# 具自我認證之國軍網路申訴機制探討

[1]蘇品長 [2]蔡建華 [3]郭文雄 [4]林明慶 [5]楊倫青

[1,3,4,5]國防大學資訊管理學系
[2]致理技術學院會計資訊學系

## 摘　要

「國軍申訴制度」，係為保障國軍官兵各項合法權益，以內部程序的形式所設置的一種行政救濟途徑。國防部提供各式申訴管道，其案件之受理申請型式有郵件信箱（端木青信箱）、電話（1985 專線）及電子郵件（國防部民意信箱）等，隨著網路的普及與便利性，國軍人員資訊素養提高，建置網路申訴系統不啻是另一申訴管道之選項，但若要發展國軍網路申訴系統，需考量如何有效保護申訴人的隱私，避免其隱私資料曝露，造成困擾，這是一值得深思的課題。本研究以密碼學理論為基礎，透過自我認證機制、盲簽章及橢圓曲線密碼學，以國軍網路申訴制度為對象，設計一個具自我認證、資料保密之網路申訴系統的安全機制，以達到學者 Girault 所提的公開金鑰密碼系統的 Level 3 安全等級，可避免憑證中心私鑰被偽照的風險，除了各階段成員身分具自我認證特性外，成員私鑰及認證簽章具不可偽造性，申訴訊息盲簽章具有不可否認性及申訴內容具有保密性等特點外，並可避免網路申訴系統遭冒名申訴所造成申訴作業之人力及時間耗費，抑制網路不實申訴之可能性。本研究具有以下優點：

一、以自我認證機制取代認證伺服器電子憑證頒發角色。
二、KGC 註冊後，不需再透過第三方執行身分認證作業，認證效率高。
三、盲簽章方式隱匿申訴資料功能，並防止過程中偽冒與竄改。
四、橢圓曲線密碼以更少的金鑰位元長度可達到 RSA 相同的安全強度。
五、申訴內容經由盲化作業，可避免內容洩漏，提高案件偵辦之公正性。

**關鍵詞：**自我認證、橢圓曲線、盲簽章。

# The Study of the Army Appealing for System with Self-Certified Function on the Internet

[1] Pin-Chang Su　[2] Chien-Hua Tsai　[3] Wing-Shaung Kau
[4] Vin-Ching Lin　and　[5] Lun-Ching Yang

[1,3,4,5]Department of Information Management, National Defense University
[2]Department of Accounting Information, Chihlee Institute of Technology

## Abstract

"The army appealing for system" can pledge various legal rights , following the internet that is very popularly and practically. Setting up the appealing for system on the internet that is another option of appealing for channels; if need expand appealing for systems that must consider how to protect the private secrets of the applicant to avoid data be exposed. The study is based on the theory of code and will pass thru a self-certified system, blinding signatures as well as the elliptic curve in order to design a fully self-certified and a safety organization to pledge data's secrets of appealing for system on the internet. The study has following some merits:

1. The issuing role of the self-certified system will replace the electric certificate of the server certified.
2. After registering KGC system that don't need pass by the third ID thru the certified process which certified efficiency will be added highly.
3. The blinding signatures which function can be hidden the appealing for information and avoid be false copied and amended during processing.
4. The code of elliptic curve can use less more length of golden key bit to achieve the safety strength same as the RSA system.
5. The appealing for contents can pass thru the blinding operation to avoid the contents be exposed and also can promote the case investigated judgment.

**Keywords**: Self-Certified, Elliptic Curve, Blinding Signatures

## 壹、前　　言

國防部為保障國軍人員及其維護眷屬合法權益，於民國五十年三月訂頒的「國軍申訴制度」，係以內部程序的形式所設置的一種行政救濟途徑，當官兵個人受到不當處分或冤屈不平或官兵家屬應享有之權益受到侵害時，能透過此種行政救濟途徑提起申訴。為強化官兵申訴案件管制，國防部提供各式申訴管道，其案件之受理申請型式舉如：端木青信箱、1985 專線、國防部民意信箱等，申訴人應填具個人資料，若有冒、匿名案件及未具真實身分資料者，概不受理，如有誣告情事者，則依情節輕重追究相關責任（職念一，2003）。隨著網路的普及與便利性，現今國軍人員資訊素養提高，建置網路申訴系統不啻是另一申訴管道之選項，可由申訴人自行操作申訴系統，降低專門申訴案件收發中心工作，且可由資訊系統自動化作業，接受與轉發案件予以偵辦單位，以減少人工作業等優點。但處於網路申訴環境時，如何有效保護當事人的隱私，避免其申訴內容曝露，便成為一值得深思的課題。因此，本研究將就現行國軍申訴制度下探討網路申訴過程中申訴人的身分認證及申訴資料隱匿機制部分，以達到建立有效申訴而無洩露個人申訴資料之憂的網路申訴環境。

## 貳、文獻探討

### 一、現行國軍網路申訴流程

現行國軍申訴制度要求須留下申訴者的單位、級職、姓名、聯絡方式等個人資料，並將申訴人之申訴內容保密，但其流程多數為人工處理，往往造成申訴人對身分及申訴內容的保密性有所疑慮（陳新民、韓毓傑，1985），現行國軍申訴制度人工處理作業流程概述如圖 1(郭文雄，2010）。

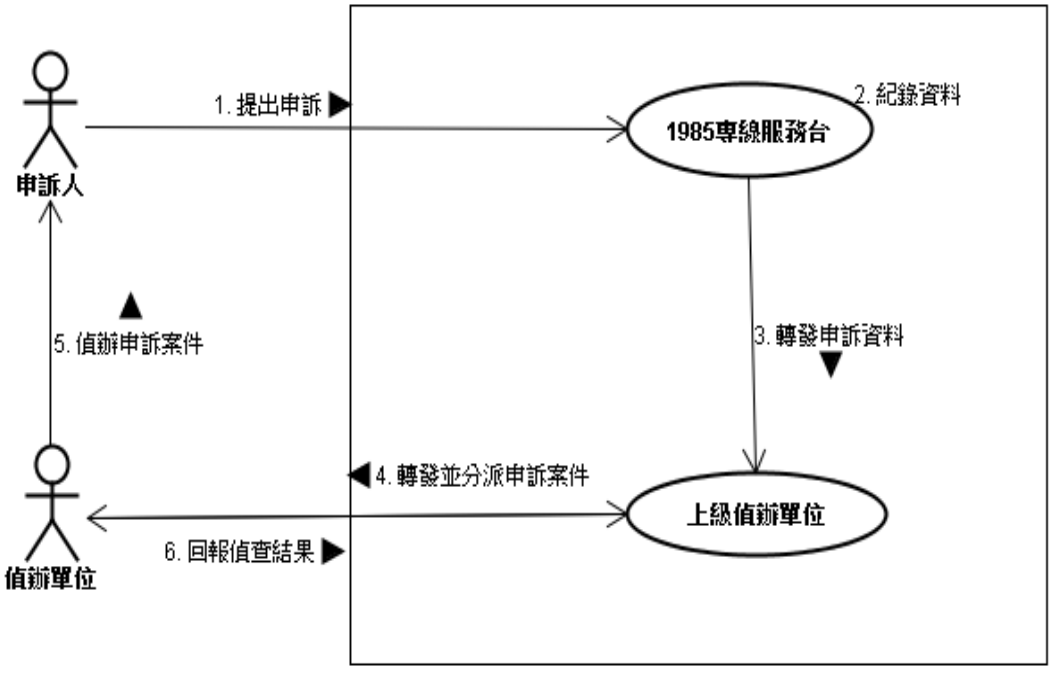


圖 1 國軍申訴制度處理作業

### 二、自我認證公開金鑰密碼系統

學者 Girault(1991)提出公開金鑰密碼系統的三個層次安全等級如表 1。

表 1　Girault( 1991 年) 提出公開金鑰系統的三個層次安全等級

| 等級 | 說明 | 認證系統 |
|---|---|---|
| Level 1 | 憑證中心知道所有使用者的私密金鑰，而且在任何時候都可以偽冒任一個使用者而不被發現 | 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。<br>2.使用者會自行驗算認證中心所傳過來的公鑰之正確性，故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 |

資料來源： Girault, M.（1991）

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 (胡國新，2000 年) ，其植基於 RSA 方法設計出來的自我認證機制，共包含三個階段：

（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，保留 d，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 $ID_A$，參數敘述如下：

1. 使用者 A 自行選定自己的私鑰 $S_A$，並計算出 $V_A = g^{-S_A} (\bmod N)$ 後，再將自己的身分識別碼 $ID_A$ 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 $P_A$，$P_A = (V_A - ID_A)^d (\bmod N)$，並將 $P_A$ 傳回給使用者 A。
3. 使用者 A 驗證 $P_A^{\,e} + ID_A = V_A$，$(V_A^{\,d} - ID_A^{\,d})^e + ID_A = V_A$，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，然後使用者 B 計算

   $V_A = (P_A^{\,e} + ID_A) (\bmod N)$ 。
2. 使用者 A 選擇一個隨機參數值 x，計算 $t = g^x (\bmod N)$ 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 $Y = x + S_A \cdot C (\bmod N)$ 後，並將 Y 傳送給使用者 B。
5. 最後使用者 B 利用驗證式

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

若等式成立則可證明使用者 A 身分；相同地，使用者 A 也可用此方式驗證使用者 B 的身分。

## 三、橢圓曲線公開金鑰密碼系統

自 1978 年美國麻省理工學院的 Rivest、Shamir 與 Adleman 等三人以數學因數分解的計算難題，提出了第一套非對稱式金鑰密碼系統，命名為 RSA 公開金鑰密碼系統。直至今日， RSA 仍是一套安全的非對稱式金鑰密碼系統，但 RSA 公開金鑰密碼系統的安全強度是有代價的，即它需要大的金鑰長度，隨著電腦計算能力的演進，這種狀況愈加明顯。因此，密碼學研究學者尋找替代方案，以期能提供相同的安全等級，但金鑰長度卻較短。其中一個最有希望的替代方案便是橢圓曲線密碼系統(Elliptic Curve Cryptosystem, ECC)。

Miller（1985）及 Koblitz（1987）分別提出將橢圓曲線用來實作公開金鑰密碼系統。橢圓曲線的通式為 $y^2+axy+by=x^3+cx^2+dx+e$ 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 $O$，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 $O$。

在 Galois Field $E(F_q)$ 中，如果 $q$ 是大於 3 的質數，則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 $4a^3+27b^2 \bmod q\neq 0$ 質數 $q$ 會固定住式程式的上限，並用於模數運算上，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 $E(F_q)$ 中的點加法定義如下：

（一）$P+O=O+P=P$

（二）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 $P+Q=O$

（三）如果 $P\neq Q$ 則 $P+Q=(x_3,y_3)$ ，

$$x_3\equiv\lambda^2-x_1-x_2 \bmod q$$

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

如果 $x_1\neq x_2$ 則 $\lambda=\dfrac{y_1-y_2}{(x_2-x_1)}$ ，若 $x_1=x_2$ 且 $y_1\neq 0$ 則 $\lambda=\dfrac{(3x_1^2+a)}{2y_1}$

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 $3P=2P+P$ ，橢圓曲線的另一個特性為純量相乘，即運算只能做單向的計算，無法再由計算的結果值反推出原始的點，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，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，換句話說，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 2(蘇品長，2007)。

表 2　RSA 與橢圓曲線密碼系統在相同安全度下金鑰長度之比較

| RSA 密碼系統 (bits) | 512 | 1024 | 2048 | 3072 | 7680 |
|---|---|---|---|---|---|
| 橢圓曲線密碼系統(bits) | 112 | 163 | 224 | 256 | 384 |
| 金鑰長度比 | 1：5 | 1：6 | 1：9 | 1：12 | 1：20 |

## 四、盲簽章

Chaum（1983）以植基於 RSA 的方法提出盲簽章機制，而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。其運用密碼學中數位簽章之特性，使用公鑰與密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。舉例來說，如同投票人「送簽者」請選委會「簽章者」在一封經彌封的選票信件上蓋時間郵戳，由於時間郵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，再將此封內

含有選票信件回覆給具合法身分的投票人，投票人於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時間郵戳的戳記，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的身分或地址，寫上寄往開票中心的地址，如此完成匿名投票的步驟。

（一）盲簽章是簽章者植基於RSA方法選定*(n, e)*、 $d$ 分別為公鑰與私鑰，送簽者想要將訊息 $M$ 送給簽章者簽章，但卻不願讓簽章者知悉訊息 $M$ 的內容。送簽者隨機挑選一整數 $R$ 為盲因子(Blinding Factor)，並滿足條件 $GCD(R,n)=1$ 計算 $M'=(R^e \times M) \bmod n$ ，將 $M'$ 傳給簽章者。

（二）簽章者收到 $M'$ 後，以其私鑰 $d$ 計算 $S'=(M')^d \bmod n$ 後，將 $S'$ 回傳給送簽者，於簽章過程中，簽章者完全不知道所簽章的資料內容。

（三）送簽者利用之前所選擇的盲因子 $R$，對此簽章做除盲化的動作（$R^{-1}$），將收到的 $S'$ 內之盲因子移除，以得到簽章者對訊息 $M$ 的簽章 $d$。

（四）需求者得到：$S=M^d(\bmod n)$，任何需求者可以使用簽章者的公鑰 $e$ 來驗證 $S$ 的有效性，$S^e=(M^d)^e(\bmod n)$
以還原訊息 $M$，若驗證成立則代表該簽章為簽章者對訊息 $M$ 的有效簽章，盲簽章運作流程如圖 2。

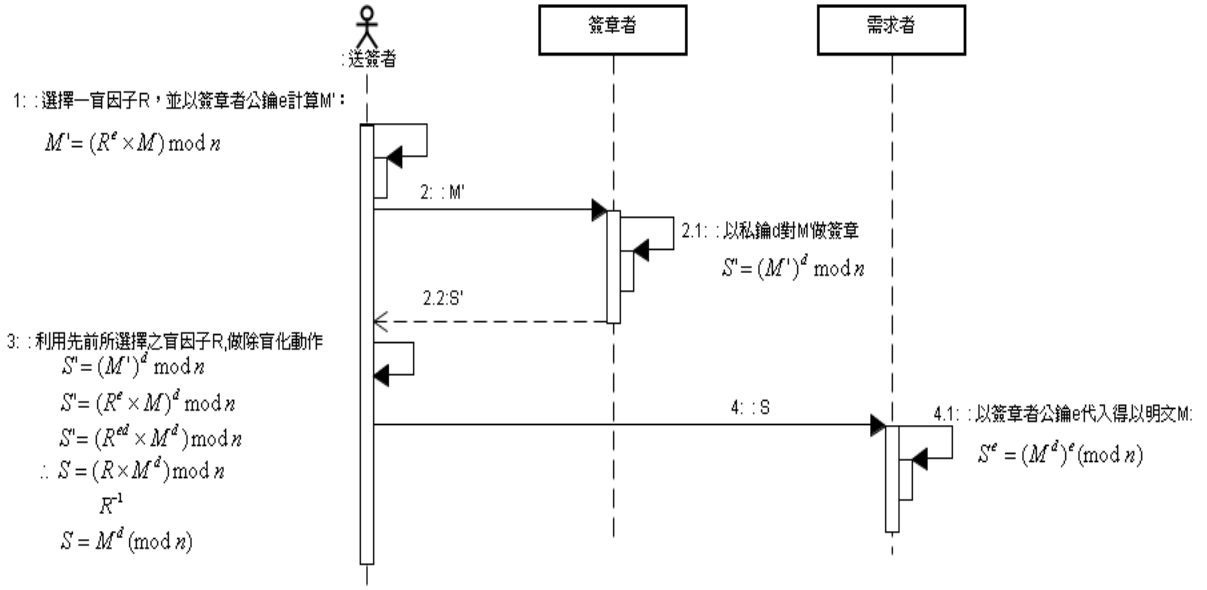


圖 2　盲簽章認證模式

## 參、設計具自我認證之國軍網路申訴制度之安全機制

本研究將就「申訴過程保密性」該項探討，將 1985 申訴專線申訴接話人之流程部分，透過加密技術的改進，如圖 2 中的電話申訴流程，改由網路申訴伺服器替代，透過密碼學技術，對申訴人身分認證及所提之申訴內容隱藏，減少因申訴過程中，降低申訴人擔心申訴資料外洩之疑慮，以提高對網路申訴之信心。

為使密碼演算可有效率地進行，本研究使用橢圓曲線密碼系統來取代需要以大指數運算的RSA為基礎的公開金鑰密碼系

統，橢圓曲線密碼系統的優點是可以更少的金鑰位元數長度即可達到RSA相同等級的安全強度。於身分認證部分，以自我認證機制取代認證伺服器所負責電子憑證頒發角色。雖然現行許多的電子商務網站所使用的都是以電子憑證基礎的公開金鑰系統，由第三方單位來簽發憑證，卻有可能發生兩個問題。首先，以憑證為基礎的認證方式需要維護金鑰目錄中各個參數之間的一致性，會多浪費儲存空間，且在使用時還需額外增加驗證系統認證中心之簽章的步驟。其次，在現實的網路環境中，我們並無法寄望於系統的電子憑證中心一定是絕對安全的，換句話說，系統的憑證中心也是有可能被駭客入侵的，伺機偽造出一個不存在的使用者。為避免系統於資料傳遞有洩漏申訴資料之虞，訊息傳遞以密文傳送，以盲簽章的方式達到保護申訴人的申訴資料的隱匿功能與確保受理申訴偵辦單位所獲資料之正確性與完整性，即使是申訴收發中心亦不得介入存取申訴內容，讓申訴人不必擔心因申訴中心伺服器的資安風險而導致申訴內容曝光，並可防止申訴過程中偽冒與竄改情事之發生，以提高網路申訴的保密性，使網路申訴系統的安全機制能更臻於完備，表 3 為系統中使用的符號說明，國軍網路申訴系統，系統運作架構流程圖如圖 3 所示。

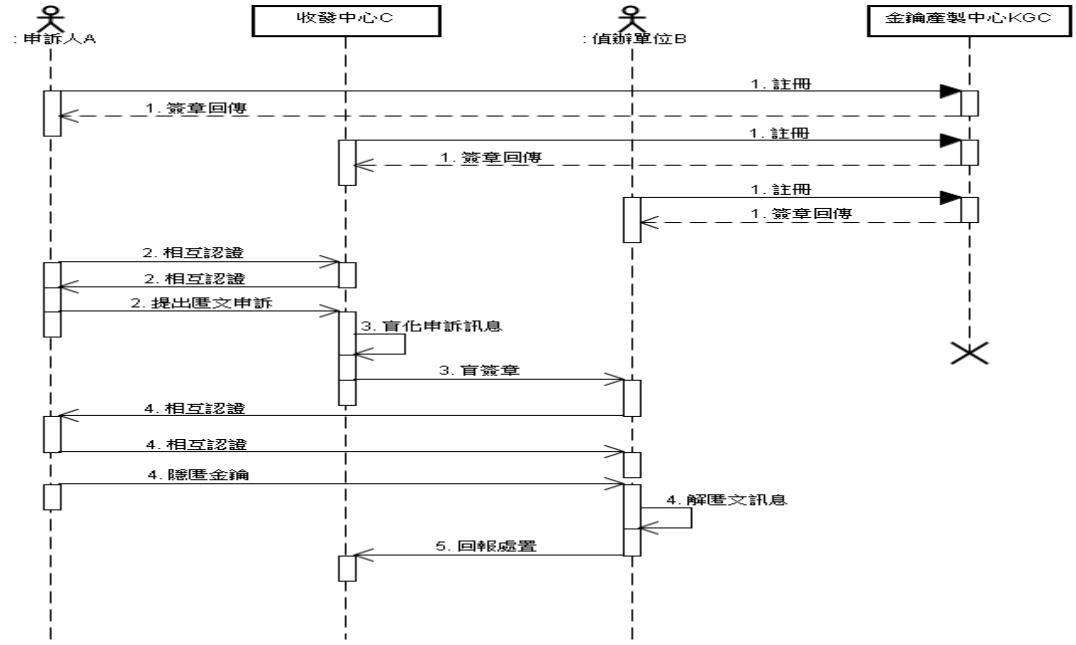


圖 3　本系統運作架構流程圖

表 3　系統使用之符號說明

| NO. | 符號 | 說明 | NO. | 符號 | 說明 |
|---|---|---|---|---|---|
| 1. | KGC | 金鑰產製中心 | 9. | $V_n$ | 註冊申請的簽章 |
| 2. | A | 申訴人 | 10. | $e_n$ | 本身資訊求得之雜湊值 |
| 3. | B | 偵辦單位 | 11. | $X_{AB}$ | 認證雙方共同之隱匿金鑰 |
| 4. | C | 收發中心 | 12. | $M$ | 申訴訊息 |
| 5. | $ID_n$ | 成員的帳號 | 13. | $t_n$ | 成員所選擇之時間戳記 |
| 6. | $PK_n$ | 成員的公鑰 | 14. | $h()$ | 座標轉成數值之雜湊函數 |
| 7. | $sk_n$ | 成員的私鑰 | 15. | $d_n$ | 成員選擇隨機參數值 |
| 8. | $W_n$ | 計算出的簽章 | 16. | $q_x,q_y$ | 橢圓曲線群中的 x,y 座標 |
| 備註：*參數* n 代表系統內的各方成員，如 $ID_A$ 即代表成員 A 的帳號。 | | | | | |

首先，於金鑰產製中心（KGC）系統建置階段，程序如下：

(一)KGC 在有限域 $Fq$ 上選取一條安全的橢圓曲線 ($q$ 為一個 160bit 以上之大質數)在 $E(F_q)$ 在上選一階數(order)為 $n$ 的基點 $G$，使得 $nP=O$，其中 O 為此橢圓曲線之無窮遠點。

(二)KGC 選擇一個單向無碰撞雜湊函數 $h()$，且計算公開金鑰 $PK_{KGC}$ 。

$$PK_{KGC} = sk_{KGC}P \qquad (1)$$

(三) KGC 公開 $E$ 、$P$ 、$n$ 、$PK_{KGC}$ 及 $h()$ 。

## 一、各方成員註冊階段

Step 1：申訴人 A 以自己 $ID_A$ 及隨機參數 $d_A \in [2, n-2]$，以 $d_A$ 參數值產生簽名檔 $V_A$，並將 $ID_A$ 與 $V_A$ 與傳給 KGC，$V_A$ 計算式如下：

$$V_A = h(d_A \| ID_A)P \qquad (2)$$

Step 2：KGC 選擇一隨機參數值 $k_A \in [2, n-2]$ 計算申訴人 A 之公鑰 $PK_A$ 及簽章 $W_A$ 並傳回給申訴人 A，計算式如下：

$$PK_A = [\ V_A + (k_A - h(ID_A))\ ]P = (q_{a_x}, q_{a_y}) \qquad (3)$$

$$W_A = k_A + sk_{KGC}(q_{a_x} + h(ID_A\ )) \qquad (4)$$

Step 3：申訴人 A 自己計算私鑰 $sk_A$，並且驗證 $PK_A$ 的正確性，計算式如下：

$$sk_A = [\ W_A + h(d_A \| ID_A)\ ] \qquad (5)$$

證明式如下：

$$S_A = sk_A P \qquad (6)$$

$$\because S_A = [\ k_A + sk_{KGC}(q_{a_x} + h(ID_A\ ) + h(d_A\ \| ID_A))\ ]P$$

由方程式(1) - 方程式(3)得知

$$PK_{KGC} = sk_{KGC}P$$

$$V_A = h(d_A \| ID_A)P$$

$$PK_A = [V_A + (k_A - h(ID_A))]P$$

$$V_A = [PK_A - (k_A + h(ID_A))]P$$

$$\therefore S_A = k_A P + V_A + [(q_{a_x} + h(ID_A))]PK_{KGC}$$

帶入後得到：

$$S_A = PK_A + h(ID_A)P + [(q_{a_x} + h(ID_A))]PK_{KGC}$$

使用者 A 與金鑰產製中心 KGC 註用程序如圖 4，各方成員與 KGC 註冊程序如上，一旦所有申訴人與各方成員（$n$）自 KGC 完成註冊並取得屬於自己的公鑰 $PK_n$ 及簽章 $W_n$ 後，即可自行與需認證的對方進行認證，而不需 KGC 替雙方執行身分認證工作。各個認證需求方（A，B，C）皆可自 KGC 完成註冊並取得屬於自己的公鑰 $PK_n$ 及簽章 $W_n$ 後，可憑認證中心核發的帳戶相關資料（$ID_n$、$PK_n$）與自行計算出來的 $S_n$，進行相互身分認證。

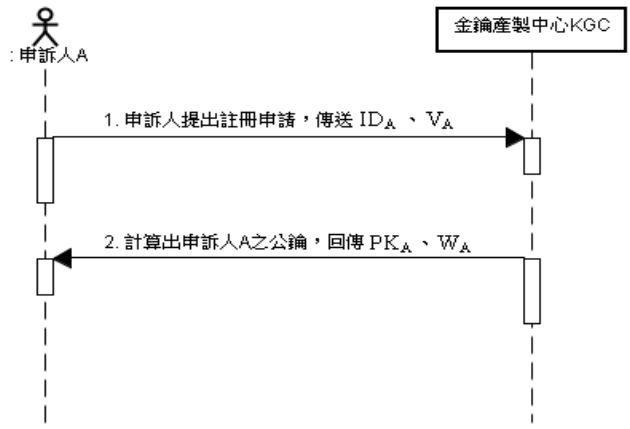


圖 4　申訴人 A 與金鑰產製中心 KGC 註冊示意圖

## 二、成員相互認證階段

申訴人 A 自 KGC 取得合法認證身分後，欲提出申訴，須於申訴前可憑 KGC 核發之帳戶資料與申訴收發中心 C 進行相互身分驗證，在產生隱匿金鑰前，申訴收發中心 C 需與申訴人 A 相互確認（$ID_A$、$S_A$ 、$PK_A$）及（$ID_C$、$S_C$ 、$PK_C$）是正確，收發中心 C 申訴人 A 驗證申訴檢查式如下：

$$S_A^{'} = PK_A + h(ID_A)P + \left[\left(q_{a_x} + h(ID_A)\right)\right]PK_{KGC} \quad (7)$$

$$S_A^{'} \stackrel{?}{=} S_A \quad (8)$$

相同的，申訴人 A 也可驗證申訴中心 C 之 $S_C^{'} \stackrel{?}{=} S_C$ 。

如果雙方驗證身分正確無誤，申訴人 A 選擇一時間戳記 $t_A \in Z_q$ 與以本身資訊求得之雜湊值 $e_A$ 做為盲因子，盲化申訴訊息 $M$，申訴中心 C 收到申訴人 A 的盲化申訴訊息 $M^{'}$ 後，以其私鑰 $sk_C$ 將盲化訊息 $M^{'}$ 簽章（如圖 5），計算式如下：

申訴人 A：　$e_A = h\left(PK_A, ID_A\right)$ (9)

$$M^{'} = e_A t_A M \quad (10)$$

申訴中心 C：　$S_M = sk_C\left(M^{'}\right)$ (11)

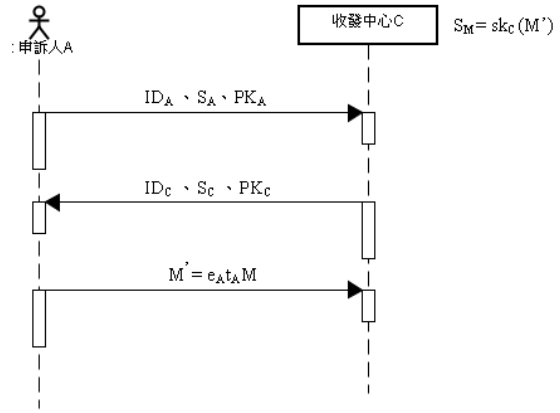


圖 5　申訴人 A 向收發中心 C 提出申訴示意圖

## 三、相互身分驗證傳送隱匿申訴訊息階段

申訴收發中心 C 將盲化申訴訊息簽章後，欲將隱匿申訴訊息 $S_M$ 轉發至所屬偵辦單位 B，申訴中心 C 與偵辦單位 B 須先進行身分認證，依其各自公開資料 $ID_B$、$S_B$、$PK_B$ 及 $ID_C$、$S_C$、$PK_C$ 進行相互驗證，檢查式如下：

申訴中心 C 驗證偵辦單位 B，檢查式如下：

$$S_B^{'} = PK_B + h(ID_B)P + \left[\left(q_{b_x} + h(ID_B)\right)\right]PK_{KGC} \quad (12)$$

$$S_B^{'} \stackrel{?}{=} S_B$$

偵辦單位 B 驗證申訴中心 C：$S_C^{'} \stackrel{?}{=} S_C$

$$S_C^{'} = PK_C + h(ID_C)P + \left[\left(q_{c_x} + h(ID_c)\right)\right]PK_{KGC} \quad (13)$$

$$S_c^{'} \stackrel{?}{=} S_C$$

相互驗證無誤後，再將盲化匿文申訴訊息轉發給所屬偵辦單位 B，示意流程如圖 6。

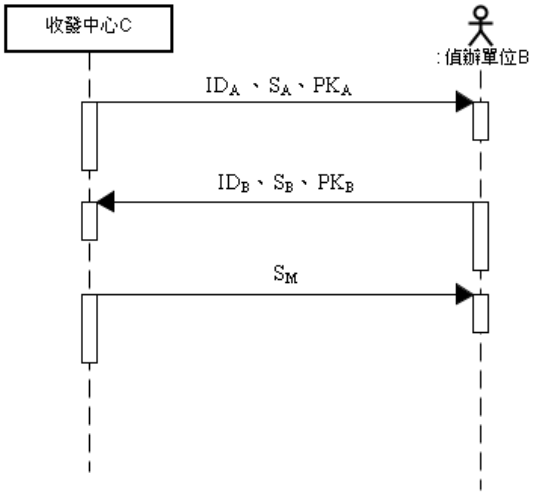


圖 6　收發中心 C 與偵辦單位 B 相互驗證後傳送隱匿申訴訊息示意圖

## 四、偵辦單位 B 與申訴人 A 認證並解開隱匿申訴訊息階段

偵辦單位 B 收到隱匿申訴息 $S_M$ 後，欲解開隱匿申訴訊息，需自申訴人 A 取得 $t_A$ 及 $e_A$ 盲因子，以解開盲化申訴訊息，故偵辦單位 B 須與申訴人 A 相互驗證，檢查式如下：

申訴人 A 驗證偵辦單位 B，檢查式如下：

$$S_B^{'} = PK_B + h(ID_B)P + \left[\left(q_{b_x} + h(ID_B)\right)\right]PK_{KGC} \quad (14)$$

$$S_B^{'} \stackrel{?}{=} S_B$$

偵辦單位 B 驗證申訴人 A，檢查式如下：

$$S_A^{'} = PK_A + h(ID_A)P + \left[\left(q_{a_x} + h(ID_A)\right)\right]PK_{KGC} \quad (15)$$

$$S_A^{'} \stackrel{?}{=} S_A$$

如果驗證無誤，偵辦單位 B 與與申訴人 A 計算雙方共同隱匿金鑰 $X_{AB}$，示意圖如圖 7，計算式如下：

Step 1：申訴人 A 以時間戳記 $t_A$，計算出 $R_A$ 並傳給偵辦單位 B，計算式如下：

$$T_A = t_A \cdot P \quad (16)$$

$$\because S_A = sk_A \cdot P$$

$$\therefore X_{AB} = sk_A \cdot S_B = sk_B \cdot S_A \quad (17)$$

$$\therefore R_A = X_{AB} + T_A \quad (18)$$

Step 2：偵辦單位 B 以所獲得資訊求得$t_A$及$e_A$，計算式如下：

$$\because R_A = X_{AB} + T_A \quad (19)$$

$$T_A = R_A - X_{AB} \quad (20)$$

$$t_A P = (sk_A \cdot sk_B)P - R_A \quad (21)$$

偵辦單位 B 以（$R_A$，$PK_A$，$PK_B$）求得$t_A$ 及$e_A = h(PK_A, ID_A)$

Step 3：偵辦單位 B 以所獲得資訊得$t_A$及$e_A$，解開自收發中心傳來的盲化匿文申訴訊息$S_M$，計算式如下：

$$\because S_M = sk_C(M')$$

$$\therefore S_M = sk_C(t_A e_A M) \quad (22)$$

偵辦單位 B 以（$PK_C$、$t_A^{-1}$、$e_A^{-1}$）解開$S_M$得原申訴訊息$M$，進行偵辦作業。

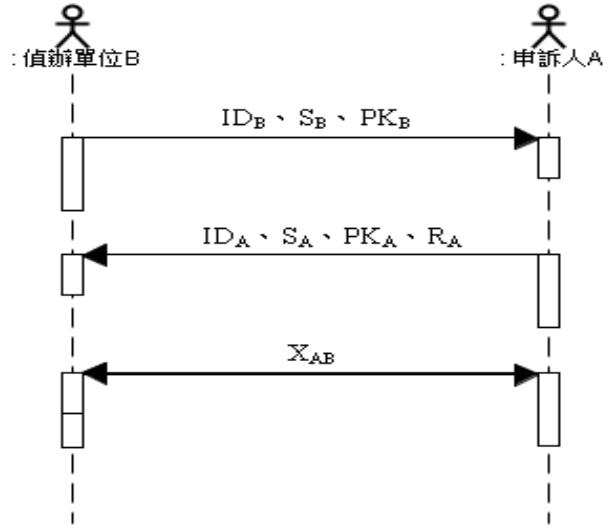


圖 7　偵辦單位 B 與申訴人 A 相互驗證示意圖

**五、回報偵辦狀況或誣告處理**

如果申訴案件經偵辦單位調查辦理後，回報處理情形或發現無具體事實，屬誣告情事，由偵辦單位將案件偵辦狀況以安全方式傳給申訴收發中心後，收發中心將處理情形記錄於系統伺服器並呈報權責長官，依情節輕重續辦懲處事宜。

## 肆、安全性分析

本研究之身分驗證機制以植基於橢圓曲線離散對數難題及與申訴內容之隱匿性，可達機密性、完整性、可驗證性與不可否認性等基本安全需求，綜整本研究之安全性分析略述如下：

一、達到 Girault 所提的公開金鑰密碼系統的 Level 3 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，成員自 KGC 註冊後不需再透過第三方（如憑證認證中心）做保證或協調。

二、避免憑證中心私鑰被偽照的風險：KGC 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（3）中的$PK_A = [\, V_A + (k_A - h(ID_A)) \,]$，且使用者的私密金鑰是依 KGC 傳回的簽章$W_A$計算得到的，如式（5）中的$sk_A = [\, W_A + h(d_A \| ID_A) \,]$，故系統認證中心不能自行產生甚至是偽照使用者的公鑰，可避免因憑證認證中心知道

所有使用者的私密金鑰，藉由系統認證中心偽造產生一個完全不存在的使用者的情事發生。

三、身分及認證簽章具不可偽造性：各方成員須先向金鑰產製中心 KGC 做註冊及身分確認，以獲得其公鑰與身分認證簽章（如 $PK_A$、$W_A$），且使用者會自行驗算認證中心所傳過來的公鑰之正確性（如式 6），認證中心無法主導使用者公鑰之產生及驗證，故驗證過程中詐偽的行為會被偵測出來。

四、各階段成員身分具可驗證性：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，須由 KGC 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。

五、申訴內容具有保密性：如申訴人 A 以其參數雜湊值 $e_A$ 及時間戳記 $t_A$ 為盲因子，故申訴文件於簽章過程中，已利用僅有申訴人知道之盲因子將申訴訊息 $M$ 進行盲化成 $M'$。因此，申訴收發中心並無法得知申訴人之申訴內容為何，無法還原原始資料，僅能依其權限進行簽署該份申訴訊息。

六、申訴訊息盲簽章具有不可否認性：僅申訴收發中心能簽署盲化申訴訊息作業，且申訴收發中心不會介入存取申訴內容，讓申訴人不必擔心因申訴收發中心的疏失而導致申訴內容曝光，且僅有申訴收發中心才可以產生合法的盲簽章（為其私鑰）$S_M = sk_C(M')$，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。故申訴收發中心（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申訴收發中心的簽章（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）。

七、申訴內容來源具有可驗證性：申訴收發中心將盲化申訴訊息轉發給偵辦單位前，需先進行身分上之驗證。而偵辦單位於收到盲化申訴訊息後，欲解開盲化申訴訊息 $S_M$，亦須先與申訴人進行身分驗證，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。

八、自我認證與以憑證為基礎之認證系統比較表如附表 4。

九、本研究所提申訴方式與現行申訴方式比較表如表 5 所示。

表 4　自我認證機制與憑證為基礎之身分認證系統比較表

| 特性比較 | 一般認證系統 | 本方法所提之自我認證系統 |
|---|---|---|
| 公鑰的有效性 | 使用公鑰時，需連線確定其公鑰的有效性。 | 在使用公鑰時，可採離線方式驗證公鑰的有效性。 |
| 金鑰目錄的維護 | 需儲存使用者的身分資料、公鑰和憑證(G 值)，並時需保持公鑰與與憑證之間的一致性。 | 僅需使用者的身分資料與公鑰。 |
| 身分認證的方式 | 連線的身分確認，接收雙方須透過簽發憑證單位來確認雙方的身分，且在每次通訊時需先確定對方公鑰的有效性。 | 可離線的身分確認性，只要有保存金鑰產製中心 KGC 的公鑰等參數，即使離線狀態，接收雙方仍可確認對方的身分。 |
| 身分認證的效率 | 若網路申訴系統有階層式的關係時，需逐層完成認證。 | 若網路申訴系統有階層式的關係時，仍可一次完成認證。 |
| 系統安全等級 | Level 2 | Level 3 |

表 5　現行申訴模式與本研究兩者特性分析比較表

| 特性 | 現行申訴方式 | 本研究所提網路申訴方式 |
|---|---|---|
| 互動模式 | 電話申訴可獲得立即回應。 | 透過網路申訴系統所提供功能，藉由文字等訊息做回應。 |
| 服務時間 | 需靠申訴專線服務人員輪值，才能達到 24 小時不中斷服務，人力時間成本大。 | 需電腦、網路設備，可 24 小時不間斷服務，人力成本較低。 |
| 非語言訊息 | 申訴服務專員可藉由申訴人語氣、情緒等做判斷。 | 無法觀察申訴個案外在情緒現做判斷，僅能由其用字遣詞揣測申訴動機。 |
| 匿名性 | 當下須留下身分資料，部分申訴人較難克服心理障礙。 | 完全經電腦認證、加密，資料隱密性高，對首次接受申訴者較能接受。 |
| 效率性 | 人工作業，作業時程較長。 | 自動化作業，接受與轉介申訴訊息快速。 |
| 完整性 | 電話會談中，申訴服務專員需額外記錄晤談內容。 | 申訴內容加密後寫入資料庫，方便日後查詢與追蹤。 |
| 資訊能力 | 不需要。 | 申訴人需具中文打字、上網等能力。 |

## 伍、結　　論

本研究以國軍網路申訴系統度為探討對象，以橢圓曲線密碼學為基礎所設計的一個自我認證法，結合盲簽章機制，設計具自我認證之網路申訴系統之安全機制，綜整本研究效益略述如下：

一、以自我認證機制取代認證伺服器所負責電子憑證頒發角色。

二、完成 KGC 註冊後，不需再透過第三方來執行身分認證作業，認證效率高。

三、以盲簽章的方式申訴資料隱匿功能，並防止過程中偽冒與竄改情事之發生。

四、以橢圓曲線密碼系統更少的金鑰位元長度即達到 RSA 相同的安全強度。

五、可避免使用者資料因人為作業造成洩漏及錯誤，申訴內容經由盲化作業，可避免內容洩漏，提高案件偵辦之公正性。

## 陸、國防相關應用

本研究以探討國軍網路申訴制度之安全機制為對象，屬於密碼學上的應用，提出結合密碼學領域中「自我認證」、「橢圓曲線」與「盲簽章」知識，謀求建立一網路申訴之身分認證與資料隱匿機制，經此數位驗證機制的建立，除能有效確認資料完整性以及使用者身分認證外，還能達到資料一致性與不可否認性，防範偽冒與竄改情事之發生，期能促進國軍網路申訴制度的發展及可信賴度。

## 柒、參考文獻

李秉禮，2007。具選票驗證之匿名電子投票機制，佛光大學資訊研究所碩士論文。

林明慶，2009。身分隱匿技術應用於國軍網路申訴制度之研究，國防大學資訊管理系碩士論文。

巫坤品、曾志光譯，2001。密碼學與網路安全：原理與實務，碁峰公司。

胡國新， 2000。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。

陳新民、韓毓傑，1985。國軍管教問題之

研究：軍隊領導統御理念與制度之分析，國防部委託中研究研究計畫，頁180。
張榮福，1996。國軍申訴制度之研究，政治作戰學校政治研究所碩士論文。
祝躍飛、張亞娟，2006。橢圓曲線公鑰密碼導引，科學出版社。
蘇品長，2008。適用於 Ad Hoc 網路之快速交換金鑰機制設計，中正嶺學報，第37卷，第1期，頁219～228。。
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學位論文。
潘妍伶，2001。國軍網路申訴系統之研究，國防大學資訊管理系碩士論文。
職念一，2003。我國軍人申訴制度之研究，佛光大學管理學研究所碩士論文。
Chaum, D., 1981, Blind signatures for untraceable payments, Department of
computer science, University of California Santa Barbara , CA.
Douglas, R. S., 2002, Cryptography: Theory and Practice 2rd, Chapman & all/CRC.
Girault, M., 1991, Self-certified public keys, Advances in Cryptology: EUROCRYPT, 490-497.
Henry, D., 1999, Who's Got the Key?, Proceedings of the 27th Annual ACMSIGUCCS Conference on User Service: Mile High Expectations, 106-110.
Miller, V. S., 1985, Use of Elliptic Curve in Cryptography, Advance in Cryptography- Crypto '85, New York: Spring-Verlag, 417-426.
Kobiltz, N., 1987, Elliptic Curve Cryptosystems, Mathematics of Comutation, 203-209.