基於雲端環境設計可提升國軍決策參考之機制研究

蘇品長　潘詩婷*

國防大學資訊管理學系

摘要

現今數位化時代，網路服務發展快速，人們利用雲端環境可自由地發表個人意見及分享專業知識,或是利用以網路投票方式調查及統整結果,可輔助決策者準確掌握方向,作為決策的重要依據；然而就軍隊而言，領導者的決策方向是否正確，攸關了整個團隊的成敗，參謀可有效提供正確且具信服力的參考建議，成為引導決策之重要關鍵，反觀現今國軍有部分的領導者，卻仍有官大學問大的老舊思維，許多參謀因為官階壓力，不敢提出具體且專業的意見，導致決策品質不佳，進而影響整個部隊的發展及戰力；本研究將利用雲端運算環境、橢圓曲線密碼學、盲簽章等理論基礎，設計具足夠安全性之網路投票機制，使參謀可統計彙整各方專業意見，利用具體且客觀的數據資料，提供領導者之決策參考，以期能提升國軍決策品質。

關鍵詞〈3-5 個〉：雲端環境、橢圓曲線，多重文件盲簽章，電子投票

國防相關應用：本研究可應用在對軍中相關制度意見表決，或對某些裝備的可用性、適用性及維修之調查，並提供領導者下達各項重要決策之依據。

通訊作者：t102292000@gmail.com，電話 605578，0912811955，桃園市八德區建德路 80 號 5 樓

Design a Mechanism To Promote Military Decision Reference under the Cloud Computing Environment

Su, Pin-Chang **Pan, Shih-Ting** *

Department of Information Management, National Defense University.

Abstract

In the digital age, Internet services are developing rapidly. People can freely express their personal opinions and share professional knowledge using the cloud environment, or use online voting to investigate and aggregate the results, which can help decision makers accurately grasp the direction and make decisions .In the military , whether the leader's decision-making direction is correct is critical to the success or failure of the entire team. The staff can effectively provide correct and convincing reference suggestions, which becomes an important key to guide decision-making; On the other hand, there are some leaders in the national army, but they still have the old thinking of being inquisitive. Many staff officers are afraid to put forward specific and professional opinions due to the pressure of the ranks. This results in poor decision-making quality and affects the development of the entire army.This research will use the theoretical basis of cloud computing environment, elliptic curve cryptography, blind signatures, etc., to design a sufficiently secure online voting mechanism, so that the staff can collect the professional opinions of all parties and use specific and objective data to provide The decision-making reference of the leader in order to improve the quality of the decision-making of the national army.

Keywords: cloud computing,elliptic curves, multiple file blind signature, electronic voting

Relevance to National Defense: This research can be used to vote on relevant military systems, or to investigate the availability, applicability and maintenance of certain equipment, and provide a basis for leaders to make important decisions.

一、前言

美國社會學家戴伊言：「正確的決策來自眾人的智慧」，在現代民主社會國家，生活中充斥著許多不同的意見和聲音，來自大眾的意見與聲音，往往也是許多領導者可以藉以參考及輔助決策的依據，而正確的決策方可帶領團體走向成功的道路，國內證券企業曾發表借專家意見提升董事會決策品質(宋佩璇，2020)，企業管理中董事並非全才，需視需求諮詢法律、財務、會計及產業等各領域專家意見，以提升其決策專業及品質；然而以團體為主的軍隊，領導幹部更是左右軍隊的靈魂角色，各主官幾乎每日都會遇到大大小小的決策，小至修正生活規定或大至戰爭時指揮部隊往正確方向進攻等，但領導幹部亦不是全才，依據我國陸軍指參作業程序之定義為指揮官藉參謀人員之協助，共同發揮思維力、判斷力與軍事素養，集思廣益，將其政策、決心透過分工作業方式，轉化為具體行動的一個過程，藉由專業的參謀及部屬，提供相關意見綜合判斷及考量後，引導領導者下達決策命令，我國海軍亦曾研究統計我國中階軍官決策風格對其決策行為之影響(陳明正與吳家純，2015)，該研究中在個人變項敘述統計分析數據顯示決策模式有 62.3%為召集幕僚個人決策，19.9%則以幕僚意見為主，因此多數領導軍官均會參考幕僚相關意見後，再行決策行為，但仍有部分的領導者，有官大學問大的老舊思維，亦或是有許多參謀因為官階，不敢提出具體且專業的意見，導致決策品質不佳，進而影響整個部隊的發展及戰力。

在現今網路雲端發展快速，人們之間的距離不再只是侷限在實體的距離，許多年輕人會利用社群軟體交流，討論表決一些需要群體決定或提供之意見，甚至統計出來的意見可以利用雲端上的資源，實施數據分析及整理，公共管理的學者提出資訊技術對政府的決策品質的影響研究(劉勇與徐曉林，2006)，研究中指出資訊技術可以改善決策者的有限理性，提升政府決策的質量並增強決策過程的公開性及公眾參與性，資訊技術與網路技術可改變傳統的訊息傳遞模式，透過網路技術可將公眾訊息傳遞至決策層，消除資訊傳遞與決策層間的人為阻滯和時空限制，有效避免資訊傳遞失真及延遲帶來的決策失誤；於國軍近年來也陸續將雲端的環境概念帶入軍中，許多軍隊的公事也都漸漸利用網路提高作業的時效，因此在不違反國軍決策體系之階層關係為前提下，各專業參謀如果利用雲端環境讓團體中的成員，透過電子投票的方式表達專業意見，再藉由雲端的資源收集、整理或分析更科學理性的數據及意見，可打破僅單一單位的時空限制，針對特定專業領域範圍之參考意見彙整，提供主官可以更清楚有效的參考依據找到決策的方向。

然而利用電子投票方式雖可解決資訊傳遞的人為阻礙、時空限制及傳遞時間等問題，但網路投票存在許多安全性問題，包含如何確保投票者的身分隱私，破除身分的成見使投票者可無後顧之憂表達自身意見，以及防止有心人士破壞或干擾投票過程，甚至竄改結果等，若能設計出安全性高的網路投票機制，對於國軍的各項事務推動與決策品質，相信會有更多的改善及發揮專業參謀更大的效益；另本研究亦可應用於群體決策或企業、董事會決議投票等時機實施，協助企業公司統整表決方針，爭取團體最大利益。

本研究將利用雲端運算、橢圓曲線密碼學、盲簽章等理論基礎，設計具足夠安全性與實用性之網路投票機制，具備以下優點：

(1)設計藉由網路身分認證與投票機制，讓各專業參謀可以利用電腦網路實施投票。

(2)將橢圓曲線密碼學理論應用在電子投票系統，利用較短位元長度的金鑰可達到與 RSA 相同等級的安全強度，降低系統負荷；另藉由多文件一次盲簽章理論，提升電子投票系統效率，縮短多餘流程；兩者使電子投票系統更具實用性，有助降低紙本與人力花費及系統運作開銷。

(3)利用橢圓曲線密碼學理論與盲簽章技術達到機密性、完整性、鑑別性及不可否認性等資安特性，強化電子投票安全度。

二、文獻探討

本章節分類整理、歸納分析與本研究相關聯之文獻，並針對電子投票及密碼學等與本研究有關的技術，加以彙整作為本研究的基礎。分述如後：

2.1 電子投票機制介紹

電子投票，顧名思義即是利用電子設備完成投票動作，也就是不透過紙本方式實施，電子投票依投票之電子設備形式不同又可分為兩類(羅子惟，2012)，一類是 Electronic-voting (E-voting)，俗稱資訊亭投票，一類是 Internet-voting (I-voting)，俗稱網路投票：

2.1.1 資訊亭投票(E-voting)

凡是以電子投票機進行投票行為者均為此類投票，此類投票，投票日前會要求投票人事先登記要在哪個投票所實施投票，投票當天投票人不須攜帶身分證、印章及選舉通知單等東西，只須親赴投票所。投票人主要透過電子投票機輸入相關身分帳號與密碼，由系統核對身分，在確認沒有重覆投票後，即出現選票畫面，投票人則以按鍵或觸控的方式操作電子投票機進行圈選，完成後，電子選票即直接燒錄在光碟，最後送至開票中心利用電腦進行計票。此類投票方式為針對較正式之人員選拔，且需付出較高之成本購買設備，對本研究僅針對決策參考機制提升不適用。

2.1.2 網路投票(I-voting)

此類投票與 E-voting 最大差異就是所有資訊傳輸都是透過網路來完成，投票日前要求投票人事先上網向選務中心註冊登記要實施網路投票，投票當天投票人不須攜帶身分證、印章及選舉通知單等東西，也不須親赴投票所，只要利用桌上型或筆記型電腦、平板電腦、手機等資訊設備，透過網路連上投票系統，輸入相關身分帳號與密碼，由系統核對身分，在確認沒有重覆投票後，一樣出現選票畫面，投票人亦以按鍵或觸控的方式操作電腦、平版或手機等設備進行圈選，完成後，電子選票即直接加密傳輸到開票中心，俟投票時間結束後開票中心利用電腦統一計票。由於投票人不需至投票所即可完成投票過程，以軍人為例，即可在營區利用有連接網際網路之電腦等相關設備完成投票。

由於此類投票須透過網路傳輸所有資訊，故有保密之安全顧慮，如該投票人的投票內容不能被知曉，投票內容不能被竄改等。為達成這些基本要求，愛沙尼亞行之有年的郵寄投票流程(GQ 網，2012)，即可實現，其流程如下：

(1)投票人須事先向選務中心註冊身分，合格選民會在投票日之前預先收到選票與兩個信封。
(2)投票人只須將填好的選票密封進其中一個信封，上面不寫任何個人資料，然後將此裝有選票的信封，再裝入另一個標有合法身分的信封並寄給投票所。
(3)投票所收到後，於投票當天驗證外層信封上的身分資料，核實身分無誤並登錄已投票後，即將外層信封拆開，把內層信封投入票櫃。

此流程後來被該國用以設計網路投票安全機制，投票人事先用電腦下載由選舉委員會提供的軟體，該軟體可將選票的電子檔編碼加密，其作用就如同郵寄投票的內信封，然後再附上選舉委員會提供的電子簽章在該加密檔上，以利確認身分，其作用就有如外信封。近年有相關學者研究基於 SEAL 庫的同態加權電子投票系統(楊亞濤，2020)、基於區塊鏈的可追踪匿名電子投票方案(孫萌，2019)及基於區塊鏈技術的匿名電子投票協議設計(周振與嚴廣樂，2020)，即以密碼學等技術，實現電子投票最基本安全性條件，以電子檔加密及電子簽章等方式強化安全性，惟該研究未針對軍中規範及環境設計，故本研究將相

關辦法設計於適用軍中環境用以輔助領導者提升決策參考之機制。此外，本研究設計除適用於軍中環境外，亦可將此研究機制導入企業或政府團體等決策所需，2020 年學者提出 Say-on-Pay 投票頻率對經理人獎酬之影響(呂明諺，2020)，可體現企業管理人亦頻繁使用投票方式，用以收整員工或是經理人之意見，進而影響獎酬等方案政策之修正，由此可見一個安全且實用的網路投票機制之重要性。

2.2 電子投票相關研究

本節主要描述 Song 和 Cui、陳淵順及周振與嚴廣樂等學者所提出之網路電子投票相關研究。

2.2.1 Song 和 Cui 電子投票機制

由 Song, F. and Cui, Z.(2012)提出，為一個利用 RSA 及 ElGamal 盲簽章建構之電子投票機制，其中 ElGaml 是由 ElGamal, T. (1985)提出，其為基於解決離散對數的難題。F. Song and Z. Cui 提出的電子投票機制主要由產生金鑰、確認身分、將票盲化、投票、計票等五個階段構成，其研究方法主要是利用 RSA 來產生金鑰，並利用 ElGamal 盲簽章機制來進行選票盲化，投票與計票則是運用 XML 文件檔傳送來完成。

(1)產生金鑰

利用 RSA 機制產生投票者的公、私鑰。

(2)確認身分

投票者向選務中心具有申請投票資格的簽章，選務中心確認人員身分後，發給投票者的公開金鑰及選務中心簽署的數位簽章。

(3)盲化選票

選務中心將票盲化後，製作成 XML 檔傳給投票者。

(4)投票

投票者將公鑰及投票內容利用 XML 檔傳回選務中心。

(5)計票

選務中心驗證選票的有效性、簽章以及是否被竄改，若皆符合，則計入票數。

2.2.2 陳淵順的電子投票機制

由陳淵順(2011)提出，為一個利用離散對數難題身分認證方法(Schnorr, C. P., 1991)及有效率的模糊簽章機制(Tso, R. et al., 2008)建構之電子投票機制，其中利用模糊簽章取代盲簽章之目的，主要是為了讓選務中心確保所簽的選票中，投票人圈選結果一定是所有候選人的其中一位(但無法得知其到底圈選哪一位)，而利用盲簽章應用於電子投票時，簽章者無法得知簽章內容為何而進行簽章，會有不確定感。各階段要點如下：

(1)準備階段

投票者至政府機構申請可證明身分之 ID-card，政府機構透過憑證中心利用離散對數難題身分認證方法製作 ID-card，內含投票者的 ID 與公、私鑰。

(2)註冊登入階段

投票者利用 ID-card 登入投票系統，投票系統確認身分正確後，傳送身分證明給投票者。

(3)驗證階段

投票者選擇候選人後，透過投票系統將身分證明及候選人名單傳給憑證中心，憑證中心驗證投票者的身分證明無誤後，對投票者所選的候選人名單做模糊簽章，並傳回給投票者。

(4)投票階段

投票者將選票利用開票中心的公鑰加密，並透過投票系統將加密選票傳送給開票中心儲存。

(5)計票階段

開票中心待全部投票結束後，將所有選票解開，並驗證憑證中心的模糊簽章，計算票數並公布結果。

(6)爭議驗證階段

開票完成後，投票人可比對選票是否有被計票，若有疑慮即向選務中心要求驗票。

2.2.3 周振與嚴廣樂提出之基於區塊鏈技術的匿名電子投票協議設計

由周振與嚴廣樂（2020）提出，其結構是使用盲簽章及時間釋放加密演算法，結合運行在以太坊上的智能合約完成電子投票的過程，智能合約將取代傳統可信第三方的工作，擺脫信任依賴，保証投票過程的完整性與安全性。流程圖如圖 1。

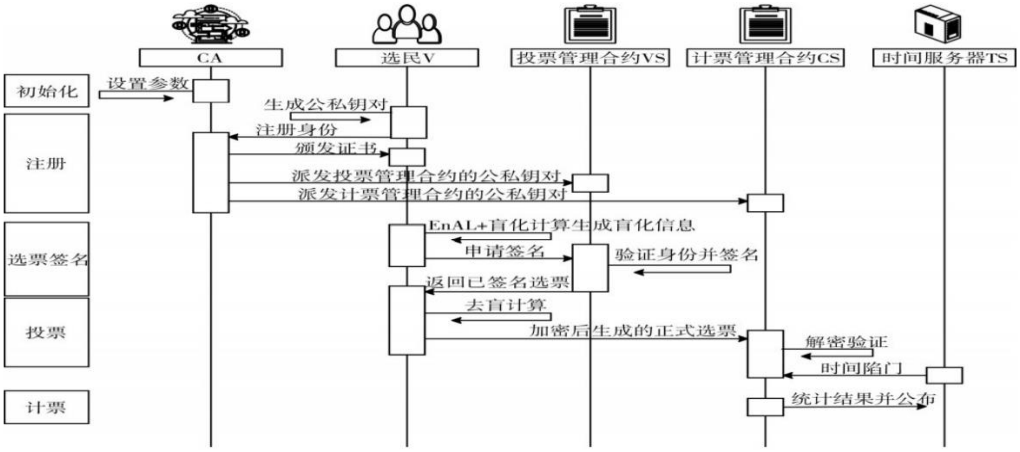

圖 1 周振與嚴廣樂提出的區塊鏈電子投票流程

2.3 密碼學理論

將進一步說明本研究將應用之密碼學理論。

2.3.1 對稱式密碼系統

對稱式密碼系統亦稱為私密金鑰密碼系統，主要將傳送方的明文利用金鑰加密處理後變成密文，接收方收到密文後經過解密處理還原成原來的明文，因為其加、解密為同一把金鑰，如何安全的把金鑰分配給通訊對方即是重要問題，且若傳遞訊息的人數增多，管理的金鑰也會變多，n 個人傳遞訊息就需要 $n(n-1)/2$ 把密鑰(梁榮哲，2012)，管理十分不易。但其優點是加、解密之運算速度快，仍有實用價值，目前常用的對稱式加密技術有 DES、3DES、AES、Blowfish、IDEA、RC5、RC6 等。

2.3.2 非對稱式密碼系統

非對稱式密碼系統又稱為公開金鑰密碼系統(Diffie, W., and Hellman, M., 1976)，主要使用兩把相對應的金鑰進行加解密，一把是可以公開的加密金鑰 (Public Key)，一把為私人擁有的解密金鑰(Private Key)。在此系統中，接收者可將加密金鑰公開，提供給所有可能與其通信的傳送者，當傳送者要將訊息傳送給接收者時，可將訊息利用接收者的加密金鑰進行加密，再傳給接收者。該加密訊息只有該接收者相對應的解密金鑰才能解密，故此系統可讓通信雙方不需事先交換金鑰即可從事秘密通訊，此加密技術可解決「對稱式加密技術」中金鑰分配與管理問題，並可達到「不可否認性」需求，但具有加、解密運算速度較慢之缺點(梁榮哲，2012)。目前較著名的非對稱式密碼系統為 RSA 公開金鑰密碼系統，

該系統由美國麻省理工學院的 Rivest、Shamir 與 Adleman 等三人於 1978 年提出，該密碼系統迄今仍是世界公認安全且仍在大量運用之非對稱式密碼系統，惟隨電腦計算能力提升，其安全強度須靠加長金鑰長度，來抵抗暴力破解法(郭文雄，2011)。故學者們希望找出以較小密碼長度就能達到相同安全性之密碼系統，橢圓曲線密碼系統即為最有希望替代方案之一(陳文彬，2012)，並已被制定為 ANSI X9.62(American Bankers Association., 1998)、FIPS PUB 186-3 (Gallagher, P., and Director, C. F., 2009)、IEEE Std 1363-2000 (Jablon, D, 2001)等多個國際或國家標準。另非對稱密碼系統還常被應用在電子簽章，主因簽章者用自己的私鑰簽章，只有相關應的公鑰能解開，故只要簽章被解開，就表示該簽章是由擁有相對應私鑰的人所簽署的。以下將針對橢圓曲線密碼系統及電子簽章進行介紹。

2.3.3 橢圓曲線密碼系統

橢圓曲線在代數學和幾何學上有超過百年的廣泛研究，其理論非常豐富且深奧(高嘉言，2009)，橢圓曲線首次應用在密碼學上是由 Miller (1985)及 Koblitz(1987)兩位學者分別提出，主要是利用橢圓曲線可以找出反元素的特性，將其運用在公開金鑰加密系統上。

依照密碼學加密演算法之橢圓曲線密碼，其橢圓曲線一般方程式為：$y^2 + axy + by = x^3 + cx^2 + dx + e$，其中 a、b、c、d、e 為實數。通常以$y^2 = x^3 + ax + b$來表示，在密碼學應用上，則主要關心在有限域 $GF(q)$中取質數 p (p>3)同餘的橢圓曲線群，以$E: y^2 = x^3 + ax + b \ (mod\ p)$來表示，其中 a、b 為小於 p 之正整數，且$4a^3 + 27b^2 \neq 0 \ (mod\ p)$。另在橢圓曲線的定義中存在一個元素 O，稱為無窮遠點或零點，一般可視為在 Y 軸上方無窮遠處 (Darrel .et.al，2004) 。令$P(x_1, y_1)$與$Q(x_2, y_2)$為 E 上的點，其具有以下規則：

(1)$P + O = O + P = P$。

(2)若$P = -Q$，則$P + Q = (x_1, y_1) + (x_1, -y_1) = O$。

(3)若$P \neq -Q$，則$P + Q = (x_3, y_3)$，且$x_3 = (\lambda^2 - x_1 - x_2)$，$y_3 = \lambda(x_1 - x_3) - y_3$，此處

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } A \neq B \\ \dfrac{3x^2 + a}{2y_1} & \text{if } A = B \end{cases}$$

註：橢圓曲線運算中，大寫參數表示點，小寫參數表示數值。

(4)橢圓曲線中的乘法運算是透過加法運算達成的。為了加快速度，可以用 doubling 運算來進行。例如：$4P = 2P + 2P$，再計算$2P = P + P$即可。

(5)反元素運算

點$A = (x, y)$的反元素為$-A = -(x, y) = (x, -y)$。(因$A + (-A) = O$，O 為乘法單位元素)

(6)橢圓曲線優點

橢圓曲線密碼系統第一個優點是加密金鑰長度較短，如表 1(蘇品長，2007)，與 RSA 相比，橢圓曲線密碼系統在 224 位元金鑰長度的安全性與 RSA 的 2048 位元金鑰長度相當，在相同金鑰長度下，橢圓曲線密碼系統的安全性較 RSA 高。

表 1 橢圓曲線密碼系統與 RSA 在相同安全度下金鑰長度之比較表

橢圓曲線密碼系統與 RSA 金鑰長度在相同安全度下之比較					
項目 ＼ 長度	金鑰長度				
橢圓曲線密碼系統	112	163	224	256	384
RSA	512	1024	2048	3072	7680
金鑰長度比	1：5	1：6	1：9	1：12	1：20

橢圓曲線密碼系統第二個優點是：假設一屬於F_q之橢圓曲線，而橢圓曲線 E 上一點為 P，給定一個橢圓曲線 E 上的點Q，假設要找到一個整數 k 使得$kP = Q$，因橢圓曲線的點加法運算，必須逐一窮舉所有可能的點才有可能遭破密。此問題至今尚無法於多項式時間內求得解答。

2.3.4 電子簽章

電子簽章最主要的功能就是確認文件傳送的過程中，內容沒有被第三人破壞或竄改(林明慶，2009)，其原理類似公開金鑰密碼系統，惟不同點是發送者利用私鑰簽章，接收者利用發送者相對應的公鑰驗證；其原理主要是發送者利用單向雜湊函數對訊息運算，獲得訊息摘要，並利用私鑰對訊息摘要進行加密認證，產生簽章，發送者將訊息及簽章傳給接收方；接收方收到後，將訊息透過單向雜湊函數產生另一個訊息摘要，並利用發送者相對應的公鑰對簽章解密取得原本的訊息摘要，比對兩個訊息摘要若相同，則確保收到的訊息是完整的，未經竄改。

此過程中，利用單向雜湊函數運算之目的，主要是因為一般傳送的文件內容都很龐大，公開金鑰長度若要大於文件內容，則加解密運算將無法負荷，故先將訊息透過單向雜湊函數轉換成固定長度之小塊訊息後再進行運算，可提升簽章效率(徐凡，2006)。本研究將用到盲簽章及基於橢圓曲線密碼系統之多重文件盲簽章技術。

2.3.4.1 盲簽章

盲簽章是由 Chaum(1983)所提出的一種電子簽章，在盲簽章協定中主要有使用者、簽章者及驗證者三個角色，使用者將要簽章的訊息利用盲因子(亂數)盲化後，傳給簽章者利用私鑰進行簽名，由於簽章者收到的是盲化過的訊息，故無法得知訊息內容，僅盲目的進行簽名動作，然後將盲簽章傳給使用者。使用者收到後從中取出真正的簽章。而驗證者可利用簽章者的公鑰驗證簽章的正確性。使簽章者無法得知投票者是將票投給哪位候選人，以達到秘密投票的特性。Chaum 的演算法區分 5 個階段：

(1) 簽章者隨機選取兩個大質數 p、q，計算

$$n = p \cdot q \text{及} \emptyset(n) = (p-1)(q-1) \tag{2-1}$$

簽章者另選取兩個很大的數 e、d，使得

$$ed \equiv 1 \ \left(mod \emptyset(n)\right) \text{及} \gcd\left(e, \emptyset(n)\right) = 1 \tag{2-2}$$

則 e、n 作為簽章者的公鑰，d 為私鑰。然後公開 e、n，留著 p、q、d。

(2) 若使用者希望簽章者對訊息 m 進行簽章，則隨機選取一個亂數 r 當作盲因子，將訊息 m 盲化成

$$m' = r^e \cdot m \ \ (mod \ \ n) \tag{2-3}$$

並將m'傳給簽章者。

(3) 簽章者收到訊息m'後，用其私鑰 d 計算

$$s' = m'^d \ \ (mod \ \ n) \tag{2-4}$$

然後將s'回傳給使用者。

(4) 使用者收到s'後，計算

$$s = s' \cdot r^{-1} \ \ (mod \ \ n) \tag{2-5}$$

(5) s 即為 m 的盲簽章，任何人可以用簽章者的公鑰 e 檢查

$$s^e \equiv m \ \ (mod \ \ n) \tag{2-6}$$

是否成立，來驗證此簽章正確性。

2.3.4.2 基於橢圓曲線密碼系統之多重文件盲簽章

由梁榮哲(2012)提出，透過運用橢圓曲線密碼系統金鑰長度短特點，設計基於可以一次多重盲簽章之演算法，系統處理速度較快，演算法如下：

(1)開始階段

- 系統首先選取一條在有限域F_q上之安全的橢圓曲線$E(F_q)$，並在$E(F_q)$上選一基點 G 其階數(order)為 n，使得$n \cdot G = O$(無窮遠點)。
- 從$y^2 = x^3 + ax + b \ (mod \ p)$及$4a^3 + 27b^2 \neq 0 \ (mod \ p)$建立$E_p(a,b)$，$p$ 為一個 160bit 以上的大質數，選一個 order 極大的 n 基點$G = (x,y)$在$E_p(a,b)$上$n \cdot G = O$，送簽者$\{R_i | 1 \leq i \leq n, n \in N\}$。
- 送簽者選擇私鑰$n_i \in Z_n^*$；產生公鑰$P_i \equiv n_i \cdot G \ (mod \ p)$。
- 簽章者隨機選擇私鑰$n_s \in Z_n^*$；產生公鑰$P_s \equiv n_s \cdot G \ (mod \ p)$。

(2)盲化階段

- 訊息分成數個區塊且定義$m_{ij} = m_{11}, m_{12}, \cdots, m_{n1}, m_{n2}$，$1 \leq i \leq n$，其中每份文件各切割為兩塊，並雜湊明文$m_{ij}$，以明文轉點的方式將明文轉為點座標。

$$\overline{m_{ij}} = \{m_{11}, m_{12}, \cdots, m_{n1}, m_{n2}\} \quad (2\text{-}7)$$

$$h_1(\overline{m_{ij}}) = m \quad (2\text{-}8)$$

$$f_{m2p}(m) = P_1, P_2, \cdots, P_n \quad (2\text{-}9)$$

$$\overline{P_i} = \{P_1, P_2, \cdots, P_n\} \quad (2\text{-}10)$$

$$h_2(\overline{P_i}) = M \quad (2\text{-}11)$$

- 接著送簽者選擇一個盲因子 b 將多個訊息盲化，計算

$$m' = b \square M \square n_i \quad (2\text{-}12)$$

之後將m'傳給簽章者。

(3)簽章階段

簽章者收到m'後，利用自己的n_s(*私鑰*)對盲化訊息m'簽章，再用私鑰n_s加密於送簽者公鑰 P_i，計算

$$s_{m'} = m' \cdot n_s \quad (2\text{-}13)$$

$$s_s = n_s \cdot P_i \quad (2\text{-}14)$$

將$s_{m'}$與s_s傳送給送簽者。

(4)解盲階段

送簽者用盲因子與自己私鑰n_i解盲，計算

$$s_m = b^{-1} \cdot {n_i}^{-1} \cdot s_{m'} \quad (2\text{-}15)$$

(5)驗證階段

將簽章者送來之s_s進行驗證簽章值是否正確，計算

$$s_s = s_m \cdot P_i \cdot M^{-1} \quad (2\text{-}16)$$

是否成立，若成立，則將$\overline{m_i'}$所得到的多重訊息集合實施一次雜湊

$$h_2(\overline{m_i'}) = m' \quad (2\text{-}17)$$

驗證：

$$m' \square m \quad (2\text{-}18)$$

三、系統設計

本研究提出一種利用雲端環境於軍中建置安全電子投票機制，結合梁榮哲(2012)所提之基於橢圓曲線多重文件盲簽章原理的優點，將投票文件加密後實施盲簽章來強化其安全性，透過多份投票文件內容一次盲簽密機制，可縮短系統重覆簽章之程序，提升執行效率，並可使各承辦參謀在簽署過程中，不知道投票內容為何，以確保投票者身分隱蔽及投票內容不被偷窺，使各階層人員可不受身分階級影響投票意願及結果，以下將說明本研究所提出之電子投票系統架構及其運作流程。

3.1 系統架構

系統整體運作架構如圖 2 所示，投票人 A 向保防部門 D 註冊，取得公私鑰和簽章，與承辦單位 C 確認身分，將多張選票進行一次加密，選票密文除直接傳給承辦單位 C，另並產生一份密文摘要，盲化後傳給監察部門 B 做簽章；監察部門 B 對盲化密文摘要簽章，傳給承辦單位 C，由承辦單位 C 進行最後的解盲化、驗證與解密開票。

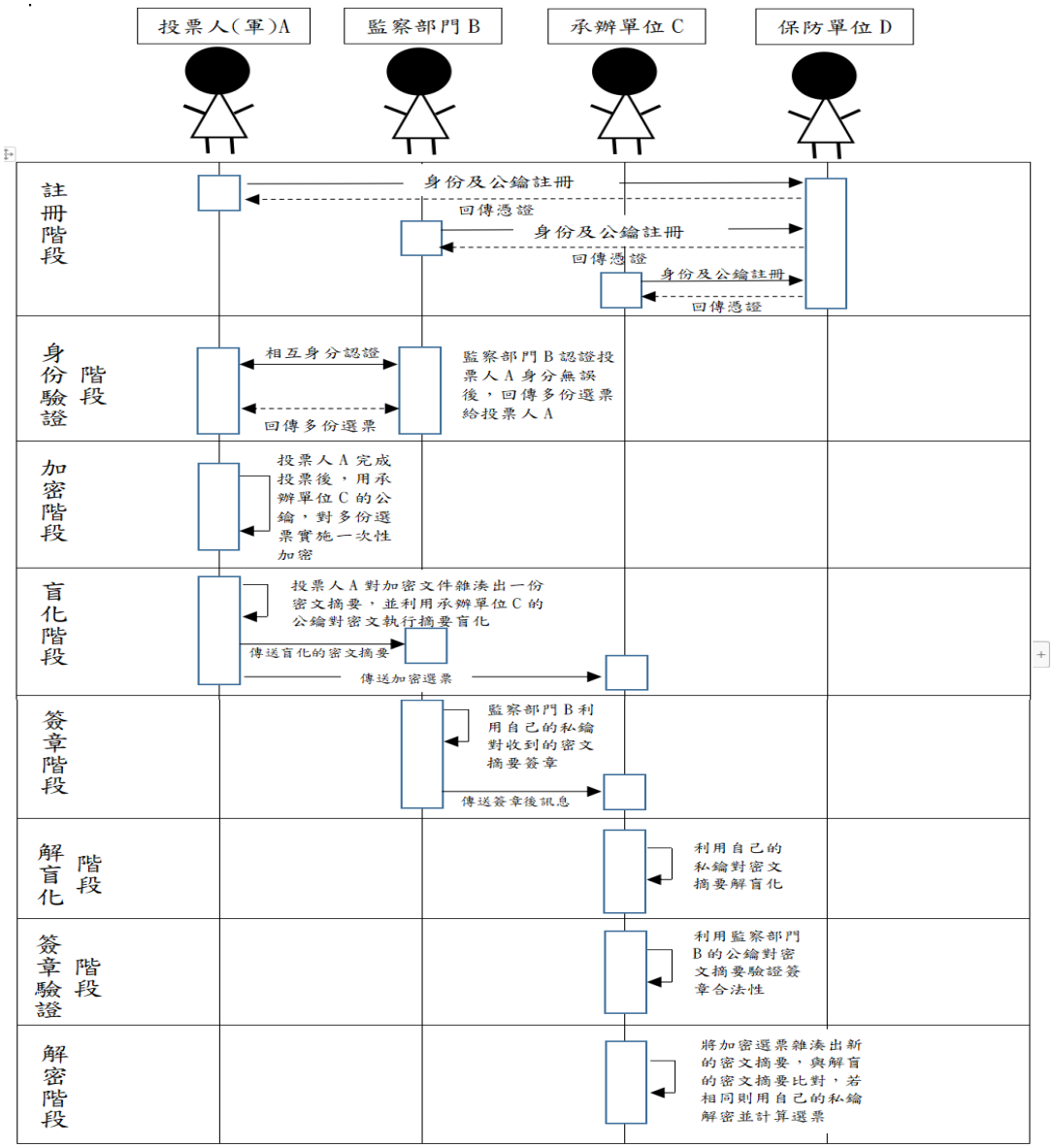

圖 2 系統整體運作架構圖

3.2 系統運作流程及演算法

系統運作流程區分系統初始、身分驗證、加密、盲化、簽章、解盲化、簽章驗證、解密等八階段，各階段說明如下。

3.2.1 系統初始階段

系統初始時會針對密碼系統進行參數選定，本研究中各參數說明如表 2 所示。

表 2 系統各參數說明

項目	符號	說明
1	G	為橢圓曲線內之基點
2	$E(F_q)$	有限域F_q中之橢圓曲線
3	n	橢圓曲線上基點的階數(order)
4	q	$q > 2^{160}$的大質數
5	id_A、id_B、id_C	投票人 A、監察部門 B、承辦單位 C 的 ID 資訊
6	PK_A、PK_B、PK_C、PK_{AS}	投票人 A、監察部門 B、承辦單位 C、保防部門 D 之公鑰
7	n_A、n_B、n_C、n_{AS}	投票人 A、監察部門 B、承辦單位 C、保防部門 D 之私鑰
8	e_A、e_B、e_C	投票人 A、監察部門 B、承辦單位 C 之公鑰與 ID 資訊的關聯值
9	l_A、l_B、l_C	憑證中心為投票人 A、監察部門 B、承辦單位 C 計算關聯值時所隨機選取的值
10	ca_A、ca_B、ca_C	投票人 A、監察部門 B、承辦單位 C 之憑證
11	$h_1(\ )$	值轉值的雜湊函數
12	$h_2(\ )$	點序列轉值的雜湊函數
13	$f_{mp(\ )}$	將訊息 m 轉化為橢圓曲線點 p 的函數
14	$f_{pm(\ )}$	將橢圓曲線點 p 轉化為訊息 m 的函數
15	w	選票訊息之 0、1 背包值
16	b	盲因子
17	m	選票訊息
18	m_{ij}	選票訊息之分解區塊
19	M	將選票訊息雜湊函數後的值

系統選取一條安全的橢圓曲線$E(F_q)$（在有限域F_q上且q>160bit以上之大質數)，並且在$E(F_q)$上選一基點G其階數(order)為n，使

$$n \boxdot G = O \tag{3-1}$$

此橢圓曲線之無窮遠點(O)；另選擇兩個為單向且無碰撞的雜湊函數$h_1(\ )$及$h_2(\ )$。

投票人A、監察部門B、承辦單位C、保防部門D分別選擇n_A、n_B、n_C、n_{AS} (n_A、n_B、n_C

、$n_{AS} \in Z_n^*$且$\in [2, n-2]$)作為私鑰，則公鑰

$$PK_A = n_A \cdot G \tag{3-2}$$

$$PK_B = n_B \cdot G \tag{3-3}$$

$$PK_C = n_C \cdot G \tag{3-4}$$

$$PK_{AS} = n_{AS} \cdot G \tag{3-5}$$

投票人A、監察部門B、承辦單位C利用一個絕對安全的通道將自己的公鑰及身分id_A、id_B、id_C送至保防部門D計算出關聯值

$$e_A = h_1(id_A, PK_A) \tag{3-6}$$

$$e_B = h_1(id_B, PK_B) \tag{3-7}$$

$$e_C = h_1(id_C, PK_C) \tag{3-8}$$

保防部門D為投票人A、監察部門B、承辦單位C分別選擇l_A、l_B、l_C(l_A、l_B、$l_C \in Z_n^*$且$\in [2, n-2]$)，使

$$Z_A = l_A \cdot G = \left(x_{Z_A}, y_{Z_A}\right) \tag{3-9}$$

$$Z_B = l_B \cdot G = \left(x_{Z_B}, y_{Z_B}\right) \tag{3-10}$$

$$Z_A = l_A \cdot G = \left(x_{Z_C}, y_{Z_C}\right) \tag{3-11}$$

產生憑證

$$ca_A = l_A\left(e_A + \left(x_{Z_A}, y_{Z_A}\right)\right) \tag{3-12}$$

$$ca_B = l_B\left(e_B + \left(x_{Z_B}, y_{Z_B}\right)\right) \tag{3-13}$$

$$ca_C = l_C\left(e_C + \left(x_{Z_C}, y_{Z_C}\right)\right) \tag{3-14}$$

保防部門D分別將(ca_A、e_A、Z_A)，(ca_B、e_B、Z_B)，(ca_C、e_C、Z_C)傳回投票人A、監察部門B、承辦單位C，最後公開$E\left(F_q\right)$、G、q、PK_A、PK_B、PK_C、PK_{AS}、$h_1(\ )$及$h_2(\ )$。

3.2.2 身分驗證階段

當監察部門B收到投票人A傳過來的(ca_A、e_A、Z_A)之後，先行驗證身分，計算如下：

$$u_1 = {ca_A}^{-1} \ mod \ n \tag{3-15}$$

$$u_2 = e_A \cdot u_1 \ mod \ n \tag{3-16}$$

$$u_3 = x_{Z_A} \cdot u_1 \ mod \ n \tag{3-17}$$

接著以保防部門D的公開金鑰PK_{AS}來驗證投票人A身分之正確性，計算：

$$u_2 \cdot \mathrm{G} + u_3 \cdot PK_{AS} = \left(v_x, v_y\right) \tag{3-18}$$

驗證：

$$\mathrm{x}_{Z_A} \stackrel{?}{=} \mathrm{v}_x \tag{3-19}$$

同理，投票人A也驗證監察部門B的身分：

$$x_{Z_B} \stackrel{?}{=} v_x \tag{3-20}$$

雙方驗證無誤後，監察部門B將n份選票傳給投票人A。

3.2.3 加密階段

投票人A收到選票並勾選後，將多份投票文件內容的明文，區分成多個區塊且定義

$$m_{ij} = m_{11},m_{12},\ldots,m_{n1},m_{n2}，1 \le i \le n \tag{3-21}$$

其中每份文件各切割為兩塊，並雜湊明文m_{ij}，以將明文轉換為點座標，其計算如下：

$$\overline{m_{ij}} = \{m_{11},m_{12},\ldots,m_{n1},m_{n2}\} \tag{3-22}$$

$$h_2\left(\overline{m_{ij}}\right) = m \tag{3-23}$$

$$f_{mp}(m) = p_1, p_2, \ldots, p_n \tag{3-24}$$

定義：

$$\bar{x} = \{x_1, x_2, \ldots, x_i\} \in (0,1) \tag{3-25}$$

其中對應1及右邊對應0，代表右移一個區塊，對應0及右邊對應1，代表左移一個區塊，對應1及右邊對應1，則右移三個區塊，對應0及右邊對應0，則左移三個區塊：

$$\text{if } x_i = 1；x_{i+1} = 0 \gg 1 \tag{3-26}$$

$$x_i = 0；x_{i+1} = 1 \ll 1 \tag{3-27}$$

$$\text{if } x_i = 1；x_{i+1} = 1 \gg 3 \tag{3-28}$$

$$x_i = 0；x_{i+1} = 0 \ll 3 \tag{3-29}$$

計算二進位值w：

$$\mathrm{w} = \{x_1 \otimes 2^{1-1}, x_2 \otimes 2^{2-2}, \ldots, x_n \otimes 2^{n-n}\} \tag{3-30}$$

隨選一個值$k \in Z_n^*$且$b \in [2, n-2]$，計算：

$$K = k \otimes G \tag{3-31}$$

利用承辦單位C的公鑰及隨選值k對實施密文加密計算：

$$C_0 = \left[f_{mp}(w, m) + k \otimes PK_C\right] \tag{3-32}$$

$$C_1 = [P_1 + x_1 \otimes C_0 + k \otimes PK_C] \tag{3-33}$$

$$C_2 = [P_2 + x_2 \otimes C_1 + k \otimes PK_C] \tag{3-34}$$

$$C_n = [P_n + x_n \otimes C_{n-1} + k \otimes PK_C] \tag{3-35}$$

$$\bar{C} = \{C_0, C_1, C_2, \ldots, C_n\} \tag{3-36}$$

密文$\bar{C}$利用$h_2(\ )$運算，產生M(密文摘要)：

$$h_2(\bar{C}) = M \tag{3-37}$$

3.2.4 盲化階段

投票人A利用承辦單位C的公鑰PK_C及隨選值k對密文摘要M進行盲化，計算：

$$X = \left[f_{mp}(k) + n_A \otimes PK_C\right] \tag{3-38}$$

$$Y = k \otimes M \otimes PK_C \tag{3-39}$$

運算後將密文$\bar{C}$及隨選值k、K及X傳給承辦單位C，盲化後密文摘要Y傳給監察部門B簽章

3.2.5 簽章階段

監察部門B收到投票人A傳來Y後，並利用自己的私鑰n_B對Y運算，產生簽章文件S：

$$S = n_B \otimes Y \tag{3-40}$$

隨後將簽章S傳給承辦單位C。

3.2.6 解盲化階段

承辦單位C收到投票人A傳來密文$\bar{C}$、k、K、X，以及監察部門B傳來的簽章文件S後，先對投票人A傳來之密文$\bar{C}$利用$h_2(\ )$做運算，產生第二份M'密文摘要，再用自己的私鑰n_C及投票人A的公鑰PK_A對簽章文件S解盲化，計算如下：

$$h_2(\bar{C}) = M' \tag{3-41}$$

$$f_{m2p}(k) = X - n_C \cdot PK_A \tag{3-42}$$

3.2.7 簽章認證階段

承辦單位C接著利用監察部門B的公鑰PK_B對S'進行簽章認證，計算如下：

$$k = f_{p2m}\left[f_{m2p}(k)\right] \tag{3-43}$$

$$S' = k \cdot M' \cdot n_C \cdot PK_B \tag{3-44}$$

承辦單位C比對S'及S：

$$S' \stackrel{?}{=} S \tag{3-45}$$

若S'與S相同，除表示未被竄改以外，也代表承辦單位C的簽章是有效的。

3.2.8 解密階段

承辦單位C以自身私鑰n_C及K對密文$\bar{C}$運算解密：

$$f_{mp}(w, m) = C_0 - n_C \cdot K \tag{3-46}$$

$$(w, m) = f_{pm}\left[f_{mp}(w, m)\right] \tag{3-47}$$

將w還原成$\bar{x}$數列，在二進位所表示的值中，對應0及右邊對應1，代表右移一個區塊，對應1及右邊對應0，代表左移一個區塊，對應0及右邊對應0，則右移三個區塊，對應1及右邊對應1，則左移三個區塊：

$$w = \{x_1 \cdot 2^{1-1}, x_2 \cdot 2^{2-2}, \dots, x_n \cdot 2^{n-n}\} \tag{3-48}$$

$$\text{if } x_i = 1\ ;\ x_{i+1} = 0 \ \ll 1 \tag{3-49}$$

$$x_i = 0\ ;\ x_{i+1} = 1 \ \gg 1 \tag{3-50}$$

$$\text{if } x_i = 1\ ;\ x_{i+1} = 1 \ll \ 3 \tag{3-51}$$

$$x_i = 0\ ;\ x_{i+1} = 0 \ \gg 3 \tag{3-52}$$

$$\bar{x} = \{x_1, x_2, \dots, x_n\} \tag{3-53}$$

依序解開密文$\bar{C}$：

$$P_1' = [C_1 - x_1 \cdot C_{1-1} - n_C \cdot K] \tag{3-54}$$

$$P_2' = [C_2 - x_2 \cdot C_{2-1} - n_C \cdot K] \tag{3-55}$$

$$P_i' = [C_i - x_i \cdot C_{i-1} - n_C \cdot K] \tag{3-56}$$

$$\bar{P}' = \{P_1', P_2', P_3', \dots, P_n'\} \tag{3-57}$$

$$f_{p2m}(\bar{P}') = \overline{m_{ij}}' \tag{3-58}$$

$\overline{m_{ij}}'$即為多重選票的集合，此時可利用$h_2(\ )$對$\overline{m_{ij}}'$再進行一次雜湊，取得m'：

$$h_2\left(\overline{m_{ij}}'\right) = m' \tag{3-59}$$

利用比對m與m'，便可以再次驗證選票內容的正確性，如果無誤則計入投票結果。

四、安全性及效益分析

4.1 安全性分析

以橢圓曲線密碼系統理論為基礎，結合多重文件盲簽章機制，達到安全分配金鑰、投票人身分保密及選票內容安全傳輸效果，本研究預期達到以下安全性：

4.1.1 機密性

機密性是指文件不可以被未經過授權之實體、個人或程序取得，亦或是遭揭露的特性，且文件在傳遞過程中，內容都是被保密的，不被傳送及接收雙方以外的人獲知內容之特性，在本研究中投票人A對選票訊息利用自己的私鑰n_A及承辦單位C的公鑰PK_C加密，如式(3-35)，$C_n = [P_n + x_n \cdot C_{n-1} + k \cdot PK_C]$，若第三方想要竊取加密資訊，因無法獲得其公鑰及私鑰，須面對的是以暴力破解方式解決橢圓曲線離散對數難題，因此本機制在實際安全上可確保選票機密性。

4.1.2 完整性

完整性是指確保文件完整且正確的特性，在傳遞時不被干擾或破壞，即內容不能被任意增減或修改。在本研究中，監察部門B簽章之密文摘要是由投票人A利用單向雜湊函數$h_2(\ )$雜湊出來的，如式(3-23)，$h_2(\overline{m_{ij}}) = m$，如果有第三方中途攔截投票人A發送的密文並且進行竄改或偽造發送給承辦單位C，因為單向雜湊函數具不可逆推特性，若密文被竄改，則簽章驗證時，其衍生出的密文摘要勢必無法相同，將不被通過，故若承辦單位C最後驗證通過，則可代表選票內容是正確且完整的(因為可以雜湊出相同的密文摘要)，本系統可以確保選票內容之完整性。

4.1.3 鑑別性

鑑別性是指接收方可利用公開的參數用以驗證合法的訊息來源，確保訊息是由宣稱的傳送方所傳來的。在本研究中，傳送方為投票人A，接收方為監察部門B，在身分驗證階段時，監察部門B可用式(3-18)、(3-19)，$u_2 \cdot G + u_3 \cdot PK_{AS} = (v_x, v_y)$、$x_{Z_A} \stackrel{?}{=} v_x$，來驗證投票人A的身分，如有第三人意圖偽冒身分，須面對的是以暴力破解方式解決橢圓曲線離散對數難題，故本機制在實際安全上可確保身分鑑別性。

4.1.4 隱匿性

隱匿性是指簽署人無法獲知其簽署的文件內容訊息，本研究中，透過生成密文摘要方式，讓監察部門B僅對密文摘要簽屬，無法直接得知選票內容，且利用盲簽章技術，使投票人A盲化其密文摘要，如式(3-38)、(3-39)，$X = [f_{mp}(k) + n_A \cdot PK_C]$、$Y = k \cdot M \cdot PK_C$，透過亂數$k$，不會生成固定的密文摘要，使監察部門B無法比對何種選票內容會生成何種密文摘要，投票人A不必擔憂在簽章過程中造成文件曝光。

4.1.5 不可否認性

不可否認性指的是在證明已發生的事件或行為，發生之後不可以被否認。由於投票人A的相關憑證只有投票人A擁有，其與監察部門B相互認證後領取選票，即無法否認其已

領票，以防重複領票，至於領票後是否要投票則是投票人A自由的權利，但已能確保投票人A只能投一次票；另在盲簽章方面，監察部門B簽署文件後，如式(3-40)，$S = n_B \bmod Y$，因其私鑰只有其擁有，承辦單位C可以用公式(3-44)，$S' = k \cdot M' \cdot n_C \cdot PK_B$，驗證其有效性，防止監察部門B否認簽章。

4.1.6 不可追蹤性

不可追蹤性是指選票內容不可被任何人知道是誰投的，本機制中，由於設計了密文摘要機制，讓監察部門B僅知道簽署的是選票密文摘要Y，如式(3-39)，$S = n_B \bmod Y$，無法知道投票人A投給誰；另承辦單位C解開選票是用他自己的私鑰n_C解開，如式(3-56)，$P_i' = [C_i - x_i \cdot C_{i-1} - n_C \bmod K]$，所以即使他最後得知選票內容，也與投票人A無關，可確保投票人A身分不被追蹤。

4.2 效益分析比較

將區分兩部分來進行效益比較，其一是現行決策制度與本研究設計機制之效益比較；其二是本研究與其他電子投票機制之效益比較。

4.2.1 現行軍中決策投票制度與本研究設計機制之效益比較

表3係針對現行軍中傳統投票決策制度與本研究設計之利用雲端環境於軍中建置安全電子投票機制進行各項效益比較，可發現本機制在便利性、實用性均占優勢，在安全性的完整性上亦可避免人工開票出錯情況。

表3軍中傳統投票決策制度與本研究設計機制之效益比較表

比較項目		軍中傳統投票決策制度	本研究設計機制
便利性		承辦單位需透過各單位幹部調查統計所屬意見，並統整討論後編訂建議方案。	利用雲端環境，設計出網路電子投票機制，各單位投票人可利用個人電腦實施投票，具便利性，有助提升投票率。
實用性	時間	承辦單位須將相關議題製作投票單後，發放單位調查後，需耗時發放及收整時間。	操作網路電子投票時間一般，惟承辦單位無須印製紙本選票，可節省不少時間；此外計票係利用電腦運算統計，速度較快；另本研究機制應用橢圓曲線密碼學理論，利用較短金鑰長度即具高安全強度，縮短選票加解密時間，可降低系統負荷；而多選票一次盲簽章亦有助降低簽章次數，減少時間浪費。
	成本	需要龐大紙本花費，成本高。	網路電子投票毋須紙本，花費成本低。
承辦安全性	機密性	選票可無須註記姓名，具機密性，惟如單位幹部以統一調查表決，則人員須公開表達意見，或不表達真實專業意見。	本機制運用橢圓曲線金鑰系統，破解選票須面臨離散對數問題，可確保選票機密性。
	完整性	無法確保人工統計不發生誤失，將選票內容錯看，導致計票錯誤。	運用簽章機制，選票內容若被竄改，則簽章將不被驗證通過，可用以檢驗選票內容的完整性。
		選票為統一印製，有印製單位之浮水印及承辦單位用印，不易被偽造。	第三方若欲模仿監察部門 B 的簽章，須面臨單向雜湊函數無法逆推之特性。

	鑑別性	選票為統一印製，有印製單位之浮水印及承辦單位用印，可鑑別為有效選票。	本機制運用簽章機制，簽章若被驗證通過，即為有效選票。
	隱匿性	選票上無須記名，惟如單位幹部以統一調查表決，則人員須公開表達意見，無隱匿性。	本機制設計將選票內容盲化，監察部門 B 簽章時無法知悉選票內容，可達到無法由資訊內容追蹤到投票人 A 身分的效果，具隱匿性。
	不可否認性	無確切發放選票或名冊登載，導致結果容易被竄改。	投票者的憑證只有投票人 A 擁有，其與監察部門 B 相互認證後領取選票，即無法否認其已領票。
	不可追蹤性	選票可無須註記姓名，具不可追蹤性，惟如單位幹部以統一調查表決，則人員須公開表達意見，人員身分將被公開。	設計密文摘要機制，讓監察部門 B 僅知道簽署的是選票密文摘要，無法知道選票內容；另承辦單位 C 用其私鑰解開選票，也與投票人 A 無關，具不可追蹤性。

4.2.2 本研究與其他電子投票機制之效益比較

表4係針對本研究與其他電子投票機制進行各項效益比較，可發現Song和Cui的電子投票機制不具隱匿性，選票會被知道是何人所投，另本研究具有較快速之運算速度或較高之機密性。

表4本研究設計機制與其他電子投票機制之效益比較表

比較項目		Song, F. and Cui, Z. 電子投票機制	陳淵順的電子投票機制	本研究設計機制
便利性		為網路電子投票機制，具便利性。	為網路電子投票機制，具便利性。	為網路電子投票機制，具便利性。
實用性	時間	運用 RSA 公開金鑰系統，相較於私密金鑰系統，加解密時間較長。	運用基於離散對數難題之公開金鑰系統，相較於私密金鑰系統，加解密時間較長。	應用橢圓曲線密碼學理論，利用較短金鑰長度即具備同等級之安全強度，縮短選票加解密時間；而多選票一次盲簽章亦有助降低簽章次數，減少時間浪費。
	成本	毋須紙本，也不須聘用投票所選務人員，成本低。	毋須紙本，也不須聘用投票所選務人員，成本低。	毋須紙本，也不須透過單位幹部統計或收整，成本低。
安全性	機密性	運用 RSA 公開金鑰系統，具機密性。	運用基於離散對數難題之公開金鑰系統，具機密性。	本機制運用橢圓曲線公開金鑰系統，在同樣的金鑰長度下，具備比 RSA 等其他公開金鑰系統更高之安全強度。
	完整性	運用簽章機制，選票內容若被竄改，則簽章將不被驗證通過，具完整性。	運用簽章機制，選票內容若被竄改，簽章將不被驗證通過，具完整性。	運用簽章機制，選票內容若被竄改，則簽章將不被驗證通過，具完整性。

	鑑別性	運用簽章機制，簽章若被驗證通過，即為有效選票，具鑑別性。	運用簽章機制，簽章若被驗證通過，即為有效選票，具鑑別性。	運用簽章機制，簽章若被驗證通過，即為有效選票，具鑑別性。
	隱匿性	經羅子惟(2012)研究指出，該機制可被查出選票為何人所投，不具備隱匿性。	另添加亂數機制，具隱匿性。	設計將選票內容盲化，監察部門B簽章時無法知悉選票內容，具隱匿性。
	不可否認性	具備憑證驗證機制，投票人不可否認其領過票，具不可否認性。	具備憑證驗證機制，投票人不可否認其領過票，具不可否認性。	具備憑證驗證機制，投票人不可否認其領過票，具不可否認性。
	不可追蹤性	選務中心對選票簽章時，可知悉投票內容，不具不可追蹤性。	設計模糊簽章機制，簽章時不知所選何人，具不可追蹤性。	本機制設計了密文摘要機制，讓監察部門B僅知道簽署的是選票密文摘要，無法知道選票內容；另承辦單位C用其私鑰解開選票，也與投票人A無關，具不可追蹤性。

4.2.3 運算成本效益分析及比較

美軍重大軍事決策鏈條之一環為美軍智庫，其採軍民融合方式打造龐大的智庫方陣，以科學的分析、精準的研判和巨大的社會影響力，廣泛影響著美國政治、經濟、外交等各方面的重大決策，因此精進我國軍中現行決策投票制度，參謀可透過本研究機制統整相關數據及意見，用以提升決策品質，本研究機制採多選票一次盲簽密方式，針對選票文件份數越來越多，經過運算成本效益的計算及比較，可凸顯本研究提出之多選票盲簽密機制之效益；運算成本計算量分析方式及相互關係如表5(Wang et al, 2008)，於2017年所提之新型態電子投票機制設計中(蘇品長與葉昱宗，2017)，該設計以代理簽章為主軸設計，與本研究為符合軍隊環境提出之多文件盲簽密機制不同，故本研究將與其所提之各系統盲簽章及2012年梁榮哲所提之多重文件盲簽章階段進行運算成本效益比較，多文件盲簽章運算成本效益比較如表6及圖3。

表5 運算成本參考表

符號	定義
T_{ECMUL}	進行一次ECC乘法運算所需時間≈ 29 T_{MUL}
T_{ECADD}	進行一次ECC加法運算所需時間≈ 5 T_{MUL}
T_{INVS}	進行一次模式乘法反元素運算所需時間≈ 240 T_{MUL}
T_{EXP}	進行一次模式指數運算所需時間≈ 240 T_{MUL}
T_{ADD}	進行一次模式加法運算時間(可忽略不計)
T_{MUL}	進行一次模式乘法運算時間
t_h	進行一次hash(SHA-1)所需時間≈ 0.4 T_{MUL}
T_h	進行一次點hash所需時間≈ 23 T_{MUL}

表6 各系統盲簽章運算成本效益比較表

演算法	Pradhan et al.(2011)		梁榮哲(2012)		Sadat et al.(2016)		本研究機制	
階段	運算成本	概估	運算成本	概估	運算成本	概估	運算成本	概估
盲簽運算	$3\ T_{ECMUL}$ $+2\ T_{ECADD}$ $+1\ T_{MUL}$ $+5\ T_{ADD}$ $+1t_h$	$\approx 98\ T_{MUL}$	$4\ T_{ECMUL}$ $+1\ t_h$ $+1\ T_h$	$\approx 140\ T_{MUL}$	$4\ T_{ECMUL}$ $+2\ T_{ECADD}$ $+1\ T_{MUL}$ $+4T_{ADD}$ $+1\ T_{INVS}$	$\approx 367\ T_{MU}$	$3\ T_{ECMUL}$ $+1\ T_{ECADD}$ $+1\ T_{MUL}$	$\approx 93\ T_{MUL}$
文件數量	運算成本概估		運算成本概估		運算成本概估		運算成本概估	
1	$\approx 98T_{MUL}$		$\approx 140\ T_{MUL}$		$\approx 367\ T_{MUL}$		$\approx 93\ T_{MUL}$	
2	$\approx 196T_{MUL}$		$\approx 140\ T_{MUL}$		$\approx 734\ T_{MUL}$		$\approx 93\ T_{MUL}$	
3	$\approx 294T_{MUL}$		$\approx 140\ T_{MUL}$		$\approx 1101\ T_{MUL}$		$\approx 93\ T_{MUL}$	
4	$\approx 392T_{MUL}$		$\approx 140\ T_{MUL}$		$\approx 1468\ T_{MUL}$		$\approx 93\ T_{MUL}$	
5	$\approx 490\ T_{MUL}$		$\approx 140\ T_{MUL}$		$\approx 1835\ T_{MUL}$		$\approx 93\ T_{MUL}$	

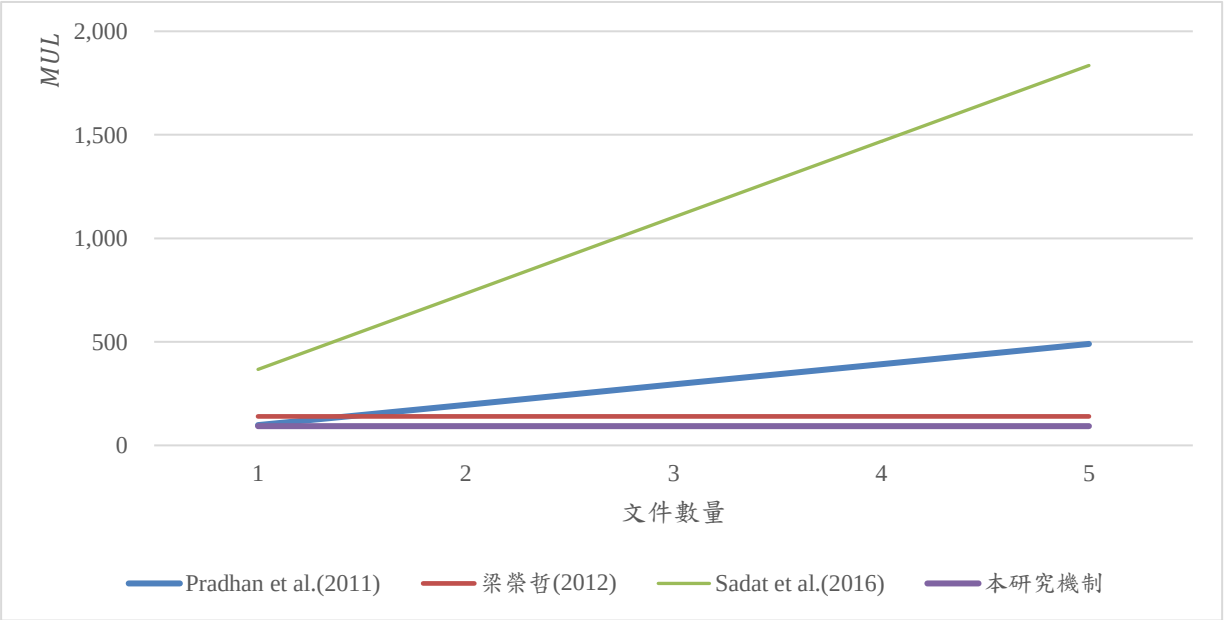

圖 3 多文件盲簽(密)章運算成本效益比較圖

五、結論

本研究設計之具足夠安全性之網路投票機制，運用橢圓曲線密碼系統可以以較短長度之金鑰，達到與現行 RSA 及 ElGamal 等方法相同安全度之特性，亦使系統執行加解密效率更快；另採用多選票一次盲簽密機制，可應用於多項議題同時表決時機，有助於降低多合一投票時之大量簽章次數，可減少投票系統負荷；本研究基於雲端環境建構此電子投票機制除具便利性與實用性，在安全性上滿足機密、完整、鑑別、隱匿、不可否認、不可追蹤等特點，可便於快速掌握及統整投票結果，提供具體且客觀的數據資料，輔助決策者執行決策，實務上之應用亦能適合於現行民主社會中特定電子投票型態，例如國家定期及不定期之選舉、公投、政府施政方案、企業與客戶滿意度調查等屬數據蒐整單向性的決策程序，若相關單位須採雙向性決策回饋，例如企業決策評鑑、產品測試意見調查等相關之實務應用需求，可滿足現今社會及企業未來許多實際應用。

5.1 國防領域之應用

本研究可在不違反國軍決策體系之階層關係為前提下，應用於對軍中相關制度意見表決時機，參謀利用此網路投票機制，打破原時空之限制，向各領域之專業部隊及幹部，統整專業意見或表決方案，以提供指揮官作為下達決策之依據；另針對國防裝備之可用性、適用性及維修狀況等議題執行調查，有效掌握現行所屬部隊裝備現況及妥善率，進而研擬精進方案，同步修正國軍現行之後勤維護等系統，提升國防武器裝備整體戰力，而在國軍人事評議及採購招標廠商評鑑等場景，亦可考量運用本研究機制，以利縮短參謀人員作業時效；另本研究設計在安全性部分具有機密、隱匿及不可追蹤等特性，可使投票之官兵無需顧慮官階文化組織，表達其專業且真實之意見，作為領導者執行決策之參考依據，有效提升國軍決策品質。

5.2 未來運用方向

本次研究設計著重於網路投票機制之便利性及安全性，可應用於我國現行民主社會選舉投票利用，並能解決我國多合一選舉造成選務工作耗時且繁重之問題，未來運用則可針對選票內容及投票族群，探討加入權重概念，藉此方式以強化專業的意見部分，增加決策參考議題之多元化及可靠性，有利未來軍隊、企業及社會實務應用；另現在生物特徵認證之技術也已漸漸普及社會各行業機構，若未來國軍及各企業配合相對應政策與規定，以本研究提出認證方式來強化身分認證安全性，亦可針對較敏感之決策議題增加其實務運用的可能性。

參考文獻

丘昌泰，2004，從各國電子投票經驗看我國選務的改革方向，*研考雙月刊*，第 28 卷第 4 期，25-35。

朱近之主編，2010，智慧的雲端運算-成就物聯網的未來基石，博碩文化，37-45。

宋佩璇，2020，借專家意見提升董事會決策品質，*證券服務第 677 期*，26-27。

呂明諺，2020，*Say-on-Pay 投票頻率對經理人獎酬之影響*，國立台灣大學管理學院會計學研究所碩士論文。

林明慶，2009，*隱匿技術應用於國軍網路申訴制度之研究*，國防大學資訊管理學系研究所碩士論文。

周振、嚴廣樂，2020，基於區塊鏈技術的匿名電子投票協議設計，*軟件導刊*，229-233。

徐凡，2006，*跨領域之匿名行動付款機制*，世新大學資訊管理學系研究所碩士論文。

孫萌，2019，基於區塊鏈的可追踪匿名電子投票方案，*網路空間安全*，85 - 91。

高嘉言，2009，*植基於背包型態之橢圓曲線數位簽章系統設計*，國防大學資訊管理學系研究所碩士論文。

梁榮哲，2012，*多重文件盲簽章機制之設計*，國防大學資訊管理學系研究所碩士論文。

郭文雄，2011，*設計具有自我認證之國軍網路申訴制度安全機制探討*，國防大學資訊管理學系研究所碩士論文。

陳淵順，2011，*基於模糊簽章之電子投票系統*，國立政治大學資訊科學系研究所碩士論文。

陳文彬，2012，*運用動態存取控制方法於雲端服務之研究*，國防大學資訊管理學系研究所碩士論文。

陳明政、吳佳純，2015，決策風格對中階軍官決策行為之影響，*海軍學術雙月刊*，68 - 86。

張鈞富，2014，*具自我認證之安全並存簽章方法*，國防大學資訊管理學系研究所碩士論文。

楊亞濤，2020，基於 SEAL 庫的同態加權電子投票系統，*計算機學報*，711 - 723。

劉勇、徐曉琳，2006，信息技術對政府決策品質的影響研究，*湖北社會科學 2006 卷 4 期*，36-38。

羅子惟，2012，有關 Song 和 Cui 的電子投票機制匿名性之探討，*企業架構與資訊科技研討會*，德明財經科技大學主辦。

蘇品長、黃俊傑，2015，適用於網路電子投票之安全機制設計－以不在籍投票為例，*國防管理學術暨實務研討會*。

蘇品長，2007，*植基於 LSK 和 ECC 技術之公開金鑰密碼系統*，長庚大學電機工程系研究所博士論文。

蘇品長、葉昱宗、黃俊傑，2015，跨軍種服務之國防雲設計，*中正嶺學報*。

蘇品長、葉昱宗，2017，新型態之電子投票機制設計，*電子商務學報*，29-50。

American Bankers Association., 1998 Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA). ANSI X9, 62

Chaum, D., 1983. Blind signatures for untraceable payments. *In Advances in cryptology . Springer, Boston, MA.*, 199-203.

Diffie, W., and Hellman, M., 1976. New directions in cryptography. *IEEE transactions on Information Theory, 22(6)*, 644-654.

ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete

logarithms. *IEEE transactions on information theory*, *31*(4), 469-472.
Gallagher, P., and Director, C. F., 2009. FIPS PUB 186-3 federal information processing standards publication digital signature standard (DSS).
Hankerson, D., Menezes, A. J., and Vanstone, S., 2006. Guide to elliptic curve cryptography. Springer Science & Business Media.
Jablon, D., 2001. IEEE P1363 standard specifications for public-key cryptography. In CTO Phoenix Technologies Treasurer, IEEE P1363 NIST Key Management Workshop.
Koblitz, N., 1987. Elliptic curve cryptosystems. *Mathematics of computation*, *48*(177), 203-209.
Miller, V. S., 1985. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*. Springer, Berlin, Heidelberg. 417-426
Pradhan, S., and Mohapatra, R. K., 2011. Proxy blind signature scheme based on ECDLP. *International Journal of Engineering Science & Technology*, *3*(3), 2244-2248.
Sadat, A., Ullah, I., Khattak, H., and Ullah, S., 2016. Proxy blind signcrypion based on elliptic curve. *International Journal of Computer Science and Information Security*, *14*(3), 257-262.
Schnorr, C. P., 1991. Efficient signature generation by smart cards. *Journal of cryptology*, 4(3), 161-174.
Song, F., and Cui, Z., 2012. Electronic voting scheme about Elgamal blind-signatures based on XML. *Procedia Engineering, 29*, 2721-2725.
Tso, R., Okamoto, T., and Okamoto, E., 2008. 1-out-of-n oblivious signatures. In *International Conference on Information Security Practice and Experience* . Springer, Berlin, Heidelberg. 45-55
Wang, R. C., Juang, W. S., and Lei, C. L., 2008. A web metering scheme for fair advertisement transactions. In *2008 International Conference on Information Security and Assurance (isa 2008)* . IEEE., 53-456.
美國在臺協會，美國選舉程序，下載於 http://www.ait.org.tw/infousa/zhtw/PUBS/USElection2004/procedure.htm. (2015/01/20)
美軍智庫:重大軍事決策鏈條的重要一環 http://military.people.com.cn/BIG5/n/2015/1120/c1011-27836286.html. (2015/11/20)
GQ 網，愛沙尼亞超先進，網路投票、手機投票都通！，下載於 http://wired.tw/posts/electronic_election. (2015/01/20)
See Gartner Inc., Cloud Computing, GARTNER.COM http://www.gartner.com/it-glossary/cloudcomputing/ (last visited Jun. 21, 2019).
淺談雲端 https://www.catespotr.com/2010/07/introduction-cloud-computing.html
NIST，“The NIST Definition of Cloud Computing”，2010，http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf。
iThome 電腦報，吳其勳，https://www.ithome.com.tw/article/93006(2011 年 6 月 21 日)