具自我認證之多重文件盲簽章機制設計
-以國軍電子採購業務為例
Design Self-Certified and Multi-Document Blind Signature Schemes-Evidence from Military E-Procurement

蘇品長 [1]　蕭柏薰 [2,*]
[1,2] 國防大學資訊管理學系
[*]Email: pohsun3@gmail.com

摘　要

本研究的目的為設計一個具自我認證機制的多重盲簽章方法，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，並以國軍電子採購業務的應用為例。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，更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，本研究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；目前大部分之盲簽章都僅於一次盲簽章，本研究能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，強化廠商身分及投標文件內容遭窺探與篡改等安全問題。

關鍵字：軍事採購，盲簽章，自我認證，多重文件。

一、前言

隨著網路科技日新月異，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，以節省成本及大幅提升整體採購流程效率。國軍在電子化政策下，也將軍事採購作業逐漸改為電子化採購，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平與公正。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，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。

雖然目前電子化採購系統運用 RSA、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[16]，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，本研究係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[18]，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。

二、文獻探討

(一)、現行軍事採購流程

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[20]，其採購流程如圖 1。

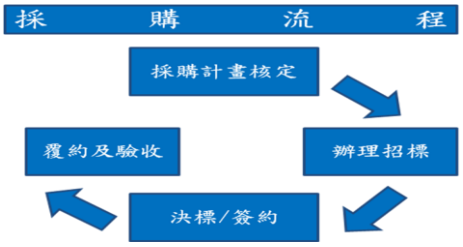

圖 1　採購流程圖

(二)、橢圓曲線公開金鑰密碼系統

自從 Miller[11]與 Koblitz[6]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 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[12]：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 $A+B=C$；否則 $A+B=(x_3,y_3)$，其中 $x_3=\lambda^2-x_1-$，$y_3=\lambda(x_1-x_3)-y_1$。

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

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，如表 1。

表 1　RSA 與 ECC 相同安全度金鑰長度比較表

RSA 與 ECC 相同安全度金鑰長度比較					
RSA	512	1024	2048	3072	7680
ECC	112	163	224	256	384
Key	1:5	1:6	1:9	1:12	1:20

資料來源:蘇品長[15]

(三)、盲簽章

Chaum[2]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。有了這兩個特性，使得盲簽章得以應用在電子投票[4,7,8]及電子現金[1,9,10]。而盲簽章演算法流程如圖 2。

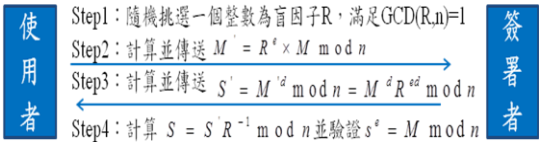

圖 2 盲簽章流程關係圖

(四)、自我認證公開金鑰密碼系統

Girault[5]提出公開金鑰密碼系統下的自我認證機制，其三個層次安全等級如表 2。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。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。其中 Level 3 安全等級指的是系統驗證過程中所有詐偽的行為會被偵測出來，即是 Girault 所提出來的自我認證公開金鑰密碼系統[14]。

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

三、具自我認證之多重文件盲簽章機制設計-以國軍電子採購業務為例

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，本研究整體運作示意循序圖如圖 3 所示：

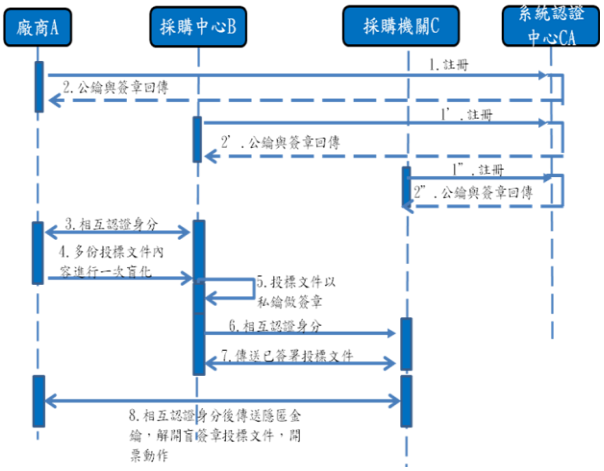

圖 3 本研究整體運作示意循序圖

(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
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, id_c	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(點序列轉值)
16	$f_{m2p}()$	將訊息轉為橢圓曲線點之函數
17	$f_{p2m}()$	將橢圓曲線轉為訊息之函數
18	t_n	成員所選擇之時間戳記
19	m	明文訊息
20	m_{ij}	明文之分解區塊
21	M	將明文雜湊函數(點序列轉值)後的值
22	r_A 、k_A	廠商、CA 之隨機秘密參數
23	$h()$	CA 公開之雜湊函數

(二) 系統初始階段

Setp1：金鑰產製中心(Key Generatin Center, CA)系統建置階段

首先系統認證中心(CA)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 160 bit 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：

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

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：

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

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

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：

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

證明式如下：

$$S_A = sk_A G \tag{7}$$

$$S_A = [\ k_A + s\ k_{C}(\ q_{A}+\ (h\ i)) +\ \ (h\ \| \ i_{A} \tag{8}$$

$$S_A = [k_A + sk_{CA}(q_{ax} + h(id_A))]G + h(r_A \| id_A)G \tag{9}$$

$\because PK_{CA} = sk_{CA}G$

$\therefore S_A = \left[k_A + h(r_A \| id_A)\right]G + \left[(q_{Ax} + h(id_A))\right]PK_{CA}$

$\therefore S_A = k_A G + h(r_A \| id_A)G + \left[(q_{Ax} + h(id_A))\right]PK_{CA}$

$\because V_A = h(r_A \| id_A)G$

$\therefore S_A = k_A G + V_A + \left[(q_{Ax} + h(id_A))\right]PK_{CA}$

$\because PK_A = V_A + (k_A - h(id_A))G$

$\because V_A = PK_A - (k_A + h(id_A))G = PK - k_A G + h(id_A)G$

$\therefore S_A = k_A G + PK_A - k_A G + h(id_A)G + \left[(q_{Ax} + h(id_A))\right]PK_{CA}$

$\therefore S_A = PK_A + h(id_A)G + \left[(q_{Ax} + h(id_A))\right]PK_{CA}$

各方成員與 CA 註冊程序如上，一旦所有申訴人與各方成員（n）CA 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。

(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:

$$S'_A = PK_A + h(id_A)G + \left[\left(q_{Ax} + h(id_A)\right)\right]PK_{CA} \quad (10)$$

$$S'_A \stackrel{?}{=} S_A \quad (11)$$

接著以憑同理，廠商也可驗證採購中心:

$$S'_B \stackrel{?}{=} S_B \quad (12)$$

(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 n 份投標文件 $\overline{m}$ 傳送給採購中心 B，$\overline{m}=\{m_1,m_2,m_3,...,m_n\}$。並將每份投標文件明文 m_i，$i=1,2,...,n$ 分成 2 個區塊。

$\overline{m_{ij}}=\{m_{11},m_{12},...,m_{n1},m_{n2}\}$，$i=1,2,...,n$，$j=1,2$ (13)

並對明文 $\overline{m_{ij}}$ 實施雜湊利用明文轉點方式將明文轉為點座標計算如下：

$$h_1(\overline{m_{ij}}) = m \quad (14)$$

$$f_{m2p}(m) = P_1, P_2, ...P_n \quad (15)$$

$$\overline{P_i} = \{P_0, P_1, P_2, ..., P_n\} \quad (16)$$

$$h_2(\overline{P_i}) = M \quad (17)$$

接著廠商 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，盲化多個訊息 M，計算:

$$M' = e_A t_A \cdot M \quad (18)$$

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，以其私鑰 sk_B 對盲化訊息 M' 執行簽章作業，再用私鑰 sk_B 加密於廠商公鑰，以證明此投標文件為合法有效票，計算如下：

$$S'_M = M' \cdot sk_B \quad (19)$$

(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，計算如下：

$$S'_B = PK_B + h(id_B)G + \left[\left(q_{Bx} + h(id_B)\right)\right]PK_{CA} \quad (20)$$

$$S'_B \stackrel{?}{=} S_B \quad (21)$$

接著以憑同理，採購中心也可驗證採購機關:

$$S'_C \stackrel{?}{=} S_C \quad (22)$$

(七)、採購機關 C 進行(解盲簽章階段)

採購機關 C 收到隱匿投標文件 S'_M 後，卻解開隱匿投標文件，需自廠商 A 取得 t_A 及 e_A 盲因子，以進行解盲動作，故採購機關 C 須與廠商 A 相互驗證，計算如下：

$$S'_C = PK_C + h(id_C)G + \left[\left(q_{cx} + h(id_C)\right)\right]PK_{CA} \quad (23)$$

$$S'_C \stackrel{?}{=} S_C \quad (24)$$

接著以憑同理，採購機關 C 也可驗證廠商 A:

$$S'_A \stackrel{?}{=} S_A \quad (25)$$

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：

$$T_A = t_A \cdot G \quad (26)$$
$$\because S_A = SK_A G$$
$$\therefore X_{AC} = sk_A S_C = sk_C S_A$$
$$\therefore R_A = X_{AC} + T_A$$

Setp2：採購機關 C 以所獲得資訊求得 t_A 及 e_A，計算如下：

$$\because R_A = X_{AC} + T_A$$
$$T_A = X_{AC} - R_A \quad (27)$$
$$t_A G = (sk_A \cdot sk_C)G - R_A \quad (28)$$

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 以所獲得資訊得 t_A 及 e_A，解開自採購中心 B 傳來的盲化隱匿投標文件 S'_M，計算如下：

$$s_M = e_A^{-1} \cdot t_A^{-1} \cdot s'_M \quad (29)$$

Setp4：接著將多文件進行解密動作，計算如下：

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

$f_{p2m}(\overline{P}) = \overline{m_{ij}}\{m_{11}, m_{12}, m_{21}, m_{22}, ..., m_{n1}\}$， $i=1,2,...,n$，$j=1,2$。(30)

對明文 $\overline{m_{ij}}'$ 做雜湊值運算 $h_2(\overline{m_{ij}}') = m'$，驗證

$$m' \stackrel{?}{=} m \quad (31)$$

若等式成立則確認收方所收之訊息正確無誤。

四、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，以達到資訊的完整性、不可否認性、隱匿性、不可追蹤性、不可偽造性等特性，以下針對本研究之安全性及效益分析進行探討：

(一)、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、可驗證性、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：

1.可離線作業的身分自我認證

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)（$V_A = h(r_A \| id_A)G$）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，如式子(4) $w_A = k_A + sk_{CA}(q_{Ax} + h(id_A))$，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。

2.機密性

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(18) $M' = e_A \cdot M \cdot t_A$ 與式(19) $S'_M = M' \cdot sk_B$，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。

3.完整性

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 m，如本方法式子(14)中 $h_1(\overline{m_{ij}}) = m$，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。

4.不可否認性

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(19)中 $S'_M = M' \cdot sk_B$，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）。

5.可驗證性

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(10) $S'_A = PK_A + h(id_A)G + \left[\left(q_{Ax} + h(id_A)\right)\right]PK_{CA}$ 及(11) $S'_A \stackrel{?}{=} S_A$。而採購中心將盲化投標文件訊息轉發給採購機關前，需先進行身分上之驗證如式子(20) $S'_B = PK_B + h(id_B)G + \left[\left(q_{Bx} + h(id_B)\right)\right]PK_{CA}$ 及(21) $S'_B \stackrel{?}{=} S_B$。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分驗證如式子(23) $S'_C = PK_C + h(id_C)G + \left[\left(q_{cx} + h(id_C)\right)\right]PK_{CA}$ 及(24) $S'_C \stackrel{?}{=} S_C$，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。

6.不可追蹤性

經過加盲的訊息，簽章者無法得知真正的文件內容如式子 $M' = e_A \cdot t_A \cdot M$ (18)中，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。

7.不可偽造性

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) $PK_A = V_A + (k_A - h(id_A))G = (q_{Ax}, q_{Ay})$，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) $w_A = k_A + sk_{CA}(q_{Ax} + h(id_A))$，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(17)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。

(二)、效益分析

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。

表 4　效益分析比較表

比較項目	現行運作機制	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	以 RSA 密碼系統進行檔案	以橢圓曲線密碼系統加密，且僅針對需要加密

性	之加密	之資訊機密，在有限之頻寬內可有效降低資訊耗費。
可離線之身分認證	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。
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。

五、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，由其是在目前嚴峻的經濟環境中，並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，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

[1] C. I. Fan, and W. K. Chen, "An Efficient Blind Signature Scheme for Information Hiding," International Journal of Electronic Commerce, vol. 6, no. 1, pp. 93-100, 2001.

[2] D. Chaum, "Blind signatures for untraceable payments," In Proceedings of Advances in Cryptology—CRYPTO , pp. 199-203, 1982.

[3] F. G. Jeng, T. L. Chen, T. S. Chen, "An ECC-Based Blind Signature Scheme," Journal of Networks, vol. 5, no. 8, pp. 921-928, August 2010.

[4] L. Wang, J. Guo, and M. Luo, "A More Effective Voting Scheme based on Blind 25 Signature," Proceedings of International Conference on Computation Intelligence and Security , vol. 2, pp. 1507-1510, 2006.

[5] M. Girault, "Self-certified public keys," Advances in Cryptology-Euro, vol. 547, pp. 491-497, Spring-Verlag, 1991.

[6] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation American Mathematical Society , vol. 48, pp. 203-209, 1987.

[7] S. H. Yun, and S. J. Lee, "An Electronic Voting Scheme based on Undeniable Blind Signature Scheme," Proceedings of IEEE 37th Annual International Carnahan Conference on Security Technology , pp. 163-167, 2003.

[8] S. Ibrahim, M. Kamat, M. Salleh, and S. R. A. Aziz, "Secure E-voting with Blind Signature," Proceedings of 4th National Conference on Telecommunication Technology , pp. 193-197, 2003.

[9] T. Nakanishi, and Y. Sugiyama, "Unlinkable Divisible Electronic Cash," Proceedings of 3rd International Workshop on Information Security , pp. 121-134, 2000.

[10] T. Nakanishi, M. Shiota, and Y. Sugiyama, "An Efficient on-line Electronic Cash with Unlinkable Exact Payments," Proceedings of the 7th Information Security Conference, pp. 367-378, 2004.

[11] V. S. Miller, "Use of Elliptic Curve in Cryptography," Advance in Cryptography Crypto , pp. 417-426, New York: Spring-Verlag 1985.

[12] 肖攸安，"橢圓曲線密碼體系研究，" *台北:華中科技大學出版*，2006年。

[13] 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。

[14] 胡國新，"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*，2000年。

[15] 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。

[16] 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，第29卷，第2期，頁數51-62*，2008年。

[17] 蘇品長，梁榮哲，"多重文件盲簽章機制之設計，" *聯合國際研討會*，2011年。

[18] 蘇品長，梁榮哲，"設計具自我認證之多重文件盲簽章機制探討，" *玄奘大學2011全國資訊管理前瞻技術研討會*，2011年。

[19] 楊倫青，"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所碩士論文*，2010年。

[20] 國防部軍備局，"軍事機關採購作業規定，" 2003年。