強化國軍電子採購業務
－具自我認證暨多文件盲簽章機制之設計

蘇品長[1]　蕭柏薰[2]　陳明心[3]

[1, 3]國防大學資訊管理學系　[2]國防部訓練參謀次長室

論文編號：3502-7
收稿 2014 年 10 月 14 日 → 第一次修訂 2014 年 11 月 05 日 → 同意刊登 2015 年 02 月 04 日

摘要

現行國軍所使用的電子化採購系統雖說已完成電子化的初步目標，但距離真正的全面使用電子化尚有努力的空間，其原因不外乎安全性的考量。由於電子資料必須在網際網路上進行處理、儲存，可能提高資料外洩風險帶來的疑慮，本文以密碼學理論為基礎，強化國軍電子化採購系統的安全性，並導入自我認證之多重文件盲簽章機制來強化目前採購系統上的安全疑慮，避免製發憑證的過程中會有偽冒用戶身分的安全弱點，同時也可以降低公鑰儲存、計算與管理的成本與風險；本研究的具體優點為有效的減少盲簽章次數、簡化傳輸作業時間及多重盲簽章手續，強化廠商身分認證及投標文件內容遭窺探與篡改等安全問題。

關鍵詞：軍事採購、橢圓曲線密碼系統、盲簽章、自我認證機制

Strengthen the Military E-Procurement－Design of Self-Certified and Multi-Document Blind Signature Schemes

Pin-Chang, Su [1]　Po-Hsun, Hsiao [2]　Ming-Hsin, Chen [3]

[1, 3] Department of Information Management, National Defense University, Taiwan, R.O.C

[2] Office of Deputy Chief of General Staff for Training, Ministry of National Defense, Taiwan, R.O.C

Abstract

Although the military e-procurement system has reached the beginning goal of the electronic, but still have efforts to achieve comprehensive utilizes. The reason is the security consideration. Electronic data processed and stored on the Internet may increase the risk of data leakage. The study based on cryptography theory to enhance the security of military e-procurement system, and further to induce self-certified Multi-document blind signature scheme to mitigate the security concerns on the current procurement system and to avoid the counterfeiting user identity weakness of issue certificate process. At the same time, it can also reduce the cost and risks of public key storage, computation and management. Our study is not only to reduce blind signature times, to simplify the transmission time and multiple blind signature operation, but also solves the snooping and tampering problems of identification and document.

Keywords: Military procurement, Elliptic Curve Cryptosystem, Blind signature, Self-certified scheme.

壹、前言

我國政府於民國 87 年制定了政府採購法，建立一套標準化採購作業程序，以確保採購品質及效率，而隨著採購法的施行，國軍除依政府採購法、政府採購法施行細則及有關法令之規定外，亦依「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」、「履約驗結」等三階段執行，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，俾利支援國軍建軍備整的需求，並落實國家安全為目標。但重於防止舞弊，也因此而衍生出相關多作業流程，就採購效率而言，浪費更多的人力資源及時間成本。

隨著網路科技日新月異，造就所謂的資訊時代來臨，網際網路對於各大企業營運、政府政策以及一般民眾的日常生活帶來的重大影響，政府為了能夠讓民眾更容易取得政府所提供的資訊與服務，正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，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。但由於電子資料必須在網際網路上進行處理、儲存，可能提高資料外洩帶來的風險，而國軍採購通常涉及龐大金額，易引起心懷不軌的人在中途攔截，因此在廠商在進行投標作業傳遞資料時可能遭受竊取、篡改等資安問題的發生，而造成廠商身分及投標文件內容洩漏，發生不法情事。如何有效保護廠商身分隱密性及投標文內容的機密性，便成為值得深思的議題。

目前電子化採購系統運用 RSA 演算法、電子憑證(CA)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，也會很容易地洩露使用者的身分。以實作 RSA 公開金鑰系統為例，若某銀行欲對一個訊息 m 進行簽章以認定其為有效的電子現金，因此可利用雜湊函數計算出訊息雜湊值的簽章。當商店送來卻結算存入帳戶的電子現金時，銀行能將所紀錄的訊息 m 和使用者識別資訊進行比對，就能輕易瞭解及追蹤使用者的消費行為(蘇品長，2008)，另現今採購系統在設計配發電子憑證(CA)上大多採用以公正的第三方為基礎的方式來執行身分安全認證事宜，但這個先決條件必須是這個系統認證中心是安全且可靠的，不會有偽冒使用者的金鑰之行為發生，這此因素都將會增加使用者對於傳送資料文件及存放安全產生疑慮，而且目前在採購系統作業上大多是採用一個標項文件就必須加密一次，一個標案有多份標項文件就必須多次加密作業，造成作業程序繁雜。有鑑於此，本研究以基於橢圓曲線密碼學為理論基礎，應用具自我認證之多重文件盲簽章機制(蘇品長，梁榮哲，2011)，可以避免製發憑證的過程中會有偽冒用戶身分的安全弱點，同時也可以降低公鑰儲存、計算與管理的成本與風險；並能以多份投標文件項目執行一次盲簽章及加密的方法，將多文件的資訊藉由混淆機制，將其變成一份密文來傳送，直接增加密文破解的難度，進而提高網路傳送資訊更高的安全性，將它應用於軍事電子化採購作業，以確保廠商身份不被偽冒及進行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。

貳、軍事採購概述

一、軍事採購

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、履約驗結階段等三階段編組執行，依據 100 年國防報告書，自民國 99 年起至民國 100 年 5 月為止，國軍各級機關辦理採購作業計有 1 萬 4 千餘件，金額更達新臺幣 2 千餘億；如此龐大的金額，易引起心懷不軌的人貪念，所以如何精進軍事採購作業安全則相對重要，其採購流程如圖 1(軍備局，2003)。

圖 1　採購流程圖

二、軍事電子化採購作業流程

將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，步驟過程說明如后：

(一)註冊作業(申請憑證)：

廠商自行註冊加入會員，再相關文件送至認證中心(國防部認證中心，規劃建置中)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(CA)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，及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圖詳如圖 2 所示。

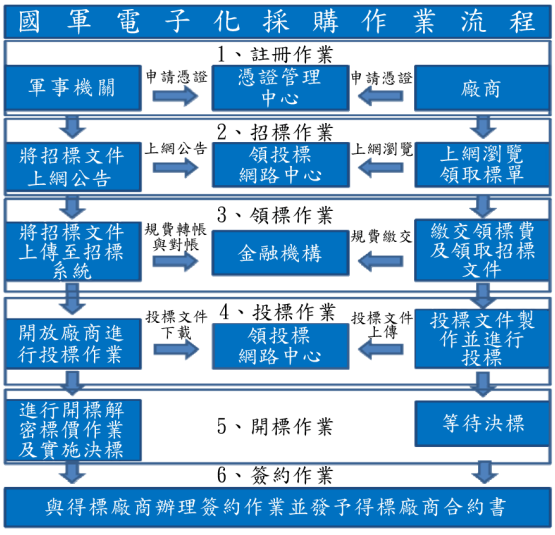

圖 2　軍事電子化採購作業流程

參、密碼學技術應用

一、電子簽章法

政府為推動電子交易普及化，及確保相關電子交易安全，於民國 90 年 11 月 14 日制定此法。相關用詞定義如下：

(一) 電子簽章：指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。

(二) 數位簽章：指將電子文件以數學演算法或其他方式運算為一定長度之數位資料，以簽署人之私密金鑰對其加密，形成電子簽章，並得以公開金鑰加以驗證者。

(三) 加密：指利用數學演算法或其他方法，將電子文件以亂碼方式處理。

(四) 憑證：指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。

二、橢圓曲線公開金鑰密碼系統

自從 Miller (1985)與 Koblitz (1987)兩位學者分別提出利用橢圓曲線來實作公開金鑰密碼系統，發展出一套能提供與 RSA (Rivest, Shamir and Adleman)及 ELGamal 非對稱式金鑰密碼系統相同安全強度且所需要金鑰長度卻較短的橢圓曲線密碼系統。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 是實數。在橢圓曲線中，點加法運算是經過特別定義的，除此之外，也另外定義一個無窮遠點 O，對任一點 $A\in E$，$A+O=O+A=A$。

橢圓曲線定義(肖攸安，2006)：令 p 是大於 3 的質數，在 $GF(p)$ 中的橢圓曲線 $E: y^2=x^3+ax+b \bmod p$，其中 $4a^3+27b^2\neq 0(\bmod p)$。而此橢圓曲線群 $GF(p)$ 中的點加法運算定義為如下：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 $x_3=\lambda^2-x_1-x_2$，$y_3=\lambda(x_1-x_3)-y_1$。

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

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要較小的密鑰長度，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，詳如表 1 (蘇品長，2011)。

表 1　RSA 與 ECC 之金鑰長度比較表

RSA 與 ECC 在相同安全度下金鑰長度之比較					
長度 / 項目	金鑰長度(bits)				
RSA	512	1024	2048	3072	7680
ECC	112	163	224	256	384
Key	1:5	1:6	1:9	1:12	1:20

三、盲簽章

Chaum (1982)利用 RSA 的方法提出盲簽章機制，主要概念有兩個重要的特性：送簽章者將先作盲化後將訊息傳遞給簽章者作簽章時不會洩漏文件內容，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。電子匿名投票選舉即是利用這個方法確保投票者的身分達到隱匿效果運用，密碼學中數位簽章之特性，使用公鑰與私鑰的特性對訊息做加密、解密，做為送簽者與需求者間確認之用。例如，投

票人(送簽者)請選委會(簽章者)在一封經彌封的選票信件上蓋鋼戳，鋼戳的戳記印痕會經由外層的信封複印至內層的選票，以證明此選票之合法性戳記，再將內含選票信件回覆給合法身分的投票人，投票人收到蓋有戳記的選票後，先檢查信封是否仍處於彌封狀態，再將選票自信封中取出，此選票帶有選務中心鋼戳的戳記，以證明此張選票之合法性。投票人在此選票上自行圈選後寄往開票中心，但該選票上不會記錄投票人身分或地址，如此完成匿名投票的步驟。而盲簽章演算法流程如圖3 (楊倫青，2011)。

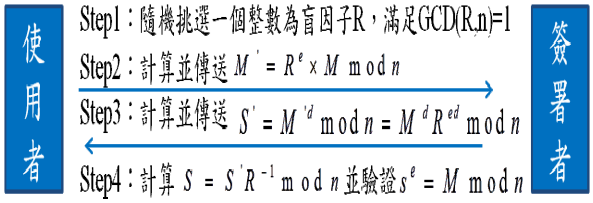

圖 3　盲簽章流程關係圖

四、數位簽章演算法

1991年，美國NIST (National Institute of Standard and Technology) 公佈DSA (Digital Signature Algorithm)為國家數位簽章標準。DSA公佈後，雖引發以下爭議，但業界及學界仍是接受此一標準：

（一）DSA不能用來做加密或金鑰分配之用，只能用來做數位簽章。

（二）DSA是由美國國家安全局(NSA)所發展出來的一種 ElGamal 數位簽章法的變形，普遍上使用者仍是存有疑慮而擔心NSA藏有暗門(trapdoor)設計，並不像 RSA 或 ElGamal 數位簽章法是由學術界人士所設計出來的而較能信任。

（三）DSA的計算速度比 RSA 要來得慢。DSA 所需簽署時間與 RSA 大約相同，但所需驗證簽章的時間要比 RSA 慢約10至40倍。

（四）RSA雖然不是政府頒布的一項標準(牽涉到專利的問題)，但是全世界的使用者早已將之視為一項重要的數位簽章標準來使用。

以下介紹DSA的系統公開參數、金鑰產生、簽署程序，與驗證程序：

Step1：系統公開參數

p：512 至 1024 位元的大質數

q：160 位元的 $p-1$之質因數 1

e_1：$e_1 = w^{(p-1)/q} \bmod p$ ，其中 $w < p-1$且$w^{(p-1)/q} \bmod p > 1$

h：一個單向雜湊函數(one-way hash function)，輸出值為 160 位元

註：搭配DSA的單向雜湊函數標準SHA-1(Secure Hash Algorithm)

Step2：金鑰產生

每一個使用者任選一個整數 $d \in Z_q$ 為私鑰，並計算公鑰 $e_2 = e_1^{\,d} \bmod p$ 。

Step3：簽署程序(欲簽署訊息為M)

任選一數 $r < q$ 。

計算 $S_1 = (e_1^{\,r} \bmod p) \bmod q$ 。

計算 $S_2 = r^{-1}(h(M) + dS_1) \bmod q$ 。

(S_1, S_2) 為M的數位簽章。

Step4：驗證程序

計算下列各數

$a = S_2^{-1} \bmod q$

$b = ah(M) \bmod q$

$c = S_1 a \bmod q$

$V = (e_1^{\,b} \times e_2^{\,c} \bmod p) \bmod q$

若 $V = S_1$，則 (S_1, S_2) 通過驗證。

圖4為數位簽章演算法示意圖：

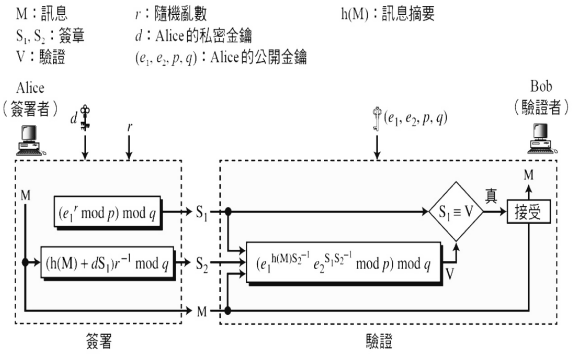

圖4 數位簽章演算法

五、自我認證公開金鑰密碼系統

Girault 於 1991 年提出公開金鑰密碼系統下的自我認證機制(Self-certified Scheme)，目的在授權階段可由使用者參與公鑰的計算；而使用階段可以獨立進行身分自我認證，而不需再透過公證第三方的身分認證的演算法。自我認證機制不但可以避免一般憑證中心(CA)在憑證製發的過程中，因憑證中心代替用戶選定私鑰，而會有憑證中心偽冒使用者身分的能力的隱憂；同時可以降低整體認證系統在公鑰儲存、計算與管理的成本與風險。它具有較高的安全性、較低的管理負擔以及完成身分認證的高效率特性，特別適合應用在點對點網路或是無線網路的環境(胡國新，2001)。針對公開金鑰密碼系統安全性，Girault(1991)提出三個層次安全等級如表 2。

表 2　Girault 公鑰系統三個層次安全等級

安全等級	說明	應用案例
Level 1	憑證中心知道所有使用者的私密金鑰與公開金鑰，而且在任何時候都可以偽冒任一個使用者而不被發現。	以身分為基礎的認證系統
Level 2	憑證中心不知道使用者的私密金鑰，但卻可以伺機偽造出一個不合法的使用者而不易被發現。	電子憑證之認證系統
Level 3	1.使用者的私鑰是自行選定的，認證中心須由使用者傳送過來的參數資料才能計算其公鑰，故認證中心不能自行產生甚至是偽照使用者的公鑰。 2.使用者會自行驗算認證中心所傳來的公鑰之正確性，認證中心無法主導使用者公鑰之產生及驗證。	自我認證公開金鑰密碼系統

肆、強化國軍電子採購業務－具自我認證暨多文件盲簽章機制之設計

設計多重文件盲簽章之機制，有別於以往學者之盲簽章侷限於一次盲簽章一份文件的傳統方法，達到文件內容具有完整性、機密性、鑑別性、不可否認性、隱匿性、不可追蹤性等需求，並利用橢圓曲線其特殊的點加法運算及其在同樣的安全度之下僅需要較小的密鑰長度，除增加密文之混淆度，可加強密文之完整性與安全性，因此本研究提出一種植基於橢圓曲線離散對數的具自我認證之多重盲簽章機制可適用於國軍事電子化採購方案中，在本研究中先讓雙方自我認證以確保雙方身分不被偽冒及改善以往一次盲簽章機制，改進成多重盲簽章之概念，這項創新機制的導入 Level 3 安全等級的自我認證及縮短系統在作業處理時多餘程序進而提升執行時的效率。本系統中的盲簽章特性，可彈性選擇所要之盲簽章數量，而所使用的機制是基於橢圓曲線具有金鑰長度短、處理速度快且安全性高的特性，使系統達到更快且更安全的運作，可增加簽章破解的困難度。其次，橢圓曲線公開金鑰密碼系統在相同安全度下所使用的加密金鑰長度較其他公開金鑰密碼系統小且處理速度較快，使得橢圓曲線密碼系統具有更高的安全性。此外在自我認證方面在使用階段可以獨立進行身分自我認證，而不需再透過公證第三方的身分認證的演算法，所以自我認證機制不但可以避免一般 CA 憑證製發的過程中，因憑證授權中心代替用戶選定私鑰，而會有憑證中心偽冒使用者身分的能力的隱憂；同時可以降低整體認證系統在公鑰儲存、計算與管理的成本與風險，使它具有較高的安全性、較低的管理負擔以及完成身分認證的高效率特性。本研究整體運作示意循序圖如圖 5。

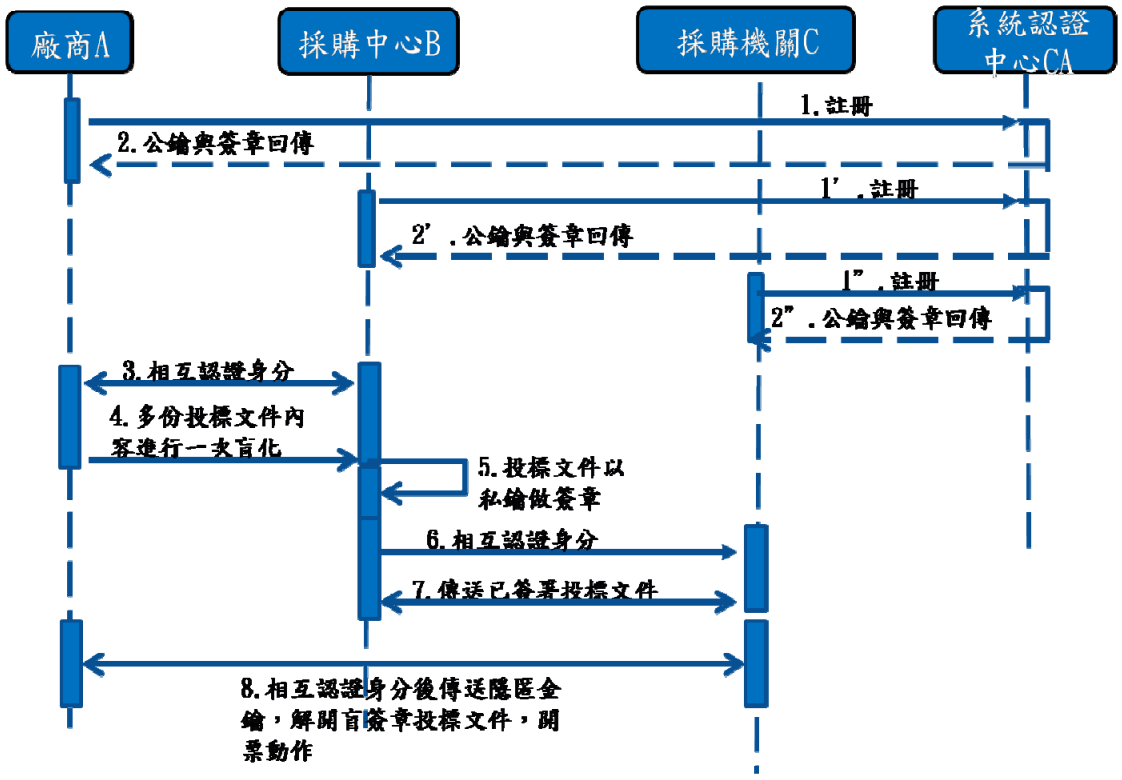

圖 5　本研究整體運作示意循序圖

本章設計的系統演算法共分成八個階段，分別為系統參數符號說明、系統初始階段、廠商與採購中心相互驗證階段、訊息盲化階段、簽章階段、採購中心與採購機關相互驗證階段、解盲簽章階段、驗證階段，各階段的詳細作法描述如下：

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 3 所示：

表 3 系統使用符號之說明

項目	符號	說明	備註
1	CA	系統認證中心	
2	$E(F_q)$	有限域 F_q 中的一條橢圓曲線	
3	G	橢圓曲線中的基點	
4	n	橢圓曲線上基點的秩(order)	
5	q	$q>2^{160}$ 之質數	
6	id_a, id_b, idc	廠商 A、採購中心 B、採購機關 C 的 ID 資訊	
7	PK_{CA}、sk_{CA}	CA 的公鑰與私鑰	
8	PK_n	系統內各成員與 CA 完成註冊所取得的驗證公鑰	
9	$sk_A, sk_B\ sk_C$	廠商 A、採購中心 B、採購機關 C 所選擇之私鑰	
10	S_A、S_B、S_C	廠商 A、採購中心 B、採購機關 C 之公開金鑰	
11	w_n	計算出的簽章	
12	V_n	註冊申請的簽章	
13	e_n	本身資訊求得之雜湊值	
14	$h_1( )$	雜湊函數(值轉值)	
15	$h_2( )$	雜湊函數(序列點轉值)	
16	$f_{m2p}( )$	將訊息轉為橢圓曲線點之函數	
17	$f_{p2m}( )$	將橢圓曲線點轉為訊息之函數	
18	t_n	成員所選擇之時間戳記	
19	m	明文之分解區塊	
20	β	將明文雜湊函數(點序列轉值)後的值	
21	r_A、k_A	廠商、CA 之隨機秘密參數	
22	$h()$	CA 公開之雜湊函數	
23	$\bar{z} = \{z_1, z_2, ..., z_i\} \in (0,1)$	1 代表右旋一個區塊，0 代表左旋一個區塊	
24	$\overline{C_i}$	n 份密文文件	

二、系統初始階段

Setp1：系統認證中心(CA)系統建置階段

首先系統在有限域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。系統選擇的一個單向無碰撞雜湊函數h()，計算公開金鑰。

$$PK_{CA} = sk_{CA} \cdot G \tag{1}$$

最後公開$E, G, q, PK_{CA}, h()$。

Setp2：各方成員註冊階段

以廠商A為例；廠商以自己的id_A及選擇隨機秘密參數值$r_A \in [2, n-2]$，以r_A產生簽名檔V_A後，再將id_A與V_A傳給CA，V_A計算如下：

$$V_A = h(r_A \| id_A) \cdot G \tag{2}$$

CA選擇隨機秘密參數值$k_A \in [2, n-2]$計算廠商之公鑰PK_A及簽章w_A後傳給廠商計算如下：

$$PK_A = V_A + (k_A - h(id_A)) \cdot G = (q_{Ax}, q_{Ay}) \tag{3}$$

$$w_A = k_A + sk_{CA}(q_{Ax} + h(id_A)) \tag{4}$$

廠商利用CA傳回來的參數(公鑰PK_A及簽章w_A)，自己計算產生私鑰sk_A並且用簽章w_A驗證公鑰PK_A的正確性，計算如下：

$$SK_A = [\ W_A + h(r_A \| id_A)\ ] \tag{5}$$

廠商A計算其公開金鑰S_A：

$$S_A = sk_A \cdot G \tag{6}$$

各方成員與CA註冊程序如上，一旦所有成員(n)與CA認證中心完成註冊並取得屬於自己的公鑰PK_n及簽章w_n後，可自行計算私鑰與驗證公鑰的正確性，並可憑(id_n、PK_n、S_n)與需認證身分的通訊方進行認證，而不在需要CA替雙方執行身分認證工作。系統初始階段循序圖如圖6所示。

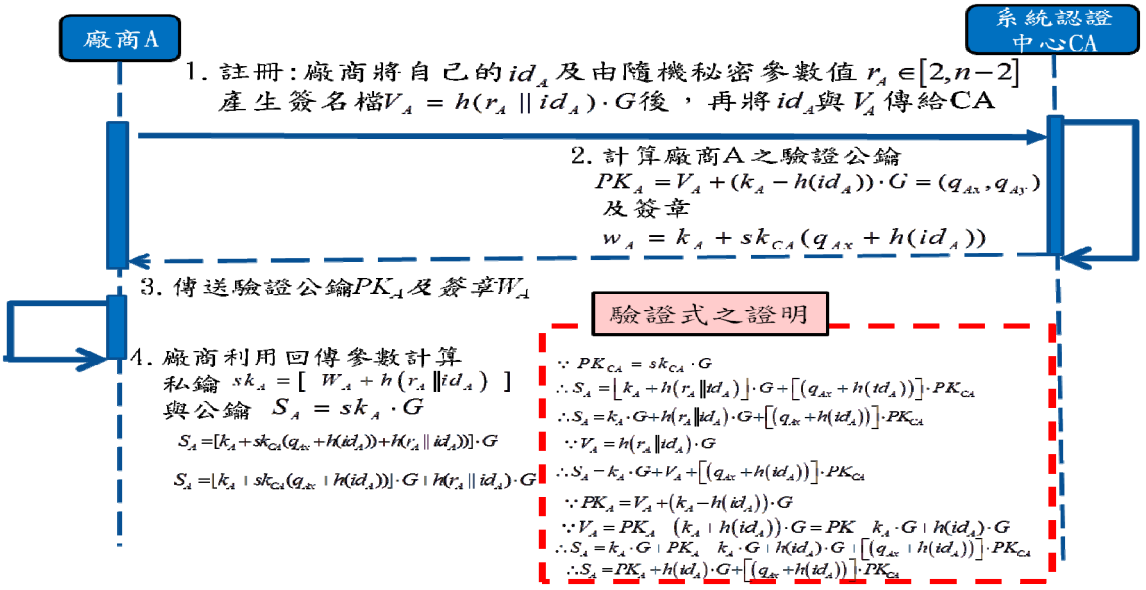

圖6 初始階段廠商註冊循序圖

三、廠商 A 與採購中心 B 進行(相互驗證階段)

廠商A與採購中心B自CA取得合法認證身分後，在進投標前可憑CA核發之身分參數資料互相身分驗證，相互確認(id_A、PK_A、S_A)及(id_B、PK_B、S_B)是否正確，採購中心驗證廠商檢察式如下：

$$S'_A = PK_A + h(id_A)\cdot G + \left[\left(q_{Ax} + h(id_A)\right)\right]\cdot PK_{CA} \quad (7)$$

$$S'_A \overset{?}{=} S_A \quad (8)$$

接著以憑同理，廠商也可驗證採購中心：

$$S'_B \overset{?}{=} S_B \quad (9)$$

廠商 A 與採購中心 B 進行相互驗證循序圖如圖 7 所示：

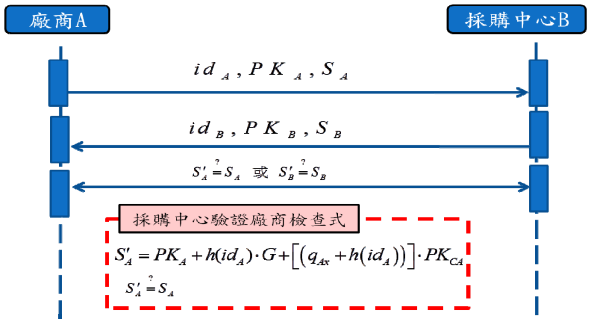

圖 7 廠商與採購中心相互驗證循序圖

四、廠商 A 與採購中心 B 進行(盲化階段)

如果雙方驗證對方身分正確無誤之後，廠商A將多份投標文件內容明文訊息分成數個區塊，其中每份文件各切割為兩塊，並對明文實施雜湊　並利用明文轉點方式將轉為點座標計算如下：

$$m=(m_{11}\|m_{12}\|m_{21}\|m_{22},...,m_{n1}\|m_{n2}), i=1,...,n, j=1,2 \quad (10)$$

$$h_1(m) = \alpha \quad (11)$$

$$f_{m2p}(m) = P_1, P_2, ...P_n \quad (12)$$

定義 $\bar{z} = \{z_1, z_2, ..., z_i\} \in (0,1)$ 算出 k，以二進位表達 k 值。

$$k=\left\{z_1 2^{i-1}, z_2 2^{i-2}, z_3 2^{i-3}, ..., z_i 2^0\right\} \in (0,1) \quad (13)$$

接著進行加密運算，利用明文轉點方式 $f_{m2p}(k,m)$ 將 k 值以十進位表示轉成點座標 P_i，實施加密的動作，C_i 為加密後的投標文件訊息，計算如下：

$$C_i = P_i + z_i \cdot C_{i-1} + sk_A \cdot PK_C, \quad 2 \le i \le r \quad (14)$$

$$\overline{C_i} = (C_1, C_2, ..., C_n) \quad (15)$$

$$h_2(\overline{C_i}) = \beta \quad (16)$$

而廠商A選擇一個時間戳記 $t_A \in Z_q$ 與以本身資訊求得之雜湊值 e_A 與時間戳記做為盲因子，及採購機關C公鑰 PK_C 對訊息 β 進行盲化動作，計算：

$$\beta' = e_A \cdot t_A \cdot \beta \cdot PK_C \quad (17)$$

之後將 $\{\overline{C_i}, \beta'\}$ 傳給採購中心 B。盲化階段循序圖如圖 8 所示：

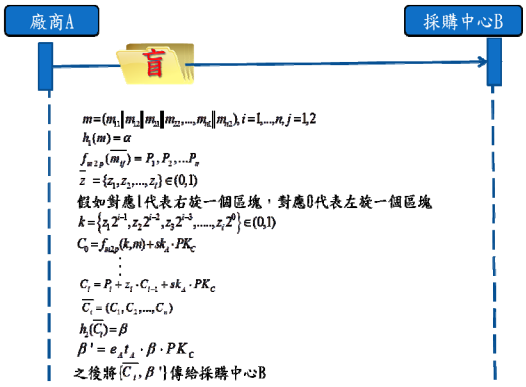

圖 8 盲化循序圖

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所傳送過來的後$\{\overline{C_i}, \beta'\}$，以其私鑰$sk_B$對盲化訊息$\{\beta'\}$執行簽章作業，以證明此投標文件為合法有效票，再用私鑰sk_B加密於採購機關C公鑰，計算如下：

$$S'_\beta = \beta' \cdot sk_B \tag{18}$$

$$PK'_C = sk_B \cdot PK_C \tag{19}$$

之後將$\{\overline{C_i}, S'_\beta, PK'_C\}$傳送給採購機關C。採購中心B簽章循序圖如圖9所示：

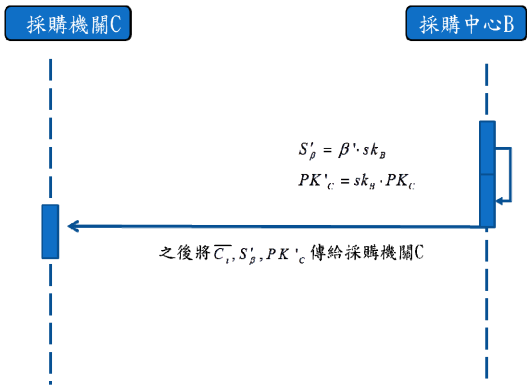

圖 9　簽章循序圖

六、採購中心 B 與採購機關 C 進行(相互驗證身分階段)

開標前，採購機關C要先和採購中心B做一個驗證身分的動作，確認無誤後才能解開標單，採購中心B與採購機關C相互驗證循序圖如圖10所示：

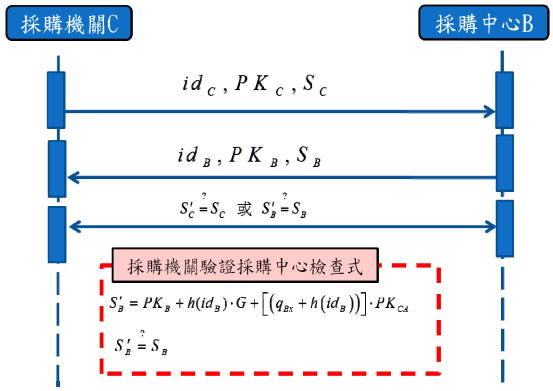

圖 10 採購機關與採購中心相互驗證循序圖

七、採購機關 C 進行解盲簽章(驗證階段)

採購機關C收到採機中心所傳送過來的$\{\overline{C_i}, S'_\beta, PK'_C\}$，進行解盲簽章程序，需自廠商A取得$t_A$、$e_A$盲因子，故採購機關C須與 廠商A相互驗證，如果驗證無誤，採購機關C與廠商A計算雙方共同隱匿金鑰X_{AC}，計算式如下：

Setp1：廠商A以時間戳記t_A，計算出R_A並傳給採購機關C，計算如下：

$$T_A = t_A \cdot G \tag{20}$$
$$\because S_A = sk_A \cdot G$$
$$\therefore X_{AC} = sk_A \cdot S_C = sk_C \cdot S_A$$
$$\therefore R_A = X_{AC} + T_A$$

Setp2：採購機關C以所獲得資訊求得t_A及e_A，計算如下：

$$\because R_A = X_{AC} + T_A$$
$$T_A = X_{AC} - R_A \tag{21}$$
$$t_A G = (sk_A \cdot sk_C) \cdot G - R_A \tag{22}$$

採購機關C以(R_A, PK_A, PK_C)求得t_A及$e_A = h(PK_A, ID_A)$

Setp3：採購機關 C 以自己的私密金鑰sk_C及t_A^{-1}與e_A^{-1}解開自採購中心 B 傳來的盲化隱匿投標文件S'_β，之後對投標文件做一個簽章驗證動作，將採購中心送來的PK'_C進行驗證簽章是否是採購中心 B 所簽署的，計算如下：

$$s_\beta = e_A^{-1} \cdot t_A^{-1} \cdot \beta' \cdot PK_C \cdot sk_B \tag{23}$$
$$PK'_C \stackrel{?}{=} S_\beta \tag{24}$$

簽章驗證循序圖如 11 所示：

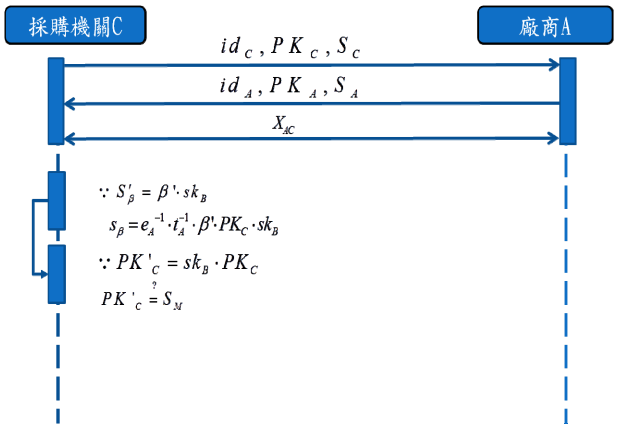

圖 11 簽章驗證循序圖

八、採購機關 C 進行開標(解密階段)

接著將簽章過的加密投標文件進行解密動作，計算如下：

$$f_{m2p}(k,m)=C_0-(PK_A\cdot sk_C)=C_0-(sk_A\cdot PK_C) \quad (25)$$

$$(k,m)=f_{p2m}\left[f_{m2p}(k,m)\right] \quad (26)$$

接著將k還原成$\bar{z}$數列，將其二進位表示的k值，計算如下：

$$k=\bar{z}=\{z_1,z_2,...,z_i\}\in(0,1) \quad (27)$$

$$P_i'=C_i-z_i\cdot C_{i-1}-sk_A\cdot PK_C \quad (28)$$

將點P_i'轉回訊息：$P_i'=\{P_1,P_2,...,P_n\}$，i=1,2,…n。

$$f_{p2m}(P_i')=m'=(m_{11}\|m_{12}\|m_{21}\|m_{22}...\|m_{n1}\|m_{n2})$$

，i=1,2,…,n，j=1,2 (29)

對明文m'做雜湊值運算$h_2(m')=\alpha'$，驗證

$$\alpha' \stackrel{?}{=} \alpha \quad (30)$$

若等式成立則確認收方所收之訊息正確無誤。採購機關C進行開標，解開密文文件循序圖如12所示：

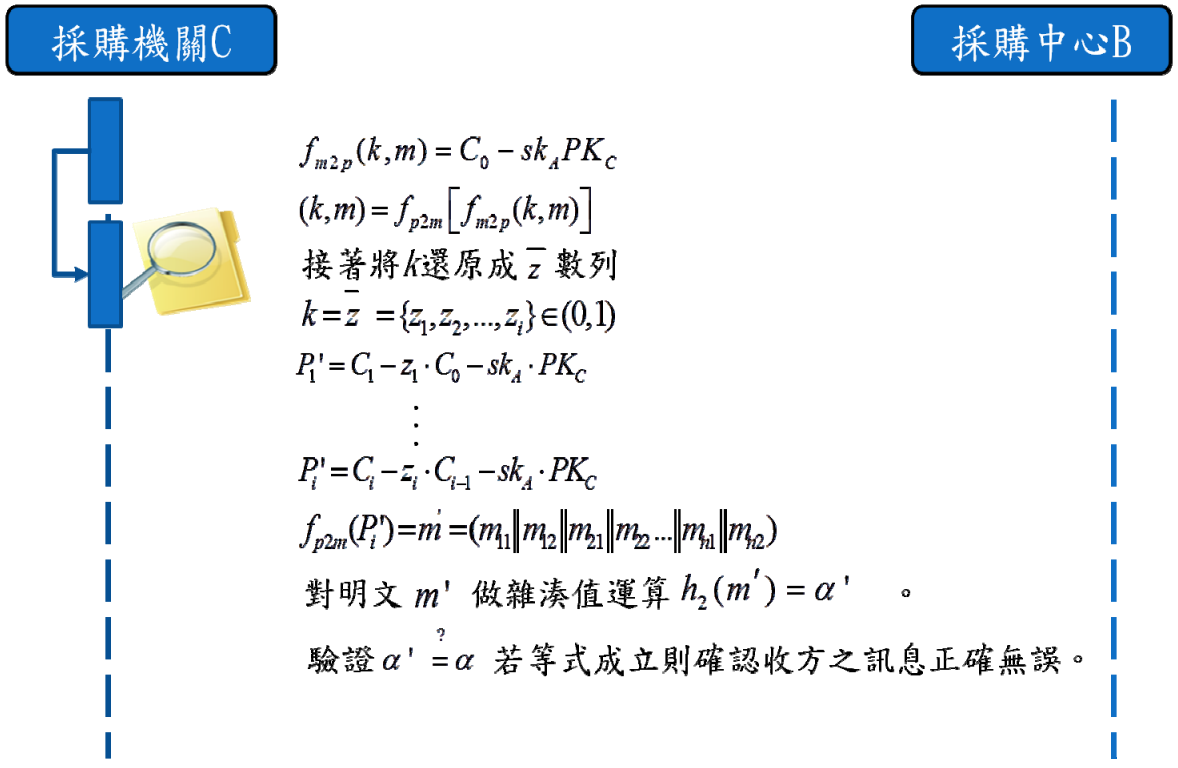

圖 12 解開密文循序圖

伍、安全性及效益分析

以密碼學理論為基礎，導入具自我認證之多重文件盲簽章機制，可以避免製發憑證的過程中會有偽冒用戶身分的安全弱點同時也可以降低公鑰儲存、計算與管理的成本與風險；並能以多份投標文件執行一次盲簽章及加密的方法，以減少檔案分批簽章次數及傳輸頻寬之需求，並達到ISO (2005)組織所提出之資訊安全管理需求，其中包含資訊之機密性、完整性、不可否認性、隱匿性、不可追蹤性、不可偽造性、鑑別性、隱匿性及自我認證機制等安全需求，以下我們分別針對安全性分析與效益評估來進行探討：

一、安全性分析

本研究之具自我認證之多重文件盲簽章機制，其安全性植基於橢圓曲線離散對數難題及與廠商身分、投標文件內容之隱匿性，可達機密性、完整性、不可否認性、鑑別性、不可追蹤性、不可偽造性等安全需求，綜整本研究之安全性分析略述如下：

(一)機密性(Confidentiality)

機密性指的是資料不得被未經授權之個人、實體或程序所取得或揭露的特性，文件在成功地送達目的地之後，所有的文件交換都是保密的。如廠商以其參數雜湊值 e_A 及時間戳記 t_A 為盲因子，故投標文件於簽章過程中，已利用僅有廠商知道之盲因子將投標文件訊息進行盲化如式(17) $\beta' = e_A \cdot t_A \cdot \beta \cdot PK_C$ 與式子(18) $S'_\beta = \beta' \cdot sk_B$，因此，採購中心並無法得知廠商之投標內容為何，無法還原原始資料，僅能依其權限進行簽署該份投標文件，而攻擊者如要竄取就必須面臨破解橢圓曲線離散對數之難題。

(二)完整性(Integrity)

完整性是指訊息在傳遞過程中，不能被破壞或干擾的特性。文件的內容在用戶端和伺服器端間傳遞的過程中確認沒有被改變，也就是訊息在交易的處理過程中不能被任意地加入、刪除或修改。如廠商A將多份投標文件項目內容明文訊息分成數個區塊再對明文進行雜湊運算得 α，如本方法式子(11)中 $h_1(m) = \alpha$，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。

(三)鑑別性(Authenticity)

鑑別性指的是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，因此藉由金鑰對可達到鑑別使用者身分的功能。在本研究中各階段成員於使用系統前，皆須做註冊及身分確認，才能獲得其憑證與公鑰，且在運用其身分時，須使用由 CA 所給予之公鑰等參數資料進行相互身份驗證，因此各階段成員身分都有可驗證性例如式子(7) $S'_A = PK_A + h(id_A) \cdot G + \left[\left(q_{Ax} + h\left(id_A\right)\right)\right] \cdot PK_{CA}$ 及(8) $S'_A \stackrel{?}{=} S_A$。而採購機關於收到盲化投標文件後，欲解開盲化投標文件，亦須先與廠商進行身，驗證無誤後才可以所得之身分驗證訊息與雙方共同之隱匿金鑰獲得盲因子如式子。

(四)不可否認性(Non-repudiation)

不可否認性指的是對一已發生之行動或事件之證明，使該行動或事件往後不能被否認的能力。不論是傳送方或接收方皆不能否認訊息曾被傳送的事實，保證任一個網路節點不能否認其所發送出去的訊息及不能否認它以前傳送訊息的行為。如採購中心能簽署盲化的投標文件訊息，而且採購中心不會介入存取投標內容，讓廠商不必擔心因採購中心的疏失而導致投標內容曝光，且僅有採購中心才可以產生合法盲簽章，如式子(18)中 $S'_\beta = \beta' \cdot sk_B$，因為偽造者無法知道簽章者產生簽章的私密金鑰，因此無法偽造出盲簽章。故採購中心

(簽章者)不能否認自己簽署過之訊息，且如果攻擊者要從中求得採購中心的簽章(私密金鑰)是很困難的，因為會面臨橢圓曲線離散對數的難題(ECDLP)。

(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或簽章，任何人能夠經由參數驗證得知文件或簽章是否偽造。系統認證中心須由使用者傳送過來的參數資料(如id_A、V_A)才能計算其公鑰，如式子(3) $PK_A = V_A + (k_A - h(id_A)) \cdot G = (q_{Ax}, q_{Ay})$，且使用者的私密金鑰是依CA傳回的簽章$W_A$計算得到的，如式子(4) $w_A = k_A + sk_{CA} \cdot (q_{Ax} + h(id_A))$，所以系統認證中心不能自行產生甚至是偽照使用者的公鑰，可避免因系統認證中心知道所有使用者的私密金鑰，偽造產生一個完全不存在的使用者的情事發生。另在本式子(16)中$h_2(\overline{C_i}) = \beta$，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)不可追蹤性 (Unlinkability)

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，因盲因子是隨機的，簽章者僅知道這些文件是經由自己簽署的。在本研究中經過加盲的訊息，簽章者無法得知真正的文件內容如式子(17)中$\beta' = e_A \cdot t_A \cdot \beta \cdot PK_C$，因為盲因子「$e_A$」是隨機的，簽章者僅知道這些資訊是經由自己簽署過的，此時簽章者與文件脫離了的關係(unlinkability)，以達到匿名的效果。

(七)隱匿性(Hide)

隱匿性指的是一種利用密碼學將訊息經過密碼學的加密其他資訊加以遮蓋以達到隱匿效的，亦是簽署人對簽署的文件內容無法獲知該內容的訊息，在本研究如式子(18) $S'_\beta = \beta' \cdot sk_B$中，有此功能，不必擔憂在廠商將訊息傳遞給採購中心進行簽章過程中而造成投標文件曝光。

(八)自我認證機制(Self-certified Scheme)

自我認證機制指的是可以提供線上另一使用者的確認性服務，在連線導向的傳輸中，它於建立連線過程中提供發送者或接收者的身分確認。 本研究系統內成員以自己的*id*及選擇機密參數值*r*產生簽名檔 V，如式(2)($V_A = h(r_A \| id_A) \cdot G$)後將*id*與$V$傳給CA做註冊才能獲得其簽章與公鑰，並可驗證公鑰之正確性，如式(4) $w_A = k_A + sk_{CA} \cdot (q_{Ax} + h(id_A))$，一旦所有成員取得簽章與公鑰，之後運用其身分時，須使用由CA所授予之公鑰等參數進行相互身分驗證，而不須與CA保持連線狀態，可達與認證中心CA離線作業之效，並且個階段成員都有可驗證性。本系統符合 Girault 所提之公開金鑰密碼系統的 Level 3 之安全等級：認證的雙方僅需雙方的公開資訊，即可達成雙方身分的確認；系統內成員自憑證中心CA註冊後，不需再透過第三方(如憑證認證中心)中介機構做保證或協調。

二、效益分析

設計多重盲簽章之機制，有別於以往學者之盲簽章侷限於一次盲簽章一份文件的傳統方法，達到文件內容具有完整性、機密性、鑑別性、不可否認性、隱匿性、不可追蹤性等需求，並利用橢圓曲線其特殊的點加法運算及其在同樣的安全度之下僅需要較小的密鑰長度，除增加密文之混淆度，可加強密文之完整性與安全性，因此本研究提出一種植基於橢圓曲線離散對數的自我認證之多重盲簽章機制可適用於國軍事電子化採購方案中，在本研究中先讓雙方自我認證以確保雙方身分不被偽冒及改善以往一次盲簽章機制，改進成多重盲簽章之概念，這項創新機制的導入Level 3 安全等級的自我認證及縮短系統在作業處理時多餘程序進而提升執行時的

效率，本節效益特針對國軍現行電子化採購與本研究比較各項安全性，如表 4。而從表 5 可得知在本研究各階段運算時間之概估，而因模數加法、模數減法運算時間低，予以忽略不計。

表 4 安全及效益分析比較表

比較項目	現行電子採購系統運作機制	具自我認證之多重文件盲簽章機制(本研究)
核心原理	RSA 加密機制、單一文件加密機密。	橢圓曲線簽密機制、自我認證、多重文件盲簽章機制。
運算速度	慢。	快。
不可否認性	密文資料僅透過數位簽章進簽章驗證。	透過橢圓曲線簽密法來進行簽章驗證，達到不可否認性。
使用者認證	僅透過設定值設定辨識使用者身分，無法驗證資料來源的合法性。	公鑰及簽章由認證中心產生，公鑰由使用者自行驗證及參數資訊輔助產生私鑰；金鑰產生之順序為公鑰→私鑰→驗證式，以確保參與者身分合法性，並防範惡意者的偽冒。
密文完整性	使用雜湊函數及數位簽章進行密文完整性。	1.除檢查密文之雜湊值外，密文具有雪崩效應，除非密文全部正確，否則無法解密。 2.解密時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。
密文機密性	以 RSA 密碼系統進行檔案之加密。	以橢圓曲線密碼系統加密，且僅針對需要加密之資訊機密，在有限之頻寬內可有效降低資訊耗費。
內容不可追蹤性	無。	本研究之簽章者無法得知真正的內容，因盲因子是隨機的，簽章者僅知道這些文件是經由自己簽署的。簽章者僅知道這些資訊是經由自己簽署過的，此時簽章者與文件脫離了的關係(unlinkability)，以達到匿名的效果。
身分隱匿性	無。	簽署人對簽署的文件內容無法獲知該內容的訊息，不必擔憂在廠商將訊息傳遞給採購中心進行簽章過程中而造成投標文件曝光。
自我認證機制	無。	通訊雙方完成註冊程序後可不需再透過 CA 來執行認證作業，以達到自我認證之效。
雪崩效果	無。	有。
安全性提升	無。	1.攻擊者須能破解橢圓曲線離散對數之難題及不可逆單向雜湊函數且還須完成認證階段，故可避免中間人資料竄改攻擊。 2.橢圓曲線加密法與自我認證機制可減少在無線網路裡往返的通訊與計算量，可提升效率；並減少通訊中遭截取的機會。

表 5 本研究時間複雜度運算參考表

演算法	本研究方法	
項目	時間複雜度	概估
初始階段	6 T_{ECMUL} + 1 T_{ECADD} + 6 t_h	≈178.12 T_{MUL}
廠商A與採購中心B相互驗證階段	2 T_{ECMUL} + 2 t_h + 1 T_{ECADD}	≈60.12 T_{MUL}
盲化階段	1 T_h + 1 t_h + 3 T_{ECMUL} + 1 T_{ECADD}	≈111.12 T_{MUL}
簽章運算	1 T_{ECMUL}	≈29 T_{MUL}
採購中心B與採購機關C相互驗證階段	2 T_{ECMUL} + 2 t_h + 1 T_{ECADD}	≈60.12 T_{MUL}
解盲簽章驗證階段	5 T_{ECMUL} + 2 t_h + 3 T_{ECADD}	≈147.36 T_{MUL}
解密階段	3 T_{ECMUL} + 2 T_{ECADD} 1 T_h	≈110.24 T_{MUL}
合計		≈696.08 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，故無法以時間複雜度比較。		

陸、結論

本研究的目的為設計一個多重盲簽章之機制，有別於以往學者之盲簽章侷限於一次盲簽章一份文件的傳統方法，並利用橢圓曲線其特殊的點加法運算及其在同樣的安全度之下僅需要較小的密鑰長度，除增加密文之混淆度，可加強密文之完整性與安全性，且結合自我認證機制，不但可以避免製發憑證的過程中會有偽冒用戶身份的情事，同時也可以降低公鑰儲存與管理的成本，將此機制導入國軍電子採購業務的應用，以期建立一個更加公開、透明及安全的國軍電子化採購系統。

綜整本研究，除系統安全性可滿足密碼系統安全的需求，尚可達成之貢獻如下：

一、採橢圓曲線密碼系統以較短的密鑰長度與計算複雜度較低的特性，在同樣的密鑰長度之下，可達 RSA 相同的安全強度，並具有運算快速之特點。而攻擊者解密時必須面對橢圓曲線離散對數之難題。

二、於密文間執行橢圓曲線特殊的點加法運算，令密文與密文之間具有關聯性，使密文產生雪崩效果，破密者除了逐一的窮舉所有可能的點外，別無他法直到目前為止，這個問題仍無法於多項式時間內求出解答。

三、採用自我認證的機制，除了能降低對於第三方認證中心的依賴，亦能有效的防止認證中心偽冒使用者的金鑰，提升系統的安全性。系統內經過註冊的使用者，皆可利用公鑰與簽章的參數資訊，進行相互的認證，不需再透過認證中心進行認證作業，可提高使用效率，可與金鑰產製中心離線作業的自我認證機制。

四、多份投標文件內容進一次盲簽章及加密的方法，將多文件的資訊藉由混淆機制，將其變成一份密文來傳送，直接增加密文破解的難度，進而提高網路傳送資訊更高的安全性，並可達到系統效率的提升及縮短作業時多餘的流程。

五、投標文件內容經由盲化，攻擊者並無法得知廠商之投標內容為何，而且如要竄改就必須臨破解橢圓曲線離散對數之難題，並且採購中心僅能依其權限進行簽署該份投標文件，可避免內容洩漏，提高採購之公平性。

柒、國防領域之運用

隨著時代的演進，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，透過網路運作，如何避免投標廠商身分及文件內容洩漏，而發生弊案情事，尤其是在目前嚴峻的經濟環境中，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，這些的後果往往損及國防效能，進而使得國家安全遭到威脅，因此強化國軍電子化採購作業，以基於橢圓曲線密碼學為理論基礎，應用多文件盲簽章機制，以多份投標文件內容進行一次盲簽章，達到系統效率提升，並以盲簽章技術來達到廠商身分隱匿性，達到資料傳遞的完整性、鑑別性及簽署的不可否認性之需求外，還能達到資料隱私性及不可偽造性，防範資料洩漏，減少弊端，俾能提升整體戰力，達到廉節軍風及支援建軍備戰之目標。

參考文獻

全國法規資料庫，2011，電子簽章法，http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=J0080037。

肖攸安，2006，橢圓曲線密碼體系研究，武漢：華中科技大學出版社。

胡國新，2001，設計植基於自我驗證公開金鑰系統之安全線上電子拍賣機制，大葉大學資管理研究所碩士論文。

國防部軍備局，2003，軍事機關採購作業規定，台北：國防部。

國防部國防報告書編纂小組，2011，中華民國 100 年國防報告書，台北：國防部。

楊倫青，2011，植基於橢圓曲線之多重盲簽密機制--具一次投領多重選票之設計，國防大學管理學院資訊管理學系研究所碩士論文。

賴溪松、韓亮、張真誠，2004，近代密碼學及其應用，台北市：旗標出版社。

蘇品長，2008，適用於國軍電子採購的盲簽章系統設計，國防管理學報。

蘇品長，梁榮哲，2011，設計具自我認證之多重文件盲簽章機制探討，新竹 2011 全國資訊管理前瞻技術研討會。

Chaum, D, 1982., “Blind signatures for untraceable payments,” In Proceedings of Advances in Cryptology-CRYPTO, 199-203.

Girault, M., 1991, “Self-certified public keys,” Advances in Cryptology-Euro, Vol. 547, 491-497.

ISO, ISO/IEC 17799: 2005-06-15, “Information technology-Security techniques-Code of practice for information security management,” 1.

Koblitz, N., 1987 “Elliptic curve cryptosystems,” Mathematics of Computation American Mathematical Society, Vol. 48, 203-209.

Miller, V. S., 1985, Use of elliptic curves in cryptography, International Crytology Conference 85, New York: Spring-Verlag, 417-426.