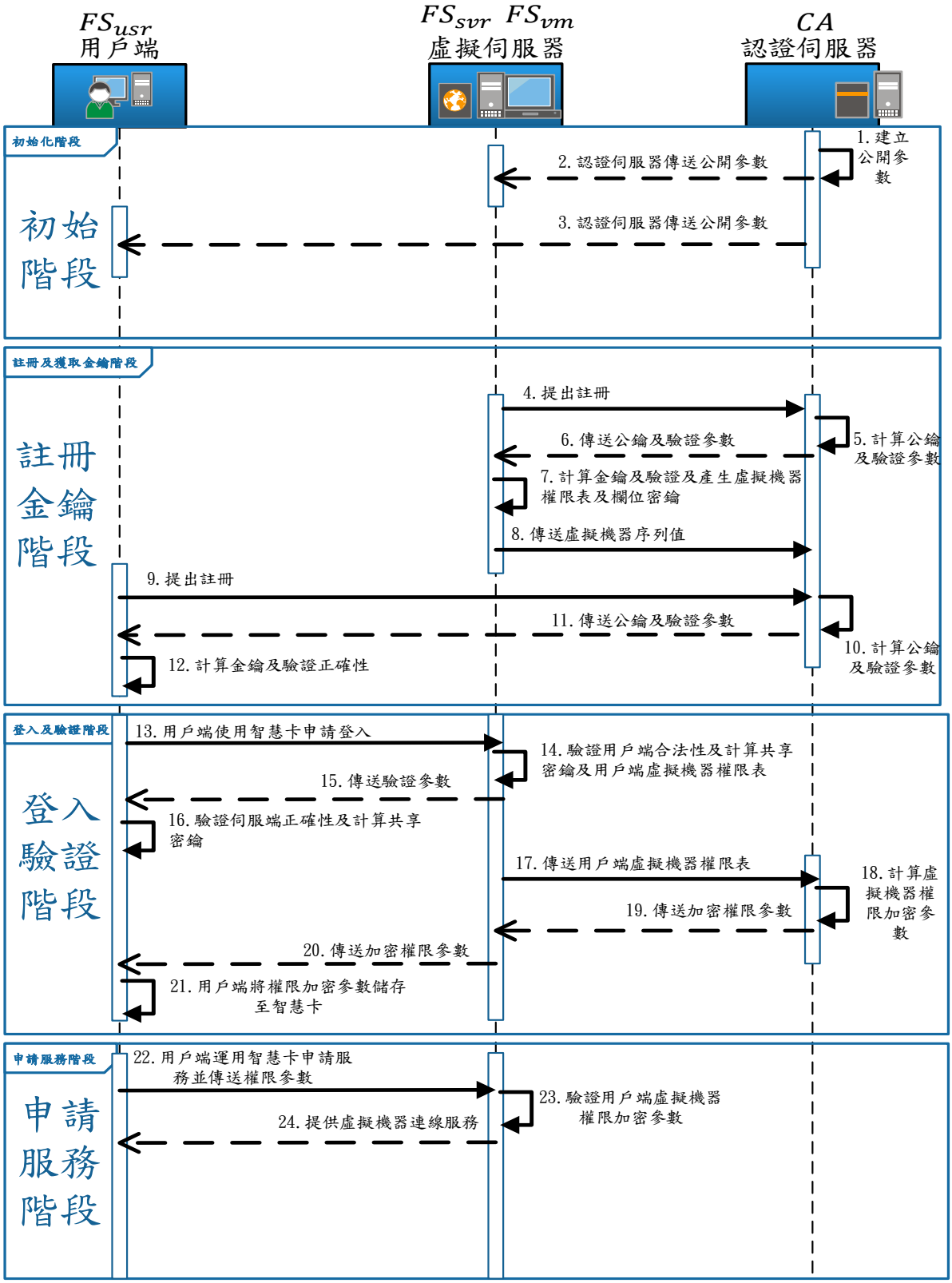
$FS_{usr}$
用戶端
$FS_{svr}$ $FS_{vm}$
虛擬伺服器
$CA$
認證伺服器
初始化階段
初始階段
1. 建立公開參數
2. 認證伺服器傳送公開參數
3. 認證伺服器傳送公開參數
註冊及獲取金鑰階段
註冊金鑰階段
4. 提出註冊
5. 計算公鑰及驗證參數
6. 傳送公鑰及驗證參數
7. 計算金鑰及驗證及產生虛擬機器權限表及欄位密鑰
8. 傳送虛擬機器序列值
9. 提出註冊
10. 計算公鑰及驗證參數
11. 傳送公鑰及驗證參數
12. 計算金鑰及驗證正確性
登入及驗證階段
登入驗證階段
13. 用戶端使用智慧卡申請登入
14. 驗證用戶端合法性及計算共享密鑰及用戶端虛擬機器權限表
15. 傳送驗證參數
16. 驗證伺服端正確性及計算共享密鑰
17. 傳送用戶端虛擬機器權限表
18. 計算虛擬機器權限加密參數
19. 傳送加密權限參數
20. 傳送加密權限參數
21. 用戶端將權限加密參數儲存至智慧卡
申請服務階段
申請服務階段
22. 用戶端運用智慧卡申請服務並傳送權限參數
23. 驗證用戶端虛擬機器權限加密參數
24. 提供虛擬機器連線服務

圖 5　系統流程架構圖

表3　系統符號說明表

| 項次 | 符號 | 說明 |
|---|---|---|
| 1. | $E_q$(a,b) | 橢圓曲線 |
| 2. | $q$ | 為一個 256 bit 以上之大質數 |
| 3. | $H()$ | 單向無碰撞雜湊函數 |
| 4. | $FS_{usr}$、$FS_{svr}$、$FS_{vm}$ | 用戶端、虛擬伺服器、虛擬機器 |
| 5. | $CA$ | 認證伺服器 |
| 6. | $U$、$\tilde{U}$、$\overline{U}$、$\hat{U}_{usr}$ | 隨機向量、向量參數、超增序列值、用戶申請 |
| 7. | $k_n$、$l_n$、$k_m$與$l_m$ | 隨機參數 |
| 8. | $uFS_{usr}$、z$FS_{usr}$ | 虛擬機器用戶註冊欄位、位址欄位 |
| 9. | $ad_{usr}$ | 用戶端註冊序列值 |
| 10. | $ip_{usr}$ | 用戶端虛擬機器位址值 |
| 11. | $FSC1_{usr}$、$FSC2_{usr}$ | 用戶端權限密文 |
| 12. | $M_{usr}$、$J_{usr}$ | 權限計算值 |
| 13. | $colu_{vm}$ | 虛擬機器欄位加密金鑰 |
| 14. | RquestViewer | $FS_{usr}$向$FS_{svr}$提出使用虛擬機器 |
| 15. | $w_{usr}$ | $FS_{usr}$國軍智慧卡 |
| 16. | $SK_{svrCA}$、$UK_{usrCA}$ | $FS_{svr}$與$CA$、$FS_{usr}$與$CA$之共享祕鑰 |
| 17. | $id_{usr}$、$id_{svr}$、$id_{vm}$ | $FS_{usr}$、$FS_{svr}$、$FS_{vm}$之身分識別 ID |
| 18. | $ps_{svr}$、$ps_{usr}$ | $CA$選取之隨機參數 |
| 19. | $rm_{svr}$、$rm_{usr}$ | $FS_{svr}$、$FS_{usr}$選取之隨機參數 |
| 20. | $UK$、$SK$、$CK$ | $FS_{usr}$、$FS_{svr}$、$CA$之公開金鑰 |
| 21. | $uk$、$sk$、$ck$ | $FS_{usr}$、$FS_{svr}$、$CA$之私秘金鑰 |
| 22. | $PD_{usr}$、$PD_{svr}$ | $FS_{usr}$、$FS_{svr}$之身分憑證 |
| 23. | $sig_{usr}$、$sig_{svr}$ | $FS_{usr}$、$FS_{svr}$之數位簽章 |
| 24. | $(Fss_x, Fss_y)$、$(Uss_x, Uss_y)$ | $FS_{svr}$之公鑰、$FS_{usr}$之公鑰 |
| 25. | $ac_u$、$pw_u$ | 使用者設定的帳號密碼 |
| 26. | $\overline{W}$ | $FS_{usr}$用戶端加密權限(智慧卡) |
| 27. | $\overline{R}$ | $FS_{svr}$計算$FS_{usr}$之權限值 |
| 28. | $SK_{us}$ | $FS_{svr}$與$FS_{usr}$共同金鑰 |
| 29. | $NK_{us}$ | $FS_{svr}$與$FS_{usr}$通訊金鑰 |
| 30. | $T_{usr}$、$T_{svr}$ | 時戳驗證參數 |
| 31. | $\Delta T$ | 時戳門檻 |
| 32. | $rt_{usr}$、$rt_{svr}$ | 隨機亂數用來建立通訊金鑰 |
| 33. | $Check(FS_{svr}A)$、$Check(FS_{svr}B)$ | 驗證$FS_{svr}$、$FS_{svr}$身分之參數 |

資料來源：本研究整理

### 3.2 初始階段

本階段由$CA$公開相關系統參數

一、在一個有限域$F_q$上，設計一條橢圓曲線，選取$q$為一大質數(至少為256bit以上)，其中a, b為整數，$E_q$(a,b)=$y^2 = x^3 + ax + b\ (mod\ q)$，且滿足$4a^3 + 27b^2 \neq 0$，確保沒有重根，具有唯一解。

二、在$E_q$(a,b)上選取一階數秩(Order)為n的基點G，使得 $n \times G = \mathcal{O}$ ($\mathcal{O}$為無窮遠點)，另外給定一單向無碰撞雜湊函數$H(\ )$。

三、選取認證伺服器$CA$的私密金鑰$ck$，計算其公開金鑰$CK$(3-1)式並公開系統參數$E_q$(a,b)、G、n、$H(\ )$、$CK$。

- $CK = ck \times G$ (1)

### 3.3 註冊及獲取金鑰階段

當用戶端$FS_{usr}$與虛擬伺服器$FS_{svr}$第一次上線時會先與認證伺服器$CA$執行註冊，以取得彼此共享公鑰參數，俾利後續驗證。

#### 3.3.1 虛擬伺服器認證

一、$FS_{svr}$向$CA$註冊，接收$CA$其公開參數$CK$及產生一組隨機參數$rm_{svr} \in [2, n-2]$，$FS_{svr}$將身分識別$id_{svr}$與$CA$提供公開參數經計算求出身分憑證$PD_{svr}$(2)式，透過安全通道傳送$id_{svr}$、$PD_{svr}$至$CA$註冊。

- $PD_{svr} = H(rm_{svr} \| id_{svr}) \cdot G$ (2)

二、$CA$當接收到$FS_{svr}$的$id_{svr}$、$PD_{svr}$，經計算後回傳公鑰$SK$、簽章$sig_{svr}$給$FS_{svr}$ (3~4)式。

- $SK = PD_{svr} + [ps_{svr} - H(id_{svr})] \cdot G = (Fss_x,\ Fss_y)$ (3)
- $sig_{svr} = ps_{svr} + ck(Fss_x + H(id_{svr}))$ (4)

三、$FS_{svr}$將利用接收到$CA$回傳的公鑰$SK$、簽章$sig_{svr}$，產生自己的私鑰$sk$(5)式，並透過$sig_{svr}$驗證$SK$的合法性(6)式，若驗證符合將建立共享金鑰$SK_{svrCA}$(7)式。

- $sk = sig_{svr} + H(rm_{svr} \| id_{svr})$ (5)
- $SK' = sk \cdot G = SK$ (6)

$$= [sig_{svr} + H(rm_{svr} \| id_{svr})] \cdot G$$
$$= ps_{svr} + ck(Fss_x + H(id_{svr})) \cdot G + H(rm_{svr} \| id_{svr}) \cdot G$$
$$= (ps_{svr} + H(rm_{svr} \| id_{svr})) \cdot G + ck(Fss_x + H(id_{svr})) \cdot G$$
$$= SK + H(id_{svr}) \cdot G + (Fss_x + H(id_{svr})) \cdot CK$$

- $SK_{svrCA} = sk \cdot CK = ck \cdot SK$ (7)

四、$FS_{svr}$產生用戶崗位與服務權限序列，分別計算於用戶崗位與虛擬機器權限服務向量如(8～9)式，並取隨機四個質數$k_n$、$l_n$、$k_m$與$l_m$ (12～13)式。

- 取隨機$n$向量$U = \{u_1, u_2, \dots, u_n\}$，$u_i$為正整數。 (8)
- 取隨機$m$向量$Z = \{z_1, z_2, \dots, z_m\}$，$z_i$為正整數。 (9)
- 計算向量$\tilde{U} = \{\widetilde{u_1}, \widetilde{u_2}, \dots, \widetilde{u_n}\}$，$\widetilde{u_i} = u_i - 2^{n-1}$，$i = 1, \dots, n$ (10)

- 計算向量$\tilde{Z}=\{\widetilde{z_1},\widetilde{z_2},\dots,\widetilde{z_m}\}$，$\widetilde{z_i}=z_i-2^{n-1}$，$i=1,\dots,m$ (11)
- $k_n>\sum_{i=1}^{n}u_i$，$l_n>2\,max\{\sum_{\widetilde{u_i}>0}\widetilde{u_i},-\sum_{\widetilde{u_i}>0}\widetilde{u_i}\}$ (12)
- $k_m>\sum_{i=1}^{m}z_i$，$l_m>2\,max\{\sum_{\widetilde{z_i}>0}\widetilde{z_i},-\sum_{\widetilde{z_i}>0}\widetilde{z_i}\}$ (13)

五、$FS_{svr}$透過$k_n$、$l_n$、$k_m$與$l_m$使用餘式定理求出用戶服務與權限序列值$\bar{U}$與$\bar{Z}$(14~17)式，並傳送至$CA$供用戶端註冊用。

- $\overline{u_i}\equiv u_i(mod k_n),\overline{u_i}\equiv\widetilde{u_i}(\mathrm{mod}l_n),i=1,\dots,n$ (14)
- $\overline{z_i}\equiv z_i(mod k_m),\overline{z_i}\equiv\widetilde{z_i}(\mathrm{mod}l_m),i=1,\dots,n$ (15)
- $\bar{U}=\{\overline{u_1},\overline{u_2},\dots,\overline{u_n}\}$，其中 $0\le\overline{u_i}\le k_n l_n-1$ (16)
- $\bar{Z}=\{\overline{z_1},\overline{z_2},\dots,\overline{z_m}\}$，其中 $0\le\overline{z_i}\le k_m l_m-1$ (17)

### 3.3.2 用戶端認證

一、$FS_{usr}$在使用服務前，需先與$CA$進行註冊，在一個安全的管道下，$FS_{usr}$插入智慧卡$W_{usr}$及一組隨機碼$rm_{usr}\in[2,n-2]$，與$CA$所提供公開參數執行計算出$\mathrm{PD}_{usr}$(18)式後將$\mathrm{PD}_{usr}$、$W_{usr}$傳給$CA$執行註冊。

- $PD_{usr}=H(W_{usr}\,\|\,rm_{usr})\cdot G$ (18)

二、$CA$當接收到$FS_{usr}$的$\mathrm{PD}_{usr}$、$W_{usr}$，經計算後回傳公鑰$UK$、簽章$\mathrm{sig_{usr}}$給$FS_{usr}$ (19~20)式。

- $UK=PD_{usr}+[ps_{usr}-H(w_{usr})]\cdot G=\left(Uss_x,\,Uss_y\right)$ (19)
- $sig_{usr}=ps_{usr}+ck\left(Uss_x+H(w_{usr})\right)$ (20)

三、$FS_{usr}$將利用接收到$CA$回傳的公鑰$UK$、簽章$\mathrm{sig_{usr}}$，產生$FS_{usr}$的私鑰$uk$(21)式，並透過$\mathrm{sig_{usr}}$驗證$UK$的合法性(22)式，若驗證符合將建立共享金鑰$UK_{usrCA}$(23)式。

- $uk=sig_{usr}+H(w_{usr}\,\|\,rm_{usr})$ (21)
- $UK'=uk\cdot G=UK$ (22)

$$=sig_{usr}+H(w_{usr}\,\|\,rm_{usr})\cdot G$$
$$=\left(ps_{usr}+ck\left(Uss_x+H(w_{usr})\right)\right)\cdot G+H(w_{usr}\,\|\,rm_{usr})\cdot G$$
$$=\left(ps_{usr}+H(w_{usr}\,\|\,rm_{usr})\right)\cdot G+ck\left(Uss_x+H(w_{usr})\right)\cdot G$$
$$=ps_{usr}\cdot G+PD_{usr}+\left(Uss_x+H(w_{usr})\right)\cdot CK$$
$$=UK+H(w_{usr})\cdot G+\left(Uss_x+H(w_{usr})\right)\cdot CK$$

- $UK_{usrCA}=uk\cdot CK=ck\cdot UK$ (23)

### 3.4 登入與驗證階段

$FS_{usr}$插上智慧卡執行登入$FS_{svr}$執行驗證，$FS_{svr}$收到請求後將開始受理並驗證，驗證為合法使用者時則執行虛擬機器$FS_{vm}$權限表計算派給CA註冊後回傳$FS_{usr}$使用，若驗證未過則阻斷用戶端連線。

一、$FS_{usr}$使用智慧卡初次連線登入至伺服器端$FS_{svr}$，$FS_{usr}$會先傳送時戳參數$\mathrm{T}_{usr}$給$FS_{svr}$進行驗證(24)式，通過後提供連線，若未能通過則取消構聯。

・ $(T_{svr} - T_{usr}) \leq \Delta T$ (24)

二、連線後$FS_{svr}$與$FS_{usr}$互相驗證身分是否合法(25～28)式。

・ $uk' = UK + H(w_{usr}) \cdot G + [(Uss_x + H(w_{usr}))] \cdot CK$ (25)
$= PD_{usr} + [ps_{usr} - H(w_{usr})] \cdot G + H(w_{usr}) \cdot G + \left[\left(Uss_x + H(W_{usr})\right)\right] \cdot CK$
$= H(w_{usr} \parallel rm_{usr}) + [(ps_{svr} - H(w_{usr})] + H(w_{usr})] \cdot G + \left[\left(Uss_x + H(w_{usr})\right)\right] \cdot CK$
$= ps_{usr} + H(w_{usr} \parallel rm_{usr}) + \left(Uss_x + H(w_{usr})\right) \cdot ck$

・ $uk = uk'$ (26)

・ $sk' = SK + H(id_{svr}) \cdot G + \left[\left(Fss_x + H(id_{svr})\right)\right] \cdot CK$ (27)
$= PD_{svr} + [ps_{svr} - H(id_{svr})] \cdot G + H(id_{svr}) \cdot G + \left[\left(Fss_x + H(id_{svr})\right)\right] \cdot CK$
$= [H(rm_{svr} \parallel id_{svr}) + [(ps_{svr} - H(id_{svr})] + H(id_{svr})] \cdot G + \left[\left(Fss_x + H(id_{svr})\right)\right] \cdot CK$
$= ps_{svr} + H(rm_{svr} \parallel id_{svr}) + \left(Fss_x + H(id_{svr})\right) \cdot ck$

・ $sk = sk'$ (28)

三、$FS_{usr}$建立隨機參數$\mathrm{RT}_{usr}$(29)式並計算出共享金鑰$SK_{us}$(30)式及 Diffie-Hellman金鑰$DH\mathrm{RT}_{usr}$(31)式傳送至伺服器端$FS_{svr}$。

・ $\mathrm{RT}_{usr} = \mathrm{rt}_{usr} \cdot \mathrm{G}$ (29)

・ $SK_{us} = sk \cdot UK = uk \cdot SK$ (30)

・ $DH\mathrm{RT}_{usr} = \mathrm{RT}_{usr} + SK_{us}$ (31)

四、$FS_{svr}$建立隨機參數$\mathrm{RT}_{svr}$(32)式計算共享金鑰$SK_{us}$(33)式及雙方 Diffie-Hellman金鑰$\mathrm{DH}_{us}$(36)式，求出雙方通訊金鑰$NK_{us}$(37)式，傳送驗證參數至$FS_{svr}$ (38～39)式。

・ $\mathrm{RT}_{svr} = \mathrm{rt}_{svr} \cdot \mathrm{G}$ (32)

・ $SK_{us} = uk \cdot SK = sk \cdot UK$ (33)

・ $DH\mathrm{RT}_{svr} = \mathrm{RT}_{svr} + SK_{us}$ (34)

・ $\mathrm{RT}_{usr} = DH\mathrm{RT}_{usr} - SK_{us}$ (35)

・ $\mathrm{DH}_{us} = \mathrm{rt}_{svr} \cdot \mathrm{RT}_{usr}$ (36)

・ $NK_{us} = \mathrm{DH}_{us} + SK_{us}$ (37)

・ $Check(FS_{svr}A) = H(w_{usr} \parallel id_{svr} \parallel \mathrm{DH}_{us})$ (38)

・ $Check(FS_{svr}B) = H(w_{usr} \parallel id_{svr} \parallel NK_{us})$ (39)

五、$FS_{usr}$驗證$FS_{svr}$所傳來之參數來比對確認合法性 40～44)式，並回傳$Check(FS_{usr}B)$參數至$FS_{svr}$驗證是否正確。

・ $RT_{svr} = DH\mathrm{RT}_{svr} - SK_{us}$ (40)

・ $\mathrm{DH}_{us}{}' = \mathrm{rt}_{usr} \cdot \mathrm{RT}_{svr}$ (41)

・ $NK_{us}{}' = \mathrm{DH}_{us}{}' + SK_{us}$ (42)

・ $Check(FS_{usr}1) = Check(FS_{svr}A)$ (43)

- $Check(FS_{usr}2) = H(w_{usr} \| id_{svr} \| NK_{us}')$ (44)

六、$FS_{svr}$依$FS_{usr}$任務屬性與單位來賦予虛擬機器用戶參數$\hat{U}_{usr}$及服務參數$\hat{Z}_{usr}$，計算出$uFS_{usr}$ 、$zFS_{usr}$、$ad_{usr}$、$ip_{usr}$ (45～49)式，在運用$SK_{svrCA}$計算出$FSC1_{usr}$提供給$CA$註冊(49)式。

- $\hat{U}_{usr} = (\hat{u}_1, \hat{u}_2, \dots, \hat{u}_n), \hat{u}_n \in [0,1]$ (45)
- $\hat{Z}_{usr} = (\hat{z}_1, \hat{z}_2, \dots, \hat{z}_n), \hat{z}_n \in [0,1]$ (46)
- $uFS_{usr} = \sum_{i=1}^{n} \bar{U} \times \hat{U}_{usr}$ (47)
- $zFS_{usr} = \sum_{i=1}^{m} \bar{Z} \times \hat{Z}_{usr}$ (48)
- $ad_{usr} = uFS_{usr} \oplus w_{usr}$ (49)
- $ip_{usr} = zFS_{usr} \oplus w_{usr}$ (50)
- $FSC1_{usr} = (uFS_{usr}, ad_{usr} + ip_{usr}) + SK_{svrCA}$ (51)

七、$CA$使用共享密鑰$SK_{svrCA}$解出$uFS_{usr}$、z$FS_{usr}$、$ad_{usr}$、$ip_{usr}$(52) 式。

- $FSC1_{usr} - SK_{svrCA} = (uFS_{usr}, ad_{usr} + ip_{usr})$ (52)

八、$CA$透過$uFS_{usr}$值對應出$\bar{U}$用戶註冊欄位，使用對應虛擬機器註冊參數在VM_table 並判斷是否已註冊，若未註冊將建立其欄位加密金鑰$\text{colu}_{vm}$(53)式，計算後將加密之權限表$FSC2_{usr}$以安全管道回傳到$FS_{usr}$ (54 ~ 57)式。

- $\text{M}_{usr} = (m_1, m_2) = [(uFS_{usr}, ad_{usr} + ip_{usr}) + \text{colu}_{vm}]$ (53)
- $FSC2_{usr1} = ps_{svr} \cdot \text{G}$ (54)
- $J_{usr} = ps_{svr} \cdot SK = (\text{j}_1, \text{j}_2)$ (55)
- $FSC2_{usr2} = \text{M}_{usr} \cdot J_{usr} = (m_1 \cdot \text{j}_1, m_2 \cdot \text{j}_2) = (C_1, C_2)$ (56)
- $FSC2_{usr} = (FSC2_{usr1}, FSC2_{usr2})$ (57)

九、$FS_{usr}$運用通訊金鑰$NK_{us}$計算出$\bar{W}$存放於智慧卡中(58)式。

- $\bar{W} = FSC2_{usr} + NK_{us}$ (58)

### 3.5 申請服務及虛擬機器使用階段

本階段為用戶$FS_{usr}$向伺服端$FS_{svr}$申請服務階段，其流程。

一、申請服務前$FS_{usr}$運用通訊密鑰$NK_{us}$解出$FSC2_{usr}$(59) 式，向$FS_{svr}$傳送RquestViewer 虛擬機器服務申請訊息及虛擬機器加密參數$FSC2_{usr}$。

- $FSC2_{usr} = \bar{W} - NK_{us}$ (59)

二、$FS_{svr}$於接收$FS_{usr}$的服務申請RquestViewer 及虛擬機器加密參數$FSC2_{usr}$執行計算出$\overline{\text{R}}$並對$FSC2_{usr2}$解出虛擬機器用戶及位址加密欄位，在依其註冊欄位確認其欄位金鑰後解出$FS_{usr}$所使用的虛擬機器位址，$FS_{svr}$運用通訊密鑰$NK_{us}$將用戶服務權限加密後回傳AceptViewer 訊息供$FS_{usr}$正常使用服務。 (60～63)式。

- $\overline{\text{R}} = (\text{r}_1, \text{r}_2) = sk \cdot FSC2_{usr1}$ (60)
  $\overline{\text{R}} = ps_{svr} \cdot (\text{G} \cdot sk) = ps_{svr} \cdot SK$
- $M_{usr} = (FSC2_{usr2} \cdot \overline{\text{R}}^{-1}) = (m_1, m_2)$ (61)
- $(uFS_{usr}, ad_{usr} + ip_{usr}) = M_{usr} - \text{colu}_{vm}$ (62)
- $ip_{usr} = (ad_{usr} + ip_{usr}) - (uFS_{usr} \oplus w_{usr})$ (63)

- $\mathrm{z}FS_{usr} = ip_{usr} \oplus w_{usr} = (\mathrm{z}FS_{usr} \oplus w_{usr}) \oplus w_{usr}$ (64)
- $(\hat{U}_{usr})_2 = (uFS_{usr} modk_n) - (uFS_{usr} modl_n)$ (65)
- $(\hat{Z}_{usr})_2 = (zFS_{usr} modk_m) - (zFS_{usr} modl_m)$ (66)

# 四、 安全性分析

因現行空軍空情前遞系統運作方式，僅利用輸入帳號、密碼作為系統登入方式，若未能夠有效及更安全的身分驗證機制，將導致敵偽冒侵入攻擊情事發生，並可能產生用戶端帳戶遭敵盜取，延伸出機敏資料或情資外洩。本研究將植基於橢圓曲線密碼系統及背包問題理論為基礎，設計具有混和式加密及多因子的身分驗證及安全管控機制，能抵抗偽冒攻擊等以符合高安全性防護機制來完善系統妥善。安全性及效能分析將分別敘述如後：

## 4.1 安全性分析

本研究將以國際標準化組織 ISO/IEC 27001:2013 資訊安全管理系統:(ISO, 2013)及 NIST SP 800-63-3 數位身分認證指南(Paul et al., 2017)所要求之資訊安全規範，其中以其機密性、完整性、可用性及不可否認性。

### 4.1.1 機密性

機密性(Confidentiality)，是避免讓具有機敏性資料暴露在無權限人員或程式上的一種安全保護機制，主要是保護資料在傳輸、儲存時，不讓無授權人員接收、處理及使用。(Leadership, 2016)

在本研究其登入驗證階段中，$\mathrm{FS}_{\mathrm{svr}}$可從$\mathrm{FS}_{\mathrm{usr}}$身分別中配賦虛擬機器使用權限表密文，將$\mathrm{FS}_{\mathrm{usr}}$相關註冊資訊送至CA；透過CA計算$\mathrm{FS}_{\mathrm{usr}}$之虛擬機器使用權限密文$FSC1_{usr}$(51)式及$\mathrm{FS}_{\mathrm{usr}}$並透過智慧卡安全存放$\overline{W}$訊息(58) 式達到多因子認證方式。

1. $FSC1_{usr} = (uFS_{usr}, ad_{usr} + ip_{usr}) + SK_{svrCA}$ (51)
2. $\overline{W} = FSC2_{usr} + NK_{us}$ (58)

於申請服務階段中，若敵偽冒身分，除了需具備智慧卡多因子認證外，若欲使用中間人攻擊來獲得解密密文時，首先要破解取得虛擬機器欄位及權限類別序列值與欄位加密金鑰(59)式、(61～62)式及(64)式而將面對橢圓曲線離散對數難題；即使敵方以其他不當方式取得欄位及權限類別序列值，對於要解出欄位及權限類別序列，也將面臨隨機背包難題而不易破解。

3. $FSC2_{usr} = \overline{W} - NK_{us}$ (59)
4. $M_{usr} = (m_1, m_2) = (FSC2_{usr2} \cdot \bar{R}^{-1})$ (61)
5. $(uFS_{usr}, ad_{usr} + ip_{usr}) = M_{usr} - \mathrm{colu}_{vm})$ (62)
6. $\mathrm{z}FS_{usr} = Ip_{usr} \oplus w_{usr} = (\mathrm{z}FS_{usr} \oplus w_{usr}) \oplus w_{usr}$ (64)

4.1.2 完整性

完整性(Integrity)，確保資訊保持原來的狀態，並使資訊只允許有權限的用戶端使用或修改資料內容，並可利用訊息摘要(Digest)來作為判斷資料的完整性，確保資料從產生、編碼、傳送、解碼後到使用者手上的資料為原始資訊且未經未授權的人修改(劉子瑜，2018)。

本研究於註冊金鑰階段中，$FS_{usr}$與$FS_{svr}$持虛擬機器識別表與選取隨機參數，計算其身分憑證(2～4)式及(8～10)式傳送至$CA$；$CA$將$FS_{usr}$、$FS_{svr}$之虛擬機器識別表進行雜湊運算並結合$FS_{usr}$、$FS_{svr}$之身分憑證，分別產生其數位簽章並相互完成認證。

$$7.\ PD_{svr} = H(rm_{svr} \parallel id_{svr}) \cdot \mathrm{G} \tag{2}$$

$$8.\ SK = PD_{svr} + [ps_{svr} - H(id_{svr})] \cdot G = \left(Fss_x,\ Fss_y\right) \tag{3}$$

$$9.\ sig_{svr} = ps_{svr} + ck\left(Fss_x + H(id_{svr})\right) \tag{4}$$

$$10.PD_{usr} = H(w_{usr} \parallel rm_{usr}) \cdot G \tag{8}$$

$$11.UK = PD_{usr} + [ps_{usr} - H(w_{usr})] \cdot G = \left(Uss_x,\ Uss_y\right) \tag{9}$$

$$12.sig_{usr} = ps_{usr} + ck\left(Uss_x + H(w_{usr})\right) \tag{10}$$

敵若欲破解將面臨單向雜湊函數及橢圓曲線離散難題；就算取得系統管理員權限存取資料，但未能獲得管理者私鑰(1)式，或是竊得共享金鑰，否則將面對橢圓曲線解離散對數難題。

$$13.CK = ck \times \mathrm{G} \tag{1}$$

4.1.3 可用性

可用性(Availability)， 如何讓使用者有效使用本系統為本研究重要課題之一，其影響為兩個層面一是網路連線情況，另一為虛擬機器使用狀況，若在網路情況良好下，應確保使用者所使用的虛擬機器為其所分配，並保證無相關或無授權的人占用，確保系統可用性(徐豪謙，2019)。

於登入驗證階段中，$FS_{usr}$與$FS_{svr}$確認身分無誤後，則用戶與伺服將相互執行交換共同(30)式與通訊之金鑰(37)式；驗證後$FS_{usr}$申請虛擬機器使用服務時、$FS_{svr}$再依據$FS_{usr}$其身分別權限(65~66)式，將用戶與伺服的通訊秘鑰運算結果以加密後、回傳AceptViewer 訊息給$FS_{usr}$來使用虛擬機器服務。

$$14.SK_{us} = sk \cdot UK = uk \cdot SK \tag{30}$$

$$15.NK_{us} = \mathrm{DH}_{us} + SK_{us} \tag{37}$$

$$16.(\widehat{U}_{usr})_2 = (uFS_{usr}modk_n) - (uFS_{usr}modl_n) \tag{65}$$

$$17.(\hat{Z}_{usr})_2 = (zFS_{usr}modk_m) - (zFS_{usr}modl_m) \tag{66}$$

敵若偽冒$FS_{usr}$或$FS_{svr}$身分，將遇到橢圓曲線離散對數難題使無授權之人士因無法通過身分驗證而停止連線服務、可避免$FS_{svr}$遭分散式阻斷服務攻擊(Distributed Denial-of-Service Attack, DDoS)而造成的服務中斷，避免用戶端因無法執行對應服務而影響任務成效。

4.1.4 不可否認性

不可否認性(Non-repudiation)，指用戶不能否認自己曾做過的任何行為，其相關聯之行動可分為五個階段：服務申請、資料(訊息)產生、資料(訊息)傳送與儲存、資料(訊息)驗證及問題查找與解決，在這些階段中有不同階段不同的角色，在關鍵的事件上為不可否認之項目格外重要(陳守國，2015)。

於登入驗證階段中，$FS_{usr}$將產生虛擬機器欄位權限密文，而$FS_{usr}$ 與$FS_{svr}$間生成共享秘鑰(30)式與通訊金鑰(37)式；後續於申請服務階段中，$FS_{usr}$提出資料存取服務、$FS_{svr}$再依據$FS_{usr}$其身分別及虛擬機器使用權限，運算結果將以其通訊密鑰加密後，回傳給$FS_{usr}$。

$$18.SK_{us} = sk \cdot UK = uk \cdot SK \tag{30}$$

$$19.NK_{us} = \mathrm{DH}_{us} + SK_{us} \tag{37}$$

本研究申請服務階段中，$FS_{svr}$以其私鑰解密且產製通訊密鑰(36 式)過程中，其$FS_{usr}$與$FS_{svr}$之個人資訊包含其中(41)式(60)式，雙方無法否認之前所執行過的關鍵行為。

$$20.\mathrm{DH}_{us} = \mathrm{rt}_{svr} \cdot \mathrm{RT}_{usr} \tag{36}$$

$$21.\mathrm{DH}_{us}{}' = \mathrm{rt}_{usr} \cdot \mathrm{RT}_{svr} \tag{41}$$

$$22.\overline{\mathrm{R}} = (\mathrm{r}_1, \mathrm{r}_2) = sk \cdot FSC2_{usr1} \tag{60}$$

4.1.5 存取控制

存取控制(Access Control)，為一控制措施，要求使用者在獲得使用服務前，使用者需經過正式的註冊程序，在通過審核可之後，賦予唯一識別代號，來管控並留下存取資訊的紀錄，方可使用服務；思考重點在於如何確保所有的資訊存取，在其系統流程中都應基於標準安全規範(花俊傑，2011)。

本研究於登入驗證中，首先將驗證雙方時戳(3-24)式，保證在時效內連線，否則將取消，通過後將依照$FS_{usr}$所分配的虛擬機器，以序列方式定義權限表並利用隨機背包密碼系統計算分配服務之權限值(49～51)式；於申請服務階段中，僅回傳$FS_{usr}$虛擬機器使用權限之運算結果。

$$23.(T_{svr} - T_{usr}) \leq \Delta T \tag{24}$$

$$24.ad_{usr} = uFS_{usr} \oplus w_{usr} \tag{49}$$

$$25.ip_{usr} = zFS_{usr} \oplus w_{usr} \tag{50}$$

$$26.FSC1_{usr} = (uFS_{usr}, ad_{usr} + ip_{usr}) + SK_{svrCA} \tag{51}$$

若發生未授權人士盜用$FS_{usr}$身分，利用$FS_{usr}$來向$FS_{svr}$提出虛擬機器申請服務時，將經過$FS_{svr}$驗證，期間$FS_{svr}$判斷為非法授權用戶，$FS_{svr}$將否絕其申請服務之請求，以達存取控制與使用權管控之目的。

4.1.6 身分認證

身分認證(Authentication)，可解釋為使用者或群組等帳號再登入系統時，提供身分驗證的功能，依登入帳號輸入相對的密碼，來認證使用者的身分是否為合法，而所謂認證，就是要確認是否為正確的用戶端所提出服務的申請，以確保合法的用戶端使用權不

受侵害(洪杰文、歸偉夏，2019)。

本研究註冊金鑰階段中，$FS_{usr}$及$FS_{svr}$與$CA$完成註冊後獲得各自公鑰及簽章後(4～7)式及(10～13)式，相互傳送認證資訊而無需與$CA$保持連線，可離線相互完成身分認證後，建立共享秘鑰與加密通訊(以$FS_{usr}$對$FS_{svr}$實施認證為例(15～16)式。

$$27.sig_{svr} = ps_{svr} + ck\left(Fss_x + H(id_{svr})\right) \quad (4)$$

$$28.sk = sig_{svr} + H(rm_{svr} \| id_{svr}) \quad (5)$$

$$29.SK' = sk \cdot G = SK \quad (6)$$

$$30.SK_{svrCA} = sk \cdot CK = ck \cdot SK \quad (7)$$

$$31.sig_{usr} = ps_{usr} + ck\left(Uss_x + H(w_{usr})\right) \quad (10)$$

$$32.uk = sig_{usr} + H(w_{usr} \| rm_{usr}) \quad (11)$$

$$33.UK' = uk \cdot G = UK \quad (12)$$

$$34.UK_{usrCA} = uk \cdot CK = ck \cdot UK \quad (13)$$

$$35.uk' = UK + H(w_{usr}) \cdot G + [(Fss_x + H(w_{usr}))] \cdot CK \quad (15)$$

$$36.sk' = SK + H(id_{svr}) \cdot G + [(Uss_x + H(id_{svr}))] \cdot CK \quad (16)$$

$FS_{usr}$、$FS_{svr}$雙方執行身分認證時，在持有對方之公開認證資訊與$CA$之公鑰，可不用經過$CA$來獨立進行身分認證。若敵如偽裝$FS_{usr}$或$FS_{svr}$身分，將面臨橢圓曲線離散對數難題而被否決;另外再登入驗證階段中,以標準政策給予合法用戶端所能擁有之使用權限,防止未經授權使用者構連藉以提升系統安全性。

4.1.7 抗同謀碰撞攻擊

抗同謀攻擊(Avoid Collusion Attacks)，指內部管理人員的帳戶遭駭或是與非授權人員有掛鉤，導致用戶權限服務遭非法使用，進而發生盜用行為。

相關本研究登入驗證階段中，$FS_{usr}$公鑰及私鑰非直接由$CA$產製及保管，為結合身分識別、簽章、隨機參數(8 ~ 10)式及$CA$之隨機參數計算而來，避免遭非授權人員與$CA$串聯所竊取。

$$37.PD_{usr} = H(w_{usr} \| rm_{usr}) \cdot G \quad (8)$$

$$38.UK = PD_{usr} + [ps_{usr} - H(w_{usr})] \cdot G = \left(Uss_x, Uss_y\right) \quad (9)$$

$$39.sig_{usr} = ps_{usr} + ck\left(Uss_x + H(w_{usr})\right) \quad (10)$$

本研究中，$CA$僅參與計算公鑰過程，無法直接產生、偽造$FS_{usr}$之公鑰及私鑰。另$CA$未參與申請服務階段，且$FS_{svr}$以私鑰、而非透過$CA$解密資訊取得$FS_{usr}$相關權限值資料，有效避免非授權人員藉$AS$之便，防阻同謀攻擊。

4.1.8 資料保密

資料保密(Data Confidentiality)，資料庫裡所儲存資料合法用戶端共享的資料，所以盡可能要有一套安全的管理機制,以避免遭敵方滲透盜取重要機敏資料( 陳會安,2012 )。

本研究註冊金鑰階段中，由$FS_{svr}$產生超增序列值(8～11)式建立虛擬機器欄位用戶與服務權限表並依加密欄位數量建立加密金鑰(14～17)式。

40.取隨機$n$向量$U = \{u_1, u_2, \dots, u_n\}$，$u_i$為正整數。 (8)

41.取隨機$m$向量$Z=\{z_1,z_2,\dots,z_m\}$，$z_i$為正整數。 (9)

42.計算向量$\widetilde{\mathrm{U}}=\{\widetilde{u_1},\widetilde{u_2},\dots,\widetilde{u_n}\}$，$\widetilde{u_i}=u_i-2^{n-1}$，$i=1,\dots,n$ (10)

43.計算向量$\widetilde{\mathrm{Z}}=\{\widetilde{z_1},\widetilde{z_2},\dots,\widetilde{z_m}\}$，$\widetilde{z_i}=z_i-2^{n-1}$，$i=1,\dots,m$ (11)

44.$\overline{u_i}\equiv u_i(mod k_n),\overline{u_i}\equiv\widetilde{u_i}(\mathrm{mod}l_n),i=1,\dots,n$ (14)

45.$\overline{z_i}\equiv z_i(mod k_m),\overline{z_i}\equiv\widetilde{z_i}(\mathrm{mod}l_m),i=1,\dots,n$ (15)

46.$\overline{U}=\{\overline{u_1},\overline{u_2},\dots,\overline{u_n}\}$，其中 $0\le\overline{u_i}\le k_nl_n-1$ (16)

47.$\bar{Z}=\{\overline{z_1},\overline{z_2},\dots,\overline{z_m}\}$，其中 $0\le\overline{z_i}\le k_ml_m-1$ (17)

敵方如欲由數值反推欄位屬性及權限序列，將面臨破解隨機背包難題、而欲破解權限值密文(47～48)式，將面臨破解橢圓曲線離散對數難題而難以達成(51)式。

48.$uFS_{usr}=\sum_{i=1}^{n}\overline{U}\times\widehat{U}_{usr}$ (47)

49.$zFS_{usr}=\sum_{i=1}^{m}\bar{Z}\times\hat{Z}_{usr}$ (48)

50.$FSC1_{usr}=(uFS_{usr},ad_{usr}+ip_{usr})+SK_{svrCA}$ (51)

針對本研究基於橢圓曲線密碼系統並導入多因子身分認證協定機制，與現行系統運作機制之機密性、完整性、可用性、不可否認性、存取控制、身分認證、抗同謀攻擊及資料保密等項作效益分析比較，本研究除符合機密性、存取控制之要求外，亦就可用性及連線資料保密進行改良精進與補足完整性、不可否認性、身分認證及抗同謀攻擊之不足處，故本研究可達到安全性要求（如表 4）。

表4　本研究與現行系統之效益分析表

| 項次 | 比較項目 | 現行系統運作機制 | | 本研究 | |
|---|---|---|---|---|---|
| 1 | 機密性 | 未使用多因子認證，且用戶端僅使用輸入帳號密碼來登入系統，登入方式無法判斷是否為合法用戶。 | △ | 用戶端使用服務前均須完成註冊與執行身分認驗證後，搭配智慧卡多因子認證，始可連線至虛擬伺服器進行虛擬機器使用服務。 | V |
| 2 | 完整性 | 未使用雜湊函數或 RSA 數位簽章等方法，確保資訊傳遞間之完整性。 | X | 敵若欲偽冒簽章或竄改，則面對破解單向無碰撞雜湊函數及橢圓曲線離散對數難題將難以破解。 | V |
| 3 | 可用性 | 僅利用防火牆阻擋可疑來源位址進行管控及用戶帳密表；若其未設定於黑名單，將會面臨阻斷式攻擊。 | △ | 用戶端若未能與伺服端完成身分驗證，將限制或拒絕該終端與伺服器連線，使系統伺服器能抵禦阻斷式攻擊。 | V |
| 4 | 不可否認性 | 目前各用戶僅使用固定憑證，用戶端於執行動作之後，將有可能遭遇到事後否認行為。 | X | 運用智慧卡及個人憑證等方式，雙方使用共同通訊金鑰，資訊傳達可避免曾執行過的關鍵事件或動作遭到否認。 | V |
| 5 | 存取控制 | 目前運用實體保密器保護並與用戶帳密表來限制登入，用戶端若遭盜用將可面臨機敏資料外洩。 | △ | 運用時戳來限制服務申請及登入認證，給予用戶端虛擬機器使用權限，若判斷為非授權時間或身分，拒絕終端服務申請，達到管理使用權限之目的。 | V |
| 6 | 身分認證 | 目前僅使用用戶帳密表來限制登入，沒有第三方安全認證機制。 | △ | 因應任務特性，為了降低用戶端對第三方認證系統之依賴，採用採自我認證機制，以期達成於受限網路環境下依然能完成相關認證連線。 | V |
| 7 | 抗同謀攻擊 | 管理方式為採主從管控，若管理人員其身分帳密遭偽冒或盜用，則用戶端將失去安全保障。 | X | 本研究運用我認證方式，在用戶端及虛擬伺服器彼此間權限密文建立之間及服務存取時認證伺服器都未參加，故能抵禦同謀攻擊。 | V |
| 8 | 資料保密 | 本系統具備實體保密器並與使用用戶帳密表來限制登入，但無多因子認證保護機制。 | △ | 具備有橢圓曲線離散對數及隨機背包雙重難題，藉此保護用戶及伺服端所計算出權限密文以保障服務及資料安全。 | V |
| 附註：V代表符合、△代表部分符合、X代表不符合 | | | | | |

資料來源：本研究整理

### 4.2 執行效能分析

本研究之效益評估將整理各階段運算成本及時間複雜度運算參考表(蘇品長等，2020)為基準(如表 5)，囿於本研究屬國軍客製化系統且原系統無相關參照演算法，故無從比較，僅針對本研究執行各事件之運算成本及時間複雜度評估(如表 6)。

表 5　運算成本參考表

| 符號 | 定義 | 運算成本 |
|---|---|---|
| $T_{MUL}$ | 執行一次模式乘法運算所需時間 | 參考備註一 |
| $T_{ECMUL}$ | 執行一次 ECC 乘法運算所需時間 | $29T_{MUL}$ |
| $T_{ECADD}$ | 執行一次 ECC 加法運算所需時間 | $5T_{MUL}$ |
| $T_{INVS}$ | 執行一次模式乘法反元素運算所需時間 | $240T_{MUL}$ |
| $T_{EXP}$ | 執行一次模式指數運算所需時間 | $240T_{MUL}$ |
| $t_h$ | 執行一次值雜湊函數所需時間 | $0.4T_{MUL}$ |
| $T_h$ | 執行一次點雜湊函數所需時間 | $23T_{MUL}$ |
| $T_{\sum mul}$ | 執行一次數值序列乘法運算所需時間 | 參考備註二 |
| $T_{\sum add}$ | 執行一次數值序列加法運算所需時間 | 參考備註三 |
| $T_{ADD}$ | 執行一次模式加法運算所需時間 | 因運算時間短，可忽略不計 |
| $T_{\oplus}$ | 執行一次 XOR 運算所需時間 | |
| $T_{\|}$ | 執行一次串接運算所需時間 | |
| 一、本研究僅以$T_{MUL}$作為運算成本計算基準，詳細視不同機器，規格及執行環境而異。<br>二、$T_{\sum mul}$:若該序列長度為 n，則成本為$nT_{MUL}$<br>三、$T_{\sum add}$若該序列長度為 n，則成本為$(n-1)T_{ADD}$ | | |

資料來源：蘇品長等，2020

表6　本系統運算成本估計表

| 事件 | 運算式 | 運算成本概估 |
|---|---|---|
| 初始階段 | $CK = ck \times$ G(3-1) | $1T_{ECMUL}$ |
| subtotal | | $29T_{MUL}$ |
| 註冊及獲取金鑰階段 | $PD_{svr} = H(rm_{svr} \| id_{svr}) \cdot G$ | $T_{ECMUL}+1t_h+T_{\|}$ |
| | $SK = PD_{svr} + [ps_{svr} - H(id_{svr})] \cdot G$ | $T_{ECMUL}+2T_{ADD}+t_h$ |
| | $sig_{svr} = ps_{svr} + ck(Fss_x + H(id_{svr}))$ | $T_{ECMUL}+2T_{ADD}+t_h$ |
| | $sk = sig_{svr} + H(rm_{svr} \| id_{svr})$ | $T_{ADD}+t_h+T_{\|}$ |
| | $SK' = sk \cdot G = SK$ | $T_{ECMUL}$ |
| | $SK_{svrCA} = sk \cdot CK = ck \cdot SK$ | $2T_{ECMUL}$ |
| | $PD_{usr} = H(w_{usr} \| rm_{usr}) \cdot G$ | $T_{ECMUL}+1t_h+T_{\|}$ |
| | $UK = PD_{usr} + [ps_{usr} - H(w_{usr})] \cdot G$ | $T_{ECMUL}+2T_{ADD}+t_h$ |
| | $sig_{usr} = ps_{usr} + ck(Uss_x + H(w_{usr}))$ | $T_{ECMUL}+2T_{ADD}+t_h$ |
| | $uk = sig_{usr} + H(rm_{usr} \| w_{usr})$ | $T_{ADD}+t_h+T_{\|}$ |
| | $UK' = uk \cdot G = UK$ | $T_{ECMUL}$ |
| | $UK_{usrCA} = uk \cdot CK = ck \cdot UK$ | $2T_{ECMUL}$ |

| | | |
|---|---|---|
| subtotal | | $176T_{MUL}$ |
| 登入與驗證階段 | $uk' = UK + H(w_{usr}) \cdot G + [(Fss_x + H(w_{usr}))] \cdot CK$ | $2T_{ECMUL}+2T_{ECADD} + t_h+T_{ADD}$ |
| | $sk' = SK + H(id_{svr}) \cdot G + [(Uss_x + H(id_{svr}))] \cdot CK$ | $2T_{ECMUL}+2T_{ECADD} + t_h+T_{ADD}$ |
| | $RT_{usr} = rt_{usr} \cdot G$ | $T_{ECMUL}$ |
| | $SK_{us} = sk \cdot UK = uk \cdot SK$ | $2T_{ECMUL}$ |
| | $DHRT_{usr} = RT_{usr} + SK_{us}$ | $T_{ADD}$ |
| | $RT_{svr} = rt_{svr} \cdot G$ | $T_{ECMUL}$ |
| | $SK_{us} = uk \cdot SK = sk \cdot UK$ | $2T_{ECMUL}$ |
| | $DHRT_{svr} = RT_{svr} + SK_{us}$ | $T_{ECADD}$ |
| | $RT_{usr} = DHRT_{usr} - SK_{us}$ | $T_{ECADD}$ |
| | $DH_{us} = rt_{svr} \cdot RT_{usr}$ | $T_{ECMUL}$ |
| | $NK_{us} = DH_{us} + SK_{us}$ | $T_{ECADD}$ |
| | $Check(FS_{svr}A) = H(w_{usr} \parallel id_{svr} \parallel DH_{us})$ | $T_h + 3T_{\parallel}$ |
| | $Check(FS_{svr}B) = H(w_{usr} \parallel id_{svr} \parallel NK_{us})$ | $T_h + 3T_{\parallel}$ |
| | $RT_{svr} = DHRT_{svr} - SK_{us}$ | $T_{ADD}$ |
| | $DH_{us}' = rt_{usr} \cdot RT_{svr}$ | $T_{ECMUL}$ |
| | $NK_{us}' = DH_{us}' + SK_{us}$ | $T_{ECADD}$ |
| | $Check(FS_{usr}1) = Check(FS_{svr}A)$ | $T_h$ |
| | $Check(FS_{usr}2) = H(w_{usr} \parallel id_{svr} \parallel NK_{us}')$ | $T_h + 3T_{\parallel}$ |
| | $uFS_{usr} = \sum_{i=1}^{n} \bar{U} \times \hat{U}_{usr}$ | $T_{\sum mul} + (n-1)T_{\sum add}$ |
| | $zFS_{usr} = \sum_{i=1}^{m} \bar{Z} \times \hat{Z}_{usr}$ | $T_{\sum mul} + (m-1)T_{\sum add}$ |
| | $ad_{usr} = uFS_{usr} \oplus w_{usr}$ ， $ip_{usr} = zFS_{usr} \oplus w_{usr}$ | $T_{\oplus}$ ， $T_{\oplus}$ |
| | $FSC1_{usr} = \left(uFS_{usr}, ad_{usr} + ip_{usr}\right) + SK_{svrCA}$ | 2 $T_{ECADD}$ |
| | $M_{usr} = (m_1, m_2) = [(uFS_{usr}, Ip_{usr}) + colu_{vm}]$ | $T_{ECMUL}$ |
| | $FSC2_{usr1} = ps_{svr} \cdot G$ | $T_{ECMUL}$ |
| | $J_{usr} = ps_{svr} \cdot SK = (j_1, j_2)$ | $T_{ECMUL}$ |
| | $FSC2_{usr2} = M_{usr} \cdot J_{usr} = \left(m_1 \cdot j_1, m_2 \cdot j_2\right) = (C_1, C_2)$ | $T_{ECADD}$ |
| subtotal | | $(589.8+n+m)T_{MUL}$ |
| 申請服務階段 | $FSC2_{usr} = \overline{W} - NK_{us}$ | $T_{ECADD}$ |
| | $\overline{R} = (r_1, r_2) = sk \cdot FSC2_{usr1}$ | $T_{ECMUL}$ |
| | $M_{usr} = (FSC2_{usr2} \cdot \overline{R}^{-1}) = (m_1, m_2)$ | $T_{INVS}$ |
| | $(uFS_{usr}, ad_{usr} + ip_{usr}) = M_{usr} - colu_{vm}$ | $T_{ECADD}$ |
| | $zFS_{usr} = ip_{usr} \oplus w_{usr} = (zFS_{usr} \oplus w_{usr}) \oplus w_{usr}$ | $T_{\oplus}$ |
| subtotal | | $263T_{MUL}$ |
| Total | | $(1057.8+n+m)T_{MUL}$ |
| 備註：本研究屬客製化系統設計，囿於原系統無相關參照演算法，故無從比較。 | | |

資料來源：本研究

# 伍、結論

目前資安威脅無所不在，伴隨者科技技術與資訊架構的成長，傳統的資安防禦機制稍嫌不足以應付新型態的攻擊威脅，因此本研究提出基於橢圓曲線密碼系統及隨機背包密碼系統，利用橢圓曲線密鑰小的優點與隨機背包密碼系統運算效能快，且適用於空情前遞系統之身分認證暨金鑰交換機制，並導入國軍智慧卡運用自我認證與存取控制之設計，強化空情前遞系統安全性以達到資料安全存取管理。綜整本研究貢獻如下：

一、 使空情系前遞統於身分認證上能配合多因子認證，將具備有更高的安全性，能防止用戶端偽冒、敵攻擊及抵禦竊聽。

二、 本系統設計架構將植基於橢圓曲線密碼系統，故在相同的安全強度下，其金鑰長度遠較 RSA 短且處理速度較快，加解密應用效率較佳。

三、 運用自我認證使在有限環境資源下，除能完善系統安全性及執行效益外，且功能正常運作並達機密性、完整性、可用性之各項標準。

國軍針對資訊服務內需，越來越重視，大至軍事武器系統，小至後勤維補自動管理，都可見到資訊化與數據化的改變與成長，反觀其便利資訊服務伴隨而來是網路安全及資料外洩等問題，國軍為政府整體資安防護之一環，除應落實網路實體隔離外，建置嚴密的資安防護機制更為重要，本研究方向相關參考文獻以多方規劃、蒐整後，針對未來研究方向歸納規劃如下：

一、 目前國軍針對智慧卡的運用，僅使用於雲端門禁管理系統與國軍線上公文系統，後續若能依本研究所推導的演算法，針對國軍各資訊網頁平台之整合，作為其多因子認證或存取控制媒介，進行實測其可行性及安全性。

二、 有鑑於生物特徵認證已漸漸普及各行政機關機構，若未來國軍開放配合相對應政策與規定，若以本研究提出認證方式來強化多重身分認證安全性，期能降低身分偽冒發生機率。

三、 本研究雖僅運用於空軍空情前遞系統之資料庫，未來可針對各指管系統、戰情或各相關異質平台進行整合。

## 【參考文獻】


**中文部分**

方俊斌，2012，基於一次性動態密碼及行動裝置進行身分驗證，國立臺灣科技大學資訊工程系碩士學位論文。

邱英捷，2011，強化數位化戰場經營—可快速自我認證之研究，國防大學管理學院資訊管理研究所碩士論文。

林政宏，2011，智慧卡的科技，科學研習月刊，第 44 卷，第 2 期：4-7。

洪杰文、歸偉夏，2019，新媒體技術，崧燁文化事業有限公司。

徐豪謙，2019，以虛擬桌面技術建置高可用性 AI 虛擬雲端教室。國立臺南大學數位學習科技學系碩士在職專班碩士論文。

陳柏諭，2014，強化國軍智慧卡身分認證及串流加密機制之設計，國防大學管理學院資訊管理研究所碩士論文。

陳守國、付安民、秦寧元，2015，異構無線網絡中基於自更新哈希鏈的不可否認性計費協議，計算機科學，第四十二卷，第三期，111-116 頁。

陳會安，2012，SQL Server 2012 資料庫管理實務，碁峰資訊股份有限公司。

張志義，2004，從「女書」到「量子密碼」—講悄悄話的科學與藝術，科學發展，第 373 期，62-67。

國家安全會議，2018，國家資通安全戰略報告-資安即國安，國家安全會議 國家資通安全辦公室。

國防部部本部，2012，國軍資訊安全政策 2.0，國防部部本部。

國防部空軍司令部，2012，通資電運用教則，國防部空軍司令部。

鄧安文，2018，密碼學-密碼分析與實驗(第三版)，新北市:全華圖書股分有限公司。

謝定芳，2017，設計具多因子之身分認證協定機制－以空軍指管通情系統為例，國防大學管理學院資訊管理研究所碩士論文。

龔建丞，2018，一個增強型的智慧卡認證及金鑰協商機制之研究，中國文化大學商學院資訊管理學系碩士論文。

劉子瑜，2018，安全智慧電表韌體更新，國立中興大學資訊科學與工程學系碩士論文。

蘇品長、高晨栩、許孟華，2020，具彈性調整權重之門檻秘密分享機制研究，國防管理學報，第四十一卷，第一期，33-52 頁。

**英文部分**

Burr, W. E., Dodson, D. F. and Polk, W. T., 2006, Electronic Authentication Guideline, NIST Special Publication, 800, 62-63.

Chaudhry, S. A., Farash, M. S., Naqvi, H., Kumari, S. and Khan, M. K., 2015, An enhanced privacy preserving remote user authentication scheme with provable security. Security and Communication Networks, 3,782-3,795.

Chang, Y. F. and Chang, H. C., 2009, Security of dynamicID-based remote user authentication scheme. Fifth International Joint Conferenceon, 2,108-2,110.

Chang, Y. F., Tai, W. L. and Chang, H. C., 2014, Untraceable dynamic identity based remote user authentication scheme withverifiable password u-pdate. International Journal of CommunicationSystems, (27:11), 3,430-3,440.

Das, M.L., Saxena, A and Gulati, V.P., 2007, A dynamic ID-based remote u-ser authentication scheme. IEEE Transactions onConsumer Electronics, (50:2), 629-631.

Elaine B., 2016, Recommendation for Key Management Part 1: Gener-al, NIST Special Publication 800, 56-57.

Kumari, S., Khan, M. K., and Li, 2014, An improved remote user authentication scheme with key agreement. Computers &Electrical Engineering, 40-41.

Koblitz, N., 1987, elliptic curve cryptosystems, Mathematics of Computation, (177:22), 203-209

Paul, A. G., Michael, E. G., and James, L. F., 2017, Digital Identity Guidelines, NIST Special Publication 800, (63:3).

Shi, Y., Shen, H., Zhang, Y., and Chen, J.,2015, An Improved Anonymous Remote user Authentication Scheme with Key Agreementbased on Dynamic Identity. International Journal ofSecurity and Its Applications, (9:5), 255-268.

Tsai, C.H., and Su, P.C., 2021, The application of multi-server authentication scheme in internet banking transaction environments, Information Systems and e-Business Management, (19:1), 77-105.

網路部分

ISO/IEC 27001:2013:Information technology — Security techniques — Information security management systems — Requirements(available online athttps://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en).[visited in 2019/08/12]

Leadership Editors, ISO/IEC 27001：2013 資訊安全管理系統 Information Security Management System, ISMS,https://www.isoleader.com.tw/home/iso-coaching-detail/ISO27001.[visited in 2019/08/12]。

花俊傑，2011，存取控制的資安要求，參見網管人網站 https://www.netadmin.com.tw/netadmin/zh-tw/market/2B64821384D2495586F81F9DAFF2BE5B.[visited in 2019/09/16]。

黃建衛，網際網路服務使用者身分驗證機制之安全性研析，參見財金資訊股分有限公司網站 https://www.fisc.com.tw/tc/knowledge/quarterly1.aspx?PKEY=0abc938c-0f9b-4ed3-a131-8c9ff86e946b〔visited in 2019/06/22〕。

資策會，企業對網路安全感到疑慮，參見資訊網路安全與智慧財產權保護簡介簡報 http://sna.csie.ndhu.edu.tw/~cnyang/CO/sld009.htm〔visited in 2019/07/12〕。

維基百科，RSA 加密演算法，參見維基百科網站 https://zh.wikipedia.org/wiki/RSA 加密演算法[visited in 2019/07/16]。

羅正漢，網際網路服務使用者身分驗證機制之安全性研析，參見 iThome 網站 https://www.ithome.com.tw/news/128035〔visited in 2019/06/15〕。