適用於國軍電子採購的盲簽章系統設計

蘇品長

國防大學管理學院資訊管理學系

摘　要

鑑於網路與密碼技術的成熟，許多商業機制的研究已經受到重視，如何將國軍採購作業導入安全的系統運作，減少弊端，值得研究。在過去的數十年中，有許多根基於私密金鑰密碼理論的電子採購系統被提出，雖然這些系統執行效率有改善，但是他們皆無法提供隱私性保障的功能。因此，在考慮電子資料安全性的同時亦需顧慮到使用者的隱私性問題。由於群數對密碼演算法具有簡潔及效率之優點，近來研究密碼學領域的專家學家，發表諸多植基於橢圓曲線上的雙線性群數對的應用於密碼學領域的期刊上。本研究的目的在於整合背包理論(Knapsack)及 Gap Diffie-Hellman 難題來實現盲簽章的可行性探討並導入國軍電子採購作業構想，期待後續系統的開發及研討。

關鍵詞：雙線性群數對、盲簽章、背包理論

New Blind Signature Design for Military E-Procurement System

Pin-Chang Su

Department of Information Management, Management College, NDU, ROC

ABSTRACT

The ratio of military procurement to government budget is high every year. A model to evaluate the efficiency of procurement performance is an important issue. Blind signatures enable users to obtain valid signatures for a message without revealing its content to the signer. Recently the bilinear pairings such as Weil or Tate pairings on elliptic curves have found various applications in cryptography. We present a new verifiable blind signature based on knapsack and bilinear pairings for military procurement system. It is best to compare systems based on the best knowledge currently available. Only then can less tangible factors, like guessing the likelihood of new developments in mathematics be considered. The proposed scheme has all of the advantages of a blind signature scheme and overcomes drawbacks such as impracticality assumption. The security of the proposed method is analyzed and presented.

Keywords: Bilinear pairings, blind signature, Knapsack

壹、前　言

行政院於 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，大幅降低企業營運成本，並提升產業的競爭力。因此，中央行政部門決定率先運用網際網路，提供政府採購資訊與建置相關採構機制，帶動相關產業參與。「電子採購作業」是利用數位化資訊系統取代傳統文書往來繁瑣冗長的採購

流程，透過 Internet 和 Intranet 完成傳統 B2B 採購相關的互動業務。經由數位化的互動提昇效率，節省支出。以國際線上競標網站著名的 eBay 來說，已經被視爲新一波電子商務的成功典範。

在過去的數十年中，有許多根基於私密金鑰密碼理論的系統被提出(Dukach, 1992)、(Low et al., 1996)、(Lysyanskaya and Ramzan, 1998)、(Medvinsky and Neumann, 1993)、(Stein et al., 1994)，卻無法提供隱私性保障的功能。若只利用公開金鑰系統來實作系統(Rivest et al., 1979)，雖可達到對數位訊息的機密性、完整性、鑑別性及不可否認性，但是也會很容易地暴露使用者的身份。因此，在考慮安全性的同時亦需顧慮到使用者的隱私性問題，以防止有心人士能輕易監視或追蹤使用者的消費習慣或模式。以實作 RSA 公開金鑰系統爲例，若某銀行使用欲對一個訊息 m 進行簽章以認定其爲有效的電子現金，因此可利用雜湊函數計算出訊息雜湊值的簽章。當商店送來欲結算存入帳户的電子現金時，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爲。

David Chaum 在 1982 年提出一個能保障使用者隱私性亦能證明交易以達到不可否認目的之盲簽章技術，它奠定系統實作的良好基礎。使用盲簽章技術來實作系統時，除能達到交易雙方不可否認性或稱無法僞造性的功能外，還可因爲其具有無法連結性質而能保護使用者的隱私性，這對合法商業交易的使用者來說當然是優點，然而對於犯罪份子強迫勒索或進行洗錢等不法事情時，完全地隱藏身分可能就會大大提高執法機關破案的困難度，甚至更會讓犯罪份子恃無忌憚的從事違法事件。故 Stadler 等三位學者在 1995 年的 EUROCRYPT 會議中發表公平盲簽章方法，有使用者、簽章者及具有第三公正者的法官共三種角色參與此協定(Camenisch et al., 1994)，使用者可將訊息送給簽章者進行簽署作業，而每次簽署過程的所有連結資訊皆會被法官紀錄下來。當需要法官提供資訊連結的證據時，簽章者在通過申請核准程序後就可找出連結性。否則簽章者就無法得到電子現金與使用者之間的關係，而能充分保障使用者的隱私性。故本方法能在犯罪情事與隱私性之間取得一個較佳的平衡點。相較於 Chaum (1990) 所提出的盲簽章技術採用大整數的因數分解，Camenisch、Piveteau 及 Stadler(1995) 三位學者則提出植基於離散對數(ElGamal, 1985)問題的兩種方法，其中包含有 DSA 演算法的變形及根據 Nyberg-Rueppel 簽章方法所發展的盲簽章技術，雖然 1994 年 Horster 等學者將上述的研究成果一般化，但後來被 Harn(1995)學者證明其一般化的盲簽章是可追蹤的。而 Mohammed(2002)等三位學者最近也發表植基於 ElGamal 簽章法的盲簽章技術，可達到即使簽署相同訊息多次但簽章結果會有所不同，能增加盲簽章技術的匿名性，同時其所需的計算複雜度較 Chaum 方法低而運算速度快，這些學者的研究提供實作的另一種選擇。

回顧過去的簽章系統，大部份所運用的安全機制皆是植基於解因式分解或離散對數的困難性。評估密碼系統的執行效率，以相同的安全等級條件下，取決於加、解密速度、簽章、驗證速度、使用頻寬、簽章大小、金鑰產生速度及大小等因素。自從公開金鑰密碼產生以來，人們基於各種數學難題提出大量的密碼方法，但能夠經得起時間考驗而廣泛爲人們所接受的只有基於大質數分解及離散對數問題的方法，且不說這兩種問題受到次指數演算法的嚴重威脅，就如此簡單的數學背景來說，難免引起人們的擔憂，尋找新的數學難題作爲密碼系統，早就是人們努力的一

個方向。同時，橢圓曲線系統具有此特性，在同一個有限域上存在著大量不同的橢圓曲線，這是安全性增加額外的保證，這也使得軟、硬體設計上更加安全。為強化系統的安全性，Harn 於 1994 年提出一個植基於因式分解和離散對數的數位簽章系統，Lee 和 Hwang 於 1996 年改進 Harn 的方法以避免偽造攻擊，之後陸續有專家學者針對不同的因式分解與離散對數問題設計不同的演算機制，強化系統遭受攻擊的容忍強度 (Shao,1998)、(Lee, 1999)、(He, 2003)、(Su, et al., 2005)。

一個密碼系統的安全與否與攻擊者破解系統所需要的計算複雜度有關，以因式分解和離散對數為基礎的密碼系統，已被證實屬於 NP 問題(Michael, et al., 1979)。即若所有 NP 問題可以在多項式時間內利用定性涂林機求解，則 NP = P。而背包問題已被證實為一個 NP-Complete 問題，如何將背包理論導入公開金鑰密碼機制內，而又避免先前學者設計的方法所遭受攻擊而導致失敗的原因(Shamir, 1984)，即可達成密碼學領域所追求的目標 - 暨快速又安全的公開密碼機制。近來研究密碼學領域的專家學家，發表諸多植基於橢圓曲線上的雙線性群數對的應用於密碼學領域的期刊上，儼然成為密碼學上一個熱門的研究領域(Boneh, and Franklin, 2001)。群數對首先是被用來破解橢圓曲線密碼學的密碼分析方法，適用於特殊的橢圓曲線，可將離散對數問題簡化對應成等同於一般的有限場的離散對數，進而使得這類的橢圓曲線喪失密碼機制中的實用性和可靠性。由於群數對密碼演算法具有簡潔及效率之優點，近年來基於群數對的密碼機制的相關研究。群數對為基礎的密碼機制其安全性建立在解 Bilinear Diffie-Hellman 或 Computational Diffie-Hellman 問題之困難度。即 e:$G_1 \times G_1 \rightarrow G_2$，$G_1$ 為有限場之橢圓曲線上所有點的子群，G_2 為在相同的有限場之乘法群的子群，在安全的假設上，在 G_1 與 G_2 之中要計算離散對數問題必須是計算上不可行的。從已發表的學術論文中發現群數對的數位簽章方法均將訊息藉由單向赫序函數轉換成曲線上之一點 (Verheul., 2001)，在研究的過程中發現群數對簽章法均基於假設情況，並無提供實作的方法，遂引起探討既安全且快速的群數對數位盲簽章方法。本研究的目的在於導入背包理論來實現單向赫序函數的可行性，期能有助於雙線性群數對國軍未來推動電子採購系統的強化及後續研討。

貳、電子採購系統簡介

近年來，政府正大力推動「產業電子化推動方案」政策，目的在以現今電子商務發展的趨勢，善加利用資訊科技與資訊管理兩項重要的觀念與技術，促進國內產業全世界的競爭力。在全世界正極力發展電子商務的過程中，可以看到許多因應網際網路的掘起，而帶動若干在網際網路進行的製造、行銷或作業獲得新的模式。在發展與研究產業電子化的應用中，有關於商務系統採用電子化方案，也是不容忽視的一項工作。目前架構在網際網路上之電子化服務包括：電子付款、電子拍賣、電子投票、電子採購……等，成功基礎在於能夠提供方便、安全的電子付款方式，但因所有過程與交易行為均經由網路來進行，因此在安全上有諸多問題點需詳加考慮，如偽冒、竊取、竄改等。

一、 政府採購電子化發展現況

我國政府採購法於民國 87 年 5 月 27 日公佈，規劃採購作業的運作規則，俾利採購相關單位能有依循法則，另於民國 88 年正式施行，經由法律規範期使各種弊病減到最低。為求提昇國家整體競爭力，政府於推動國家資訊通訊基本建設 (National Information Infrastructure, NII) 中，亦擬定「電子化 / 網路化政府」推動

計畫，民國 86 年 11 月 13 日於行政院通過以網路爲主，推展 10 項子計畫，其中第 2 項子計畫便是電子採購。電子採購爲電子商務之一環，所謂的電子商務即是將傳統上的商業行爲經由電子網路來實現，他的好處在於：降低產業生產成本、增進交易速度、加強買賣雙方互動、提昇產業競爭力。

電子化採購主旨爲利用網際網路快速傳輸訊息、設計完善的安全演算法及安控機制等特色，並配合電子簽章法使其具備法律的效力並受法律的規範，可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。公共工程委員會與中華電信合作建立電子化採購規範，工作成果爲實現電子化的領標及投標系統，目的在建立操作簡便、安全可靠的電子領投標作業系統，減少繁瑣的人工介入、降低採購成本，建立網路上安全的電子簽章身分驗證及安全的網路傳輸環境，並期能杜絕圍標、綁標的不法情事，更加速電子商務的蓬勃發展。由於政府採購在內需市場佔相當大的比例，若能推動政府採購電子化與網路化，並建立一公正完善的競標環境，可對國內產業發展起帶頭示範的作用。網頁：http://www.pcc.gov.tw/PCCWeb2/upload/lawDB/44/44.html。

二、電子採購系統

國內已有多個研究計畫探討電子採購系統，其中以賴溪松等教授(2004)所提的架構完整性最佳，綜整國內外各學術單位研究成果及文獻探討，摘整適合導入國軍電子採購系統作業功能及說明如后：

■註冊階段(申請憑證)

1.廠商填寫自公告中心(國防部軍備局採購中心等)下載之註冊基本資料表(含申請單)，並親自將相關文件(如：營業登記證)送至認證中心註冊審查(國防部認證中心，規劃建置中)。
2.需另外再與廠商來往之金融機構查核確定(Option)。
3.審查通過後，發給廠商類別(依營業項目分文具、電腦、材料、儀器等)、等級(依資本額分甲、乙、丙等)相關文件與憑證。
4.中心公告註冊廠商 MCA 或 GCA 憑證。

■標單產生階段

1.提出招標要求 / 簽章 / 金鑰
2.要求底標估算及招標文件
3.傳送底標估標及招標文件
4.傳送底標
5.辦理機關需將各個步驟所產生的各項資料傳至資料庫。
6.標單上網公告

■標單公告階段

1.一般及合格廠商均可上網瀏覽
2.領取標單
3.存證

■投標階段

1.招標機關(委採購中心等採購單位辦理)向金鑰中心要求系統公鑰。
2.會員廠商至銀行壓標金。
3.投標單位利用私有金鑰及系統公鑰進行加密後投標，投標資料資料上載。
4.資料庫進行標單完整性與正確性驗證，並於監標單位備份投標資料。
5.招標機關以 e-mail 的方式送出「標單收到憑證」給廠商。若資料不全，招標機關亦將以 e-mail 通知廠商補送資料，會員廠商需於期限截止前回傳資料，否則視同放棄。

■審標階段

1.判斷是否有不予開標決標之情形。
2.判斷是否有三家以上會員廠商投標。

3.條件審查不符合，退件。
4.條件審查符合，則判斷「審查後是否有三家以上合格會員廠商」。
5.「廠商」通過審查即稱「合格廠商」，超過三家合格廠商時，進行開標。
6.少於三家合格會員廠商時進入步驟 7。
7.流標。進入第二次招標程序。

■開標階段

1.進行開標，解密標價、底價
2.依有訂底價最低決標作業流程
3.決標
4.廢標，並通知銀行退還押標金
5.依採購法 48 及細則 56.57 重新辦理
6.資料庫將開標結果備份至監察單位

■簽約階段

1.發予合約書
2.驗證簽章並審視廠商填妥合約書內容
3.將廠商填妥之合約書及簽章加密後送給需求單位
4.驗證簽章並審視需求機關填妥合約書之內容
5.招標機關將合約書簽章後送予監察單位簽章
6.合約傳送
7.回函
8.資料庫傳回一份開標與簽約相關處理訊息給監察單位

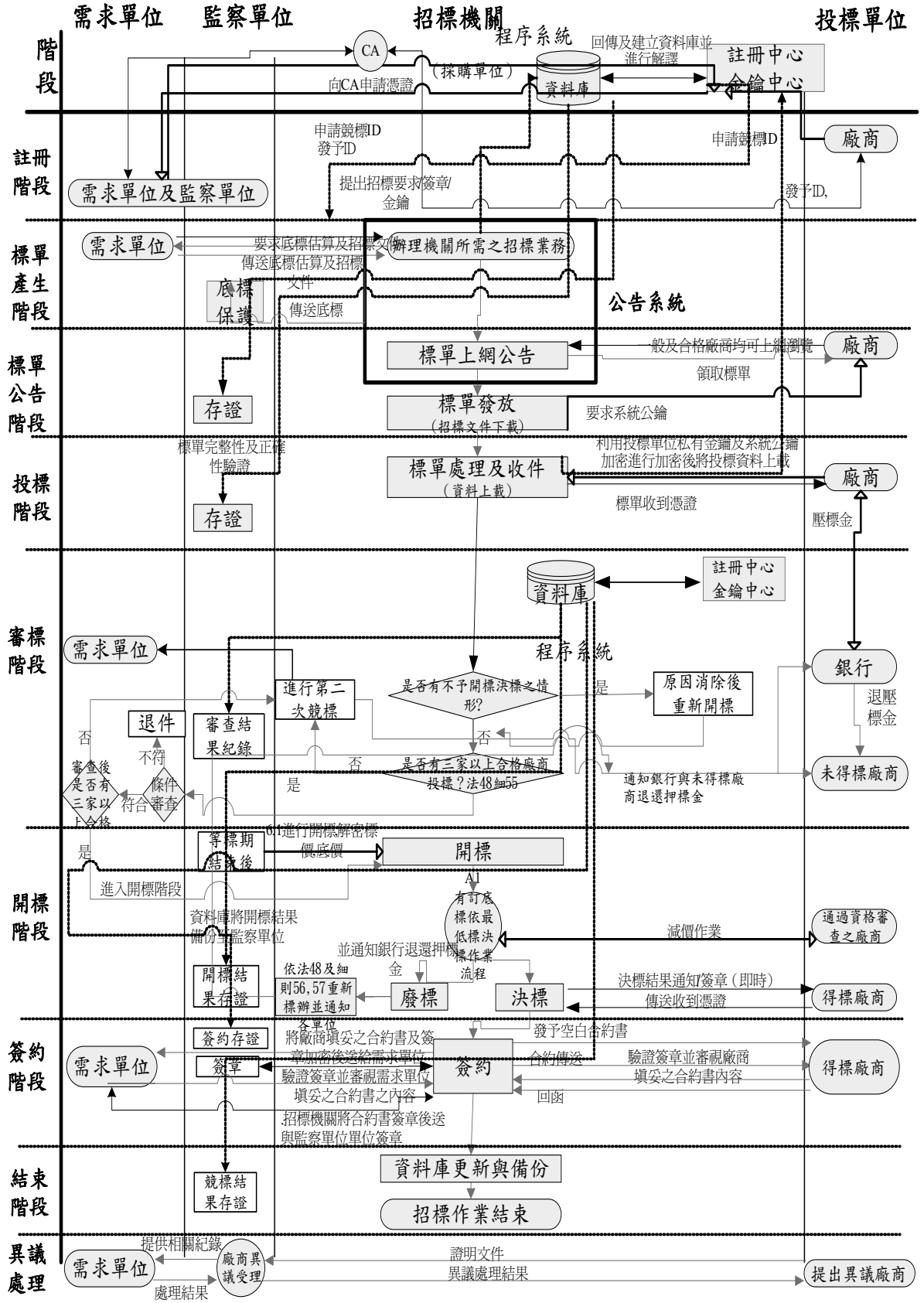
■結束階段

1.資料庫進行更新與備份
2.招標作業結束
3.競標結果存證

■異議處理

1.檢查異議提出廠商身分
2.廠商身分不符之處理
3.檢驗廠商電子簽章
4.檢驗外國廠商在本國代理人電子簽章
5.檢查異議處理人員身分
6.異議處理人員身分不符之處理
7.判斷輸入之異議表單是否齊全
8.異議表單輸入不齊全之處理
9.異議分類
10.判斷是異議表單之提出是否逾期
11.異議處理人員下載異議表單
12.異議處理人員處理異議表單
13.資料庫之聯繫
14.中止標案或暫停標案

電子採購系統導入國軍採購流程架構圖詳如圖一所示。



圖一　電子採購系統流程架構圖

下一段章節將就本研究所設計之電子採購系統核心部份所使用的盲簽章演算法，導讀相關文獻探討及演算法論述。

參、相關理論說明

一、背包理論

背包問題亦稱爲子集總和問題，在給定的數列 $A' = \{ a_1, a_2, \cdots, a_n \}$ 及整數 S，是否存在子序列 $A' = \{ a'_1, a'_2, \cdots, a'_m \} \subseteq A$，使得 $\sum_{i=1}^{m} A'_i = S$。背包問題已經被證實爲一個 NP-Complete 問題 (Merkle and Hellman, 1978)，不能在多項式時間內解決，雖然如此，包括 1978 年 Merkle-Hellman、1985 年 Chor-Rivest 及其 1988 年修訂版之背包密碼系統等，幾乎所以的背包系統均可被破解。在各式的破密法中以 Lagarias 及 Odlyzko 的低密度攻擊法最著名，一背包序列 $A = \{a_1, a_2, ..., a_n\}$ 的密度定義爲 $n/\log_2(\max(a_i))$，現行背包系統的密度幾乎均小於 0.50，當系統密度小於 0.645 的背包問題，均可採行 Lagarias 攻擊法。

背包系統的特性爲其加解密及簽章驗證的速度，比其他非對稱鑰匙密碼系統而言快速得多，因此引起許多研究學者的重視，然而至今尚未有顯著性的研究可改進背包系統不安全的疑慮。由於目前的所設計的背包密碼系統均爲超增結構(Superincreasing Sequence)，即留下被破解的空間，如何克服本項限制因數，方能導入快度且安全的背包理論的密碼系統，亦爲本論文所設計的目標。

二、雙線性群線對

雙線性群數對(簡稱群數對)是由數學家 Andre Weil 所設計用來解決費馬最後定理的雙線性映射函數，一般所謂的群數數，是由一個群對應到另一個群，除 Weil pairing 之外，學者 Tate 亦提出群數對的運算且具有效率上的優勢，專家學者對群數對的原始定義可參考相關文獻 (Boldyreva., 2003)。

根據上述文獻探討的作法，在一個橢圓曲線的有限場上所有點的子群爲 G_1，而在相同有限場之乘法群的子群爲 G_2，在安全的考量下，G_1 與 G_2 之中要計算離散對數問題時，必須爲計算上是不可行的。在公開密碼學的發展過程中，群數對首先是被用來破解橢圓曲線密碼學的密碼分析方法，適用於特殊的橢圓曲線(如 supersingular curve)，可將離散對數問題簡化對應成等同於一般的有限場的離散對數，進而使得這類的橢圓曲線喪失密碼機制中的實用性和可靠性。所以，群數對一開始在密碼學應用領域裏是扮演破壞而非建設的角色。由於群數對密碼演算法具有簡潔及效率之優點，近年來基於群數對的密碼機制的相關研究(如金鑰交換、存取控管及各類數位簽章等)，有如雨後春筍般的發表在各個重要的學術研究會議與期刊。群數對技術是一個相當新穎的研究題目，相信在未來幾年之中，相關議題仍會是受到密碼學研究學者的青睞，本論文亦對應用機制之設計有所著墨。

三、盲簽章

盲簽章不只達成傳統數位簽章的需求，並提供另外的功能，也就是說，盲簽章有著可以保護送簽者身份的特性，即所謂的匿名性，可以用來避免送簽者的身份遭到追蹤。這種特性符合無記名投票系統，電子競標及電子現金的機制上對使用者身份保密的需求(Chaum, 1990)：

運作原理概述：

1. 首先使用者選擇一個盲因子(Blinding Factor)，連同要簽章的訊息內容一起經過盲化(Blinding)過程後，得到盲化訊息(Blinded Message)，接著再將此盲訊息傳送給簽章者要求簽章。
2. 當簽章者收到盲訊息後，對其簽章(Signing)，並回送此簽章結果。
3. 最後當使用者收到簽章者的簽章結果後，利用之前所選擇的盲因子，對此簽

章做除盲化(Un-blinding)的動作，得到對於眞正訊息的簽章。

系統演算流程：

■(x, f (x))爲 private key 與 public key

■S(x, m)爲文件 m 的簽章

■B(m, r)爲 blind document, *r* 爲 blind factor

■U(s, r')爲 un-blind signature, *r* 爲 blind factor

■A 傳送 blind document B(m, r) 給 B

■B 用 private key x 對 B(m, r)做簽章,將 S(x,B(m, r))傳給 B

■A 驗證 S(x, B(m,r))，再計算 U(S(x, B(m, r)), r')得到最後的簽章 S(x,m)。

上述說明可知盲簽章的主要精神在於，簽章者在整個簽章過程中，並不能得知他所簽章的眞正訊息爲何，因爲眞正的訊息是經過盲因子的保護；也就是對於簽章者來說，他只能知道簽章後的結果，和之後所收到使用者除盲化之後所得到的對於眞正訊息的簽章，但是簽章者卻無法得知之間的關連性，也就是日後即使簽章者看到某個對眞正訊息的簽章，但他卻無法判定是在那次所簽署的或是由那位使用者所要求的簽章；這樣的特性稱爲不可連結性。與之前的數位簽章比較，對於使用者的隱私而言，已經達到一定程度的保護，盲簽章機制確實已經改善在訊息產生者與簽章者爲不同人的情況下，數位簽章暴露使用者隱私的問題；因此，盲簽章就很適合用在之前談到許多需要考量使用者隱私的應用上，如本文所導入軍事採購作業中之投標者與開標作業之實際應用。

肆、植基於背包理論與雙線性曲數對的盲簽章系統

本章節將描述我們所提出的方法。本方法需六個階段，包括系統建置、金鑰成成、盲簽章、簽章、驗盲簽章及驗證簽章，系統演算法如后(蘇品長，2007)：

符號定義：

符號	說明
小寫字母	整數值
大寫字母	橢圓曲線上的點
δ	遞增序列
Δ	超增序列點
order( )	秩；序；階
GCD(a, b)	最大公因數

定義一：

群數對的基本安全假設爲 Gap Diffie-Hellman Problem (GDHP)。相關的安全假設如后：

- Computational Diffie-Hellman Problem (CDHP):

若 $a, b \in Z^*_q$,給定$(P, aP, bP) \in G_1$，計算 abP 的值。

- Decision Diffie-Hellman Problem (DDHP) :

若 $a, b, c \in Z^*_q$, 給定

$(P, aP, bP, cP) \in G_1$, 判斷是否 $c = ab \pmod q$。

- Gap Diffie-Hellman (GDH) Problem:

在 G_1 中，DDHP 是容易的問題，但 CDHP 在計算上是不可行的問題。

定義二：

「超增序列點」產生方法說明如后：

步驟 1：Ep(a, b)上的加法規則，對曲線上所有的點$P, Q \in E_p(a, b)$而言，須滿足：

1.$P + O = O + P = P$;

2.假如 $x_2 = x_1$ 且 $y_2 = -y_1$，亦即

$P = (x_1, y_1)$，

$Q = (x_2, y_2) = (x_1, -y_1) = -P$,

則 $P + Q = O\lambda$ 。 (4-6)

3.假如 $Q \neq P$, 則 $P+Q = (x_3, y_3)$的計算方式爲：

$x_3 = \lambda^2 x_1 - x_2 \bmod p$,

$x_3 = \lambda(x_1 - x_3) - y_1 = \bmod p$, (4-8)

where

$\lambda = (y_2 - y_1) / (x_2 - x_1) = If\ x_1 \neq x_2$

$or\ \lambda = (3x_1^2+a)/2y_1\ If\ x_1=x_2, y_1 \neq 0.$

步驟 2：挑選曲線上的一點 $P=(x_0, y_0)$

計算 $order(P)=q$。

步驟 3：選擇一個曲線上的超增序列點 (super-increasing point)

$$\Delta = \{ a_i P \mid 1 \le i \le n \}$$

$$a_1 \approx 2^n,\ a_j > \sum_{i=1}^{j-1} a_i,\ 2 \le j \le n,\ a_n \approx 2^{2n}, \sum_{i=1}^{n} a_i < p$$

定義三：

「超增序列」爲：

令 δ=$\{a_1..., a_n\}$爲一遞增序列，滿足

$a_j > \sum_{j=1}^{j-1} a_i,\ j>1$ 時，即稱爲 δ 超增序列。

定義四：

橢圓曲線離散對數問題(Elliptic Curve Discrete Logarithm Problem , ECDLP)：

給定定義一個 q 階的橢圓曲線 E，其中二個點 P 和點 Q，如果存在 a，使得 $Q = aP$，嘗到由 P,Q 找出 a 值即爲 ECDLP。ECDLP 是比因子分解問題更難的問題，從目前已知的最好求解算法來看，160bits 的橢圓曲線密碼算法的安全性相當於 1024bits 的 RSA 算法。

【系統建置】

金鑰認證中心挑選一隨機整數 $s \in Z_q^*$ 作爲系統的私密金鑰，另公佈曲線上的超增序列點(super-increasing point) $\Delta = \{a_i P \mid 1 \le i \le n\}$，並計算其公開金鑰 $P_{pub} = sP$

【金鑰生成】

Alice(招標機關)選擇一私密參數 w，必需符合 $GCD(q, w)=1$，並計算其公告訊息(U, V)：

$U = \{u_i \mid 1 \le i \le n, u_i = a_i P\}$

$V = \{v_i \mid 1 \le i \le n, v_i = wa_i P_{pub}\}$公告；有意參與投標者 Bob 逕自公告中心下載。

【盲 簽 章】

針對投標內容 m，Bob 隨機選取一私密參數 $r \in Z_q^*$，並計算簽章

$$\hat{M} = r \cdot m \sum_{j=1}^{n} w_j \quad a_j P_{pub}$$

並將 $\hat{M}$ 傳回給 Alice。

【簽　章】

Alice 計算：

$$\hat{M} = r \cdot m \sum_{j=1}^{n} w_j \quad a_j P_{pub}$$

並將 $\hat{M}$ 回傳給 Bob。

【驗盲簽章】

Bob 收到盲簽章 $\hat{X}$，執行驗證的計算：

$$X = r^{-1} \hat{X}$$

X 即爲在 $\hat{M}$ 上的簽章。

【簽章驗證】

由定義，Decision Diffie-Hellman Problem (DDHP)，驗證：

$V_{DDH}(P, mV, P_{pub}, X) = \text{true}$

$V_{DDH}(0)$爲解決在 G_1 中 DDHP 之有效率的演算法。

【決標】

由認證中心授權(監察單位)將標單解密並宣佈結果。

【異議處理】

由認證中心授權(監察單位)審視簽章過程中各自簽驗訊息，達不可否認性。

伍、安全性探討

本章將針對一般對盲簽章系統威脅性最大的三種常見攻擊模式(Boldyreva, 2003)，盲簽章安全性、僞造簽章及系統設計利用簡單的說明加以評估並檢驗其安全性。

命題 1：嘗試攻擊盲簽章機制，使其喪失盲簽章意義。

說明：由於參數 r 爲自 Z_q^* 所隨機選取，所以 $\hat{M} = rmV$ 同樣亦爲 G_1 之隨機成員。簽署者只能從接收者取得隨機資料而無法還原原始訊息。

命題 2：嘗試僞造合法者的金鑰攻擊。

說明：由於簽署章者必須擁有其他的金鑰

(w', P_{pub}')符合公開金鑰的驗證 V，在未取得私密金鑰 s 的情況下，計算(w', P_{pub}')以滿足$\hat{M} = rmV$，將面臨解 ECDLP 的難題。簽章者可利用驗證公式 $V_{DDH}(P, mV, P_{pub}, X) = \text{true}$ 來揪出偽造者。

命題 3：嘗試攻擊系統的設計機制。

說明：在簽署階段，簽章者可得到盲簽章$\hat{M} = rmV$訊息，而在驗證階段取得簽章 X，$X \equiv m\sum_{j=1}^{n} a_j b_j P_{pub}$。由給定的公開值$(\hat{M}, X)$，導出$\hat{X}$在計算上爲不可行，必須先取得隨機所選取的參數 r^{-1}；由給定的公開資訊 $\hat{X}$，導出 w^{-1} 在計算上爲不可行，同樣面臨到解 knapsack 及 ECDLP 的難題。

陸、結　論

政府採購法第一〇四條列有軍事採購之除外規定，包括軍事機關辦理武器、彈藥、作戰物資或國家安全或國防目的採購案之有關作爲，均得適用，明確界定本條款之適用範圍，使軍品採購與一般政府採購作業之差異減至最低，並能達到國際化及實際作業之需要。政府採購法之首要精神及原則即爲資訊公開，然公開與保密卻是相互衝突的，故軍事採購資料之公開，顯然與國軍部分軍機保密與安全作爲有相互衝突之虞；因此，如何能滿足政府採購法之要求，滿足資訊公開透明同時，亦能有效落實軍機安全維護。因此設計完整的電子化採購招標機制及管制作爲，爲本研究之主要目的。

本系統架構後續應與國軍認證中心、加解密標準及權限控管等安全機制相互整合，確保國軍安全認證機制之一致性外，並能使國軍各項資訊系統及機敏資料交換均能便利及安全之前提下獲取最大之效益。

不斷地設計及驗證具安全性且符合潮流需求之公鑰密碼系統，一直是密碼領域研究者努力突破的目標，在強調資訊安全的現實生活中，能提供安全且不影響執行效率的演算法並能導入實際的業務領域內，爲本研究另一積極追求的目標。自政府採購法實施，已符合世界政府採購之潮流，但不可諱言，政府採購法及其四十餘種子法，相關條文達上千條，可謂一部龐大之法案，軍事採購亦受此法案之限制及保護，唯有強化採購系統安全，方能杜絕不必要之糾紛、爭議與人爲弊端，有效提升採購效率。

柒、國防領域之應用

本研究以國防採購作業爲導入對象。國防機構爲政府機關之範疇，配合政府推動「產業電子化推動方案」政策，應善加利用資訊科技與資訊管理兩項重要的觀念與技術，促進國防事務的競爭力。目前架構在網際網路上之相關電子化服務包括：電子付款、電子拍賣、電子投票、電子採購……等，成功基礎在於能夠提供方便、安全的資料交換方式，因此在安全上有諸多問題點需詳加考慮及預防。

政府採購法之首要精神及原則即爲資訊公開，然公開與保密卻是相互衝突的，故軍事採購資料之公開，顯然與國軍部分保密與安全作爲有相互衝突之虞；因此，如何能滿足政府採購法之要求，亦能有效落實軍機安全維護，則爲導入本系統的主要構想。後續應與國軍認證中心、加解密標準及權限控管等安全機制相互整合，確保國軍安全認證機制之一致性外，亦能將軍事採購從施政計畫、作需、細分、投綱、規劃設計、預算編列、採購、發包施工、完工驗收、移交使用及效益考核等各階段作業，納入系統整合，除提供電子化機制外亦能防患缺失或弊端於未然。

參考文獻

賴溪松、邱榮輝、林祝興、盧而輝及張克章，2004。電子簽章應用與實習，旗標。

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

Dukach, S., 1992. SNNP: A simple network payment protocol, *Proceedings of Computer Security Applications Conference*, 173-179, November 1992.

Low,S., Maxemchuk, N., and Paul, S., 1996. Anonymous credit cards and its collusion analysis, *IEEE Trans. Networking*, Vol. 4, No.6, 809-816.

Lysyanskaya, A., and Ramzan, Z., 1998. Group blind digital signatures : A scalable solution to electronic cash, P*roceedings of Financial Cryptography*, LNCS 1465, Springer-Verlag, 184-197.

Medvinsky, G., and Neumann, B., 1993. NetCash: a design for practical electronic currency on the Internet, P*roceedings of the First ACM Conference on Computers and Communications Security*, 102-106, November 1993.

Stein, L., Stefferud, E., Borenstein, N., and Rose, M., 1994. *The green commerce model, Technical Report*, October 1994.

Rivest, R.L., Shamir, A., and Adleman, L.M., 1979. A method for obtaining Digitalized signatures and public-key functions as intractable as factorization, *Technical Report, MIT/LCS/ TR212, MIT Lab., Computer Science, Cambridge*, vol. 21, 120-126.

Chaum, D., 1983. Blind signatures for untraceable payments, *Advances in Cryptology-CRYPTO'82, Plenum*, 199-203.

Stadler, M., Piveteau, J.M., and Camenisch, J., 1995. Fair blind signatures, *Advances in Cryptology-EUROCRYPT'95, LNCS 921, Springer-Verlag*, 209-219.

Camenisch, J., Piveteau, J.M., and Stadler, M.A., 1994. An efficient fair payment system protecting privacy, *Proceedings of ESORICS'94, LNCS 875, Springer-Verlag*, 207-215.

Chaum, D., Fiat, A., and Naor, M., 1990. Untraceable electronic cash, *Advances in Cryptology-CRYPTO'88, LNCS 403, Springer-Verlag*, 319-327.

Camenisch, J., Piveteau, J.M., and Stadler, M.A., 1995. Blind signatures based on the discrete logarithm problem, *Advances in Cryptology-EUROCRYPT'94, LNCS 950, Springer-Verlag*, 428-432.

ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, vol. 31, 469 - 472.

Horster, P., Michels, M., and Petersen, H., 1994. Meta message recovery and Meta blind signature based on the discrete logarithm problem and their applications, *Advances in Cryptology-ASIACRYPT'94, Springer-Verlag*, 185-196.

Harn, L., 1995. Cryptanalysis of the blind signatures based on the discrete logarithm problem, *Electronic Letters*, Vol. 31, No.14, 1136.

Mohammed, E., Emarah, A.E., and Shennawy, K.E., 2002. A blind signatures scheme based on ElGamal signature, *17th National Radio Science Conference*.

Harn, L., 1994. Public-key cryptosystem de-

sign based on factoring and discrete logarithms, *IEE Proc. Comput. Digit. Tech*., Vol. 141, No. 3, 193-195.

Lee, N.Y. and Hwang, T., 1996. Modified Harn signature scheme based on factoring and discrete logarithms, *IEE Proc. Comput. Digit. Tech*., Vol. 143, No. 3, 196-198.

Shao, Z., 1998. Signature schemes based on factoring and discrete logarithms, *IEE Proc. Comput. Digit. Tech*., Vol. 145, No.1, 33-36.

Lee, N.Y., 1999. Security of Shao's signature schemes based on factoring and discrete logarithms, *IEE Proc. Comput. Digit. Tech*., Vol. 146, No. 2, 119-121.

He, W.H., 2003. Digital signature scheme based on factoring and discrete logarithms, *Electronics Letters*, Vol. 37, No. 4, 220-222.

Su, P.C., Lu, E.H., and Chang, H.K.C., 2005, A knapsack public-key cryptosystem based on elliptic curve discrete logarithm, *Applied Mathematics and Computation*, Vol.168, Issue 1, 40-46.

Michael, R., and David, S., 1979. Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman & Co., New York.

Shamir, A., 1984. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem, *IEEE Transactions on Information Theory*, Vol. 30, Issue 5, 699-704.

Boneh, D., and Franklin, M., 2001. Identity-based encryption from the weil paring, *Proc. CRYPTO 2001, Springer-Verlag*, 213-229.

Verheul, E., 2001. Self-blindable credential certificates from the Weil pairing, *Advances in Cryptology-Asiacrypt'2001, LNCS 2248, Springer-Verlag*, 533-551.

Merkle, R., and Hellman, M.E., 1978. Hiding information and signatures in trapdoor knapsack, *IEEE Transactions on Information Theory*, Vol. 24, Issue 5, 525 - 530.

Boldyreva, A., 2003. Efficient threshold signature, multisignature, and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme, *Proc. CRYPTO 2003, Springer-Verlag*, 31-46.