# 設計多重文件盲簽章運用於國軍電子化採購之探討

作者／梁榮哲少校


## 提要

一、 在網際網路如此盛行社會裡創造出電子商務這新的交易模式，而它必須仰賴電子付款及盲簽章來進行。其中盲簽章技術已被許多國家拿來應用，以達到不可偽造及不可追蹤等特性。

二、 國軍在政府推動電子化的政策下，逐步將傳統採購作業改為電子化採購，然而電子化採購是藉由網路運作，可能會造成投標時易遭擷取讓廠商身分及投標文件內容洩漏，而發生弊案情事。

三、 本研究設計在一次性加密後可多重文件盲簽章之方法，不僅能夠大量減少電子交易中的盲簽章及加密次數，來達到提升運算效率，縮短作業時間效益，且基於較高的破密難度，進而提高交易的安全性。


**關鍵詞：**橢圓曲線、盲簽章、電子商務、多重文件。

## 前言

隨著資訊科技進步，帶動網際網路盛行，使得人們生活中的所有資料，舉凡文字、聲音、影像等資訊均可轉檔成數位資料，透過資訊網路穿梭於全世界，而在彈指之間為全球人士所共享，生活上的食衣住行也慢慢地從傳統實體交易轉移至虛擬網路上交易。[1]在 1970 年銀行開始利用金融資訊網路進行電子資金轉換，而在 1980 年電子資料交換與電子郵件的技術，由於企業間因應商業資訊傳遞的即時性需求，開始蓬勃發展，商業文件以標準的電子形式流通於企業中，其優點是提高行政業務效率，且降低不必要的紙張成本。到了 1990 年全球資訊網的出現，則造就電子商務[2]時代的來臨。

政府為因應時代潮流的趨勢與國際接軌，並提升我國產能競爭力，積極推動電子化政策，並利用電子商務技術建置電子採購系統取代傳統人工採購作業以節省成本，減輕人力作業負擔及大幅提升整體採購流程效率，並使得採購流程更為透明化，減少弊端。國防部在推動電子化的政策下，[3]將舊有軍事採購作業逐漸改為電子化採購，取

---

1 黃智賢〈創新金融服務行動支付模式對顧客線上消費行為之影響〉，國防大學資訊管理學系研究所碩士論文，2017 年，頁 1-3。

2 蘇品長、張鈞富、黃棠建，〈適用於電子商務之自我認證公開金鑰架構之設計與實作〉《電子商務研究》(臺北市)，第 12 卷第 1 期，國立臺北大學資訊管理研究所，2014 年 3 月，頁 73~92。

3 謝定芳，〈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〉，國防大學資訊管理學系研究所碩士論文，2017 年，頁 73~92。

代了傳統人工作業複雜手續的採購模式，促進了採購效率的提升與節省採購成本，以期軍事機關辦理採購過程更為公開與透明。

而軍事採購係以支援國軍建軍備戰之重要手段，亦屬政府採購之一環，除依政府採購法、政府採購法施行細則及有關法令之規定外，應依「軍事機關採購作業規定」辦理，採購流程應循「計畫申購」、「招標訂約」、「履約驗收」等三階段執行。[4]其採購主要目的是依戰備演訓任務所需，在一切依法行政下及考量品質、時效與價格等因素，以如期、如質、如預算的獲得所需軍品數量，俾利支援國軍建軍整備的需求，並落實國家安全的目標。然電子化採購是藉由網際網路傳輸訊息，廠商在進行投標作業傳遞資料時可能遭受竊取、篡改等資訊安全問題的發生，而造成廠商身分及投標文件內容洩漏，發生圍標、綁標的不法情事。如何有效保護廠商身分的隱私及避免投標文內容的曝露，便成為值得深思的議題。

由於所有政府機關單位採用的電子化採購系統是公共工程委員會委由中華電信開發與管理，該系統運用電子憑證、RSA、資料加密標準(Data Encryption Standard, DES)及數位簽章等密碼學技術來實作系統，雖然可達到對資料訊息的機密性、完整性、鑑別性及不可否認性，但也很容易地洩露使用者的身分。而且目前在採購作業上，一項標案就必須投標一次，多個標案就必須多次作業，造成作業程序繁雜。因此，在考慮國軍軍機保密及採購流程有所不同，進而研究盲簽章運用，並以橢圓曲線密碼學為理論基礎，使用多份投標文件執行一次盲簽章及加密的方法，減少檔案分批簽章次數，以及傳輸頻寬之需求等優點，將它應用於軍事電子化採購作業，在廠商投標時對其投標文件作盲化，並於驗標時對投標文件及簽章作驗證，以期國軍電子化採購作業更加安全及有效率。

## 政府電子化採購進展

隨著網路普及化，政府採購電子化推陳出新，電子領標推動以來已有相當成效，近年工程會更積極鼓勵電子投標，從小規模之簡易採購著手，自 104 年推動採公開取得電子報價單之採購方式，106 年度廠商使用次數已較 104 年度大幅增加 190%。[5]

### 一、政府電子化採購簡介

由於網際網路技術的成熟，政府為因應時代潮流的趨勢與國際接軌，以及提昇我國產能競爭力，積極推動電子化政策，並於民國 88 年通過「產業自動化及電子化推動方案」，藉此運用民間企業的電子商務技術，來大幅降低企業營運成本，並提昇產業的

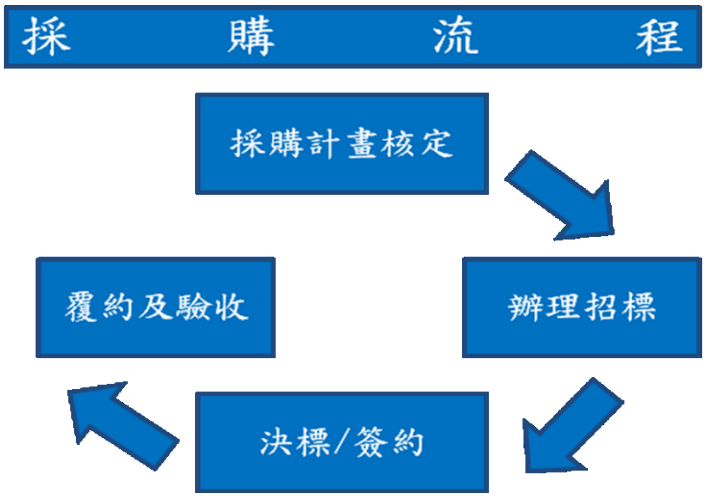
[4] 國防部軍備局，〈軍事機關採購作業規定〉，2003 年，頁 1-10。
[5] 行政院公共工程委員會〈新聞稿〉《政府採購電子化推動有成 廠商線上領投標省時又省力》，2018 年 5 月 16 日。

競爭力。[6]因此，政府部門決定率先運用網際網路，提供採購資訊與建置相關採構機制，來帶動相關產業參與。而電子化採購是利用網際網路的快速傳遞訊息，來大幅減少採購所需的龐大人力、繁雜的文書往返及作業流程，然系統則是由公共工程委員會與中華電信合作建置電子化採購系統。其目的是在網路上建立一套安全的電子簽章身分驗證及安全的網路傳輸環境，以及操作簡便而安全又可靠的電子領投標作業系統，以簡化繁複的作業程序和有效提升採購業務的效率，並降低採購成本，更可大幅提昇採購作業流程的公開透明化，以期能杜絕圍標、綁標的不法情事。

## 二、現行軍事採購流程

由於網際網路技術的成熟，軍事採購為支援國軍建軍備戰之重要手段，亦屬政府採購之一環，主要任務在於以經濟有效之方式，整體考量品質、時效與價格等因素，如期獲得適質適量之工程、財物、勞務，支援國軍戰備需要。而採購政策係秉持「建立國防自主」、「扶植本國工業」及「優先向國內廠商採購」原則辦理，對須向國外採購獲得者，則要求廠商提供工業合作，以提升國內工業科技水準。依據「軍事機關採購作業規定」，採購以集中辦理為主，惟國防部得視事實需要授權辦理，而採購時應循計畫申購階段、招標訂約階段、履約驗收階段等三階段編組執行，[7]其採購流程如圖一。

圖一 採購流程圖




資料來源：作者繪製。

## 三、軍事電子化採購作業流程

對國內外各學術單位研究成果及文獻探討後，摘整後導入國軍電子採購系統作業功能及說明，相關作業流程可區分六個階段，步驟過程說明如下：

(一)註冊作業

[6] 蘇品長，〈適用於國軍電子採購的盲簽章系統設計〉《國防管理學報》(台北市)，第 29 卷第 2 期，國防大學管理學院，2008 年，頁 51-62。

[7] 同註 2。

廠商自行註冊加入會員，再將相關文件送至認證中心註冊審查，審查通過後，發給廠商類別、等級相關文件與憑證。

(二)招標作業

軍事採購部門機關在辦理採購，將招標文件上網公告，提供相關廠商下載領取招標文件，軍事機關在傳送電子文件之前，需向憑證管理中心授權中心求證身分，確認後核發憑證及私密金鑰進行電子簽章，以確保招標文件的有效性與不可否認性，再辦理標單上網公告，讓合格廠商可上網瀏覽領取 標單。

(三)領標作業

對相關招標文件有意願的廠商，依招標單規定於網路上直接向金融機構繳交一定金額押標金，繳費完成後招標機關會送出繳費證明憑證給廠商，廠商在依此憑證下載標案文件。

(四)投標作業

決定參與競標的廠商，在投標日期截止前開始投標文件製作，利用私有金鑰及系統公鑰進加密後進行投標作業，將投標文件傳送到網路中心，系統資料庫會驗證該標單的完整性與正確性，完成後招標機關會送出標單收到憑證給廠商，以保障廠商的權益。

(五)開標作業

在開標期限到達後，使用開標憑證私密金鑰進行開標解密標價作業，依有訂底價最低決標作業流程實施決標公告，如果是廢標將通知銀行退還押標金。

(六)簽約作業

與得標廠商辦理簽約作業並發予得標廠商合約書，驗證其簽章及審視廠商填妥合約書內容。電子採購系統導入國軍採購流程架構如圖二。

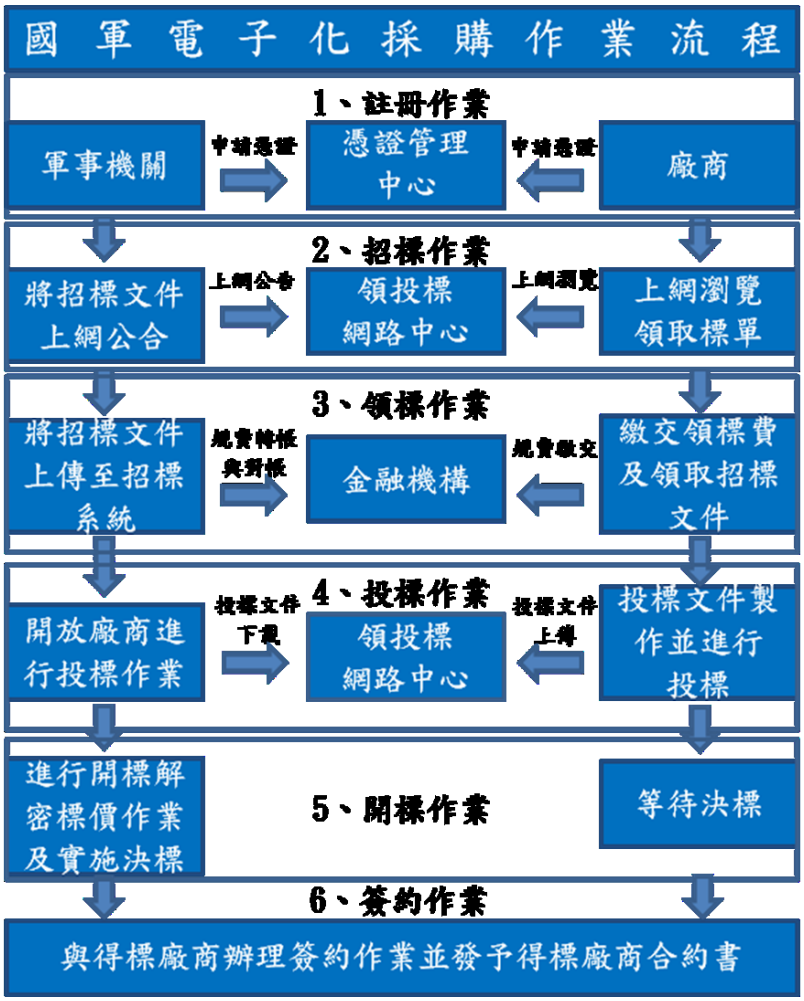
## 密碼學概述

密碼學(在西歐語文中之源於希臘語 Kryptós「隱藏的」和 Gráphein「書寫」)是研究如何隱密地傳遞訊息的學門。在現代特別指對資訊以及其傳輸的數學性研究，常被認為是數學和電腦科學的分支，和資訊理論也密切相關，著名的密碼學學者 Ron Rivest 解釋道：「密碼學是關於如何在敵人存在的環境中通訊」。[8]從古老的過去到科技的現在，密碼學的內容與觀念，因應人類科技進步而一直在演進與變化，不變的是密碼學基本上還是想辦法提供秘密安全之通訊服務。在二次世界大戰期間，美、日與英、德更於戰場上進行激烈的競爭，從 60 年代電腦開始流行，軟硬體能力不斷的發展突破

[8] 〈PGP加密原理〉《玉山科技》，https://www.asiapeak.com/PGPTheory.php，2018年9月8日。

，許多傳統的密碼規則在這些電腦面前逐漸無法維持安全性，紛紛遭到破解，因此各種新的密碼學概念相繼提出，利用了許多如數論(Number Theory)的數學理論，為的就是要加強密碼以抵擋電腦分析與運算破解的能力，這些理論使得現代密碼學成為了一種可以系統而嚴格地學習的科學，共分為兩大類：對稱式密碼系統(Symmetric Cryptosystem)及非對稱式密碼系統(Asymmetric Cryptosystem)。

圖二 軍事電子化採購作業流程



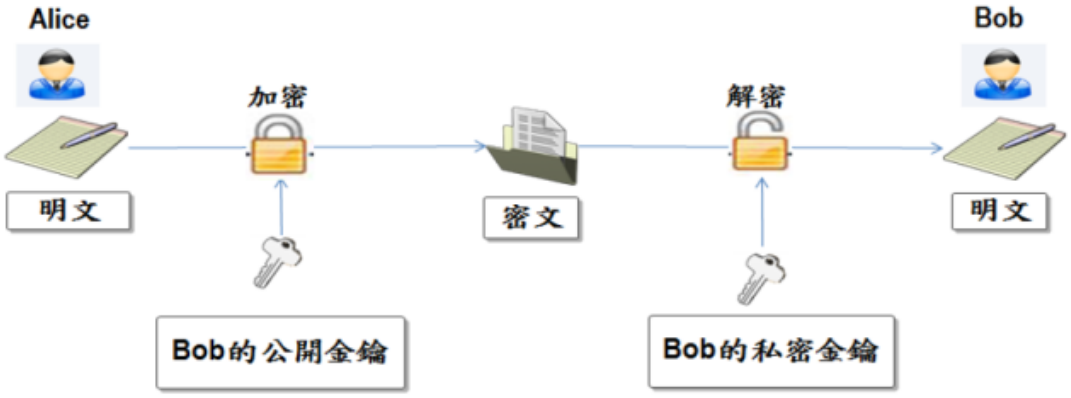

資料來源：作者繪製。

## 一、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，此類型的加解密系統中加密與解密都是使用相同的金鑰，1976 年以前電腦所使用的加密技術均屬於此類。對稱式加密法的特性是加、解密的速度快，但也因為加密與解密是共用同一把密鑰，所以一旦交易的對象數量增多時，則金鑰的管理及如何安全的將密鑰分配給通訊對方是重要問題之一，即是密鑰的管理問題。[9]舉例來說，當一個人要與 n 個人秘密通訊，則需個別保有 *n* 把密鑰，故整個密碼系統則有 n(n-1)/2 把密鑰，圖三為對稱式密碼系統示意圖。

[9] 蕭雅尹，〈強化國軍通資系統安全之金鑰交換機制設計〉，國防大學資訊管理學系研究所碩士論文，2018 年，

圖三 對稱式密碼系統

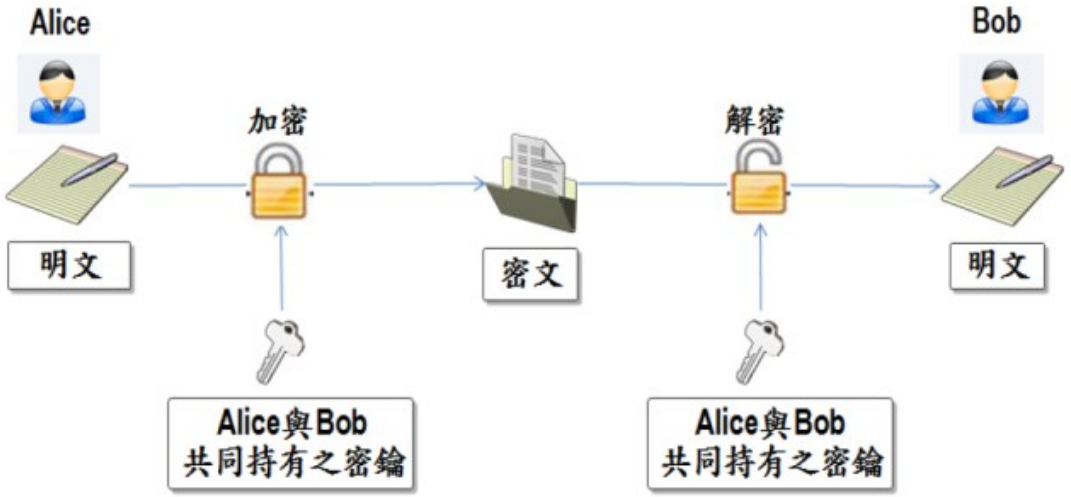



資料來源：李南逸等人，《網路安全與密碼學概論》(台北：東華書局，2014 年)，頁 22-70。

## 二、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，是由 Diffie 與 Hellman 提出非對稱式加密技術的概念，[10]可有效解決通訊雙方使用對稱式密碼系統的金鑰交換問題，並帶來了數位簽章的創新觀念。它在通訊雙方均擁有一組密鑰對(Key Pair)，即公鑰(Public Key)與私鑰(Private Key)，公開金鑰均可對外公佈，但私鑰必須自己保管。其系統運作方式，假設 Bob 與 Alice 通訊，則 Bob 應以 Alice 的公鑰加密訊息，Alice 收到訊息後以自己的私鑰解密。此加密技術之優點是解決了「對稱式加密技術」中金鑰分配及管理的問題，[11]但缺點為加、解密運算較「對稱式加密法」複雜且速度較慢，圖四為非對稱式密碼系統示意圖。

圖四 非對稱式密碼系統




資料來源：李南逸等人，《網路安全與密碼學概論》(台北：東華書局，2014 年)，頁 22-70。

---

頁 13-16。

[10] Diffie,W,and Hellman,M.e., “New Directions in Cryptography,” IEEE Transactions on Information Theory, IT-22(6), 1976, pp.644-654.

[11] 葉家維，〈設計具多重難度之混合式公開金鑰密碼系統〉，國防大學資訊管理學系研究所碩士論文，2018 年，頁 17-22。

## 三、橢圓曲線公開金鑰密碼系統(Elliptic Curve Cryptography, ECC)

公開金鑰密碼學早在百年前就已完備，而橢圓曲線在代數學與幾何學上廣泛的研究也已達百年之久，且有豐富及深奧的理論，[12]橢圓曲線第一次應用於密碼學上則是Miller[13]與 Koblitz[14]兩位學者分別提出，從此橢圓曲線在密碼學中就扮演重要的角色。

(一)橢圓曲線定義

令 $P>3$ 為質數，在 $GF(P)$ 中的橢圓曲線 $E: y^2 = x^3 + ax + b \bmod p$ ，其中 $4a^3 + 27b^2 \neq 0 (\bmod p)$ 。曲線上另定義一個無窮遠點 $O$ ，對任一點 $A \in E$ ，$A + O = O + A = A$ 。

加法運算：令 $A=(x_1, y_1)$ 與 $B=(x_2, y_2)$ 為$E$上的點，則若 $x_2 = x_1$ 且 $y_2 = -y_1$ ，則 $A + B = O$ ；否則 $A + B = (x_3, y_3)$ ，其中 $x_3 = \lambda^2 - x_1 - x_2$ ， $y_3 = \lambda(x_1 - x_3) - y_1$

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

註：橢圓曲線運算中，大寫參數表示點，小寫參數表示數值。

橢圓曲線[15]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的運算來達成。例如：計算時，由於 $4P = 2P + 2P$ ，再計算 $2P = P + P$ 即可。反元素運算:點 $A=(x, y)$ 的反元素為 $-A = -(x, y) = (x, -y)$ 。(因為 $A + (-A) = (-A) + A = O$ ，此時$O$稱為乘法單位元素)例子：在橢圓曲線 $E: y^2 = x^3 + x + 6 (\bmod 11)$ 上的點有：

(2,4)(2,7)(3,5)(3,6)(5,2)(5,9)(7,2)(7,9)(8,3)(8,8)(10,2)(10,9)

再加上$O$共有13點。注意在計算點時，要檢驗 $x^3 + x + 6$ 之值是否屬於 $QR_{11}$ 。除了$O$以外，任意點均可以視為$E$的始元素(Primitive Element)。

註：令定義於 $Z_p$ 的橢圓曲線$E$的所有點的個數為 $\#E$ ，則

$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$ 。

假設一個橢圓曲線是屬於$Fq$，而$P$是橢圓曲線$E$上的一個點，給定一個屬於橢圓曲線$E$上的一個點$Q$，若要找出一整數$K$使得$Kp=Q$，因為其特殊的點加法運算，破密者除了逐一窮舉所有可能的點外，別無他法。直至目前為止，這個問題仍無法於多項式時間內求出解答。橢圓曲線密碼系統的另一個優點是其加密的密鑰長度短，在同樣的安全度之下，橢圓曲線密碼系統僅需較小的密鑰長度；相同地，在同樣的密鑰長度下，橢圓曲線密碼系統卻擁有更高的安全性，表一為RSA與ECC在相同安全度下金鑰長度之比較：

---

[12] 高嘉言，〈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，2009年，頁 19-26。

[13] Miller,V.S., “Use of Elliptic Curve in Cryptography,” Advance in Cryptography Crypto,( 1985), pp.417-426.

[14] Koblitz,N.,1987, “Elliptic Curve Cryptosystems, ” Mathematics of Computation American Mathematical Society, Vol.48, 1987, pp.203-209.

[15] 肖攸安，《橢圓曲線密碼體系研究》(華中科技大學出版，2006 年)，頁 1-78。

表一 RSA 與 ECC 相同安全度金鑰比較表

| 長度 / 項目 | 金鑰長度(bits) | | | | |
|---|---|---|---|---|---|
| RSA | 512 | 1024 | 2048 | 3072 | 7680 |
| ECC | 112 | 163 | 224 | 256 | 384 |
| ECC 與 RSA 金鑰長度比 | 1:5 | 1:6 | 1:9 | 1:12 | 1:20 |

資料來源：蘇品長，〈植基於 LSK 和 ECC 技術之公開金鑰密碼系統〉，長庚大學電機工程系研究所博士論文，2007 年，頁 30-63。

## 四、盲簽章

由於網際網路的應用可以明顯地提升工作效率、降低成本、提昇服務品質，並且具備即時性，隱藏著無限商機，故網際網路開放商業使用之後，隨即在全球各地掀起一股銳不可當的電子商務潮流。在這過程中，Chaum[16]率先提出了盲簽章的觀念，他的簽章方法裡有兩個角色，一個是簽章者，另一個是送簽者，盲簽章能讓送簽者在不洩漏訊息的前提下，讓簽章者對該訊息加以簽名；主要提出了盲簽章兩個重要的特性：簽章者在簽署時不能知道所要簽署的文件內容，事後除了送簽者外無人可以追蹤所簽文件與送簽者的關係。有了這兩個特性，使得盲簽章得以應用在線上電子投票如圖五[17,18,19]及電子貨幣系統[20,21,22]。但是 Chaum 的盲簽章概念面臨到一些問題，如完整性、不可脅迫性及非欺騙性等，然而隨著學者們不斷改進，有 Mohammed 等學者[23]所提出基於 ElGama 的盲簽章，在論文中說明他們的演算法會比基於 RSA 的盲簽章法更少運算，速度更快並滿足盲簽章應有的四個性質。近年來，更有 Jeng 等學者[24]提出基於橢圓曲線的盲簽章，他們的演算法比 RSA 及 ElGamal 運算更快。然而網際網路是一高度透明公開的環境，有心人士可在其中竊取、偽造、竄改資料、或冒名欺騙，若要利用網路進行電子交易，須建置具保密性而又能驗證網路使用者之網路資料傳輸交易機制，

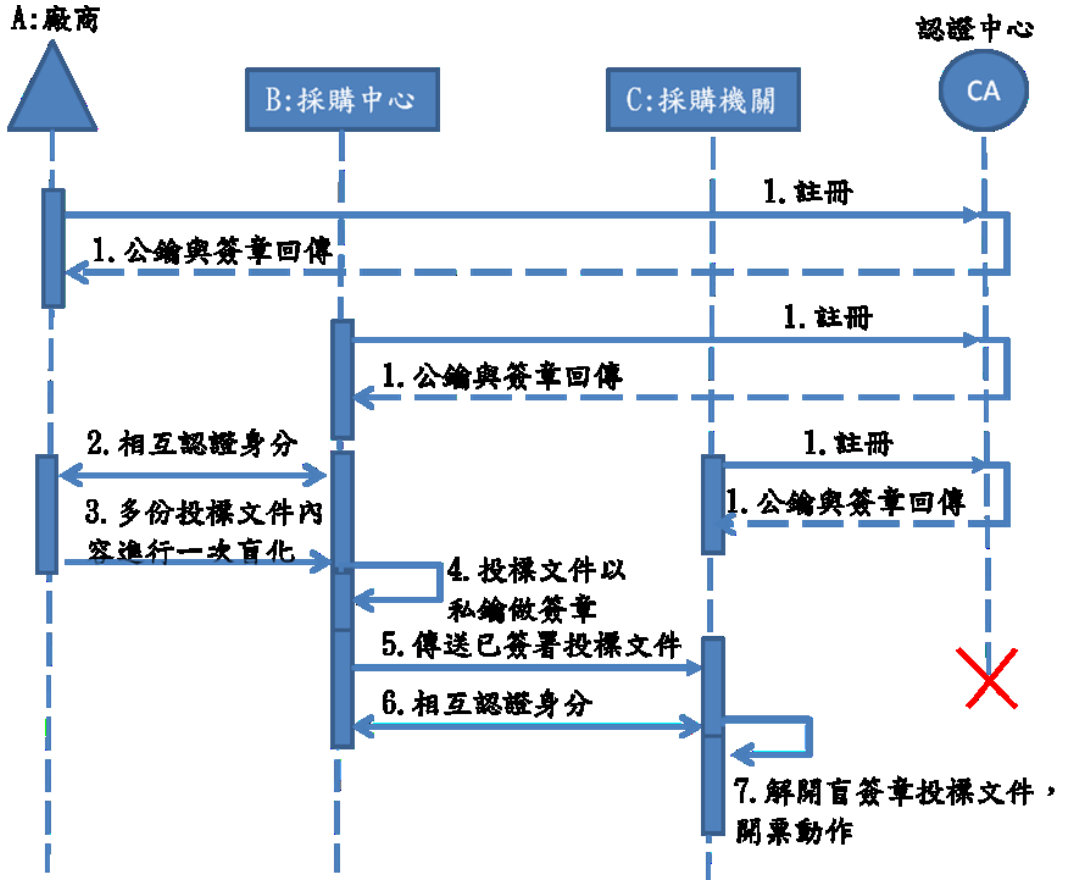
[16] Chaum, D.,“ Blind signatures for untraceable payments,” In Proceedings of Advances in Cryptology-CRYPTO, (1982), pp.199-203.
[17] Ibrahim,S.,Kamat,M.,Salleh,M.,and Aziz,S.R.A.,“Secure E-voting with Blind Signature,” Proceedings of 4th National Conference on Telecommunication Technology,(2003), pp.193-197.
[18] Wang,L.,Guo,J.,and Luo,M.,“A More Effective Voting Scheme based on Blind 25 Signature,”Proceedings of International Conference on Computation Intelligence and Security,Vol.2,(2006), pp.1507-1510.
[19] Yun,S.H.,and Lee,S.J.,“An Electronic Voting Scheme based on Undeniable Blind Signature Scheme,”Proceedings of IEEE 37th Annual International Carnahan Conference on Security Technology,( 2003), pp.163-167.
[20] Fan,C.I.,and Chen,W.K.,“An Efficient Blind Signature Scheme for Information Hiding,”,International Journal of Electronic Commerce,Vol.6,No.1(2001), pp.93-100.
[21] Nakanishi,T.,and Sugiyama,Y.,“Unlinkable Divisible Electronic Cash, ” Proceedings of 3rd International Workshop on Information Security,(2000), pp.121-134.
[22] Nakanishi,T.,Shiota,M.,and Sugiyama,Y.,“An Efficient on-line Electronic Cash with Unlinkable Exact Payments,” Proceedings of the 7th Information Security Conference,(2004), pp.367-378.
[23] Mohammed,E.,Emarah,A.E.,and Shennawy,K.E., “A blind signatures scheme based on ElGamal signature,” IEEE/ AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security,(2000), pp.51-53.
[24] Jeng,F.G.,Chen,T.L.,and Chen,T.S., “An ECC-Based Blind Signature Scheme, ” journal of networks, Vol.5, No.8 (2010), pp.921-928.

所以如何建立一個安全及可信賴的網路環境，將是電子商務能否全面普及的關鍵。[25]

圖五 電子匿名投票選舉流程圖


資料來源：作者整理。

圖六 本研究方法整體運作示意循序圖




資料來源：作者整理。

## 本研究方法

降低成本與提高效率是電子採購之趨勢，如何確保系統更趨高效率及高安全，已是近年來重要研究方向。所以針對上述問題，本研究(如圖六)提出一種植基於橢圓曲

[25] 王薏譽，〈以比特幣為基礎建構兼具公平交換和客户匿名特性之數位內容線上交易協定〉，國防大學資訊管理學系研究所碩士論文，2017 年，頁 7-15。

線離散對數的多重文件盲簽章機制可適用於軍事電子化採購方案中，以多份投標文件內容一次盲簽章及加密機制，目的是讓網路中心在簽署過程中，不知道廠商投標文件的內容，以避免廠商身分暴露及投標文件被偷窺而造成圍標、綁標之虞。採購中心把投標文件做簽署動作，代表這投標文件為合法之有效票，之後在傳送至採購機關去做開票動作，這項創新機制的導入，縮短系統作業多餘的程序，進而提升執行時的效率。

## 一、系統參數符號說明

系統初始時針對密碼系統作一個參數設定選擇，以下針對本研究中各參數進行說明：(如表二)

表二 系統使用符號之說明

| 項目 | 符號 | 說明 |
|---|---|---|
| 1 | $E(F_q)$ | 有限域 $F_q$ 中的一條橢圓曲線 |
| 2 | $G$ | 橢圓曲線中的基點 |
| 3 | $N$ | 橢圓曲線上基點的(order) |
| 4 | $q$ | $q > 2^{160}$ 之質數 |
| 5 | $id_a, id_b, id_c$ | 廠商 A、採購中心 B、採購機關 C 的 ID 資訊 |
| 6 | $PK_{as}, SK_{as}$ | CA 的公鑰與私鑰 |
| 7 | $PK_A, PK_B, PK_C$ | 廠商 A、採購中心 B、採購機關 C 之公鑰 |
| 8 | $n_a, n_b, n_c$ | 廠商 A、採購中心 B、採購機關 C 所選擇之私鑰 |
| 9 | $ca_a, ca_b, ca_c$ | 廠商 A、採購中心 B、採購機關 C 之憑證 |
| 10 | $h_1()$ | 雜湊函數(值轉值) |
| 11 | $h_2()$ | 雜湊函數(點序列轉值) |
| 12 | $f_{m2p}()$ | 將訊息轉為橢圓曲線點之函數 |
| 13 | $f_{p2m}()$ | 將橢圓曲線點轉為訊息之函數 |
| 14 | $b$ | 盲因子 |
| 15 | $m$ | 明文訊息 |
| 16 | $m_i$ | 明文之分解區塊 |

資料來源：作者整理。

## 二、系統初始階段

系統在有限域 $F_q$ 上選取一條安全的橢圓曲線 $E(F_q)$ ($q$為一個160Bit以上之大質

數)並在$E(F_q)$上選一階數(Order)為$N$的基點$G$，使得$NG=O$，其中$O$為此橢圓曲線之無窮遠點。廠商A、採購中心B、採購機關C分別選擇$n_A,n_B,n_C \in Z_q^*$當成私鑰，產生其他之公鑰。

$$PK_A = n_A.G \quad (1)$$
$$PK_B = n_B.G \quad (2)$$
$$PK_C = n_C.G \quad (3)$$
$$PK_{AS} = n_{As}.G \quad (4)$$

透過一個絕對安全之通道將本身公鑰及身分$id_a,id_b,id_c$送至憑證中心計算出關聯值。

$$e_A = h_1(id_A, PK_A) \quad (5)$$
$$e_B = h_1(id_B, PK_B) \quad (6)$$
$$e_C = h_1(id_C, PK_C) \quad (7)$$

為廠商A、採購中心B、開票中心C、分別選擇$l_a,l_b,l_c$，使$Z_A = l_A G = (x_{z_A}, y_{z_A})$，$Z_B = l_B G = (x_{z_B}, y_{z_B})$，$Z_C = l_C G = (x_{z_C}, y_{z_C})$產生憑證。

$$ca_A = l_A(e_A + x_{z_A}, y_{z_A}) \quad (8)$$
$$ca_B = l_B(e_B + x_{z_B}, y_{z_B}) \quad (9)$$
$$ca_C = l_C(e_C + x_{z_C}, y_{z_C}) \quad (10)$$

憑證中心分別將$ca_A,Z_A,PK_A,PK_{AS}$，$ca_B,Z_B,PK_B,PK_{AS}$，$ca_C,Z_C,PK_C,PK_{AS}$傳回廠商A、採購中心B、採購機關C，系統選擇的一個單向無碰撞雜湊函數$h_1()$及$h_2()$，最後公開$E(F_q),G,\alpha,PK_A,PK_B,PK_C$，$PK_{AS}$，$h_1()$，$h_2()$。

## 三、廠商 A 與採購中心 B 進行（相互驗證身分階段）

當採購中心B收到廠商A所傳過來的$\{ca_A,Z_A,PK_A,PK_{AS}\}$之後，先行驗證身分，確認無誤後才能進行投標，計算如下：

$$u_1 = ca_A^{-1} \bmod \alpha \quad (11)$$
$$u_2 = e_A \times u_1 \bmod \alpha \quad (12)$$
$$u_3 = x_{Z_A} \times u_1 \bmod \alpha \quad (13)$$

接著以憑證中心的公開金鑰來驗證身分之正確性，計算：

$$u_2 G + u_3 PK_{AS} = (v_x, v_y) \quad (14)$$

驗證：

$$x_{Z_A} \overset{?}{=} v_x \quad (15)$$

## 四、廠商 A 與採購中心 B 進行(盲化階段)

廠商A將多份投標文件內容明文訊息分成數個區塊且定義：

$m_{ij}=m_{11},m_{12},...,m_{n1},m_{n2}$，$1\le i\le n$，其中每份文件切割為兩塊，並對明文$m_{ij}$實施雜湊利用明文轉點方式，將明文轉為點座標計算如下：

$$\overline{m_{ij}}=\{m_{11},m_{12},...,m_{n1},m_{n2}\} \tag{16}$$

$$h_1(\overline{m_{ij}})=m \tag{17}$$

$$f_{m2p}(m)=P_1,P_2,...P_n \tag{18}$$

$$\overline{P_i}=\{P_0,P_1,P_2,...,P_n\} \tag{19}$$

$$h_2(\overline{P_i})=M \tag{20}$$

接著廠商A選擇一個盲因子$b$，盲化多個訊息計算如下：

$$m'=b\cdot M\cdot n_A G \tag{21}$$

之後將$\{m'\}$傳給採購中心B。

## 五、廠商 A 與採購中心 B 進行(簽章階段)

當採購中心B收到廠商A所傳送過來的$\{m'\}$後，用自己的公鑰$n_B$對盲化訊息$m'$執行簽章作業，以證明此投標文件為合法有效票，計算如下：

$$s'_m=m'\cdot n_B \tag{22}$$

## 六、採購中心 B 與採購機關 C 進行(相互驗證身分階段)

解開選票前，採購機關C要先和選務中對B做一個驗證身分的動作，確認無誤後才能解開選票，計算如下：

$$u_1=ca_B^{-1}\bmod\alpha \tag{23}$$

$$u_2=e_B\times u_1\bmod\alpha \tag{24}$$

$$u_3=x_{Z_B}\times u_1\bmod\alpha \tag{25}$$

接著以憑證中心的公開金鑰來驗證身分之正確性，計算：

$$u_2G+u_3PK_{AS}=(v_x+v_y) \tag{26}$$

驗證：

$$S_m\overset{?}{=}S_{m'} \tag{27}$$

## 七、採購機關 C 進行(解盲簽章階段)

以自已的私密金鑰$n_C$進行解盲動作，之後對投標文件做一個驗證動作，計算如下：

$$s_m=b^{-1}\cdot s_m{}' \tag{28}$$

$$S_{m'} = b \cdot M \cdot n_B n_C G \quad (29)$$

$$S_m = b \cdot M' \cdot n_B n_C G \quad (30)$$

$$S_m \overset{?}{=} S_{m'} \quad (31)$$

將 $\overline{m_i}'$ 所得到的多重訊息集合，再將多重訊息集合實施一次雜湊 $h_2(\overline{m_i}') = m'$，驗證：

$$m' = m \quad (32)$$

## 安全性分析

本研究之多文件盲簽章機制，其安全性植基於橢圓曲線離散對數難題，使廠商身分、投標文件內容之隱匿性，以多份投標文件內容執行一次盲簽章及加密的方法，解決廠商身分及投標文件內容遭窺探與篡改等問題，可以達到國際標準組織(International Organization for Standardization, ISO)提出資訊的完整性、不可否認性、隱匿性、不可追蹤性、不可偽造性及鑑別性等特性，以下針對本研究之安全性及效益分析進行探討：

### 一、完整性(Integrity)

完整性是指文件在傳遞過程中不能被破壞或干擾，意旨在過程中不能被任意地加入、刪除或修改。在本方法式子(17) $h_1(\overline{m_{ij}}) = m$ 對明文進行雜湊運算得出 $m$，若第三方想要竄改明文偽造 $m$ 而不被發現，則必須面對破解單向雜湊函數的問題及面對橢圓曲線離散對數問題，使得本系統可以得到完整性的確保。

### 二、不可否認性(Non-Repudiation)

不可否認性是指對已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。在盲簽章方面，簽章者簽署完文件後，其他人可以用公式驗證其有效性。如本方法式子(22)中 $s'_m = m' \cdot n_B$

### 三、隱匿性(Anonymity)

隱匿性是指簽章者對簽署的文件內容無法獲知該內容的訊息，本方法式子(21) $m' = b \cdot M \cdot n_A G$ 中有此功能，不必擔憂在簽章過程中造成文件曝光。

### 四、不可追蹤性(Untraceability)

不可追蹤性是指經過加盲的文件，簽章者無法得知真正的內容如式子(21)中 $m' = b \cdot M \cdot n_A G$，因為盲因子「$b$」是隨機的，簽章者僅知道這些資訊是經由自己簽署，此時簽章者與文件脫離了關係，以達到使用階段的匿名效果。

### 五、不可偽造性(Unforgeability)

不可偽造性指的是若攻擊者試圖偽造文件，任何人能夠經由參數驗證得知文件是否偽造；本方法中式子(20) 中 $h_2(\overline{P_i}) = M$，由於 hash 單向雜湊函數有無法逆推的特性，

無法正確的求得資訊或中途遭受第三方所偽造的可能，所以在 Hash 的保護下，偽造有效文件是困難的。

### 六、鑑別性(Authenticity)

鑑別性是指在公開金鑰密碼系統中，使用者的公鑰與密鑰有唯一的對應關係，只有使用者的密鑰才能對應使用者的公鑰。本方法式子(29)(30)(31)中 $S_{m'} = b \cdot M \cdot n_B n_C G$ 、$S_m = b \cdot M' \cdot n_B n_C G$ 、$S_m = S_{m'}$ 。

## 效益評估

依本研究所使用的演算法，與學者Chaum[26]基於RSA的演算法，Mohammed等學者[27]所提出基於ElGamal的盲簽章演算法，以及Jeng等學者[28]提出基於橢圓曲線的盲簽章，比較分析出各個演算法運算所需花費的時間。在比較分析前先定義各種運算符號及各種運算時的相互關係如表三，而模數加法、模數減法運算時間低，予以忽略不計。參酌學者們所提的各階段運算量，由表四說明本研究方法與植基於各系統盲簽章之各階段時間複雜度比較，從表五及圖七中可看出在一份文件至多分文件時，植基於各系統盲簽章之分析比較，也可看出本研究方法在多文件方面是優於其他系統，再針對國軍現行軍事採購與本研究設計之多重文件盲簽章機制，比較兩者之各項安全性及效益性如表六、七。

表三時間複雜度運算之相互關係參考表

| 符號 | 定義 | 相互關係 |
|---|---|---|
| $T_{MUL}$ | 進行一次模式乘法運算所需時間 | $= T_{MUL}$ |
| $T_{EXP}$ | 進行一次模式指數運算所需時間 | $\approx 240 T_{MUL}$ |
| $T_{ADD}$ | 進行一次模式加法運算所需時間 | (可忽略不計) |
| $T_{INVS}$ | 進行一次模式乘法反元素所需時間 | $\approx 240 T_{MUL}$ |
| $T_{ECMUL}$ | 進行一次ECC乘法運算所需時間 | $\approx 29 T_{MUL}$ |
| $T_{ECADD}$ | 進行一次ECC加法運算所需時間 | $\approx 0.12 T_{MUL}$ |
| $T_h$ | 進行一次點Hash所需時間 | $\approx 23 T_{MUL}$ |
| $t_h$ | 進行一次Hash所需時間 | $\approx 1 T_{MUL}$ |

資料來源：蘇品長，〈適用於 Ad Hoc 網路之快速交換金鑰機制設計〉《中正嶺學報》(桃園)，第 37 卷第 1 期，中正理工學院，2008 年，頁 219-228。

[26] 同註 1。
[27] 同註 8。
[28] 同註 9。

表四 本研究方法與植基於各系統盲簽章之時間複雜度比較表

| 演算法 | RSA-Based Blind Signatures (Chaum, 1982) | | ElGamal -Based Blind Signatures (Mohammed et. al., 2000) | | ECDLP-Based Blind Signatures (Jeng et. al., 2010) | | 本研究方法 | |
|---|---|---|---|---|---|---|---|---|
| 比較 | 時間複雜度 | 概估 | 時間複雜度 | 概估 | 時間複雜度 | 概估 | 時間複雜度 | 概估 |
| 金鑰產生 | 2 $T_{MUL}$ + 1 $T_{INVS}$ | ≈242 $T_{MUL}$ | 1 $T_{INVS}$ | ≈240 $T_{MUL}$ | 2 $T_{ECMUL}$ | ≈58 $T_{MUL}$ | 2 $T_{ECMUL}$ | ≈58 $T_{MUL}$ |
| 盲化運算 | 1 $T_{EXP}$ + 1 $T_{MUL}$ | ≈241 $T_{MUL}$ | 1 $T_{EXP}$ + 1 $T_{MUL}$ | ≈241 $T_{MUL}$ | 1 $T_{ECMUL}$ + 1 $T_{MUL}$ | ≈30 $T_{MUL}$ | 1 $T_h$ +2 $t_h$ +1 $T_{ECMUL}$ +1 $T_{MUL}$ | ≈55 $T_{MUL}$ |
| 簽章運算 | 1 $T_{EXP}$ | ≈240 $T_{MUL}$ | 2 $T_{MUL}$ + 1 $T_{INVS}$ | ≈242 $T_{MUL}$ | 2 $T_{ECMUL}$ | ≈58 $T_{MUL}$ | 2 $T_{ECMUL}$ | ≈58 $T_{MUL}$ |
| 解盲運算 | 1 $T_{INVS}$ | ≈240 $T_{MUL}$ | 4 $T_{MUL}$ + 3 $T_{INVS}$ | ≈724 $T_{MUL}$ | 1 $T_{MUL}$ + 2 $T_{ECMUL}$ | ≈59 $T_{MUL}$ | 2 $T_{ECMUL}$ | ≈58 $T_{MUL}$ |
| 驗證運算 | 1 $T_{EXP}$ | ≈240 $T_{MUL}$ | 2 $T_{EXP}$ + 1 $T_{MUL}$ | ≈481 $T_{MUL}$ | 1 $T_{ECMUL}$ +1 $T_{MUL}$ +1 $T_{ECADD}$ | ≈ 30.12 $T_{MUL}$ | 2 $T_{ECMUL}$ +1 $t_h$ | ≈59 $T_{MUL}$ |
| 備註 | 本研究演算法之時間複雜度比前3個演算法效率高。 | | | | | | | |

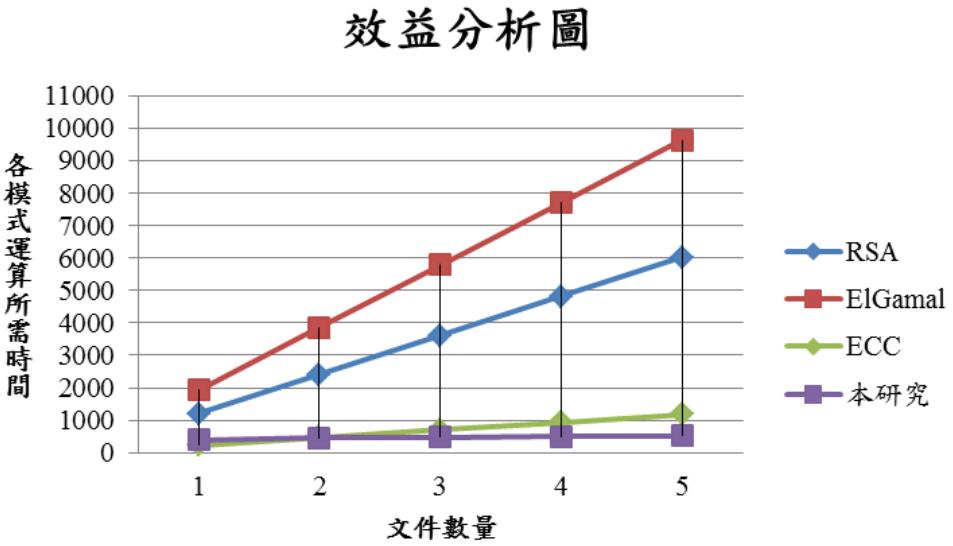
資料來源：作者整理。

表五 本研究方法與植基於各系統盲簽章之文件數量分析比較表

| 演算法 / 文件 | RSA-Based Blind signatures (Chaum, 1982) | ElGamal-Based Blind signatures (Mohammed et. al., 2000) | ECDLP-Based Blind signatures (Jeng et. al., 2010) | 本研究方法 |
|---|---|---|---|---|
| 1 | 1203 $T_{MUL}$ | 1928 $T_{MUL}$ | 235.12 $T_{MUL}$ | 400.12 $T_{MUL}$ |
| 2 | 2406 $T_{MUL}$ | 3856 $T_{MUL}$ | 470.24 $T_{MUL}$ | 449.12 $T_{MUL}$ |
| 3 | 3609 $T_{MUL}$ | 5784 $T_{MUL}$ | 705.36 $T_{MUL}$ | 473.12 $T_{MUL}$ |
| 4 | 4812 $T_{MUL}$ | 7712 $T_{MUL}$ | 940.48 $T_{MUL}$ | 497.12 $T_{MUL}$ |
| 5 | 6015 $T_{MUL}$ | 9640 $T_{MUL}$ | 1175.6 $T_{MUL}$ | 521.12 $T_{MUL}$ |
| 備註 | 文件數量越多，本研究執行時間複雜度相較其他3個演算法越低。 | | | |

資料來源：作者整理。

圖七 本研究方法整體運作效益分析圖




資料來源：作者整理。

表六 本研究方法與現行採購方法之安全性比較表

| 比較項目 | 現行採購方式 | 本研究方法 |
|---|---|---|
| 完整性 | 無法確保文件資料在傳遞過程中是否被竄改。 | 破解本方法必須面對破解單向雜湊函數的問題及橢圓曲線離散對數問題，所以本系統可以得到完整性的確保。 |
| 不可否認性 | 簽章者簽署完多份文件後，僅能用人工方式驗證原份文件之有效性。 | 簽章者簽署完多份文件後，其他人可以用公式驗證其有效性。 |
| 隱匿性 | 易曝露廠商身分及投標文件內容。 | 使用橢圓曲線密碼系統加密，且僅需加密之資訊機密，可減少於有限頻寬內之資訊耗費。 |
| 不可追蹤性 | 須留下廠商基本資料。 | 經過加盲的訊息，簽章者無法得知真正的文件內容，資料隱密性高。 |
| 不可偽造性 | 廠商身分及文件內容因人工作業方式易遭受偽造。 | 因使用 Hash 單向雜湊函有無法逆推的特性，偽造資料是不易。 |
| 鑑別性 | 無 | 使用者的公鑰與密鑰有唯一的對應關係，只有使用者的密鑰才能對應使用者的公鑰，以免黑箱作業。 |

資料來源：作者整理。

表七 本研究方法與現行採購方法之效益性比較表

| 比較項目 | 現行採購方式 | 本研究方法 |
|---|---|---|
| 效率性 | 人工作業，作業時程較長，易發生人為疏失。 | 自動化，作業時程短，省時省事提高工作效率。 |
| 服務時間 | 一般平常上班日 | 24 小時不間斷服務。 |

| | | |
|---|---|---|
| 成本 | 需要龐大人力、繁雜的文書作業往返，花費成本高。 | 線上作業以電子檔為主，簡化行政流程，無需龐大人力及文書紙張，花費成本低。 |

資料來源：作者整理。

## 結論與建議

### 一、結論

(一)謀求建立植基於高困難度破解之多重文件盲簽章機制(安全性)

本研究之設計理論基礎為密碼學領域中之「橢圓曲線密碼系統」與「盲簽章」，謀求建立植基於高困難度破解之多重文件盲簽章機制，達到文件內容具有完整性、不可否認性、隱匿性、不可追蹤性、不可偽造性及鑑別性等效果。

(二)密鑰長度短(安全性及效益性)

利用橢圓曲線其特殊的點加法運算，以及其在同樣安全度之下僅需要較短的密鑰長度，即可加強文件之完整性與安全性。

(三)有別於以往學者探討之盲簽章機制(安全性及效益性)

本研究設計有別於以往學者探討侷限於一次盲簽章，與傳統的一份文件加密一次的方法，結合上述優點提出植基於高困難度之多重文件盲簽章設計，除了可以多重文件盲簽章，也能一次加密多份文件，縮短處理流程進而提升執行時效率，避免重複性的繁雜運算與大量時間耗費，進而達到提升作業效率與安全性目的。

(四)國軍電子化採購改良

軍事採購係以支援國軍建軍備戰重要的手段，也是國防裝備獲得主要管道之一。在目前嚴峻的經濟環境中，且面對日益緊縮的國防預算下，若發生採購弊端，將嚴重損害國家資源預算，延遲國軍取得所需之裝備，並有損人民對國軍的信賴，這些後果往往損及國防效能，進而使得國家安全遭到威脅。因此，強化軍事採購作業，減少弊端，俾能提升整體戰力；而本研究則是以國軍電子採購系統為探討對象，利用橢圓曲線密碼系統較少的位元數達到相同的安全等級，應用多重文件盲簽章機制，以橢圓曲線密碼學為理論基礎，期能建立一個「公開、透明」及安全的國軍電子化採購系統，貫徹依法行政，達到廉節軍風及支援建軍備戰之目標。

### 二、建議

本研究盲簽章之設計在未來軍事運用上，可以往國軍線上電子投票及國軍網路申訴系統進行探討，藉由它的特性可以改善軍事運用上長期無法改善之隱私性保障。

(一)國軍線上電子投票進行探討

本研究盲簽章之設計在未來軍事運用上，可以探討國軍線上電子投票機制，因應本國未來多合一選舉的趨勢，如何降低選舉所耗費的社會資源，並解決國軍在選舉期

間基於保家衛國的重責大任，總會有些駐守外地或堅守崗位的國軍弟兄無法返回戶籍投票，運用此方式將可解決國軍因戰備留守而無法返鄉實施投票，導致喪失投票權的問題。[29]

(二)國軍網路申訴系統探討

發展國軍網路申訴系統，需考量如何有效保護當事人的隱私，避免資料洩露，造成困擾。而導入此機制，將有利促進網路申訴制度的發展及可信賴度，提高使用意願，降低體制外之爆料文化，提升國軍整體形象，避免內部監察行政資源之不必要耗損。[30]

## 參考文獻


一、 李南逸、王智弘、林峻立、張智超、溫翔安、葉禾田，《網路安全與密碼學概論》(台北：東華書局，2014 年)。

二、 肖攸安，《橢圓曲線密碼體系研究》(華中科技大學出版，2006 年)。

三、 王保倉、韋永壯、胡予濮，〈基於隨機背包的公鑰密碼〉(電子與訊息學報)，第 32 卷第 7 期，2010 年。

四、 王蕙譽，〈以比特幣為基礎建構兼具公平交換和客戶匿名特性之數位內容線上交易協定〉，國防大學資訊管理學系研究所碩士論文，2017 年。

五、 李瑋豪，〈具不可追蹤之多重文件盲簽密機制〉(國防大學資訊管理學系研究所碩士論文，2014 年。

六、 高嘉言，〈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，2009 年。

七、 郭文雄，〈設計具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，2010 年。

八、 葉家維，〈設計具多重難度之混合式公開金鑰密碼系統〉，國防大學資訊管理學系研究所碩士論文，2018 年。

九、 黃智賢，〈創新金融服務行動支付模式對顧客線上消費行為之影響〉(國防大學資訊管理學系研究所碩士論文，2017 年。

十、 謝定芳，〈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〉，國防大學資訊管理學系研究所碩士論文，2017 年。

十一、 蕭雅尹，〈強化國軍通資系統安全之金鑰交換機制設計〉，國防大學資訊管理學系研究所碩士論文，2018 年。


[29] 李瑋豪，〈具不可追蹤之多重文件盲簽密機制〉，國防大學資訊管理學系研究所碩士論文，2014 年，頁 64-65。

[30] 郭文雄，〈設計具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，2010 年，頁 43-72。

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

十三、蘇品長，〈適用於 Ad Hoc 網路之快速交換金鑰機制設計〉《中正嶺學報》(桃園)，第 37 卷第 1 期，中正理工學院，2008 年。

十四、〈國防部軍備局〉《軍事機關採購作業規定》，2003 年。

十五、Chaum, D.,“ Blind signatures for untraceable payments,” In Proceedings of Advances in Cryptology-CRYPTO, 1982.

十六、Diffie,W,and Hellman,M.e., “New Directions in Cryptography,” IEEE Transactions on Information Theory, IT-22(6), 1976.

十七、Fan,C.I.,and Chen,W.K.,“An Efficient Blind Signature Scheme for Information Hiding,”International Journal of Electronic Commerce, Vol.6, No.1, 2001.

十八、Ibrahim,S.,Kamat,M.,Salleh,M.,and Aziz,S.R.A.,“Secure E-voting with Blind Signature,” Proceedings of 4th National Conference on Telecommunication Technology, 2003.

十九、Jeng,F.G.,Chen,T.L.,and Chen,T.S., “An ECC-Based Blind Signature Scheme, ” journal of networks, Vol. 5, No.8, 2010.

二十、Koblitz,N.,1987, “Elliptic Curve Cryptosystems, ” Mathematics of Computation American Mathematical Society,Vol.48, 1987.

二十一、Miller,V.S., “Use of Elliptic Curve in Cryptography”,Advance in Cryptography Crypto, 1985.

二十二、Mohammed,E.,Emarah,A.E.,and Shennawy,K.E.,“A blind signatures scheme based on ElGamal signature,” IEEE/AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security, 2000.

二十三、Nakanishi,T.,and Sugiyama,Y., “Unlinkable Divisible Electronic Cash,” Proceedings of 3rd International Workshop on Information Security, 2000.

## 作者簡介

梁榮哲少校，國防大學管理學院正資管系 51 期 97 年班、國防大學管理學院資管所 101 年班、陸軍通信電子資訊訓練中心通資電正規班第 187 期，曾任區隊長、隊長、通信官、作戰官、人事官、教官，現任陸軍通信電子資訊訓練中心一般指參組教官。