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

蘇品長 [1]
國防大學資訊管理學系
Pin-Chang Su
spc.cg@msa.hinet.net

黃國維 [2]
國防大學資訊管理學系
Kuo-Wei Huang
kkwhuang@gmail.com

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

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。

一、前言

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，並令頒「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 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，提升國軍文書與檔案作業運作效能，建立完備作業機制[1]，現行並已於民國 100 年 10 月正式啟動公文線上簽核作業並結合 RSA 數位簽章機制。惟 RSA 簽章機制之運算速度及簽章長度尚無法保證能避免遭受病毒或駭客攻擊，故國軍仍應以提升安全性、效益性為首要改善目標。

二、文獻探討

(一)國軍公文處理現況

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，如圖 1，而在公文呈核的流程中，雖有代理人制度，仍因軍中特性而徒具形式，導致公文延宕情事屢見不鮮。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，若僅運用 RSA、數位簽章勢將無法達成「理論安全」之特性。專業學者曾就上述所見問題針對電子公文系統之「數位簽章與認證機制」[2]、「公文線上簽核機制」[3]進行研析，目前尚無法滿足國軍應用公文系統處理各項機敏業務時所應具備之機密性、完整性、不可否認性等需求。

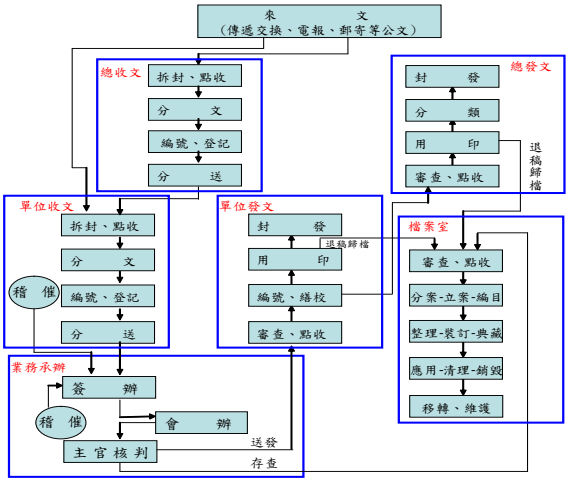

圖 1　公文處理程序圖

(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[4]及 Koblitz[5]提出。在橢圓曲線中，點加法運算是特別定義的，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 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 $E(F_q)$ 中的點加法運算為如下定義。

- $P + O = O + P = P$
- 如果 $x_1 = x_2$，$y_1 = -y_2$，$P = (x_1, y_1)$，$Q = (x_2, y_2) = (x_1, -y_1) = -P$ 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)
- $y_3 \equiv \lambda(x_1 - x_3) - y_1 \bmod q$

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[6]，可看的出 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，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 1　RSA 與 ECC 在相同安全度之金鑰長度比較

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

(三) (t, n)門檻式密碼系統

(t, n)門檻式密碼系統是由 Shamir[7]及 Blakley [8]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[9]在訊息論(Information Theory)中所定義的「完美安全」(Perfect Secrecy)特性。

(四)橢圓曲線版的門檻式密碼系統

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[10]首先提出以 RSA 為基礎的門檻式密碼系統，而由 Desmedt 和 Frankel[11]加以改良成以 RSA 為基礎的$(t,_n)$門檻式簽章協定。L. Harn[12](1993)提出以離散對數問題(DLP, Discrete Logarithm Problem)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[13]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[14]提出基於橢圓曲線可驗證的門檻式簽章協定，Chen[15]所提出的基於門檻式橢圓曲線數位簽章的演算法。

(五)自我認證機制

學者 Girault,M.[16]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[17]。針對公開金鑰密碼系統安全性，Girault 提出三個層次安全等級[18]，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	●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。 ●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、具自我認證之多文件門檻式簽密機制設計-以國軍電子公文系統為例

本研究基於原有橢圓曲線門檻式密碼系統的基礎，導入多重文件的運用，將「多文件簽密機制」[19]、「多文件門檻式加密機制」[20]、「具自我認證之多文件門檻式加密機制」[21]等概念導入國軍電子公文系統，有別於傳統只能進行單一文件的簽密機制，使其能一次簽密多份文件，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 2。

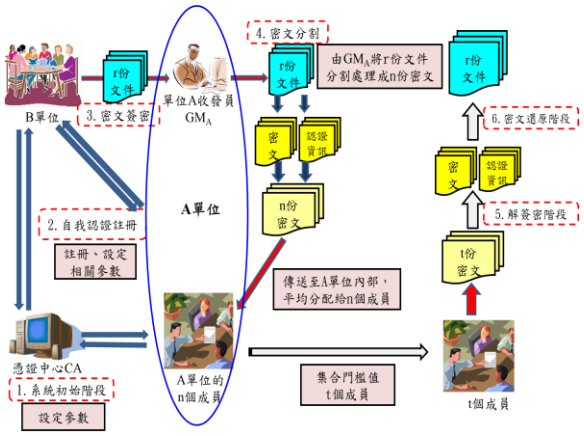

圖 2 系統流程圖

本文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 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	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 $\overline{\Gamma}$ 的密文
21	T_i	經 GM_A 切割 C 後所得之 n 份密文

(一)系統初始階段

●憑證中心 CA 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。

●CA 選定密鑰 sk_{CA}，並計算其公開金鑰：

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

●CA 選取一個單向雜湊函數 $h(\,)$。

●CA 公開 E、G、u、PK_{CA}、$h(\,)$。

●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。

(二)自我認證註冊階段

1.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：

●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。

$$V_A=h(d_A\|id_A)\cdot G \tag{1}$$

●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：

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

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

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

$$sk_A=w_A+h(d_A\|id_A) \tag{4}$$

●GM_A 計算其公開金鑰 SPK_A：

$$SPK_A=sk_A\cdot G \tag{5}$$

●其中證明式如下：

$$SPK_A=sk_A\cdot G$$

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

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

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

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

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

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

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

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

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

系統內各成員皆需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。

2.GM_A 透過 CA 建立一個密鑰為 sk_A 的(t, n)門檻，其對應的多項式為：

$f(x)=sk_A+a_1x+a_2x^2+...+a_{t-1}x^{t-1}(\mathrm{mod}u)$ 。

3.假設 A 單位參與者 P_i 所持有秘密參數(id_i, s_i)，$i=1,2,...,n$，$s_i \equiv f(id_i)\ (mod\ u)$。

4.B 經由註冊後，自行計算密鑰 sk_B，與公開金鑰 $SPK_B= sk_B \cdot G$，並對外公開 SPK_B。

(三)密文簽密階段

●今 B 欲傳遞 r 份訊息 $\overline{mm}$ 給 A 單位，$\overline{mm}=\{m_1,m_2,m_3,...,m_r\}$。 (7)

●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)

●對明文做雜湊值運算 $h(\overline{m_{ij}})=m$ 。 (9)

●利用明文轉點方式將明文轉成點坐標 P_i，$i=1,2,...,r$，$f_{m2p}(\overline{m_{ij}})=\{P_1,P_2,...,P_r\}$。 (10)

●B 隨機選取一個整數 km_B，並計算：

$\Gamma=\{\Gamma_1,\Gamma_2,\Gamma_3,...,\Gamma_r\}$，$\Gamma_i=P_i+km_B \cdot SPK_A$，$i=1,2,...,r$。 (11)

●B 計算簽章值 $st=km_B/(\mathrm{m+sk_B})$ 。 (12)

●B 計算 $C=(km_B \cdot G,\overline{\Gamma},st,m)$ 。 (13)

●*B* 將密文 *C* 傳送到 A 單位。

(四)密文分割階段

●GM_A 將 *C* 做一分散的動作，即計算：

$C=T_i$，$i=1,2,...,n$，

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

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

(五)解簽密階段

●當 A 單位欲進行密文解密時，首先由 GM_A 計算 $su=(st \cdot sk_A) mod q$。 (15)

●由 GM_A 計算驗證簽章：

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

●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 $km_B \cdot s_i \cdot b_i \cdot G$ 。 (17)

●其中 $b_i \equiv \prod_{\substack{j=1 \\ j\neq i}}^{t} \frac{-id_j}{id_j-id_i}(\mathrm{mod}u)$ (18)

●計算下列式子：

$$\sum_{\substack{j=1 \\ j\neq i}}^{t}(km_B \cdot s_i \cdot b_i \cdot G) \equiv km_B \cdot sk_A \cdot G=\begin{cases} km_B \cdot SPK_A, \text{if t is odd} \\ -km_B \cdot SPK_A, \text{if t is even} \end{cases} (\mathrm{mod}\,q) \quad (19)$$

●計算出 $km_B \cdot SPK_A$ 或 $-km_B \cdot SPK_A$ 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

●將點 *Pi* 轉回訊息，即計算：

$P_i'=\{P_1',P_2',...,P_r'\}$，$i=1,2,...,r$。 (22)

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

●對明文 $\overline{m_{ij}}'$ 做雜湊值運算 $h(\overline{m_{ij}}')=m'$。 (24)

●驗證 $m' \stackrel{?}{=} m$，若等式成立則確認收方所收之訊息正確無誤。 (25)

●將訊息還原 $\overline{mm}=\{m_1,m_2,m_3,...,m_r\}$ 。 (26)

四、安全性分析

本研究所提之簽密機制，其安全性主要植基於橢圓曲線離散對數問題(Elliptic Curve Discrete Logarithm Problem; ECDLP)、非對稱加密方式、門檻式機制與單向雜湊函數，可達到 ISO 組織所提之資訊安全管理需求[22]，而一個完善的簽密演算法需滿足機密性、完整性、鑑別性、不可否認性及不可偽造性等安全需求[23][24]，並具有自我認證機制，分析如下：

(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，用於保護資料免受洩露的攻擊。

此服務正如 X.800 所定義非常廣泛，且包含全部或部分訊息的機密性，同時可避免流量分析的攻擊。在本研究中傳輸之密文使用了橢圓曲線加密法，如被第三者竊取了傳輸密文，可獲得(13)式之 $C=(km_B \cdot G,\overline{\Gamma},st,m)$，但在破解密文 Γ 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)

完整性是指訊息在傳遞過程中，不能被破壞或干擾，即不可偽造性，且用於保護資料免於被篡改、插入、刪除與重送攻擊。

1.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)。

2.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 $m' \stackrel{?}{=} m$，如等式無法成立，則可得知密文已遭到竄改。

(三)鑑別性(Authenticity)

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。

在本研究中使用了簽密法來進行驗證訊息是否確實由 B 方所傳送，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，以及在信息傳輸過程中的幾筆資料（SPK_A、SPK_B、st）；如破密者欲從中解出 GM_A 的密鑰 sk_A 與 B 的密鑰 sk_B，則將面臨破解橢圓曲線離散對數問題。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)

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。本研究目前所完成的系統架構與演算法中，因為已經導入數位簽密機制，故已達成不可否認性的條件。

在本研究中，收方 A 在接受到密文與送方 B 之簽章 ST 後，透過(15)式 $su = (st \cdot sk_A) \bmod q$ 及(16)式 $F_{AB} = SPK_A \cdot km_B$ 計算驗證簽章 F_{AB}；而在解密過程中經由(19)式之計算產生 $SPK_A \cdot km_B$，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 km_B 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)

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。在本研究兩種方法之中，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 st，因簽章值是透過(12)式 $\mathrm{st} = km_B/(\mathrm{m}+\mathrm{sk}_B)$ 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 $F_{AB} = (st \cdot SPK_B + su \cdot m \cdot G) = SPK_A \cdot km_B$ 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)

在本研究方法之中，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_i 與公鑰 PK_i，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)式 $SPK_A = PK_A + h(id_A)G + \left[\left(q_{ax} + h(id_A)\right)\right]PK_{CA}$，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，更可避免在方法一之中，如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)。

五、效益評估

本研究主要植基於橢圓曲線的門檻式密碼系統，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。經與國軍電子公文系統所運用之簽章機制進行比較，所作出之分析結果詳如表 4：

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 簽章機制(非對稱式)，搭配使用國軍加解密軟體加密(對稱式)	橢圓曲線簽密機制、門檻式機制、自我認證(非對稱式)
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	無法保證資料是否被竄改	●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 密碼系統進行簽章，系統之用較大之網路頻寬	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

六、結論

本研究旨在改善國軍電子公文系統現行所運用之 RSA 簽章機制為探討對象，將門檻式橢圓曲線密碼系統，導入了多文件簽密、自我認證的概念，利用橢圓曲線密碼系統所具有密鑰長度較短與計算複雜度較低的特性，在同樣的密鑰長度之下，會比其他演算法具有較高的安全性，另結合了(*t*, *n*)門檻式的加密機制，除了具有門檻的限制之外，若無法湊齊 *t* 個次密鑰，由於訊息的不完全，將導致對於多項式 *h(x)*一無所知，同時亦無法窺探主密鑰，可達到 Shannon 所定義的「完美安全」的概念，本研究具有以下優點：(一)運用橢圓曲線密碼將以更少的金鑰位元長度即可達到 RSA 相同的安全強度。(二)有別於傳統的一份文件加密一次方法，結合橢圓曲線加密法與門檻式加密機制的優點，可針對公文交換、傳送時一次簽密多份文件，節省文件加密時間，有效完成保密需求。(三)不需透過公證的第三方執行身分認證，能獨立進行雙方身分的自我認證程序，降低認證系統維護成本與風險，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。

在現今大多數均以網際網路做為商業平台的時代，橢圓曲線密碼系統金鑰長度短與運算速度較快的優點，在低計算量、低頻寬、連線不穩定情況下，具有相當的優勢，除符合保密需求外，亦確保了機密性、完整性、鑑別性、不可否認性及不可偽造性的功能，將有效提昇作業效率，並以更少的金鑰位元達到 RSA 相同的安全強度，實為國軍後續所追求的最高目標。

參考文獻

[1] 國防部編印，2009。*國軍文書處理手冊*，143。

[2] 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。

[3] 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。

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

[5] Koblitz, N., 1987, Elliptic curve cryptosystems, Mathematics of Computation (48), 203-209.

[6] 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。

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

[8] Blakley, G. R., 1979, Safeguarding Cryptographic Keys, Proceedings of the National Computer Conference, AFIPS Press, New York, 313-317.

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

[10] Boyd, C., 1986, Digital Multisignature, Proceedings of the Conference on Coding and Crypto- graphy,Cirencester,15-17.

[11] 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),457-469.

[12] Harn, L., 1993, Digital Signature with (t, n) Shared Verification Based on Discrete Logarithms, Electron Lett(29:24),2094-2095.

[13] Pedersen, T. P., 1991, A threshold cryptosystem without a trusted party, Eurocrypt(547), 522-526.

[14] Han, Y., Yang, X., Sun, J. an Li, D., 2003, Verifiable threshold cryptosystems based on elliptic curve, Proceedings of the 2003 International Conference on Computer Network and Mobile Computing, 334-337.

[15] 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。

[16] Girault, M.,1991,Self-certified public keys ,Advances in Cryptology-Euro，Vol. 547, Spring-Verlag, 491-497.

[17] 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。

[18] 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。

[19] 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*。

[20] 蘇品長，呂俊成，2011，多文件門檻式加密機制之研究，*2011年聯合國際研討會*。

[21] 蘇品長，呂俊成，2011，設計具自我認證之多文件門檻式加密機制探討，*2011全國資訊管理前瞻技術研討會*。

[22] ISO,2005,Informationtechnology-Security techniques-Information security management systems-Requirements,ISO/IEC 27001,1.

[23] 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，譯自Behrouz A. F.,。

[24] 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。