設計具機密性及可自我認證之海巡通訊網

蘇品長　邱謙忠　李明忠　廖家宏　黃棠建

國防大學資訊管理研究系

摘　　要

海巡署任務多樣且特殊，如何安全的運用無線通訊網路將各類情報提供第 1 線勤務執行單位，或將前端訊息回傳後端指揮控制中心，進行決策分析，為提升海巡署各項任務執行效能之重要關鍵。本文中我們提出一個利用橢圓曲線密碼為概念的新方法。我們的方法具有除了符合機密性、完整性等基本安全需求外，同時密文具備雪崩效應效果。本研究具有以下五項優點：(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)密文中混入假資料增加第三者破解密文困難。(5)密文具備雪崩效應效果。

關鍵詞：自我身分認證、橢圓曲線密碼。

The Design of Self-certification and Confidentiality of Coast Guard Communications network

Pin-Chang Su, Qian-Zhong Qiu, Ming-Zhong Li, Chang-Hung Liao, Huang-Tang Chien

Department of Information Management, Management College,
National Defense University,Taiwan, R.O.C

Abstract

The task of Coast Guard is diverse and special, and how to safely use wireless communication network will provide various types of information service execution, and transmit information to command and control center. The key task execution will more efficient by the decision analysis, which enhances the performance of Coast Guard. In this paper, we propose a the new method using Elliptic Curve Cryptography. Our method meets not only the confidentiality, integrity, security and other basic needs, but also the effect of avalanche. This study has the following five advantages: (1) building fast and safe self-authentication mechanism. (2) not to need the certification of online centers in communication phase. (3) complying with the confidentiality, integrity, authenticity and non-denial of other basic security needs. (4) mixing with false information to increase the difficulties of deciphering. (5) effecting ciphertext with the effect of avalanche.

Key words：Self-certification, Elliptic Curve Cryptography.

壹、前言

海巡署依法執行海岸巡防，負責反走私、偷渡、維護台灣海域安全與海洋資源保護之責。海巡艦艇巡弋範圍廣闊，前端勤務人員依任務需求機動彈性往來於各區域，並透過建置於台灣周邊之無線存取點與指揮控制中心相互傳遞資訊，海巡無線通訊資訊網路示意圖如圖 1 所示，然由於不同以往電腦網路是利用線材傳送資料，無線網路係將訊息暴露於空中，相對傳送的資料易遭截取。而海巡署平時依法執行查緝走私、偷渡與海域安全維護等工作，具有司法警察身分，戰時又納入國防部統一指揮調度，其任務屬性特殊且具有一定之機敏性，有鑑於此，本研究期許以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，期能改善目前海巡署無線通訊網路既有窒礙問題。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，對未來建置海巡數位化指管系統提供有效且實用之助益。

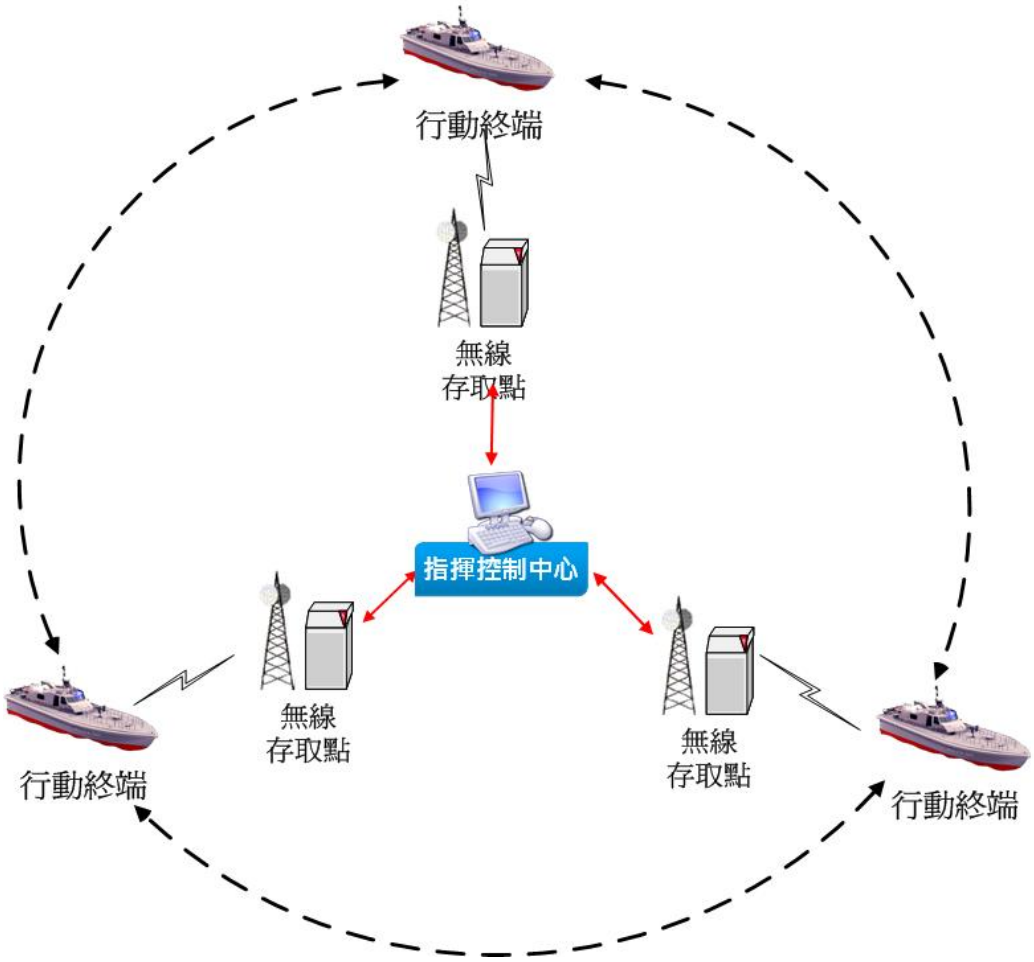

圖 1：海巡無線通訊資訊網路示意圖
(資料來源：本研究)

貳、文獻探討

一、橢圓曲線公開金鑰密碼系統

Miller (1985) 及 Koblitz (1987)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 $4a^3+27b^2 \bmod q\neq 0$。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。

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

2.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 $P+Q=O$

3.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(蘇品長，2007)。下表為 RSA 與橢圓曲線密碼系統在相同安全度下金鑰長度之比較表。

表 1：RSA 與橢圓曲線密碼系統在相同安全度下金鑰長度之比較表

RSA與ECC密碼系統在相同安全度下金鑰長度之比較					
RSA金鑰長度	1024	2048	3072	7680	15360
ECC金鑰長度	163	224	256	384	512
RSA:ECC金鑰長度比	6:1	9:1	12:1	20:1	30:1

(資料來源：楊中皇，2008)

二、Girault 的自我認證公開金鑰密碼 系統

Girault (1991) 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。
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，並計算出 $V_i = g^{-S_i} \bmod N$，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。

參、設計具機密性及自我認證之海巡通訊網

本節將基於 Miller (1985) 及 Koblitz (1987) 設計及橢圓曲線離散對數（ECDLP）設計一個改良式橢圓曲線自我身分識別加密機制。這個設計適合於無線行動之海巡通訊資訊網路，本研究區分為五個階段：系統建置階段、使用者註冊階段、共同金鑰計算階段、認證與產生會議金鑰階段及資料加解密階段；我們所提的方法是植基於橢圓曲線離散對數困難度，加密方法的完整性上面，除了單向雜湊函數的檢查之外，同時密文之間執行橢圓曲線點加運算，使得密文產生雪崩效果，亦可當成完整性檢查的一環。以下對本方法各階段進行說明：

一、系統符號說明

表 2 為系統中使用的符號說明

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 $H()$，並計算公開金鑰 Q_{KGC} ，最後認證中心公開 $E, P, n, Q_{KGC}, H()$。

$$Q_{KGC} = d_{KGC} P \qquad (1)$$

三、使用者註冊階段(如圖 2)，步驟說明如後：

步驟一：行動終端 a 拿自己 id_a 及隨機選取一個參數 $d_a \in [2, n-2]$ 計算(2)

產生簽章V_a

$$V_a = h(id_a \| d_a) \quad (2)$$

步驟二：行動終端 a 攜帶身分識別碼及簽章(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*(KGC)*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）。

步驟三：憑證中心*(KGC)*隨機選取一個參數$k_a \in [2, n-2]$計算(3)與(4)產生行動終端 a 的公開金鑰Q_a及簽章w_a。

表 2：系統使用之符號說明

項目	符號	說明
1	id_a, id_b	a 和 b 的帳號
2	Q_{KGC}, Q_c, Q_a, Q_b	憑證中心、指揮控制中心 c、a 及 b 的公鑰
3	d_{KGC}, s_a, s_b	憑證中心私鑰、a 及 b 的驗證值
4	d_a, d_b	a 和 b 隨機取的參數，用來產生簽章
5	K_{ab}	a 和 b 的共同金鑰
6	$G_{ab}\ G_{bc}$	a 和 b 的會議金鑰、b 和指揮控制中心 c 的會議金鑰
7	$H()$	認證中心公開之雜湊函數，以 SHA-512 為例
8	$H_{m2p}()$	將訊息轉為橢圓曲線點之函數
9	$H_{p2m}()$	將訊息由橢圓曲線點轉為值之函數
10	m_i	明文訊息區塊
11	N_i	利用 $H_{m2p}()$ 函數將訊息塊 m_i 編碼成為橢圓曲線之點集合
12	Q_j	一組亂數產生橢圓曲線上之點集合
13	P_n	明文轉點與混淆點的集合
14	C_n	經過加密的明文轉點與混淆點集合
15	w	背包值

$$Q_a = V_a + (k_a - h(id_a))P = (q_{a_x}, q_{a_y}) \quad (3)$$

$$w_a = k_a + d_{KGC}(q_{a_x} + h(id_a)) \bmod n \quad (4)$$

步驟四：行動終端 a 計算(5)產生驗證值S_a，並運用(6)驗證Q_a之正確性。

$$s_a = w_a + (h(id_a \| d_a)) \bmod n \quad (5)$$

$$S_a = s_a P \stackrel{?}{=} Q_a + h(id_a)P + [(q_{a_x} + h(id_a))]Q_{KGC} \quad (6)$$

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, Q_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。

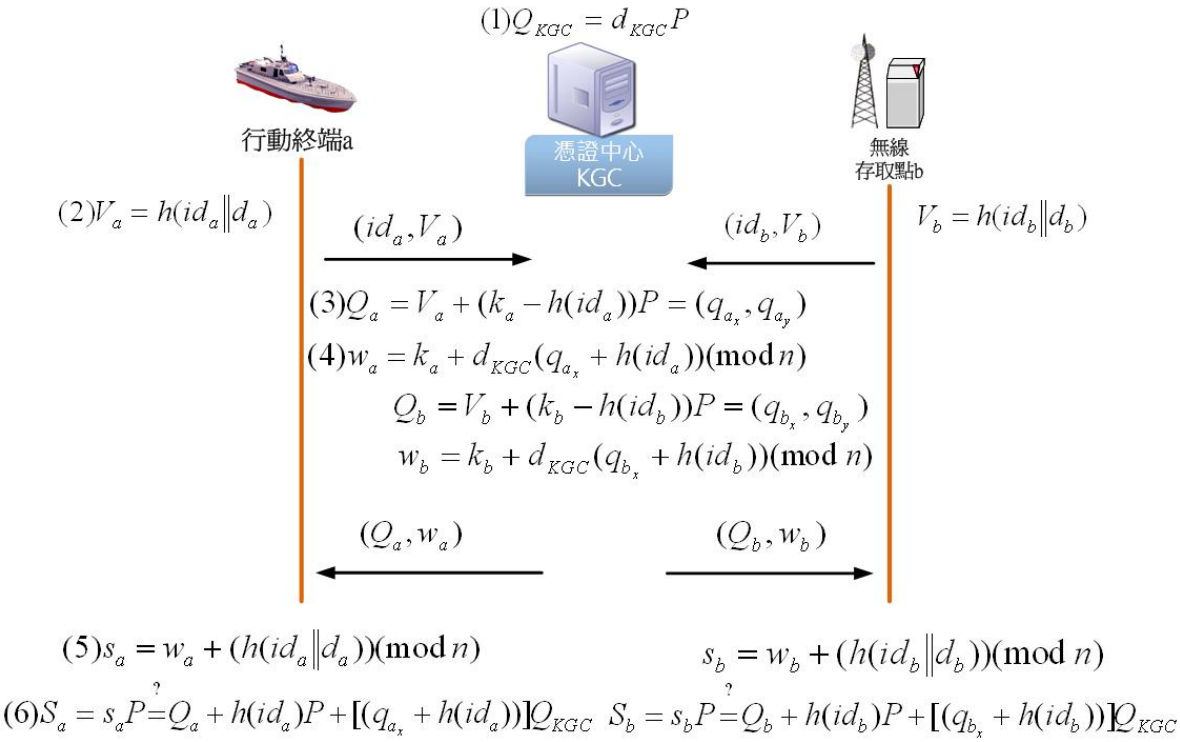

圖 2：使用者註冊階段示意圖
(資料來源：本研究)

四、共同金鑰計算階段(如圖 3)，步驟說明如後：

假設行動終端a和無線存取點b為彼此間相互通訊的對象：

步驟一：

1.行動終端 a 將識別碼、驗證值及公鑰 (id_a, S_a, Q_a) 傳送給無線存取點 b。

2.無線存取點 b 將識別碼、驗證值及公鑰 (id_b, S_b, Q_b) 傳送給行動終端 a。

步驟二：

無線存取點 b 為驗證行動終端 a 是否為合法成員，須確認 (id_a, S_a, Q_a) 是安全的，檢查式(7)及(8)如下（a 亦同）：

$$\hat{S}_a = Q_a + h(id_a)P + [(q_{a_x} + h(id_a))]Q_{KGC} \quad (7)$$

$$\hat{S}_a = S_a \quad (8)$$

1.如不符即停止通訊並依安全處理機制回報。

2.正確無誤，即各自地計算共同金鑰 K_{ab}，其算式如式(9)。

$$K_{ab} = s_aS_b = s_bS_a \quad (9)$$

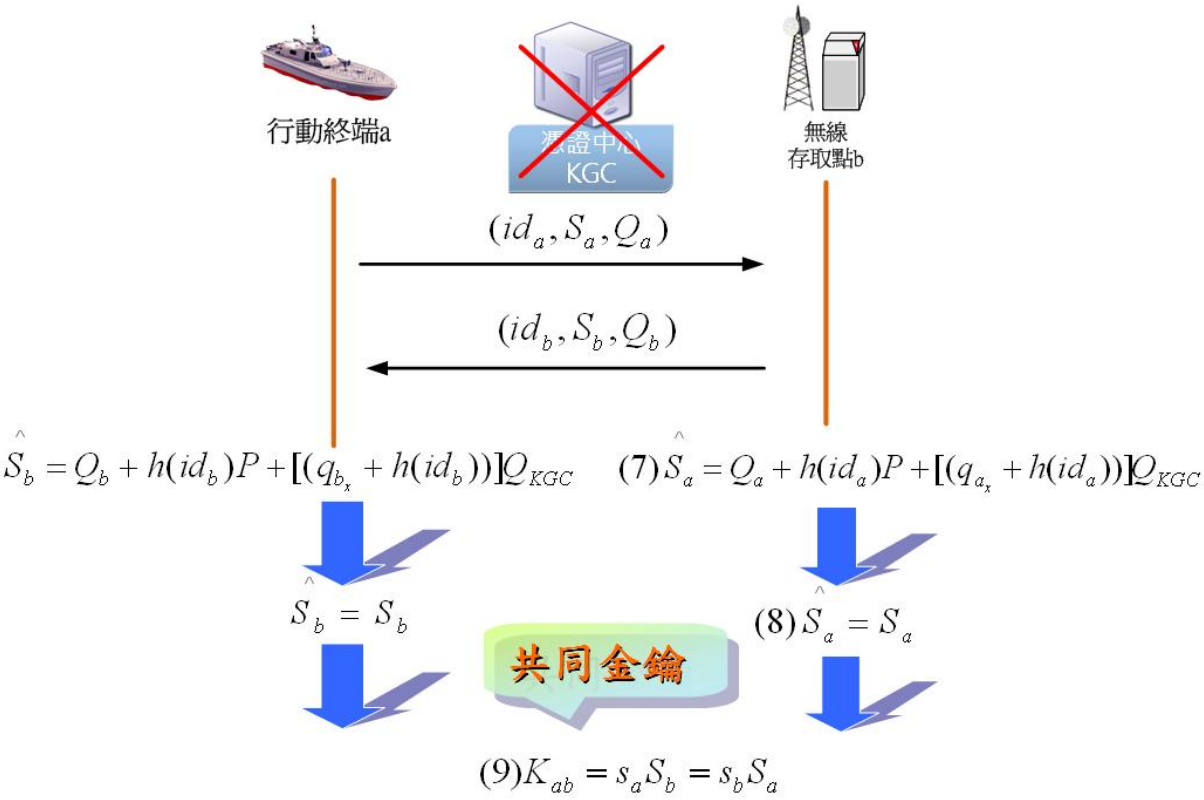

圖 3：共同金鑰計算階段示意圖
(資料來源：本研究)

五、認證與產生會議金鑰階段

(如圖 4)，步驟說明如後：

當行動終端 a 與無線存取點 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：

步驟一：

1.行動終端 a 隨機選取亂數 $t_a \in Z_n$ 並計算(10)及(11)。

$$T_a = t_a P \tag{10}$$

$$R_a = K_{ab} + T_a \tag{11}$$

2.將 (id_a, R_a) 訊息傳送給無線存取點 b。

步驟二：

1.當無線存取點 b 收到請求後也隨機選取亂數 $t_b \in Z_n$ 並計算(12)及(13)。

$$T_b = t_b P \tag{12}$$

$$R_b = K_{ab} + T_b \tag{13}$$

2.期間，無線存取點 b 利用 K_{ab} 與收到的 R_a 計算(14)。

$$\hat{T}_a = R_a - K_{ab} \tag{14}$$

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 $T_a = \hat{T}_a$，無線存取點 b 計算(15)。

$$W_b = t_b \hat{T}_a \tag{15}$$

4.接著產生本次的會議金鑰G_{ab}及認證用途上的$Auth(B)$及$Auth(A)^*$，其方程式如下：

$$Auth(B) = H(id_a, id_b, W_b) \quad (16)$$

$$Auth(A)^* = H(id_a, id_b, G_{ab}), G_{ab} = W_b + K_{ab} \quad (17)$$

5.將$(id_b, R_b, Auth(B))$訊息傳送給行動終端a。

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(18)(19)(20)。

$$\hat{T}_b = R_b - K_{ab} \quad (18)$$

$$\hat{W}_b = t_a \hat{T}_b \quad (19)$$

$$Auth(B)^* = H(id_a, id_b, \hat{W}_b) \quad (20)$$

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(21) (22)。

$$\hat{G}_{ab} = \hat{W}_b + K_{ab} \quad (21)$$

$$Auth(A) = H(id_a, id_b, \hat{G}_{ab}) \quad (22)$$

4.將$Auth(A)$訊息傳送給無線存取點b。

5.無線存取點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。

六、資料加解密階段

步驟一：行動終端a將明文作雜湊運算得到明文雜湊值u如(23)

$$u = H(M) \quad (23)$$

步驟二：行動終端a將訊息拆解成n個m_i區塊如(24)式

$$M = \{m_1, m_2, ..., m_i\} \quad (24)$$

步驟三：將明文轉為橢圓曲線點座標

接著利用$H_{m2p}()$函數將訊息塊m_i編碼成為橢圓曲線之點，得到如下訊息。

$$N_i = H_{m2p}(m_i) \quad (25)$$

步驟四：行動終端a隨機產生一組之亂數

$$v = \{v_1, v_2, ..., v_i\}, 1 < v_i < n-1 \quad (26)$$

並以此組亂數產生一組橢圓曲線上之點。

$$Q_j = v_i G \quad (27)$$

步驟五：區塊編碼成點將N_i點依序按任意間隔插入Q_j點序列中成為P_n點序列，混合完成後之點序列以(28)式表示。

$$P_n \in \{N_i, Q_j\} \quad (28)$$

步驟六：註記訊息位置製造$\overline{x}_n$數列如式(29)對應P_n點序列，若P_n點為N_i，則x_n=1，否則x_n=0。

$$if\ P_n = N_i, x_n = 1\ else\ x_n = 0 \qquad (29)$$

步驟七：計算訊息所在之背包值

$$w = \left\{x_1.2^{n-1} + x_2 2^{n-2} + ..x_n 2^0\right\} \qquad (30)$$

步驟八：加密運算行動終端 a 將點序列 P_n 進行下列方式(31) (32) (33)(34)運算。

$$C = \{C_0, C_1, C_2, ..., C_n\} \qquad (31)$$

$$C_0 = \{H_{m2P}(w,u) + G_{ab}\} \qquad (32)$$

$$C_1 = \{P_1 + C_0\} \qquad (33)$$

$$C_n = \{P_n + C_{n-1}\} \qquad (34)$$

步驟九：行動終端 a 送出下列資料給無線存取點 b

$$(id_a, C) \qquad (35)$$

步驟十：解開明文位置及明文雜湊值無線存取點 b 以(36) (37)將 (w,u) 解出。

$$H_{m2P}(w,u) = C_0 - G_{ab} \qquad (36)$$

$$(w,u) = H_{p2m}\left[H_{m2P}(w,u)\right] \qquad (37)$$

步驟十一：解譯密文無線存取點 b 使用(38)(39)解譯密文點。

$$P_1 = C_1 - C_0 \qquad (38)$$

$$P_n = C_n - C_{n-1} \qquad (39)$$

步驟十二：挑出明文點無線存取點 b 將 w 還原成 $\bar{x}_n$ 數列，還原方式如(40)。對應 1 的位置即為 N_i 存放位置，挑出所有 N_i 轉換為明文如(41)。

$$w = \bar{x}_n = (x_1 x_2 ... x_n)_2 \qquad (40)$$

$$m_i = H_{p2m}(N_i) \qquad (41)$$

步驟十三：還原明文利用(42)將所有 m_i 區塊組合成明文 $\hat{M}$ 。

$$\hat{M} = \sum_1^i m_i \qquad (42)$$

步驟十四：明文驗證若下式等號成立則訊息接收無誤，反之，訊息已遭竄改。

$$u \stackrel{?}{=} H(\hat{M}) \qquad (43)$$

步驟十五：傳送訊息

1.當無線存取點 b 收到訊息 $\hat{M}$ 後，即比照上述階段四、五與指揮控制中心 c 完成彼此間身分認證，並產生會議金鑰 G_{bc} ，並以階段六步驟一至九將訊息 $\hat{M}$ 加密成密文 $\hat{C}$ 後，傳送 $(id_a, id_b, \hat{C})$ 給指揮控制中心 c。

2.最後指揮控制中心 c 使用會議金鑰 G_{bc} 將密文 $\hat{C}$ 解密還原成明文，取得行動終端 a 傳送之訊息 $\hat{M}$ 。

肆、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(2005)，包含資訊之機密性、完整性、可驗證性及不可否認性等

基本安全外，尚可以應付網路上常見的攻擊方式。目前在網路上常見的攻擊方式有重送攻擊、竊聽攻擊、偽裝攻擊及修改攻擊等。以下我們將針對本研究所提之加密機制，其安全性主要植基於 ECDLP 及單向雜湊函數(One-Way Hash Function; OWHF)，以下針對本系統之安全需求滿足狀況進行探討：

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。本方法第三者若竊聽傳輸之密文，可獲得密文點 $C=\{C_0,C_1,C_2,...,C_n\}$，要成功解譯這些資訊點，必須能夠將方程式(32)中之 $C_0=\{H_{m2P}(w,u)+G_{ab}\}$ 解離出來，而要解離出這些密文點破譯者將面對橢圓曲線離散對數之難題。

（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。在本方法中若破密者想要變造原始明文，他必須獲得成員的共同金鑰，攻擊者一樣必須解決橢圓曲線離散對數的問題。且當接收方完成解譯密文後，可將所得明文利用雜湊函數 $H()$ 計算其摘要值是否與密文中之摘要值相同，若相同代表所得明文為原始加密之明文。

（三）鑑別性(Authenticity)：

鑑別性是指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(7)驗證對方身分，而認證方式為 $\hat{S}_a=Q_a+h(id_a)P+[(q_{a_x}+h(id_a))]Q_{KGC}$，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(7)則鑑別性可以確保。

（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(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。

（五）密文具雪崩效果(Avalanche effect)：

雪崩效應是一種加密演算法的特徵，它指明文或密鑰的少量變化會引起密文的很大的改變。本方法(33)(34)每一個 C 點座標加密前先與前一個 C 點座標進行點加運算，使得整體密文環環相扣，即使遭受敵方部分截獲，亦無法藉由片段密文進行破密。

二、相關攻擊法

（一）重送攻擊(Replaying Attack)：

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証過程中(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(Eavesdropping)：

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(Masquerade)：

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(9)節點的共同金鑰 $K_{ab}=s_aS_b=s_bS_a$，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）竄改攻擊 (Man-in-the-middle attack)：

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。若攻擊者修改再傳遞給接收者，在接收端的驗證過程中也會被檢驗出來。

三、效能分析(Performance Analysis)：

本節效益特針對海巡署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等比較兩者之各項安全性。本研究與現行方法分析比較表如表 3。

伍、國防相關應用

本文屬於密碼學上的應用，概凡任何軍事上傳遞機敏資料均需利用密碼機制將所傳送之訊息進行加密。「密碼」除了可對訊息進行加密避免訊息傳遞過程被不相關的他方竊取並洩漏資訊，這就是機密性(Shamir, 1982)，其他像是完整性可確保訊息正確無誤的傳送至對方，鑑別性可以用來確認傳送方的真實身分，不可否認性可以用來確保送方不可能發送過某訊息，之後否認未發送過某訊息，同樣的也可以確保收方不可以否認收到訊息而否認收到過訊息。上述這些都是密碼學可以在通訊上達成的要求，並且可以運用到軍事上任何需要傳遞情資的場合。

表 3：本研究與現行方法比較表

比較項目	現行運作機制	本研究所提之海巡通訊網
加密方式	對稱式。	非對稱式。
不可否認性	參與通信雙方擁有同一把金鑰，傳送端事後可否認傳送資訊。	可透過個人之憑證及簽章，實施認證，達到不可否認性。
使用者認證	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。	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。
金鑰分配	海巡署所屬單位眾多且機動高，指揮控制中心必須保管所有使用者的金鑰，造成金鑰管理困難。	使用者僅需保管自己的金鑰即可。
密文完整性	資料是否被竄改後較難判斷。	除摘要值檢查外，密文具有雪崩效應，除非密文全部正確，否則無法解密。
密文機密性	使用對稱式金鑰加密。	以橢圓曲線密碼系統加密，且僅針對需要加密之資訊機密，亦可減少於有限之頻寬內之資訊耗費。

比較項目	現行運作機制	本研究所提之海巡通訊網
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。
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，同時還須猜測明文所在位置，才有辦法成功破解密文還原明文。

陸、結論

本研究提出以橢圓曲線為基礎所設計的加密機制，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，針對海巡署特殊勤務需求，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，達成貢獻如下：

一、認證與加密功能可同時完成，減少收送雙方溝通協調所造成的時間及頻寬的浪費。

二、中心離線情況下系統成員依然能夠進行身分認證功能，這對於無法提供穩定資料傳輸的戰場環境特別適合。

三、方法滿足了機密性、完整性、鑑別性等基本安全需求。

四、密文具有雪崩效果，即使遭受第三者部分截獲，亦無法藉由片段密文進行破密，此一特徵可提供更安全的機密性。另外也因為密文的雪崩效應，如果密文於傳輸的過程中遭到部分竄改或置換則整體密文將無法解密，這也將降低訊息遭竄改可能性。

參考文獻

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。

楊中皇，2008，「網路安全理論與實務」第二版，學貫行銷股份有限公司。

Girault, M. (1991), “Self-certified public keys,” Advances. in Cryptology-EuroCrypt'91, LNCS, Vol. 547, Spring-Verlag, pp. 491- 497.

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

Koblitz, N. (1987), “Elliptic Curve Cryptosystems”, Mathematics of Computation American Mathematical Society, Vol. 48, pp.203-209.

Miller, V. S., (1985), “Use of Elliptic Curve in Cryptography”, Advance in Cryptography- Crypto ’85, New York: Spring-Verlag, pp.417-426.

Shamir, A., (1982), “A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman. Cryptosystem”,Proceedings of the

Twenty-Third Annual Symposium on Foundations of Computer Science, IEEE, pp. 145-152.