設計具機密性及可自我身分認證之無線通訊網

作者／楊博元上尉、郭尚瑋士官長、蘇品長上校

提要

一、 國軍通資電部隊任務多樣且特殊，如何安全的運用無線通訊網路將各類情報傳送予第一線勤務執行單位，並於發生重大事故執行聯合救難任務時，提供不同友軍單位間之行動通訊服務，以相互支援協助，實為提升各項任務執行效能之重要關鍵。但前端勤務人員目前僅能透過建置於移動車載或通資站臺內之有、無線存取節點與指揮部，或友軍單位成員相互傳遞資訊，尚無法直接與其他相關單位人員進行跨網域之行動通訊，不利於相互支援協助。

二、 本研究中我們提出一個利用橢圓曲線密碼為概念的新方法，具有除了符合機密性、可驗證性及不可否認性等基本安全需求外，尚可以抵禦網路上常見的攻擊方式。

三、 本研究具有以下四項優點：(1)建置可快速及安全的自我身分認證機制；(2)通訊階段不需要線上作業的憑證中心參與認證；(3)符合機密性、完整性、鑑別性及不可否認性等基本安全需求；(4)提供不同軍種單位間(跨網域)之行動通訊服務。

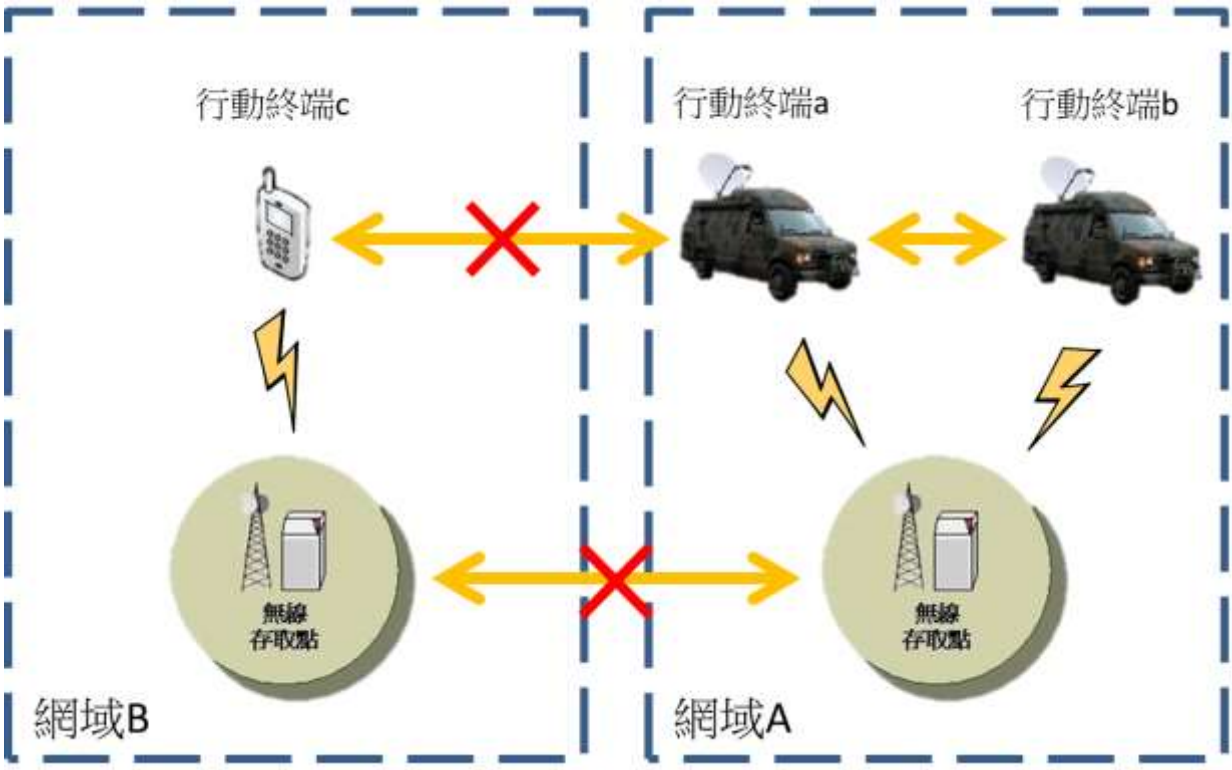
關鍵詞：自我身分認證、機密性、無線通訊。

前言

國軍通資電部隊以網路戰、電子戰為核心，通信平台為基礎，在通信電子資訊次長室的戰略引導下，藉由中科院和民間產學技術支援合作，扮演資訊、通訊和電子作戰等整合角色。平、戰時提供國軍各式指揮、管制、通信、資訊、情報、監視、偵查系統(Command, Control, Communication, Information, Intelligence, Surveillance, Reconnaissance, C^4ISR)之優質的通資基礎平臺，並執行網路資安及電子頻譜管理等任務，依命令支援國軍資通安全重大狀況處理及協助各作戰區緊急災害(難)防救任務。下轄通資站臺更遍佈本外離島各山巔海濱，惟前端勤務人員目前僅能透過建置於移動車載或通資站臺內之有、無線存取節點與指揮部或友軍單位成員相互傳遞資訊，如發生重大災難事故，尚無法直接與其他相關單位人員進行跨網域之行動通訊，不利於相互支援協助(如圖一)另由於不同以往電腦網路是利用實體線材傳送資料，無線網路係將訊息暴露於空中，傳送的資料相對容易遭擷取。

目前國軍通資系統對於通訊媒介沒有完整及統一的保護機制，故在傳遞的過程中，任何有辦法接觸到通資系統通訊媒介的人，都可以藉機取得傳遞資訊；[1]抑或互通的兩端點間執行資料傳遞時均未建立共同通信金鑰且缺乏認證能力。因此，需建置多層次的防護，以確保機敏資訊在傳輸過程的安全性。基於近年來國軍的電子資訊化作戰能力逐年不斷的提升，各項系統建置均已朝向全面資訊化作戰的方向發展，考量國軍在各項訊息傳遞時的重要性，必須於現行資訊系統架構下建置更安全的資料交換機制，俾利提升基本的安全要求，有鑑於此，本研究期許設計以橢圓曲線系統應用於通訊成員間身分識別及驗證的方法、金鑰交換協定，與強化認證及保密等安全機制，期能改善目前國軍通資電部隊無線通訊網路既有窒礙問題，並提供不同軍種單位間之行動通訊服務，滿足在各種各項法定任務環境下之運用，並藉由有效保障無線網路隱私及秘密等安全上的需求，對未來建置國軍通資電部隊數位化指管系統提供有效且實用之助益。

圖一 國軍通資電部隊無線通訊資訊網路示意圖



資料來源：作者繪製。

相關密碼系統介紹

一、橢圓曲線公開金鑰密碼系統

Miller 及 Koblitz 首先提出將橢圓曲線用來實作公開金鑰密碼系統。橢圓曲線的

[1] 蕭雅尹，〈強化國軍通資系統安全之金鑰交換機制設計〉(國防大學資訊管理學系碩士論文，2017年)，頁1。

一般通式為 $y^2+axy+by=x^3+cx^2+dx+e$ 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。

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 $4a^3+27b^2 \bmod q\neq 0$。[2]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。

(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 $3P=2P+P$，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，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。

二、Girault 的自我認證公開金鑰密碼系統

Girault 運用 RSA 系統所設計的的自我驗證公開金鑰密碼系統，共包含三個階段系統建置階段、使用者註冊階段、身分識別協定，各階段分述如下：

(一)系統建置階段

系統所使用參數如下：

1. p , q：兩個大質數。

2. N：一個很大的合成數，為 p 與 q 的相乘積。

3. h：單向雜湊函數。

[2] Miller, V. S.,"Use of Elliptic Curve in Cryptography,"Advance in Cryptography-Crypto'85, New York: Spring-Verlag, 1985, pp.417-426.

4. g：在乘法群 Z_n^* 中最大序的整數。

5. e：系統中心的公鑰，滿足 gcd(e, (p–1)(q–1))＝1。

6. d：系統中心的私鑰，讓 ed＝1 mod (p–1)(q–1)。

系統中心公開{N, e, h}，秘密保留 d，而 p 與 q 可在算完 d 後丟棄。

(二)使用者註冊階段

1.使用者 U_i 選定自己的私鑰 S_i ，計算出 $V_i = g^{-S_i} \bmod N$ ，最後將自己的身分 ID_i 與 V_i 傳給系統中心。

2.系統中心計算 U_i 的公鑰 P_i ， $P_i = (V_i - ID_i)^d \bmod N$ ，並將 P_i 傳回給 U_i 。

3.使用者 U_i 驗證 $P_i^e + ID_i = V_i$ ，若等式成立，則使用者的公鑰為 P_i ，私鑰為 S_i 。

(三)身分識別協定

1.Alice 將其 ID_A 和 P_A 傳給 Bob，然後 Bob 計算 $V_A = P_A^{\,e} + ID_A \bmod N$ 。

2.Alice 選擇一個隨機參數值 x，計算 $t = g^x \bmod N$ ，並將 t 傳送給 Bob。

3.Bob 選擇一個隨機參數值 c，並將其傳給 Alice。

4.Alice 計算 $Y = x + S_A \cdot C$ ，並將 Y 傳送給 Bob。

5.Bob 利用驗證式 $g^Y \cdot V_A^{\,C} = t \bmod N$ ，若等式成立則可證明 Alice 身分。相同地，Alice 也可用此方式驗證 Bob 的身分。

設計具機密性及自我認證之國軍通資電部隊通訊網

蔡英文總統曾於資通電軍指揮部編成典禮時指出：「資通電軍將以通訊安全為基礎，資通電軍要超越傳統的空中、海域及地面的防衛概念，成為重層嚇阻戰略下的第一層嚇阻兵力，並超越各軍種的藩籬，做為國軍聯合作戰典範」蔡總統並期許國軍通資電部隊，要積極達成整合，不僅要整合國軍各相關單位，也必須跟國防部以外的部會密切配合，攜手打造媲美先進國家的資安防護與應變機制。[3]

國軍通資電部隊主要任務包括資訊、通訊和電子作戰等，本研究著重於通訊中的無線通訊系統部分，在通訊作業單位中，主要任務是維護國軍通資系統，包括所有通信品質管控、通訊維護、軍用網路及視訊系統架設。當重大天然災害發生時，指揮管制通信系統暢通構聯，維護通信品質與架構，更是極為重要。[4]

本節將基於Miller(Miller, V. S.,1985)及Koblitz(Koblitz, N.,1987)、橢圓曲線離散對數(ECDLP)及橢圓曲線簽密法設計一個改良式橢圓曲線自我身分識別機制。這個設計適合於無線行動之國軍通資電部隊通訊資訊網路，本研究區分為三個階段：系統建置

[3] 《自由時報》， http://news.ltn.com.tw/news/politics/paper/1114892，(2017 年 6 月 30 日)，2017 年 12 月 28 日下載。

[4] 國軍人才招募中心， https://rdrc.mnd.gov.tw/rdrc/iwa/iwa_b.aspx， 2017 年 12 月 28 日下載。

階段、相同單位間(同網域)通訊階段及不同軍種單位間(跨網域)之通訊階段。以下對本方法各階段進行說明：

一、系統符號說明

本系統中使用的符號說明表，如表一：

表一 系統使用之符號說明

項目	符號	說明
1	id_a, id_b, id_c	a、b 和 c 的帳號。
2	$Q_{CA}, Q_{CB}, Q_a, Q_b, Q_c$	憑證中心 CA、CB，a、b 及 c 的公鑰。
3	$d_{CA}, d_{CB}, d_a, d_b, d_c$	憑證中心 CA、CB，a、b 及 c 的私鑰。
4	j_a, j_b, j_c	a、b 及 c 隨機選取的參數，用來產生簽名。
5	s_a, s_b, s_c	a、b 和 c 的驗證值。
6	r_{CA}, r_{CB}, r_c	憑證中心 CA、CB 和 c 隨取參數，用來產生橢圓曲線上第 1 個點。
7	$\varepsilon_c, \varepsilon_{CB}$	憑證中心 CB 和 c 的簽章。
8	$h(\ )$	雜湊函數。
9	$E(\ )$	對稱式加密函數。
10	$D(\ )$	對稱式解密函數。
11	t_a, t_b, t_c	a、b 及 c 隨機選取的參數，用來產生會議金鑰。
12	K_{ab}, K_{ac}	a 和 b、a 和 c 的共同金鑰。
13	G_{ab}, G_{ac}	a 和 b、a 和 c 當次通訊之會議金鑰。

資料來源：作者繪製。

二、系統初始階段

系統之憑證中心在有限域 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 O 為此橢圓曲線之無窮遠點。憑證中心選擇的一個單向無碰撞雜湊函數 $H()$ ，公開金鑰 Q_{KGC} ，最後認證中心公開 $E, P, n, Q_{KGC}, H()$ ，如表二算式(1)。

表二 計算公式

公式(1)	$Q_{KGC} = d_{KGC} P$
公式(2)	$v_a = h(id_a \| j_a)$
公式(3)	$Z_a = v_a + (k_a - h(id_a))P = (q_{a_x}, q_{a_y})$
公式(4)	$w_a = k_a + d_{CA}(q_{a_x} + h(id_a)) (\mathrm{mod}\, n)$
公式(5)	$s_a = w_a + (h(id_a \| j_a)) (\mathrm{mod}\, n)$

公式(6)	$S_a = s_a P = Z_a + h(id_a)P + [(q_{a_x} + h(id_a))]Q_{CA}$
公式(7)	$\hat{S}_a = Z_a + h(id_a)P + [(q_{a_x} + h(id_a))]Q_{CA}$
公式(8)	$\hat{S}_a = S_a$
公式(9)	$K_{ab} = s_a S_b = s_b S_a$
公式(10)	$T_a = t_a P$
公式(11)	$R_a = k_{ab} + T_a$
公式(12)	$T_b = t_b P$
公式(13)	$R_b = k_{ab} + T_b$
公式(14)	$\hat{T}_a = R_a - K_{ab}$
公式(15)	$W_b = t_b \hat{T}_a$
公式(16)	$Auth(B) = H(id_a, id_b, W_b)$
公式(17)	$Auth(A)^* = H(id_a, id_b, G_{ab}), where\ G_{ab} = W_b + K_{ab}$
公式(18)	$\hat{T}_b = R_b - K_{ab}$
公式(19)	$\hat{W}_b = t_a \hat{T}_b$
公式(20)	$Auth(B)^* = H(id_a, id_b, \hat{W}_b)$
公式(21)	$\hat{G}_{ab} = \hat{W}_b + K_{ab}$
公式(22)	$Auth(A) = H(id_a, id_b, \hat{G}_{ab})$
公式(23)	$v_c = h(id_c \| j_c)$
公式(24)	$I_c = r_c \cdot P(r_{c_x}, r_{c_y})$
公式(25)	$U_c = r_c \cdot Q_{CB}(u_{CB_x}, u_{CB_y})$
公式(26)	$c_c = Eu_{CB_x}(v_c)$
公式(27)	$m_c = h(v_c \| r_{c_x})$
公式(28)	$\varepsilon_c = d_c - m_c \cdot r_c$
公式(29)	$U_c = d_{CB} \cdot I_c = (u_{CBx}, u_{CB_y})$
公式(30)	$v_c = Du_{CB_x}(c_c)$
公式(31)	$m_c = h(v_c \| r_{c_x})$
公式(32)	$\hat{Q}_c = \varepsilon_c \cdot P + m_c \cdot I_c$
公式(33)	$\hat{Q}_c = Q_c$
公式(34)	$I_{CB} = r_{CB} \cdot P(r_{CB_x}, r_{CB_y})$
公式(35)	$U_{CB} = r_{CB} \cdot Q_{CA}(u_{CA_x}, u_{CA_y})$
公式(36)	$c_c = Eu_{CA_x}(v_c)$
公式(37)	$m_{CB} = h(v_c \| r_{CB_x})$

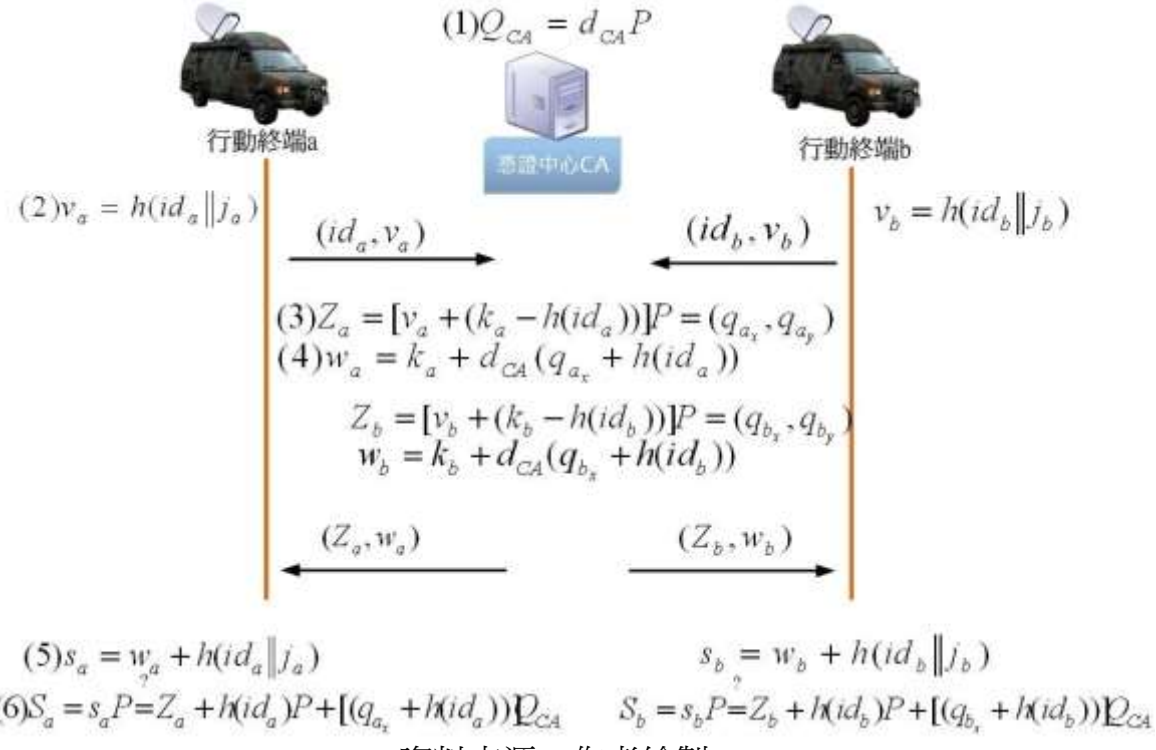
公式(38)	$\varepsilon_{CB} = d_{CB} - m_{CB} \cdot r_{CB}$
公式(39)	$U_{CB} = d_{CA} \cdot I_{CB} = \left(u_{CAx}, u_{CA_y}\right)$
公式(40)	$v_c = Du_{CA_x}(c_c)$
公式(41)	$m_{CB} = h\left(v_c \| r_{CB_x}\right)$
公式(42)	$\hat{Q}_{CB} = \varepsilon_{CB} \cdot P + m_{CB} \cdot I_{CB}$
公式(43)	$\hat{Q}_{CB} = Q_{CB}$
公式(44)	$Z_c = [v_c + (k_c - h(id_c))]P = (q_{c_x}, q_{cy})$
公式(45)	$w_c = k_c + d_{CA}(q_{c_x} + h(id_c))$
公式(46)	$\alpha = Eu_{CA_x}(w_c)$
公式(47)	$w_c = Du_{CA_x}(\alpha)$
公式(48)	$\beta = Eu_{CB_x}(w_c)$
公式(49)	$w_c = Du_{CB_x}(\beta)$
公式(50)	$s_c = w_c + h\left(id_c \| j_c\right)$
公式(51)	$S_c = s_c = Z_c + h\left(id_c \| d_c\right)P + \left(q_{c_x} + h(id_c)\right)Q_{CA}$

資料來源：作者繪製。

三、相同單位間(同網域)之通訊

(一)使用者註冊階段(如圖二)，步驟說明如後。

圖二 使用者註冊階段示意圖



資料來源：作者繪製。

1. 步驟一

行動終端 a 拿自己 id_a 及隨機選取一個參數 $j_a \in [2, n-2]$ 計算表二算式(2)產生簽名 v_a 。

2. 步驟二

行動終端 a 攜帶身分識別碼及簽名 (id_a, v_a) ，親自或者使用某種形式的安全資訊通道的環境下向憑證中心 CA 辦理登錄註冊（這裡以行動終端 a 為例說明，b 之操作步驟同 a）。

3. 步驟三

憑證中心 CA 隨機選取一個參數 $k_a \in [2, n-2]$ 計算表二算式(3)與表二算式(4)產生行動終端 a 的驗證點 Z_a 及簽章 w_a 。

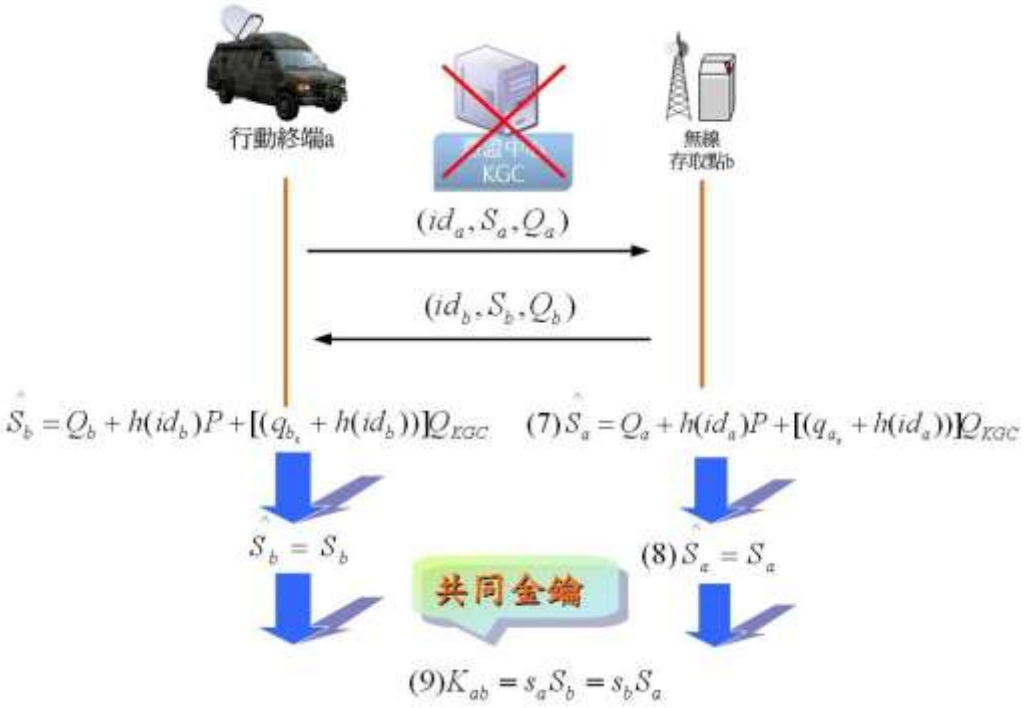
4. 步驟四

行動終端 a 表二算式(5)產生驗證值 s_a ,並運用表二算式(6)驗證 Z_a 之正確性。一旦所有使用者完成上述註冊程序，並取得自己本身的 (w_a, Z_a) 後，在後續通訊階段即可在不依靠憑證中心的情形下，直接於前端完成通訊雙方自我認證程序。

(二)共同金鑰計算階段(如圖三)，步驟說明如後。

假設行動終端 a 和行動終端 b 為彼此間相互通訊的對象：

圖三 共同金鑰計算階段示意圖



資料來源：作者繪製。

1. 步驟一

(1)行動終端a將識別碼、驗證值及驗證點 (id_a, S_a, Z_a) 傳送給行動終端b。

(2)行動終端b將識別碼、驗證值及驗證點(id_b, S_b, Z_b)傳送給行動終端a。

2.步驟二

行動終端 b 為驗證行動終端 a 是否為合法成員，須確認(id_a, S_a, Z_a)是安全的，檢查表二算式(7)及表二算式(8)如下(a 亦同)：

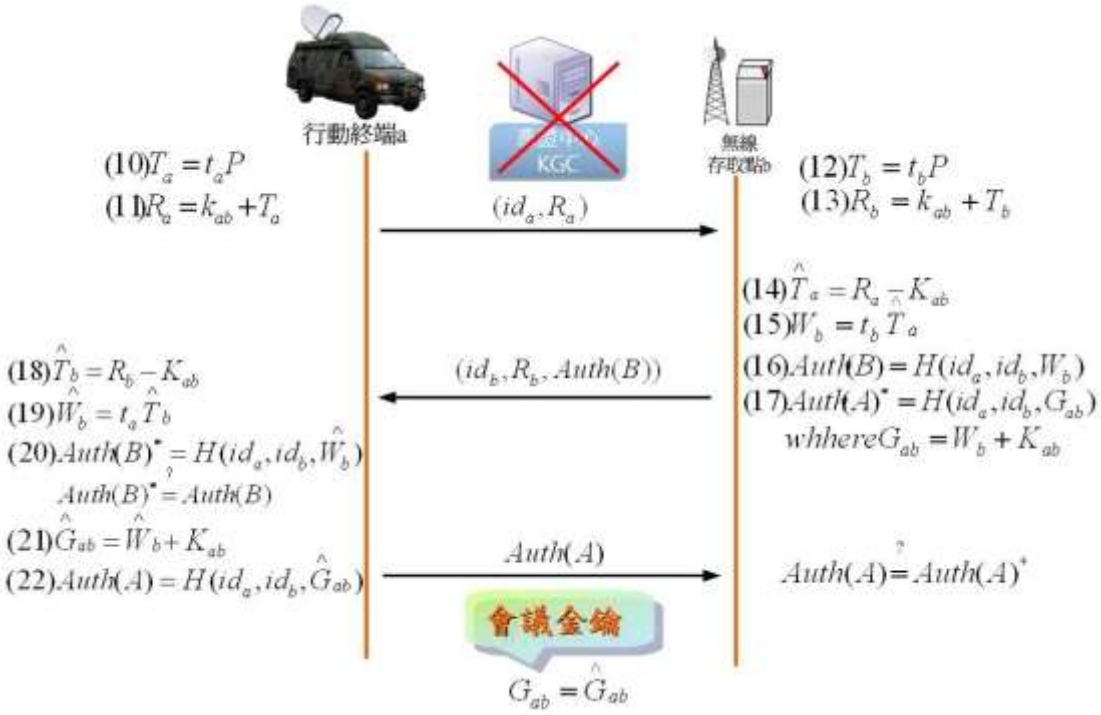
(1)如不符即停止通訊並依安全處理機制回報。

(2)正確無誤，即各自計算共同金鑰K_{ab}，其算式如表二算式(9)。

(三)認證與產生會議金鑰階段(如圖四)，步驟說明如後。

當行動終端 a 與行動終端 b 都擁有相同的共同金鑰K_{ab}後，我們使用一個「挑戰-回應」方法讓雙方做驗證，接下來描述此方法的步驟：

圖四 認證與產生會議金鑰階段示意圖



資料來源：作者繪製。

1. 步驟一

(1)行動終端a隨機選取亂數$t_A \in Z_P$並計算表二算式(10)及表二算式(11)。

(2)將(id_a, R_a)訊息傳送給行動終端點b。

2. 步驟二

(1)當行動終端b收到請求後也隨機選取亂數$t_B \in Z_P$並計算表二算式(12)及表二算式(13)。

(2)期間，行動終端b利用K_{ab}與收到的R_a計算表二算式(14)。

(3)這時對方如果是正確無誤的身分，因為他擁有正確的K_{ab}，所以在這裡$T_a = \hat{T}_a$，行動終端b計算表二算式(15)。

(4)接著產生本次的會議金鑰 G_{ab} 及認證用途上的 $Auth(B)$ 及 $Auth(A)^*$，其方程式如表二算式(16)(17)。

(5)將 $(id_b, R_b, Auth(B))$ 訊息傳送給行動終端a。

3. 步驟三

(1)收到所需要訊息後，行動終端a將實際得到所需訊息產生會議金鑰前，必須先檢查收到的 $Auth(B)$ 是否與自行計算的 $Auth(B)^*$ 相等，如表二算式(18)(19)(20)。

(2)如不相符，行動終端a就立即中止此次通訊之連線。

(3)如果相符，就可繼續計算會議金鑰與 $Auth(A)$，如表二算式(21) (22)。

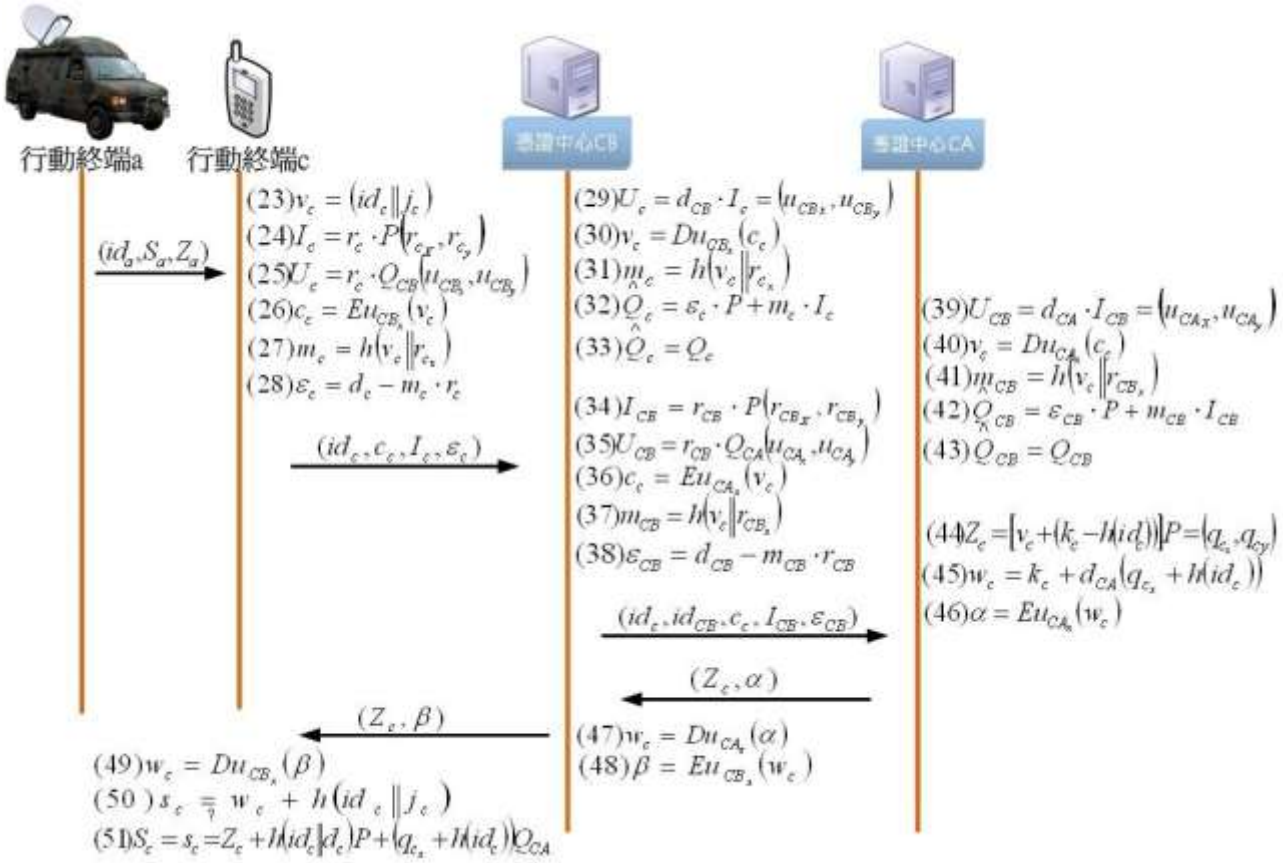
(4)將 $Auth(A)$ 訊息傳送給行動終端b。

(5)行動終端b收到訊息後，驗證收到的 $Auth(A)$ 是否與自行計算的 $Auth(A)^*$ 相等，如相等的話，本次通訊驗證程序就算完成。

四、不同軍種單位間(跨網域)之通訊

(一)使用者註冊階段(如圖五)，步驟說明如後。

圖五 使用者註冊階段示意圖



資料來源：作者繪製。

假設本單位行動終端 a（網域 A）和其他單位之行動終端 c（網域 B）為彼此間相互通訊的對象。

1. 步驟一

行動終端 a 先將相關驗證訊息(id_a, S_a, Z_a)傳送給行動終端 c，行動終端 c 因為無行動終端 a 所屬網域憑證中心 CA 簽發之憑證可驗證其合法性，須先透過自身網域憑證中心 CB 向 CA 申請，首先行動終端 c 拿自己id_C及隨機選取一個參數$j_C \in [2, n-2]$計算表二算式(23)產生簽名v_c。

2. 步驟二

(1)行動終端c為產生簽章，隨選亂數$r_c \in Z_P$，利用亂數計算曲線上的第一個點，算式如表二算式(24)。

(2)隨後再利用憑證中心*CB*的公開金鑰Q_{CB}計算出橢圓曲線上的第二點，並以u_{CB_x}對簽名v_c以對稱式金鑰加密產生相對應的密文c_c，算式如表二算式(25)(26)。

(3)將橢圓曲線上的第一個點$I_c = r_c \cdot P(r_{c_x}, r_{c_y})$中的$r_{c_x}$與簽名$v_c$透過雜湊函數運算得到$m_c$，再利用本身私鑰$d_c$在橢圓曲線上的第一個點對憑證作簽章得到$\varepsilon_c$，算式如表二算式(27)(28)。

(4)將訊息$(id_c, c_c, I_c, \varepsilon_c)$傳送給憑證中心CB。

3. 步驟三

(1)憑證中心CB收到由行動終端c傳送的訊息後，首先為了驗證是否為合法送訊者所傳送過來的資訊，會用自己的私鑰d_{CB}計算出橢圓曲線上的第二點U_c，得到u_{CB_x}，如表二算式(29)。

(2)憑證中心CB以u_{CB_x}作為對稱式解密之密鑰解開密文c_c，得到行動終端c簽名v_c，並利用收到的I_c中的r_{c_x}與v_c透過雜湊函數運算得m_c，如表二算式(30)(31)。

(3)最後利用行動終端c的公開金鑰Q_c計算出橢圓曲線上的$\hat{Q}_c = \varepsilon_c \cdot P + m_c \cdot I_c$，如得到行動終端c的公開金鑰$\hat{Q}_c = Q_c$，代表憑證中心CB接收到的簽名$v_c$確實由行動終端c所傳送，算式如表二算式(32)(33)。

4. 步驟四

當憑證中心 CB 驗證行動終端 c 身分無誤後，即比照上述步驟 2 將行動終端 c 之簽名v_c加密，並產生簽章後，將相關訊息$(id_c, id_{CB}, c_c, I_{CB}, \varepsilon_{CB})$傳送給憑證中心 CA，算式如表二算式(34)(35)(36)(37)(38)。

5. 步驟五

(1)憑證中心CA收到由憑證中心CB傳送的訊息$(id_c, id_{CB}, c_c, I_{CB}, \varepsilon_{CB})$後，即比照上述步驟3驗證憑證中心CB身分，並取得行動終端c之簽名v_c，算式如表二算式(39)(40)(41)(42)(43)。

(2)當憑證中心CA驗證憑證中心CB身分無誤後，隨機選取一個參數$k_c \in [2, n-2]$計算表二算式(44)與(45)產生行動終端c的驗證點Z_c及簽章w_c。

(3)將簽章 w_c 以對稱式金鑰加密產生相對應的密文 α 後，算式如表二算式(46)，將訊息 (Z_c,α) 傳送給憑證中心CB。

6. 步驟六

(1)憑證中心CB收到由憑證中心CA傳送的訊息 (Z_c,α) 後，計算表二算式(47)得到簽章 w_c ，再以對稱式金鑰加密產生相對應的密文 β 後，算式如表二算式(48)，將訊息 (Z_c,β) 傳送給行動終端c。

(2)行動終端c計算表二算式(49)得到簽章 w_c 後，再計算表二算式(50)產生驗證值 s_a ，並運用表二算式(51)驗證 Z_c 正確性。

一旦行動終端 c 完成在網域 A 之註冊程序，並取得自己本身的相關憑證資料 (w_c,Z_c) 後，在後續通訊階段即可在不依靠憑證中心的情形下，直接於前端與網域 A 任何成員完成通訊雙方自我認證程序。

(二)共同金鑰計算階段

假設行動終端 a 和行動終端 c 為彼此間相互通訊的對象，雙方比照上述步驟，驗證對方是否為合法成員後，並各自計算共同金鑰 K_{ac} 。

(三)認證與產生會議金鑰階段

當行動終端 a 與行動終端 c 都擁有相同的共同金鑰 K_{ac} 後，在後續每次通訊階段比照上述步驟，驗證對方身分，產生當次通訊之會議金鑰 G_{ac} ，並使用此金鑰對所傳送之訊息實施加密。

安全性及效益分析

在無線網路上，由於無線傳輸的特性，使攻擊者容易連接到無線網路範圍內，因而安全性的問題成為無線網路急需解決的問題。為了建構安全的無線網路，本研究除預期可達到 ISO 組織所提之資訊系統安全管理需求，包含資訊之機密性、鑑別性、完整性及不可否認性等基本安全，尚可抵禦網路上常見的重送攻擊、竊聽攻擊、偽裝攻擊及修改攻擊等攻擊方式，以下我們將針對本研究提出加密機制之安全需求滿足狀況及常見攻擊手法之抵禦能力進行探討，並以現況與本研究提出之機制進行比較及分析，以驗證本研究可達預期之目標：

一、安全性分析

(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。本方法通訊雙方所傳遞之訊息均是使用當次通訊階段所產生之會議金鑰加密，第三者若要竊聽並成功解譯這些傳輸之資訊密文，除不知通訊者每次所選取的隨機數(例如 t_a 及 t_b)外，亦須面對橢圓曲線離散對數之難題。

(二)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，以保證該訊息確實是由宣稱的送方所送來的，本方法中通訊雙方使用表二算式(7)驗證對方身分，而認證之方式為 $\hat{S}_a = Q_a + h(id_a)P + [(q_{a_x} + h(id_a))]Q_{KGC}$ ，對破譯者來說他必須面對破解單向雜湊函數及面對橢圓曲線離散對數問題，若第三方無法破解表二算式(7)則鑑別性可以確保。

(三)完整性(Integrity)

完整性的要求是訊息在傳輸的過程中，接收方可判斷訊息有無遭到破壞或是竄改，若在接收的過程中收到非完整的訊息，可利用設計之機制拒絕該訊息，以避免在傳輸過程中遭有心人士破壞，若惡意第三者試圖在本機制中獲得明文，必須先獲得雙方共同之通訊金鑰，該金鑰已利用橢圓曲線之離散對數進行包裝，其破解難度可有效抵禦攻擊，並使本方法滿足完整性之需求。

(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的證明，使該行動或事件往後不能被否認的能力，本方法中表二算式(32)密文使用雙方之會議金鑰加密，而這把會議金鑰只有雙方才有辦法共同擁有，其他任何人皆無法獲得此會議金鑰。若第三方想要藉由傳送方使用者 a 之公鑰推斷其私鑰，則破譯者會面對橢圓曲線離散對數之難題，這使得傳送方發出密文具有不可否認性。

二、常見攻擊法

(一)重送攻擊

指攻擊者收集合法參與者所傳送的過期資訊，將這些過期的資訊，在最近的時間內，重送給相關的參與者，本方法在每一次的認證過程中表二算式(10)，所選取的隨機數(例如 t_a 及 t_b)都不相同，故產生之會議金鑰也不同。因此，攻擊者無法藉由蒐集過去參與者所傳送的資訊來進行重送攻擊。

(二)竊聽攻擊

指攻擊者利用竊聽的方式收集使用者所傳遞的訊息，並從收集的訊息中推導出有用的資訊或是使用者的私密資料，本方法若攻擊者獲得參與者所傳遞的，在不知隨機數(例如 t_a 及 t_b)的情況下亦無法推導出有用的資訊。因此，攻擊者無法經由竊聽的方式推導參與者的私密資訊。

(三)偽裝攻擊

指攻擊者偽冒成合法參與者的身分，為網路中的其它成員提供非法的服務，本方法假如攻擊者想要偽裝成合法的節點，就必須獲得表二算式(9)節點的共同金鑰 $K_{ab} = s_a S_b = s_b S_a$ ，才能偽裝成合法使用者，所以攻擊者必須解決橢圓曲線離散對數

的問題。

(四)修改攻擊

攻擊者藉由修改通訊雙方的部分驗證資訊，使得原本傳送合法驗證訊息的通訊雙方，因遭到攻擊者修改而導致一方無法驗證成功。本方法因為參與者所傳遞的公開訊息都轉換為橢圓曲線上的點，因此攻擊者無法修改任何訊息。

三、效能分析

為驗證本研究所提出之機制可符合預期之目標，本節針對國軍通資電部隊現行無線通訊資訊網路與本研究設計之自我身分認證與加密機制，比較兩者之各項特色如表三。

(一)使用者認證

由於無線通訊系統之訊號暴露於不安全的環境中，身在環境中的人員均有機會擷取系統發送之訊號，尤其本研究之應用環境為軍事用途，故使用者合法性之認證格外重要。傳統認證方式僅透過識別碼進行合法性之認證，必須由人員相互進行辨證，不僅耗時費力且僅驗證使用者身分而非其合法性。本研究提出之通訊機制可利用註冊階段由憑證中心發送之訊息，進行通訊雙方使用者合法性之認證，不僅降低人員作業之誤失率，且透過運算即可於短時間內完成認證程序。

(二)可離線之身分認證

由於本研究提出之機制所應用之環境不確定因素多，不論是執行演訓、救災或是真實戰場，整體通訊環境及品質必定較平時為差。自我身分認證機制的優勢在於使用者雙方進行通訊前，不需每次透過憑證中心進行驗證，一方面減輕憑證中心負擔，另一方面在通訊環境不確定性高的狀況下仍可有效進行驗證，可不受環境品質之牽制，大幅提高使用之彈性。本研究提出之機制有別於現況，允許使用者雙方在無憑證中心的狀況進行驗證，可適用於多項軍事用途。

(三)跨軍種單位行動通訊

在實際通訊系統應用之環境，人員或載具必須依任務特性不同分布於不同地區或者頻繁移動，且國軍執行各項任務均強調聯合軍種作戰。因此，跨軍種單位之行動通訊更能夠有效提升整體任務遂行能力、強化聯合作戰效能，本方法允許各軍種不同單位的官兵跨網域相互通訊，僅須先行透過憑證中心註冊乙次，現階段尚無可跨軍種，且具自我認證之無線通訊機制。

(四)金鑰分配

傳統金鑰分配由使用單位定期將保密器集中至指定地點進行金鑰挹注，提高了失竊及損壞的風險，本方法提出可進行自我認證之架構後，憑證中心之負擔將大幅降低，所有經過註冊的使用者皆可在無憑證中心的狀況下進行自我驗證，可減少資源的

耗損，並減輕管理的負擔。

表三 本研究與現行方法比較表

項目	國軍通資電部隊現況	本研究
使用者認證	1. 僅透過無線電識別碼辨識使用者身分，無法驗證資料來源的合法性。 2. 使用者雙方進行辨證，以確認對方使用者之合法性，人工作業耗時且錯誤率高，使用者對裝備的熟悉度亦影響其正確性。	透過憑證中心簽發之憑證完成通訊雙方身分辨識，確保參與者身分合法性，並防範惡意者的偽冒。
可離線之身分認證	無	通訊雙方可在無憑證中心參與的情況之下離線完成彼此間身分的驗證作業，提升通訊效率並減輕後端運算負擔。
跨軍種單位行動通訊	無	不同單位間的勤務人員都能相互認證，提供勤務人員在執行跨單位任務時之通訊漫遊服務。
金鑰分配	透過定期將保密器集中以人力方式灌入金鑰，無法由系統派送，除增加人力負擔外，在保密器拆卸或運送的過程中提高了損壞或遭竊之風險。	金鑰由使用者個人保管即可。

資料來源：作者繪製。

未來發展建議

一、 結合行動寬頻網路

第四代行動通訊網路技術已十分成熟，現階段在移動中的傳輸速率最高可達 100 Mbps，不僅能夠提供數據及語音的傳輸，甚至能夠有效地傳遞視訊影像資料，結合行動寬頻網路客大幅提升本研究提出架構之應用性。不論在災害防救、戰訓整備或是聯合作戰，皆可有效將前線蒐集之寶貴資料在第一時間回傳到指揮所，以利指揮官進行決策，並達到資訊傳遞安全的要求。

二、 導入離線身分驗證機制

國軍執行任務之環境較為複雜，容易受氣象或是地形等因素影響通訊品質，甚至無法持續與憑證中心連線。在傳統的身分驗證系統中仰賴中心管理金鑰及發放憑證，不僅造成整體系統負擔提高，對於特殊環境下之使用實為不易。因此，本研究將自我認證之架構與國軍現行通訊系統整合應用，整合後的架構在實務上只要使用者(終端設備)執行任務前，在有利的環境中向憑證中心完成註冊。即便使用者前進至非

憑證中心所在之網域，仍可藉由本機制進行雙方的身分驗證，使整體通訊系統之機動性提升，並能有效適應變化性較大之環境，藉以符合建軍備戰需求。

三、 整合各軍種無線通訊系統

現代戰爭型態以三軍聯合指管為主流，而平時國軍亦將災害防救納入重點任務之一，均須藉由各軍種具有之特性進行整合，以達戰力之最大化。為落實平、戰時三軍聯合作戰機制，提升三軍聯合作戰效能，有效且安全的溝通管道為其關鍵因素。在整合各軍種系統的過程中，有關通訊雙方之身分認證可參考本研究提出之機制，使得在不同憑證中心作業下的使用者亦能透過安全的機制進行身分驗證。

四、 增加系統安全性測試及專業人才培育

戰場指管倚賴通信之遂行，通信系統好比人類的神經系統，在指揮者與執行者間進行訊息傳遞，通信系統的安全考量當然不在話下。然而隨著科技日新月異，全世界每天都有新的資訊安全漏洞被揭露，也就是說當我們持續依賴久未被檢視的系統時，在資訊安全的保障中不進則退，意即有其必要定期檢視系統的安全性，建議可採類似滲透測試的作為及其標準進行系統測試。

國軍通資電部隊負有處置國家級資訊安全事件之責任，專業人才之培訓應具備與民間相當抑或更勝之水準。日前我國參加「2017 年駭客大賽世界盃」競賽，榮獲全球第 2 名的佳績，顯示民間資訊安全專家實力匪淺，建議可定期辦理論壇或競賽等活動與民間專家技術交流，以提升國軍專業人才實力，最後，相關專案人員應須定期留意各式新型態之攻擊手法及漏洞，以確保系統保持安全無虞之狀態。

結論

隨著網路技術與通訊科技不斷地推陳出新，無論是公營機關或私人企業，均有可能面臨資訊安全的衝擊，不僅是機關的正常運作、企業的永續經營受到影響，甚或國家的整體基礎建設及安全均面臨挑戰，資訊網路安全對國家的威脅性，已從過去的竊取情報逐漸進化成主動攻擊，沒有安全就沒有一切，在國軍整體發展中安全的議題逐漸成為關鍵。

本研究提出以橢圓曲線為基礎所設計的加密認證機制，以橢圓曲線密碼系統所具有金鑰長度較短與計算複雜度較低的特性，運用在低計算量的設備、低頻寬、連線不穩定情況下，將有較大之效益，綜整本研究，其優點如下：

一、建置可快速及安全的自我身分認證機制。

二、通訊階段不需要線上作業的憑證中心參與認證。

三、符合機密性、鑑別性、完整性及不可否認性等基本安全需求。

四、提供不同軍種單位間（跨網域）之行動通訊服務。

綜合上述分析及建議，本研究藉由提出符合國軍特殊需求性之架構，盼能在整體系統之安全上貢獻一己之力，使我軍在提升戰備能量的同時也能夠保障訊息傳送之機密性，並降低系統負擔，提高資源使用率，在有限資源下達到最高的效益。

參考文獻

一、 楊中皇，《網路安全理論與實務》，第二版(台北：學貫行銷股份有限公司，2008年)。

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

三、 吳信翰，〈行動網路下之使用者認證機制研究〉(世新大學資訊管理學系碩士論文，2007年)。

四、 賴峙樺，〈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，2003年)。

五、 Diffie, W. and Hellman, M. “New Directions in Cryptography,” IEEE Trans. Inform. Theory, Vol.IT-22, 1976.

六、 Girault, M. “Self-certified public keys,” Advances in Cryptology–EuroCrypt'91, LNCS, Vol.547, Spring-Verlag, 1991.

七、 ISO, Information technology - Security techniques - Code of practice for information security management, ISO/IEC 17799, 2.6, 2005/06/15.

八、 Koblitz, N., “Elliptic Curve Cryptosystems”, Mathematics of Computation American Mathematical Society, Vol.48, 1987.

九、 Merkle, R.C. and Hellman, M. “Hiding Information and Signatures in Trap-door Knapsacks”, IEEE Trans. Inform. Theory, Vol.IT-24, 1978.

作者簡介

楊博元上尉，國防大學管理學院資訊管理學系101年班，曾任排長、人事官，現為國防大學管理學院資訊管理學系碩士班研究生。

郭尚瑋士官長，空航技術學院常士91年班、景文科大副學士、國防大學管理學院資訊管理學系碩士107年班，曾任油機士、通信士、資訊作業士 ，現任資通電軍測訓中心教官。

蘇品長上校，長庚大學電機工程博士，曾任預算財務官、程式設計官、資訊督導官，現任國防大學管理學院資訊管理學系教授。