自我認證之多文件門檻式簽密機制 －以國軍電子公文系統為例

黃國維[1] 蕭柏薰[1] 呂俊成[1] 蘇品長[2*]

[1]國防部
[2*]國防大學管理學院資訊管理學系

論文編號：

收稿2013年05月22日 → 第一次修訂2013年07月16日 → 同意刊登2013年08月08日

摘要

「國軍電子公文系統」為國軍各單位或與政府各機關團體彼此間，依照行政院所頒佈之公文程序條例所撰擬的文書，並將所產製文件透過資訊系統及網際網路相互傳遞，主要用於處理涉及政策、制度、督導、考核、管理及執行之策劃與落實。鑑於網路與密碼技術趨於成熟，資安防護機制相關研究已受到重視，故如何運用安全的機密機制導入國軍電子公文系統，減低洩密情事，值得探究。現今的加密作業大多採用一份文件執行一次加密的方式，惟當文件數目數以萬計時，將導致運算繁複與時間耗費，為提供國軍作為未來電子公文系統規劃之參考範疇，本研究利用橢圓曲線密碼系統快速運算的特點，提出多重公文一次簽密之應用方法，在相同的密鑰長度下，其運算速度將比現行RSA、ElGamal 演算法更加快速，並減少公文的簽密次數，達到提升效率、縮短作業時間與增加安全性的效益。此外亦結合了（t, n）門檻式加密機制，使其密文具有門檻的特性，當解密者人數未達到門檻值時則無法解開密文，可防止有心人惡意竊取與監守自盜的情事發生。另本研究同時設計自我認證機制，使得完成註冊程序的通訊雙方能在不依賴第三方認證中心的條件下，利用公鑰及簽章等參數資訊相互進行認證，將能更有效率的縮短作業時間，並防止憑證中心的偽冒攻擊。

關鍵詞：自我認證，橢圓曲線，多文件，門檻式，簽密機制

Self-Certified and Threshold Multi-Document Mechanism of Signature Schemes-a Case Study of Military E-Document

Kuo-Wei, Huang[1]　Po-Hsun, Hsiao [1]　Ji-Cheng, Liu [1]　Pin-Chang, Su [2*]

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

Abstract

Military e-document system of Military units follows the documents procedure ordinance of the Executive Yuan to produce electronic official documents and to exchange between government agencies and organizations through information management systems on the Internet. The e-document system is mainly used for processing, planning, and implementation of policies, supervision, assessment, management and execution. Owning to maturing Internet network and cryptographic technologies, information security studies have been emphasized. Therefore, it is worth studying to apply secure and confidential mechanisms to reduce divulgation in military e-document system. Though numbers of one-time encrypted documents will result in complicated computing and time-consuming, the study proposed a new mechanism for planning future electronic document system. The study applied elliptic curve cryptography technique to speed up computation for one-time signature multiple documents. Under the same length of encrypted key, the computation time will faster than the current RSA and ElGamal algorithms. The signcryption times and operation period will be promoted. The proposed scheme will be more secure and efficient. In addition to （t, n）threshold signcryption mechanism, the scheme also has ciphertext threshold characteristics. The document cannot be decrypted without reaching the threshold of decrypting numbers, and then the ciphertext malicious theft and embezzlement occurrences can be prevented. Furthermore, the study proposed self-certified mechanisms to use public key and signature to complete cross authentication procedures without third-party certification center. It will be able to prevent counterfeit certificate center attack more efficiently.

Keywords: Self-certified scheme, Elliptic Curve Cryptosystem, Multi-document, Threshold, Signcryption scheme

壹、前言

綜觀人類的歷史演化過程，大都根據著科技的演進而逐漸進步。人與人之間的往來與交流，有時往往會因利益關係而伴隨著機密性；故資訊安全的需求，一直以來都是一門十分重要的學問。小到個人的隱私，大至國家的軍事機密，各時代的學者皆努力的利用當代的頂尖科技與技術，來尋求一種絕對安全、無法被破解的保護秘密的方法。

那到底什麼樣的密碼系統才能稱為一個安全的密碼系統呢？Shannon (1949) 所提出的密碼系統安全定義中包含了兩種，一種為理論安全 (Theoretical Security)，另一種則為實際安全 (Practical Security)。所謂的理論安全，指的是不論被破密者截獲了多少的密文加以分析，其破解密文的難度和直接猜測明文的難度是一樣的。而所謂的實際安全是假設每一密碼系統在給定 n 位密文時，均有一個破解此系統的最少工作次數，稱為此系統的工作特性 W（n）（Work Characteristic）。若一系統的 W（n）大到使得具有有限計算能力及記憶體的破密者無法在合理的時間內破解此系統，則此系統即可稱為實際安全（Practical Security）或計算上安全（Computational Security），而這種實際安全亦為各國的專家學者共同的研究的目標。

橢圓曲線密碼系統(Elliptic Curve Cryptography; ECC)從 80 年代中期由 Miller (1985)及 Koblitz (1985) 發表以來，就因為其特性與運用性而常被人提出與 RSA 密碼系統相提並論，故雖然較晚出現，但相關研究與應用方面亦發展的十分迅速。一般認爲，160bit 位元域上的橢圓曲線密碼系統，其安全性相當於 RSA 使用 1024bit 模數（蘇品長，2007）。橢圓曲線密碼系統的誘人之處在於安全性相同的前提下，可使用較短的私密金鑰，進而達到與 RSA 相同的安全性。私密金鑰較短意味著所需要電腦網路的頻寬和記憶體較小，這在現今網際網路蓬勃發展與未來的雲端運算上，將是個決定性的關鍵。

在實際的企業中，常常存在著需要多個高階主管來共同決定一項事務通過與否的案例，或者是最高決定者因故無法對具有時效性的案子立即做出回應，需要多個次級主管共同來代替決策；在密碼學的領域之中，這被稱做為秘密分享（Secret Sharing）（張真誠、韓亮、賴溪松，1999）。最典型的例子是保險庫鑰匙的例子（張真誠、韓亮、賴溪松，1999）：一把保管了重要機密的保險庫鑰匙，如果這一支鑰匙只交給某一個經理保管，這會發生下列幾個問題：1.當需要領取保險庫的重要機密時，這位經理一定要出席才能打開。2.若這位經理發生意外，造成保險庫鑰匙遺失，則會造成保險庫不能運作。既然是保險庫，自然是不可能請人開鎖的。3.如果這位經理把鑰匙複製多份，出賣給別人，則保險庫就不再安全。如果當初就將保險庫鑰匙複製多份，由多位經理共同保管，雖然能降低鑰匙遺失的風險，但如果有任何一位經理將鑰匙複製並出賣給他人，則將無法證明是誰出賣的。而如果把保險庫鑰匙打造成 n 份次鑰匙，分別給 n 位經理保管，雖然能解決前述的安全問題，但是實際上運用效率卻很差，因為需要 n 位經理全員到齊後，才能將保險庫開啟，所以需要有一個具有安全性且有效率的方法。

由 Shamir 及 Blakley（1979） 於 1979 年分別提出的（t, n）門檻式密碼系統（Threshold Scheme），保留了秘密分享的特點並有效的改進了其中的缺點，進而使其具有門檻的限制，其主要的概念如下：1.將最初的主密鑰打造成 n 份不同的次密鑰，並讓每一位參與者都持有一支次密

鑰。2.當次密鑰的數目超過或等於門檻值 t 時，可以從中導出主密鑰。3.當次密鑰的數目小於門檻值 t 時，因資訊不足而無法導出主密鑰。

之後許多關於門檻式密碼系統的研究陸續的被學者所提出。1986 年 Boyd (1986) 首先提出以 RSA 為基礎的門檻式密碼系統，而 1991 年時由 Desmedt 和 Frankel（1991）加以改良成以 RSA 為基礎的（t, n）門檻式簽章協定。L. Harn（1993）則於 1993 提出以 DLP (Discrete Logarithm Problem，離散對數問題) 為基礎的（t, n）門檻式群體數位簽章協定。Pedersen（1991）於 1991 年時首先提出基於橢圓曲線可驗證的秘密分享協定；爾後陸續有 Han、Yang 和 Sun（2003）於 2003 年時提出基於橢圓曲線可驗證的門檻式簽章協定，Chen（2005）於 2005 年時所提出基於門檻式橢圓曲線數位簽章的演算法。由於門檻式密碼系統的用途廣泛，能使企業的決策模式更加靈活，因此一直都是學者們研究的課題。

適用於網際網路的身分認證機制種類相當的繁多，雖然目前在實務的設計上大多採用以公正的第三方所配發的電子憑證（Certificate Authority, CA）為基礎的方式來處理與相關的身分安全認證事宜，但這必須有個很重要的先決條件，就是必須確保這系統認證中心是可靠且能安全的保護金鑰目錄，不會有偽冒使用者的金鑰之情事發生。為了改善這種過度依賴第三方憑證中心的情形，1991 年時由學者 Girault（1991）提出建立於公開金鑰密碼系統下的自我認證機制，金鑰產製中心無法直接得知註冊者的私密金鑰，而在使用階段通訊雙方在完成註冊程序後，即可不再需透過公證的第三方來執行身分認證作業，能獨立進行雙方身分的自我認證程序。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，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（沈誼中，2002）。

現今的加密作業，大多是採用一份文件作一次加密的方法，但當文件數目數以萬計時，將導致大量的運算繁複與時間耗費。因此在本研究之中，有別於傳統的一份文件加密一次的方法，我們提出多重文件的加密方法，除了能一次性的加密多份文件（蘇品長、高嘉言，2010）外，在傳送密文方面，收方訊息的檢查除了單向雜湊函數的檢查之外，同時於密文間執行橢圓曲線點加運算，使得密文產生雪崩效果，可加強密文之完整性與安全性。本研究植基於橢圓曲線的多重文件門檻式加密機制，除了結合橢圓曲線加密法與門檻式加密機制的優點，更能一次加密多份文件，使其能節省文件加密的時間，避免重複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的目的。

貳、文獻探討

一、電子公文沿革與發展

電子公文系統為各機關團體彼此間，依照行政院所頒佈之公文程序條例所撰擬的文書，並將所產製文件透過資訊系統及網際網路相互傳遞之系統。經綜整國內各學術單位研究成果及文獻探討後，電子公文及電子公文系統相關定義如下：

（一）沈誼中（2002）：電子公文系統是一套軟體程式，用來取代傳統紙張式的公文，改以電腦來處理公文。

（二）唐台生（2006）：電子公文系統可視為一種資訊系統，此系統使公文電子化管理確實能達到政府所預期的效能，就過程而言，使電子公文的

製作品質與傳遞品質能有效控管。

（三）白美貞（2004）：電子公文係將人工傳遞的紙本公文書，藉由電腦處理後，透過網際網路傳遞給受文者。

（四）楊增祥（2010）：電子公文係辦公室自動化管理系統的一部份，藉由公文電子化的實施，可提升辦公室行政效率與效能。

針對國軍電子公文發展情況，國軍公文係依照行政院指導於民國 88 年開始導入電子公文系統，並頒行「國軍文書處理手冊」，以利各單位執行公文相關作業能有所依循，期間於民國 94 年因應精進案政策實施國軍文書、檔案作業流程具體簡化檢討，推動「公文書橫式書寫推動方案」實施計畫，於民國 98 年為配合政府節能減碳要求及公文減紙減量計畫、強化機密文書之管理、公文書資訊化之要求，以提升國軍文書與檔案作業運作效能，建立完備作業機制(國防部，2009)，並於民國 100 年 10 月正式啟動公文線上簽核作業並結合 RSA 演算法的數位簽章機制，期配合行政院指導達成公文處理全程電子化之目標。

依國軍現存電子公文處理程序，採用的是公文一次簽辦一份公文的模式，公文處理程序如圖 1，而在公文呈核的流程中，利用的則是層級逐步往上的方法，雖有代理人制度，仍因軍中特性而徒具形式，若因單位指揮官因任務需求(例：演習或開會)無法批閱機密公文，而機密公文往往具有時效性將於限定日期辦畢，此時代理人雖可代為決行，惟因機密公文之重要性係取決於指揮官之決策權，因此常錯過最佳決策時機而導致公文延宕情事屢見不鮮。基於國軍所處理各項業務有其保密需求，若機密外洩將使國防安全遭致嚴重損害，故運用電子公文系統執行線上簽核作業應具備更有效率、安全之加密機制，惟基於 RSA 的簽章機制之運算速度及簽章長度無法符合效率及安全的需求，故國軍仍應以提升安全性、效益性為首要改善目標，目前國軍電子公文系統線上簽核及公文交換流程圖如圖 2。

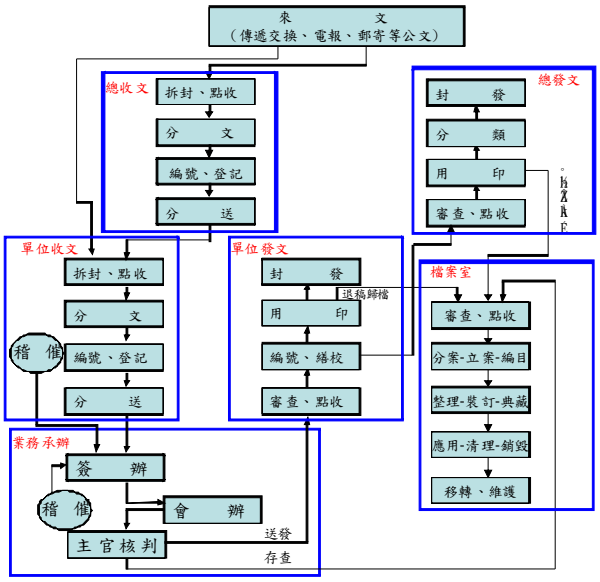

圖 1 公文處理程序圖

圖 2 電子公文系統線上簽核及公文交換流程圖

二、橢圓曲線公開金鑰密碼系統

最早提出將橢圓曲線用來實作公開金鑰密碼系統，是由 Miller（1985）於 1985 年及 Koblitz（1987）於西元 1987 年首先提出。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，假使一條直線與此橢圓曲線相交於三點，則此三點的和為無窮遠點 O。如果 q 是大於 3 的質數，則在 Galois Field $E(F_q)$ 中，橢圓曲線的通式如下，

$y^2 = x^3 + ax + b \bmod q$ 其中 $0 \le x \le q$，a、b 為小於 q 的正整數且 $4a^3 + 27b^2 \bmod q \neq 0$。我們假設下面兩點 $P(x_1, y_1)$ 及 $Q(x_2, y_2)$ 為橢圓曲線群 $E(F_q)$ 中的兩個點，則此橢圓曲線群 $E(F_q)$ 中的點加法運算如下定義：

- $P + O = O + P = P$
- 如果 $x_1 = x_2$，$y_1 = -y_2$，則 $P = (x_1, y_1)$ $Q = (x_2, y_2) = (x_1, -y_1) = -P$ 且 $P + Q = O$。
- 如果 $P \neq Q$ 則 $P + Q = (x_3, y_3)$

  $x_3 \equiv \lambda^2 - x_1 - x_2 \bmod q$（mod 為模數計算）

  $y_3 \equiv \lambda(x_1 - x_3) - y_1 \bmod q$

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

在橢圓曲線的求點運算中，若要計算 $2P$ 則等同計算 $P + P$，相同的若要計算 $3P$ 則等同計算 $3P = 2P + P$，假設一個橢圓曲線是屬於 F_q，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，破密者除了逐一的窮舉所有可能的點之外，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，從表 1 所示，RSA 與 ECC 之金鑰長度與安全性比較（蘇品長，2007），可看的出 160 位元域上的橢圓曲線密碼系統，其安全性相當於 RSA 使用 1024 模數，在同樣的安全度之下， ECC 僅需要較小的密鑰長度，運算效率較佳；相同地，在同樣的密鑰長度下， ECC 擁有更高的安全性了。

表 1RSA 與 ECC 之金鑰長度比較表

RSA與ECC於相同安全度下之金鑰長度比較表					
RSA	512	1024	2048	3072	7680
ECC	112	160	224	256	384
Key	1:5	1:6	1:9	1:12	1:20

三、橢圓曲線加密方法

橢圓曲線加密一般使用 ElGamal 的橢圓曲線加密法，方法總共分為三部分，系統初始階段、加密階段及解密階段，各階段分述如下：

（一）系統初始階段

1. 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 $nG=O$，其中為 O 此橢圓曲線之無窮遠點。
2. 簽章者隨機選擇一整數 n_A 當成私鑰，其中 n_A 介於 $[1, n\text{-}1]$。
3. 計算加密者公鑰 $Q = n_A G$。
4. 將 (E, G, n_A, Q) 公開。

（二）加密階段

1. 令明文 m 為 E 上的一點 M。
2. 加密者任選一個整數 $k \in [1, n-1]$。
3. 計算密文 $(C_1, C_2) = (C_1 = kG, C_2 = M + kQ)$，其中 Q 為收方之公鑰。

（三） 解密階段

計算明文 $M = C_2 - n_A C_1$。

四、(t, n) 門檻式密碼系統

（t, n）門檻式密碼系統是 Shamir 及 Blakley（1979） 於 1979 年分別提出，而其中由 Shamir 所提出的 Lagrange 多項式插入法是最被廣為討論的門檻方法，主要是因為兩個原因：(1) 方法簡單明瞭；(2) 方法的安全性可以達到 Shannon 在訊息論（Information Theory） 中所定義的『完美

安全』（Perfect Secrecy ）特性（1985）。

其（t, n）門檻式密碼系統做法如下：

1. 假設莊家選定主密鑰K及一個質數p，滿足$p > K$。
2. 莊家任選一個 *t-1* 次方的多項式$h(x) = k + a_1 x + a_2 x^2 + ... + a_{t-1} x^{t-1} (\mathrm{mod}\ p)$。其中參數$a_{t-1}$, ... , a_1都是任意整數分佈於[$1, p-1$]範圍內。
3. 注意的是主密鑰事實上是隱藏於多項式h（x）的常數項內。從h（x)可以輕易的求得主密鑰，因為h（0）＝K。
4. 假定每一位參與者都有一個獨一無二的公開識別名字，ID_i。
5. 莊家將依據各人的ID_i 來產生不同的次密鑰 k_i=h（ID_i），i=1,2 ,... ,n。每對（ID_i, h（ID_i））可視為多項式h（x）在二維空間上的一個座標點。
6. 當知道t 對的次密鑰K_{i1}, K_{i2} ,..., K_{it}，可以藉由 Lagrange 多項式插入法恢復如下：

$$h(x) = \sum_{i=1}^{t} K_i \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{x - ID_j}{ID_i - ID_j} (\mathrm{mod}\ p)$$

由於h（x）是 *t-1* 次方的多項式，因此t 對或t 對以上的座標點可以決定唯一的h（x)。若只擁有少於t 對座標點時，由於訊息的不完全，這種情況相當於對h(x)一無所知。正因如此，這個方法可達到 Shannon 所定義的『完美安全』。

五、植基於橢圓曲線的門檻式密碼系統

自從 Shamir 在 1979 年所提出的門檻式秘密分享方案後，許多關於門檻式密碼系統的研究就開始被廣泛的討論。Boyd（1986）於 1986 年首先提出以 RSA 為基礎的門檻式密碼系統，而 1991 年時由 Desmedt 和 Frankel（1991）加以改良成以 RSA 為基礎的（t, n）門檻式簽章協定。L. Harn（1993）則於 1993 提出以 DLP（Discrete Logarithm Problem，離散對數問題）為基礎的（t, n）門檻式群體數位簽章協定。

此外基於橢圓曲線密碼系統的門檻式研究，則由 Pedersen（1991）於 1991 年時首先提出基於橢圓曲線可驗證的秘密分享協定；爾後陸續有 Han、Yang 和 Sun（2003）於 2003 年時提出基於橢圓曲線可驗證的門檻式簽章協定，2005 年時由 Chen（2005）所提出的基於門檻式橢圓曲線數位簽章的演算法。

依據橢圓曲線加密方法改良而成的門檻式密碼系統，共分成二個階段，分別為加密階段與解密階段。各階段的詳細作法描述如下：

（一）準備階段

1. 選取一橢圓曲線 E（Fq），q 是一個大質數，並在曲線上選一階數（order）為u 的基點G，使得$uG=O$，其中 O 為此橢圓曲線之無窮遠點。
2. A 選取密鑰a，計算$\beta = a \cdot G$。
3. 公開（E, G, β） 。
4. 透過一個公正的憑證中心建立一個密鑰為a 的（t, n）門檻，其對應的多項式為：
$f(x) = a + a_1 x + a_2 x^2 + ... + a_{t-1} x^{t-1} (\mathrm{mod}\ u)$
5. 假設機制中的參與者P_i所持有的秘密參數為（x_i, s_i）, i=1,2,…,n，其中 $s_i \equiv f(x_i)$ （ mod u）。

（二）加密階段

1. 今B 欲傳遞一訊息m 給A，先將 m 轉換橢圓曲線上的一個點P_m。
2. B 隨機選取一整數 k，並計算密文 CA = （$kG, P_m + k\beta$ ）。

（三）再處理階段

1. B 將密文 C_A 上傳至憑證中心。
2. 憑證中心將密文 C_A=C 做一分散的動作，計算密文：$C_i = (x_i^a, ks_i G, P_m + k\beta)$ ，其中

i=1,2, $\cdots$, n。

（四）　解密階段

1. A 從憑證中心傳送來的密文中，選取 t 份文件，即 $C = \{ C_1 , C_2 , \cdots , C_t \}$，並先使用自己的密鑰 a 解出每個 x_i 的值，而後再計算 ks_ib_iG。
2. 其中

$$b_i \equiv \prod_{\substack{j=1 \\ j\neq i}}^{t} \frac{-x_j}{x_j - x_i} (\mathrm{mod}\, u) 。$$

$$\sum_{\substack{j=1 \\ j\neq i}}^{t} ks_ib_iG \equiv kaG = \begin{cases} k\beta, & \text{if t is odd} \\ -k\beta, & \text{if t is even} \end{cases} (\mathrm{mod} q)$$

3. 運算（$P_m + k\beta$ ）$- k\beta = P_m$，即可還原點 P_m 。
4. 將 P_m 轉換回訊息原本的訊息 m。

六、自我認證機制

1991 年學者 Girault, M.（1991）提出公開金鑰密碼系統下的自我認證機制，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 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。

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。針對公開金鑰密碼系統安全性，Girault 提出三個層次安全等級如表 2。植基於 RSA 的方法設計出來的自我認證機制，共包含四個階段，活動圖如圖 3。

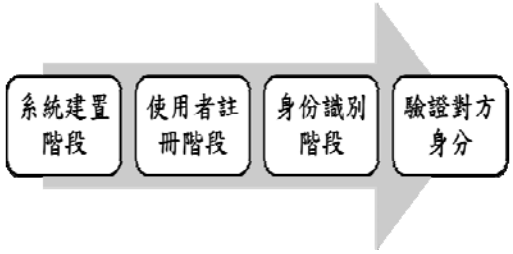

圖 3 自我認證階段活動圖

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

（一）系統建置階段

認證中心以 RSA 的方式取得 e，d 與 N，其中 e 為系統中心的公鑰；d 為私鑰，參數敘述如下：

1. p , q：選擇兩個大質數。
2. N：為 p 與 q 的相乘積之合成數。$N = p \cdot q$。
3. e：認證中心的公鑰。$GCD(e,(p-1)(q-1)) = 1$
4. d：認證中心的私鑰。$ed = 1 \bmod (q-1)(q-1)$
5. g：在乘法群 Z_n^* 中最大序的整數。
6. 公開 N, e, h，d 保密，p 與 q 則在算完 d 後丟棄。

（二）使用者註冊階段

使用者 A 有其身分識別碼 ID_A，步驟如下：

1. 使用者 A 自行選定自己的私鑰 S_A，並計算出 $V_A = g^{-S_A} (\mathrm{mod} N)$ 後，再將身分識別碼 ID_A 與 V_A 傳給系統認證中心。
2. 系統認證中心計算使用者 A 的公鑰 P_A，$P_A = (V_A - ID_A)^d (\mathrm{mod} N)$，並

將 P_A 傳回給使用者 A。

3. 使用者 A 驗證 $P_A^e + ID_A = V_A$，因 $(V_A^d - ID_A^d)^e + ID_A = V_A$，若成立則使用者 A 的公鑰為 P_A，私鑰為 S_A。

（三）身分識別階段

當使用者 A 和使用者 B 兩人相互通訊時，他們之間的身分確認如下：

1. 使用者 A 將其 ID_A 和 P_A 傳給使用者 B，然後 B 計算：$V_A = (P_A^e + ID_A) (\mathrm{mod}\, N)$
2. 使用者 A 選擇一個隨機參數值 x，計算 $t = g^x (\mathrm{mod}\, N)$ 後，將 t 傳送給使用者 B。
3. 使用者 B 選擇一個隨機參數值 C，並將其傳給使用者 A。
4. 使用者 A 計算 $Y = x + S_A \cdot C (\mathrm{mod}\, N)$ 後，並將 Y 傳送給使用者 B。最後使用者 B 利用驗證式：

$$g^Y \cdot V_A^C = t (\mathrm{mod}\, N)$$
$$g^{x+S_A C} \cdot g^{-S_A C} = g^x (\mathrm{mod}\, N)$$

5. 若等式成立則可證明使用者 A 的身分；同理，使用者 A 也可以此方式驗證 B 的身分。

參、具自我認證之多文件門檻式簽密機制設計

在本研究方法中，基於橢圓曲線門檻式密碼系統之基礎上，提出多重文件的運用，使其能一次性的簽密多份文件，並導入可自我認證的機制。使系統內使用者在完成註冊後，能在不依賴第三方認證中心的情況下，利用公鑰及簽章等參數資訊相互進行認證，將能更有效率的縮短作業時間。其系統流程圖如圖 4。

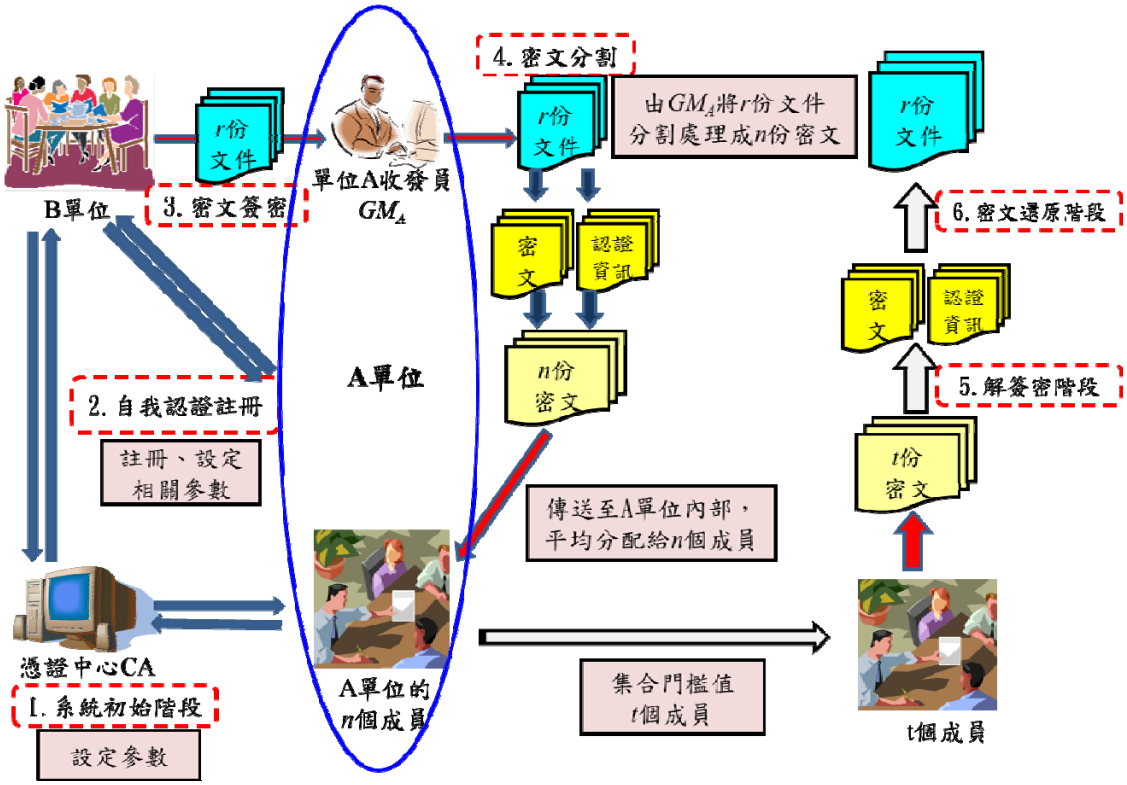

圖 4 系統流程圖

本章設計的系統雛型演算法共分成六個階段，分別為系統初始階段、自我認證註冊階段、密文簽密階段、密文分割階段、解簽密階段、密文還原階段。各階段的詳

細作法描述如下，參數說明表如表 3：

表 3 參數說明表

項次	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	u	橢圓曲線上基點的秩（order）
4	q	$q>2^{160}$ 之質數
5	sk_{CA}	憑證中心 CA 的密鑰
6	PK_{CA}	憑證中心 CA 的公開金鑰
7	$h(\ )$	CA 公開之雜湊函數
8	sk_A、sk_B	GM_A 與傳送者 B 之密鑰
9	SPK_A、SPK_B	GM_A 與傳送者 B 之公開金鑰
10	PK_n	系統內各成員與 CA 完成註冊所取得的驗證公鑰
11	w_n	系統內各成員與 CA 完成註冊所取得的驗證簽章
12	$f(x)$	GM_A 利用密鑰 sk_A 所建立之門檻多項式
13	id_i	A 單位成員之身分參數
14	s_i	A 單位成員之秘密參數
15	$f_{m2p}(\ )$	將訊息轉為橢圓曲線點之函數
16	$f_{p2m}(\ )$	將橢圓曲線點轉為訊息之函數
17	km_B	B 隨機選取的一個整數
18	F_{AB}	GM_A 與傳送者 B 的驗證簽章
19	$\overline{\Gamma}$	傳送者 B 欲傳送之 r 份密文
20	C	包含認證資訊、解密訊息及密文
21	T_i	經 GM_A 切割 C 後所得之 n 份密文

一、系統初始階段

Step1：憑證中心 CA 選取一橢圓曲線 $E(F_q)$，q 是一個大質數，並在曲線上選一階數（order）為 u 的基點 G，使得 $uG=O$，其中 O 為此橢圓曲線之無窮遠點。

Step2：CA 選定密鑰 sk_{CA}，並計算其公開金鑰：$PK_{CA}=sk_{CA}\cdot G$

Step3：CA 選取一個單向雜湊函數 $h(\ )$。

Step4：CA 公開 E、G、u、PK_{CA}、$h(\ )$。

Step5：A 單位之中共有 n 位成員，並設有經主官授權專責審查資料的管理員 GM_A。

Step6：假設 A 單位中的參與者 PN_i 所持有的身分資訊為 id_i，則透過 $f(x)$ 計算秘密參數 S_i 為：

$s_i \equiv f(id_i)(\mathrm{mod}\,u)$，$i=1,...,n$。

二、自我認證註冊階段

在使用者註冊階段，以 GM_A 為例，GM_A 與憑證中心 CA 註冊程序計算式如下：

Step1：GM_A 以自己的 id_A 及隨機參數 d_A，$d_A\in[2,u-2]$，以 d_A 參數值產生簽名檔 V_A，並將 id_A 與 V_A 傳送給 CA，其計算式如下：

$$V_A=h(d_A\|id_A)\cdot G \quad (1)$$

Step2：CA 選擇一隨機參數 $k_A\in[2,u-2]$，並計算 GM_A 之驗證公鑰 PK_A 及簽

章 w_A，並將 PK_A 與 w_A 回傳給 GM_A，其計算式如下：

$$PK_A=\left[V_A+\left(k_A-h(id_A)\right)\right]\cdot G=\left(q_{a_x},q_{a_y}\right) \quad (2)$$

$$w_A=k_A+sk_{CA}\left(q_{a_x}+h(id_A)\right) \quad (3)$$

Step3：GM_A 自行計算私鑰 sk_A，並且驗證金鑰 SPK_A 的正確性，其計算式如下：

$$sk_A=w_A+h\left(d_A\|id_A\right) \quad (4)$$

GM_A 計算其公開金鑰 SPK_A：

$$SPK_A=sk_A\cdot G \quad (5)$$

Step4：其中證明式如下：

$$SPK_A=sk_A\cdot G$$

$$SPK_A=[k_A+sk_{CA}(q_{ax}+h(id_A))+h(d_A\|id_A))]\cdot G$$

$$SPK_A=[k_A+sk_{CA}(q_{ax}+h(id_A))]\cdot G+h(d_A\|id_A)\cdot G$$

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

$$SPK_A=\left[k_A+h\left(d_A\|id_A\right)\right]\cdot G+\left[\left(q_{ax}+h\left(id_A\right)\right)\right]PK_{CA}$$

$$\because V_A=h\left(d_A\|id_A\right)\cdot G$$

$$\because PK_A=\left[V_A+\left(k_A-h\left(id_A\right)\right)\right]\cdot G$$

$$V_A=\left[PK_A-\left(k_A+h\left(id_A\right)\right)\right]\cdot G$$

$$SPK_A=k_AG+V_A+\left[\left(q_{ax}+h\left(id_A\right)\right)\right]PK_{CA}$$

$$SPK_A=PK_A+h\left(id_A\right)G+\left[\left(q_{ax}+h\left(id_A\right)\right)\right]PK_{CA} \quad (6)$$

計算式（6）之代表目的，表示運用相關公開參數演算出一個驗證值後，即可驗證對方公鑰是否正確，故系統內各成員皆須於自我認證註冊階段與 *CA* 完成註冊，一旦各成員自 *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，並可藉由認證中心核發的帳戶相關資料（id_n、PK_n、SPK_n）與需認證身分的通訊方進行認證，而不再需經由憑證中心 *CA* 執行身分認證工作。

三、密文簽密階段

Step1：今 B 欲傳遞 r 份訊息 $\overline{mm}$ 給 A 單位：

$$\overline{mm}=\{m_1,m_2,m_3,\ldots,m_r\}。 \quad (7)$$

Step2：將每份訊息明文 m_i，$i=1,2,...,r$ 分成 2 個區塊。

$$\overline{m_{ij}}=\{m_{11},m_{12},m_{21},m_{22},...,m_{r1},m_{r2}\}$$

，$i=1,2,...,r$，$j=1,2$。 (8)

Step3：對明文做雜湊值運算：

$$h(\overline{m_{ij}})=m。 \quad (9)$$

Step4：利用明文轉點方式將明文序列區塊轉成點坐標 P_i，$i=1,2,...,r$，

$f_{m2p}(\overline{m_{ij}})=\{P_1,P_2,...,P_r\}$。 (10)

Step5：B 隨機選取一個整數 km_B，並計算：$\Gamma=\{\Gamma_1,\Gamma_2,\Gamma_3,\ldots,\Gamma_r\}$，

$\Gamma_i=P_i+km_B\bullet SPK_A$，$i=1,2,...,r$。 (11)

Step6：B 計算簽章值：

$$st=km_B/(m+sk_B)。 \quad (12)$$

Step7：B 計算 $\overline{C}=\left\{km_B\cdot G,\overline{\Gamma},st,m\right\}$，將密文 $\overline{C}$ 傳送到 A 單位。 (13)

四、密文分割階段

Step1：GM_A 將 $\overline{C}$ 做一分散的動作（分給每個成員），即計算：

$\overline{C}=T_i$，$i=1,2,...,n$，

$\overline{T_i}=\{id_i^{sk_A},s_i\cdot km_B\cdot G,\overline{\Gamma},st,m\}$。(14)

Step2：GM_A 將密文 *T 平均分配給* A 單位內的 n 個人，即 $T_1,T_2,\ldots,T_n$。

五、解簽密階段

Step1：當 A 單位欲進行密文解密時，首先由 GM_A 計算以下式子：

$$su=(st\cdot sk_A)\bmod q。 \quad (15)$$

Step2：由 GM_A 計算以下驗證簽章：

$$F_{AB}=(su\cdot SPK_B+su\cdot m\cdot G)=SPK_A\cdot km_B \quad (16)$$

Step3：齊聚 t 份文件後，即 $T=\{T_1,T_2,\cdots,T_t\}$，依單位作業流程請求 GM_A 使用密鑰 sk_A 解出每個 id_i 的值，再計算以下式子：$km_B\cdot s_i\cdot b_i\cdot G$。 (17)

Step4：運用以下式子執行門檻還原計算：

$$b_i\equiv\prod_{\substack{j=1\\ j\neq i}}^{t}\frac{-id_j}{id_j-id_i}(\bmod u) \quad (18)$$

$$\sum_{\substack{j=1\\ j\neq i}}^{t}(km_B\cdot s_i\cdot b_i\cdot G)\equiv km_B\cdot sk_A\cdot G=$$

$$\begin{cases}km_B\cdot SPK_A,\text{if t is odd}\\ -km_B\cdot SPK_A,\text{if t is even}\end{cases}(\bmod q) \quad (19)$$

Step5：驗證簽章的正確性：

計算出 $km_B\cdot SPK_A$ 或之後，與驗證簽章 F_{AB} 做檢驗，確認式子：

$F_{AB} \stackrel{?}{=} \pm km_B \cdot SPK_A$ 是否成立，若等式不成立則否定其簽章；若等式成立則進行密文解密。　（20）

如簽章驗證成功，將 F_{AB} 代入 $\Gamma_i = P_i + (km_B \cdot SPK_A)$ 之中，運算計算式：$P_i + (km_B \cdot SPK_A) - (km_B \cdot SPK_A)$，即可還原點 P_i'。　（21）

六、密文還原階段

Step1：已聚集符合門檻值的 t 的成員，密文 $T = \{T_1, T_2, \cdots, T_t\}$。

Step2：將點 P_i 轉回訊息，計算：

$$P_i' = \{P_1', P_2', \ldots, P_r'\}。\quad (22)$$

Step3：$f_{p2m}(P_i) = \overline{m_{ij}}' = \{m_{11}', m_{12}', m_{21}', m_{22}', \ldots, m_{r1}', m_{r2}'\}$，$i=1,2,\ldots,r$，$j=1,2$。　（23）

Step4：對明文 $\overline{m_{ij}}'$ 做雜湊值運算

$$h(\overline{m_{ij}}') = m'。\quad (24)$$

Step5：驗證 $m' \stackrel{?}{=} m$，若等式成立，則可立即確認收方所收之訊息正確無誤。　（25）

Step6：將訊息還原：

$$\overline{mm} = \{m_1, m_2, m_3, \ldots, m_r\}。\quad (26)$$

肆、安全性分析與效益評估

本研究所提之加密機制，其安全性主要植基於橢圓曲線離散對數難題（ECDLP）、非對稱加密方式、門檻式機制、單向雜湊函數，可達到ISO組織所提之資訊安全管理需求（ISO, 2005），其中包含 Zheng（1997）所提出簽密法所必備之機密性、完整性、鑑別性、不可否認性與不可偽造性等安全需求（李南逸等，2008）、（楊中皇，2008），並具有自我認證機制。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

本研究所提出之具自我認證之簽密機制，能符合上述各項所需之機密性、完整性、鑑別性、不可否認性、不可偽造性及自我認證等安全需求，以下則針對各項安全需求進行分析與討論。

（一）機密性（Confidentiality）

所謂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。在本研究兩種方法之中，傳輸密文皆使用橢圓曲線加密法，如被第三者竊取了傳輸密文，可獲得（13）式之 $\overline{C} = \{km_B \cdot G, \overline{\Gamma}, st, m\}$，但在破解密文 $\overline{\Gamma}$ 的計 算過程上，因需從 $km_B \cdot G$ 之中推算出 km_B 的數值，破密者將面臨橢圓曲線離散對數的難題。

（二）完整性（Integrity）

所謂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。在本研究中，驗證多重文件之完整性的機制共有兩項，第一項：當單位成員數量低於門檻值時，如果想還原密文，必須要偽造多個子金鑰來還原多項式 $h(x)$，但因對於訊息的不完全，偽造子金鑰是十分困難的，因此無法重建內插多項式 $h(x)$。第二項：若破密者無法破解明文，而隨意捏造密文傳送至單位A，則單位A經由驗證（25）式之 $m' \stackrel{?}{=} m$，如等式無法成立，則可知密文已遭到竄改。

（三）鑑別性（Authenticity）

所謂鑑別性指的是交易資訊的收方可以利用一些公開參數來驗證該訊息來源的合法性，以確保該訊息確實是由宣稱的送方所送來的。本研究使用橢圓曲線簽密演算法（Zheng, 1998）來進行驗證訊息是否確實由送方B所傳送，如果網路中有第三者想竊取資料或進行第三方攻擊，則只能取得系統公開的橢圓曲線參數與基點G及信息傳輸過程中的幾筆資料 SPK_A、SPK_B 與簽章值 st；如破密者欲從中解出 GM_A

的密鑰 sk_A 與送方 B 的密鑰 sk_B，則將面臨破解橢圓曲線離散對數難題。而A單位如欲驗證資料是否確實由 B 所傳送，則由 GM_A 計算（20）式 $F_{AB} \stackrel{?}{=} \pm km_B \cdot SPK_A$，如等式成立，則可驗證確實由 B 方所傳送。

（四）不可否認性（Non-repudiation）

所謂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。在本研究中，假設收方A在接受到密文與送方 B 之簽章值 st 後，透過（15）式驗證值 $su = (st \cdot sk_A) \bmod q$ 及（16）式 $F_{AB} = (su \cdot SPK_B + su \cdot m \cdot G) = SPK_A \cdot km_B$ 來計算驗證簽章 F_{AB}；而在解密過程中經由（19）式 $SPK_A \cdot km_B$ 之計算產生，收方 A 再藉由（20）式 $F_{AB} \stackrel{?}{=} \pm km_B \cdot SPK_A$ 來驗證簽章之正確性；其中隨機數僅只有送方B所知悉，這使得傳送方所發出之密文具有不可否認性。

（五）不可偽造性（Unforgeability）

所謂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。在本研究中，送方B在加密時透過（9）式 $h(\overline{m_{ij}}) = m$ 對明文進行單向雜湊值運算，如密文在傳輸過程之中遭到偽造，則收方A透過（24）式 $h(\overline{m_{ij}}') = m'$ 對解密後之明文進行單向雜湊值運算，並藉由（25）式 $m' \stackrel{?}{=} m$ 驗證文件是否遭到偽造。

如破密者欲偽造送方之簽章，因簽章值是透過（12）式 $st = km_B/(m + sk_B)$ 所計算，破密者無法得知送方 B 所選取之密鑰 sk_B、隨機數 km_B 及明文經由單向雜湊值運算之 m，故無法偽冒送方B之簽章。而收方A亦可藉由（16）式之驗證簽章 $F_{AB} = (su \cdot SPK_B + su \cdot m \cdot G) = SPK_A \cdot km_B$ 與（20）式 $F_{AB} \stackrel{?}{=} \pm km_B \cdot SPK_A$ 來檢驗簽章之正確性。

（六）自我認證機制（Self-certified Scheme）

所謂自我認證是指交談的雙方僅需要靠雙方傳送一些公開的資訊，即可達成雙方身分的確認，而不需透過第三者來做保證或協調。在本研究中，系統內成員以自己的 id_i 及隨機選擇的秘密參數值 d_i 產生簽名檔 V_i，如（1）式 $V_A = h(d_A \| id_A) \cdot G$，而後將 id_i 與 V_i 傳給憑證中心 CA 進行註冊，才能獲得其簽章 w_n 與公鑰 PK_n，並可驗證公鑰之正確性，如（3）式 $w_A = k_A + sk_{CA}\left(q_{a_x} + h(id_A)\right)$。

一旦系統所有成員皆取得公鑰與簽章之後，僅需要使用由 CA 所賦予之公鑰及簽章等參數資料進行相互的身分認證，如（6）$SPK_A = PK_A + h(id_A)G + \left[\left(q_{a_x} + h(id_A)\right)\right]PK_{CA}$，而不需要與 CA 保持連線狀態來進行認證與協調，可達與憑證中心 CA 離線作業之效，並且各階段各成員身分都可有驗證性。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。由於憑證中心 CA 只進行系統使用者註冊與驗證公鑰及簽章的計算及配發，並無進行密文的分割作業。此舉除了使 CA

無法直接進行使用者的公私鑰參數設定，更可避免在遭遇多個傳送者在同一時間內皆傳送大量密文至 *CA* 要求進行密文分割的類似分散式阻斷服務攻擊（Distributed Denial of Service, DdoS）。

二、效益評估

本研究與植基於橢圓曲線的門檻式密碼系統作比較，並打破傳統單一文件加密方法，導入多重文件機制後，可完成多項文件一次性簽密；在處理多份文件時，運算速度所花費的時間預期較傳統單一文件加密方法來的快，可減少加解密次數及傳輸頻寬之需求，降低系統負荷並提升效率及安全性；並設計具自我認證機制，使其系統內每個使用者僅需完成第一次的註冊，爾後在各階段皆不需依賴公正第三方，即可自行完成身分之認證。

利用本研究之系統架構及演算法與國軍電子公文系統所運用之簽章機制進行比較，所作出之分析結果如表 4；另針對本系統雛型演算法所分成六個階段，分別為系統初始階段、自我認證註冊階段、密文簽密階段、密文分割階段、解簽密階段、密文還原階段等，經參酌演算法複雜度效益分析之時間複雜度運算參考表（蘇品長，2007）如表 5，已完成各階段演算法的時間複雜度運算量如表 6。

表 4 現行機制與本研究之比較表

比較項目	現行運作機制	具自我認證之多文件門檻式簽密機制（本研究）
核心原理	RSA 演算法的簽章機制。	橢圓曲線簽密機制、門檻式機制、自我認證。
不可否認性	透過RSA來進行簽章驗證，達到不可否認性。	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。	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，系統內經註冊之使用者，皆可利用公開參數進行相互的身分認證，具備離線作業功能。
密文完整性	使用雜湊函數及RSA數位簽章達到密文之完整性。	●檢查密文之雜湊值，驗證密文須全部正確，否則無法解密。 ●解密時必須達到設定之門檻值，否則無法進行解密。
密文機密性	以RSA演算法的密碼系統進行檔案簽章，另使用國軍加解密軟體達到密文機密性，惟增加金鑰管理複雜度。	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。
安全性提升	無。	要破解本方法之密文，除了面對橢圓曲線離散對數之難題外，同時還須破解 (t, n) 門檻式秘密分享機制之難題，才有辦法成功破解密文還原明文。

表 5 時間複雜度運算參考表

時間複雜度運算量參考表	
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≈0.12 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所需時間（可忽略不計）
T_{MUL}	進行一次模式乘法運算所需時間
t_h	進行一次 hash 所需時間≈1 T_{MUL}

表 6 本研究各階段演算法的時間複雜度運算量

演算法	本研究：具自我認證之多文件門檻式簽密機制	
比較項目	時間複雜度	概估
系統初始階段	1 T_{ECMUL} + 1 T_{ADD}	29 T_{MUL}
自我認證註冊階段	3 T_{ECMUL} + 2 t_h + 6 T_{ADD}	89 T_{MUL}
密文簽密階段	1 t_h +1 T_{ECADD} +3 T_{ECMUL} +1 T_{ADD} + 1 T_{MUL}	89.12 T_{MUL}
密文分割階段	1 T_{EXP}	240 T_{MUL}
解簽密階段	1 T_{MUL} +3 T_{ECADD} +3 T_{ECMUL} +1 T_{INVS}	299.36 T_{MUL}
密文還原階段	1 t_h	1 T_{MUL}
總計	747.48 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，故無從比較。	

伍、結論

本研究提出植基於橢圓曲線簽密法的多文件門檻式簽密機制，能一次性的對多份文件進行簽密，減少文件的簽密次數，達到縮短作業時間之目的。另除了利用門檻機制使密文具有門檻特性外，在運算過程中採用 ECC 來進行文件的簽密，使經過本研究方法簽密之密文具備加解密複雜度，擁有更高的安全性；同時並在第三章的研究方法中導入自我認證機制，使其可降低第三方認證中心的依賴。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、 國軍電子公文系統執行公文交換、呈核時，可利用橢圓曲線密碼系統快速運算的特點，在相同的密鑰長度下，其運算速度將比現行 RSA 演算法更快速。

二、 國軍電子公文結合多重文件一次簽密性之應用方法，能夠減少文件的加密次數，達到提升效率、縮短作業時程的效益。

三、 國軍電子機密公文調閱作業結合（t, n）門檻式加密機制，將使其密文具有門檻的特性，當解密者人數未達到門檻值時將無法解開密文，有效避免機密資訊外洩。

四、 國軍電子公文系統將具自有我認證機制，使得完成註冊程序的通訊雙方不需再透過公正的第三方做驗證，可相互進行身分認證的作業，能有效提高安全性並防止憑證中心的偽冒攻擊。

陸、國防領域之運用

隨著時代的演進，國軍逐漸推動軍隊資訊化、公文電子化，亦運用了管理資訊系統改變了軍中管理模式，如電子郵件系統、電子公文系統、戰情回報系統和人力資源管理系統等，「國軍電子公文系統」為現行國軍各單位間依公文格式所撰擬的文書作業，並透過電腦系統將文件與相關單位相互傳遞，主要在於落實政策、制度之需求、規劃、執行及管理相關業務。鑑於網路與密碼技術逐步趨於成熟，資安防護機制提昇的相關的研究逐漸受到重視，故如何運用安全的機密機制導入國軍電子公文系統中，減低洩密情事，值得探究。

為強化國軍機密資訊管理之應用範疇，本研究所簽密之密文具備門檻性質，使其在某些特定狀況如最高決策者因故無法立即解開密文之情形，可由特定門檻人數的次級決策者或三級決策者來共同進行機密文件之解密，使其更能靈活運用在瞬息萬變的戰場之中。同時亦探討自我認證機制，除了能減少對國軍認證中心之依賴與提升認證速度，更可避免認證資訊在往返國軍認證中心之過程中遭到敵軍之竊取或偽冒。在分秒必爭的戰場上，越快完成機密資訊的加解密代表著擁有更多的時間來進行戰術決策與軍事部屬，因此能加快機敏文件處理效率與縮短作業時間的多文件簽密機制則更顯重要。

參考文獻

王志民，2009，適用於國軍群體資訊管理之身分識別加密機制，國防大學管理學院資訊管理研究所碩士論文。

白美貞，2004，電子公文及檔案管理流程再造之研究-以 A 特殊學校為例，國立彰化師範大學會計學系研究所碩士論文。

李南逸，王智弘，林峻立，張智超，溫翔安，葉禾田譯，2008。網路安全與密碼學概論，台中：滄海書局。

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。

李士勳，2007，可追蹤簽署者的識別身分多門檻簽章，逢甲大學資訊工程學系研究所論文。

呂俊成，2012，多文件門檻式簽密機制之研究，國防大學管理學院資訊管理學系碩士論文。

林修範，2008，電子公文結合數位簽章與認證機制之研究-以空軍電子公文傳送系統為例，國防管理學院資訊管理研究所碩士論文。

沈誼中，2002，電子公文系統安全評估方法之研究與設計，國立成功大學資訊工程學系研究所碩士論文。

唐台生，2006，國軍部隊內部行政公文處理流程之研究－以憲兵某單位電子公文處理系統為例，義守大學資訊管理研究所碩士論文。

國防部，2009，國軍文書處理手冊，台北：國防部。

黃顯舒，2009，安全的公文線上簽核系統，長庚大學資訊管理研究所碩士論文。

邱英捷，2012，強化數位化戰場經營-設計具機密性及可自我身分認證之地空指揮管制通訊網，國防大學管理學院資訊管

理學系碩士論文。
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。
郭文雄，2011，設計具自我認證之國軍網路申訴制度安全機制探討，國防大學管理學院資訊管理學系碩士論文。
陳煜弦，2005，門檻式橢圓曲線數位簽章演算法，臺灣大學電機工程學研究所碩士論文。
張真誠、韓亮、賴溪松，1999，近代密碼學及其應用，台北：旗標出版股份有限公司。
楊增祥，2010，公文電子化政策執行之研究-以國立臺北護理學院為例，銘傳大學公共事物學系研究所碩士論文。
楊中皇，2008，網路安全-理論與實務，台北：學貫行銷股份有限公司。
廖家宏，2011，植基於橢圓曲線之多文件偽造即停簽密機制，國防大學管理學院資訊管理學系碩士論文。
賴峙樺，2003，以橢圓曲線為基礎之簽密法的研究，淡江大學資訊工程學系碩士論文。
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。
蘇品長、胡智卿，2009，植基於橢圓曲線之自我認證加密法，98 年度國防管理學術暨實務研討會。
蘇品長、高嘉言，2010，新的多重文件簽密方法之研究，苗栗 2009 資訊科技應用學術研討會。
戴慧明，公文交換 G2B2C 計畫，參見公文 G2B2C 客戶服務中心網站 http://cs.good.nat.gov.tw/front/F_fcabdl.asp?fid=3559486 [visited 2012/2/15]
行政院研考會，電子公文節能減紙推動方案，參見行政院研考會網站 http://www.rdec.gov.tw/DO/DownloadControllerNDO.asp?CuAttachID=20772[visited 2012/3/1]
Blakley, G. R., 1979, Safeguarding Cryptographic Keys, Proceedings of the National Computer Conference, AFIPS Press, New York, pp. 313-317.
Boyd, C., 1986, Digital Multisignature, Proceedings of the Conference on Coding and Crypto-graphy, Cirencester, pp. 15-17.
Desmedt, Y., and Frankel, Y., 1991, Shared Generation of Authenticators and Signatures, Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, Lecture Notes In Computer Science（576）, pp. 457-469.
Girault, M., 1991, Self-certified public keys, Advances in Cryptology-Euro（547）, Spring-Verlag, pp. 491-497.
Hankerson, D., Menezes, A., and Vanstone, S., 2004, Guide to Elliptic Curve Cryptography, Springer, New York, pp. 15-16.
Harn, L., 1993, Digital Signature with（t,.n） Shared Verification Based on Discrete Logarithms, Electron Lett（29:24）, pp. 2094-2095.
Han, Y., Yang, X., Sun, J. and Li, D., 2003, Verifiable threshold cryptosystems based on elliptic curve, Proceedings of the 2003 International Conference on Computer Network and Mobile Computing, pp. 334-337.
ISO, 2005, Information technology-Security techniques-Code of practice for information security management, ISO/IEC 17799, pp. 1.
Koblitz, N., 1987, Elliptic curve cryptosystems, Mathematics of Computation （48）, pp. 203-209.
Menezes, A. j., and Vanstone, S. A., 1993, Elliptic curve cryptosystems and their implementation, Journal of Cryptology（6:4）, pp. 209-224.
Miller, V. S., 1985, Use of elliptic curves in cryptography, International Crytology Conference 85, New York: Spring-Verlag, pp. 417-426.
Pedersen, T. P., 1991, A threshold cryptosystem without a trusted party, Eurocrypt （547）, pp. 522-526.
Pedersen, T. P., 1992, Non-interactive and information-theoretic secure verifiable secret sharing, Advances in Cryptology Crypto （576）, pp. 129-140.

Qingqi P., and Jianfeng M., 2008, ECC-Based Threshold Digital Signature Scheme without a Trusted Party, 2008 International Conference on Computational Intelligence and Security, pp. 288-292.

Shannon, C. E., 1949, Communication Theory of Secret Systems, Bell system Technical Journal （28:4）, pp. 656-715.

Shamir, A., 1979, How to Share a Secret, Communications of the ACM （22:11）, pp. 612-613

Shiuh, J. W., Yuh, R. T., and Chien, C. S., 2011, Verifiable Threshold Scheme in Multi-Secret Sharing Distributions upon Extensions of ECC, Wireless Personal Communications: An International Journal archive（56:1）, pp. 173-182

Sutikno, S., Surya, A. and Effendi, R., 1998, An implementation of ElGamal elliptic curves cryptosystems, Circuits and Systems, pp. 483-486.

Xueming, W., and Yurong D., 2010, Threshold Group Signature Scheme with Privilege Subjects Based on ECC, 2010 International Conference on Communications and Intelligence Information Security, pp. 84-87.

Zheng, Y., 1997, Digital Signcryption or How to Achieve Cost（Signature & Encryption）<< Cost（Signature）+ Cost（Encryption）（1997）, Advances in Cryptology-Crypto 97 （1294）, Spring-Verlag, pp. 165-179.

Zheng, Y. and Imai, H., 1998, How to construct Efficient Signcryption Schemes on Elliptic Curves, Information Processing Letters （68）, pp. 227-233.