強化國軍智慧卡身分認證及機密機制之設計

蘇品長　陳柏諭　楊顓豪*

國防大學管理學院資訊管理學系

摘　要

為精進身分認證及機密機制，國軍智慧卡於 2012 起即提供國軍入口網站身分認證及公文系統線上簽核運用。惟其認證機制未臻完整，且運用 RSA 演算法所支援之 1024 及 2048 位元（bits）金鑰長度較長，使其在認證及加解密的計算成本及安全強度產生疑慮。有鑑於此，本研究以國軍某單位內部線上影音系統為例，提出：(1)採橢圓曲線建置快速安全的身分認證機制，符合鑑別性及不可否認性等安全需求。(2)採低運算成本之串流加密演算法，符合快速加解密目的。(3)結合會議金鑰與隨機亂數π（PI），使對稱式加密金鑰長度恆大於訊息，增加暴力破密難度，並提昇約 4 倍運算速度。(4)通訊階段不需線上憑證中心參與認證。

關鍵詞：國軍智慧卡、身分認證、橢圓曲線、自我認證、機密機制

The Design of Identity Authentication and Confidentiality Mechanism for Enhancing Military Smart Card Functionality

Pin C. Su, Po Y. Chen, and Chuan H. Yang*

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

ABSTRACT

To improve the identity authentication and confidentiality mechanism, the military smart card has been used for identity authentication at web portals as well as submission/authorization in the online documentation system since 2012. However, its functionality is not complete, and the RSA-supported keys (1024/2048 bits) are fairly long to cause issues of increasing authentication and encryption/decryption costs as well as providing an insufficient security strength. To resolve this, this research takes the intranet AV system of a military organization as an example, and proposes the following: (1) using elliptic curves for building a rapid/secure mechanism to meet the authenticity and non-repudiation requirements, (2) adopting the computationally low-cost stream cipher to achieve rapid encryption and decryption, (3) combining session keys with the user-defined random number π to make symmetric encryption keys longer than messages for increasing brute-force decryption difficulty and enhancing the computation speed by 4 times, and (4) not requiring participation of online key generation centers during communication sessions.

Keywords: military smart card, identity authentication, elliptic curve, self-certified, confidentiality mechanism

文稿收件日期 104.8.11;文稿修正後接受日期 105.3.29; *通訊作者
Manuscript received August 11, 2015; revised March 29, 2016; * Corresponding author

一、前言

我國自建軍備戰以來，無不時時刻刻恪遵保密防諜工作，在實體隔離的政策下，設置國軍網路（Minet），具獨立且與網際網路隔離之特性，如何在國軍網路中建構身分確認之方法及架構，成為國軍非常重要的一項研究課題。現階段國軍各單位的系統認證，大多採用網域服務集中式控管（Activity Direction, AD），以使用者帳戶、密碼、權限等識別，作有效之管理憑藉，惟此機制對部分需要嚴格管制機敏識別或資料的機關或部隊而言，無法滿足安全管理需求。為了精進相關身分認證機制及整併相關功能，特別委由中科院研製配發國軍智慧卡，另於 2012 年逐步提供部分單位入口網站身分認證及全軍公文系統線上簽核運用試行，部份單位亦將國軍智慧卡整合至門禁系統管制，達到一卡多用的設計目的；惟目前的智慧卡其身分認證機制未臻完整，以演算法及金鑰為例，使用 RSA 演算法及支援金鑰長度有 1024 及 2048 bits 二種規格，囿於金鑰長度較長，導至計算量過大，若應用於受限制的運算環境，成本及安全強度將產生疑慮[1]。試想是否能提出具快速且符合安全性要求的方法，並導入國軍智慧卡目前的應用，以滿足國軍實需，為研究動機。本研究採用橢圓曲線密碼學為概念的演算法，運用較少的位元數達到相同的安全等級，導入國軍智慧卡的應用，具強化身分認證機制；另採用串流加密法（Stream Cipher）架構[2]，將隨機亂數（PI）的無限不循環特性，藉由混淆及擴張設計，將對稱金鑰整合成虛擬隨機金鑰，達快速加解密的成效。

本文架構一共區分為五章，各章說明如下：第一章：說明研究背景、動機與目的；第二章：針對論文、期刊等文獻，整理歸納出「身分認證及機密機制」的相關資料；第三章：導入橢圓曲線密碼系統及串流加密機制，設計符合國軍智慧卡認證及加解密系統架構；第四章：針對本研究方法與現行的機制進行安全與效益分析；第五章：針對本文做簡單的結論、探討其貢獻度，並為有興趣於此鑽研之研究學者提供目標。

二、文獻探討

本章節將研究內所述及之主要文獻略為整理及探討，共區分為國軍廣域網域與智慧卡、橢圓曲線公開金鑰密碼系統、自我認證公開金鑰密碼系統等 3 個部分，分別說明如下：

2.1 國軍廣域網域與智慧卡

資訊時代來臨，改變了我們對 IT 基礎設施管理及資訊應用系統開發的思維方式，國軍亦希望藉由資訊系統的建置來改善資源佈署、資安防護及工作遂行等任務，以利在人力精簡狀況下，不影響任務的執行，更有效發揮國軍堅強戰力。以國防部參謀本部為例，已有數個重要的大型資訊管理系統，運用 AD 架構，以網頁式（Web-Base）為使用介面，採三層式架構（3-Tier），取代原有主從式軟體架構的系統[3][4]；國防部另建置國軍網路入口網站，整合上述各業管系統及管理人員身分與相關權限。由於建置初期功能有限且各系統無一致性規範要求，導致需持續強化身分認證功能，以收納各中、小型管理資訊系統。配合行政院公文系統開發案，國防部引進大同資訊公司開發之公文系統，並改進原入口網站的設計，使國軍於公文編寫、處理、管制更是向前邁進一大步，有效精進公文處理品質。近期為配合行政院節能減碳、無紙化等政策，特別委請中科院研製國軍智慧卡，期望推行至全軍，運用於各公務系統，諸如公文線上簽核；系統為使用 RSA 演算法，金鑰長度可選擇 1024 或 2048 bits，目前已初具身分認證之雛型功能[1]。

IC 卡（Integrated Circuit Card, IC Card）又稱智慧卡（Smart Card）、集成電路卡。IC 卡最早在 1970 年代發明，第一次大量使用是在 1983 年法國的付款公用電話卡，直到 1990 年代 IC 卡才在歐洲迅速蓬勃發展，終於演進成以 SIM（Subscriber Identity Module, SIM）卡形式，被廣泛使用於 GSM 行動電話設備中。在 1993 年，由國際付款組織 VISA、萬事達卡（Master Card）和 Europay 等組織，同意共同開發用於現金卡或信用卡的 IC 卡規格，並於 1994 年發布了 EMV 系統的第一版本，經過不斷測試與精進，終於 1998 年發行較穩定的版本。1996 年，Java 卡規範被推出，該規範支持一卡多用的功能，在 Java 卡上可以同時存在多個不同的應用及載入不同的執行

碼，同時處理不同的應用[5]。

國軍第一代電子憑證系統於 2001 年誕生，當時只運用 IC 卡（後續稱作智慧卡）進行電子公文交換。2011 年，因應網路架構由 Client-Server 演進成三層式架構，並由國防部試辦智慧卡對公文系統試行線上簽核機制，2012 年逐步推廣至各軍種。2013 年個人用智慧卡正式發放、啟用。綜整國軍智慧卡與一般民間智慧卡之需求差異如表 1。

智慧卡與讀卡機的傳輸資料方式，可分為接觸式（Contact Card）、非接觸式（Contactless Card）與混合式（Hybrid-Card 或 Combi-Card）三種：接觸式，讀取或寫入資料時，需要卡片與讀卡機接觸；非接觸式，透過 RF、紅外線、感應電流等來驅動其運作，讀取或寫入資料時，無需卡片與讀卡機接觸；混合式，同時擁有接觸與非接觸介面[5]。

表 1. 國軍智慧卡與一般民間應用需求差異表

國軍現行智慧卡與一般民間應用之需求差異		
	國軍智慧卡	一般民間應用
身分認證	∨	∨
自我認證	×	×
資料加密	△ (RSA非對稱式演算法)	×
應用用途	國軍公文線上簽核、入口網站登錄、電子郵件簽章及檔案加解密等	政府電子公文、台鐵及高鐵票證、自然人憑證、網路銀行、網路下單及企業安全等

2.2 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 [6]及 Koblitz [7]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 $x_1 = x_2$，$y_1 = -y_2$，$P = (x_1, y_1)$，則 $Q = (x_2, y_2) = (x_1, -y_1) = -P$ 且 $P + Q = O$

(3) 如果 $P \neq Q$ 則 $P + Q = (x_3, y_3)$

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

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

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，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。下表 2 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[8]。

表 2. RSA 與 ECC 金鑰長度比較表

RSA與ECC在相同安全度下金鑰長度之比較					
長度 / 項目	金鑰長度				
RSA	512	1024	2048	3072	7680
ECC	112	163	224	256	384
金鑰長度比	1:5	1:6	1:9	1:12	1:20

2.3 自我認證公開金鑰密碼系統

Girault [9]提出自我認證的演算法，它是一種在授權階段由用戶參與公鑰的計算、使用階段可以獨立進行自我驗證的演算法。Girault 之後有許多的學者提出基於 RSA 與離散對數的改良演算法[10][11][12][13]，近期亦有學者提出基於橢圓曲線離散對數的相關研究[14][15][16][17]。自我認證機制不但可以避免

製發憑證的過程中，因為傳統的憑證中心代替用戶選定私鑰，因此具有偽冒用戶身分的能力所產生的安全弱點；同時可以減低整體系統在公鑰儲存、計算與管理的成本與風險。它的較高的安全性、較低的管理負擔以及可以在單一回合即可完成身分認證的高效率特性，實務上的公鑰基礎建設設計大多採用以數位憑證為基礎的方式來處理相關的身分安全認證事宜，但其先決條件須建立在憑證中心的安全與公正的基礎上，是屬於公開金鑰密碼系統 Level 2 安全等級。而自我認證的機制是讓憑證中心與用戶可以共同參與公鑰的計算，註冊後的交談的雙方僅需靠雙方傳送一些公開的資訊，即可達成雙方身分的確認，而不需再透過第三者來做保證或協調，自我認證則是屬於公開金鑰密碼系統 Level 3 安全等級。綜整各層次安全等級說明如表 3。

表 3. 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

Girault 自我認證的演算法步驟如后：

(1) 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：

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

(2) 註冊階段

使用者 A 其身分碼 ID_A，註冊步驟如下：

- 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，再將身分識別碼 ID_A 與 V_A 傳給系統認證中心。
- 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。
- 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。

(3) 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：

- 使用者 A 將其 ID_A 和 P_A 傳給使用者 B，然後 B 計算：$V_A = (P_A^{\,e} + ID_A) (\bmod N)$
- 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。
- 使用者 B 選擇一個隨機參數值 C，並將其傳給使用者 A。
- 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。最後使用者 B 利用驗證式：$g^Y \cdot V_A^{\,C} = t (\bmod N)$ $g^{x+S_AC} \cdot g^{-S_AC} = g^x (\bmod N)$
- 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。

三、設計可強化國軍智慧卡身分認證機制之架構

本章為論文之研究方法，提出植基於橢圓曲線離散對數（Elliptic Curve Discrete Logarithm Problem, ECDLP）難題的認證機制及串流架構的加解密方法，應用於國軍智慧卡身分識別及資料保護設計。本方法具有較短金鑰長度、降低認證次數及快速加解密等特色，

適用在國軍有限的頻寬及大國軍網路，並解決原僅能運用 AD 伺服主機單一驗證之運算能力不足，以及瀏覽線上機敏影音資料庫系統速度緩慢等情形，本研究共區分為六個階段：(1)系統起始階段、(2)註冊與取得公鑰階段、(3)共同金鑰產生階段、(4)認證及會議金鑰產生階段、(5)串流金鑰產生階段及(6)串流加解密階段；圖 1 為本研究之架構圖，各階段執行步驟依序如后說明。

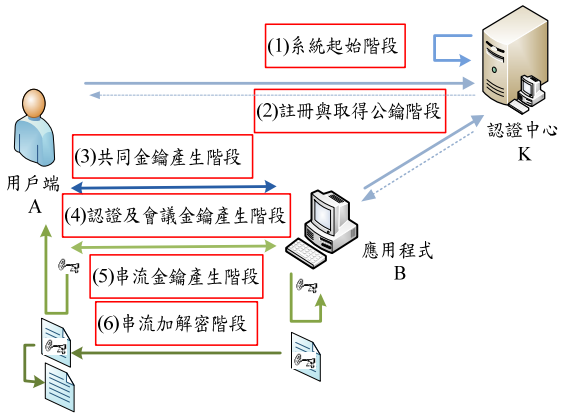

圖 1. 本研究系統流程圖

3.1 系統符號說明

綜整本系統所使用之符號說明如表 4：

表 4. 參數說明表

項目	符號	說明
1	A	用戶端
2	B	應用程式
3	KGC	憑證中心
4	$E(F_q)$	有限域中的一條橢圓曲線
5	G	橢圓曲線系統的基點
6	O	橢圓曲線系統之無窮遠點
7	P	明文轉點與混淆點的集合
8	Q_{KGC}	憑證中心公鑰
9	Q_i	用戶端或應用程式之公鑰
10	d_{KGC}	憑證中心私鑰
11	n	橢圓曲線上基點的階數
12	q	大於2^{160}之質數
13	$h(\ )$	認證中心公開之雜湊函數
14	id_i	成員之身分參數
15	d_i	成員隨機參數
16	k_i	憑證中心隨機參數
17	V_i	成員簽章
18	T_i	隨選亂數
19	K_{ab}	認證後產生之共同金鑰
20	G_{ab}	會議金鑰
21	$S_S\{i\}$	為串流加解密用之金鑰種子陣列
22	L	反饋多項式的級數
23	Ci	反饋多項式之項數
24	K_S	串流金鑰
25	$\|\|$	將訊息連接之用
26	M	訊息明文

3.2 設計強化國軍智慧卡身分認證及串流加密機制架構

(1) 系統起始階段

憑證中心 K 位於國軍 AD Trust Zone 中，首先在起始階段時，先擇一大質數 q，且長度為 160 bits 以上，並在一個有限域 F_q 上選取一條安全的橢圓曲線 $E(F_q)$，並在 $E(F_q)$上選一階數（Order）為 n 的基數 G，使得 $n \cdot G=O$，該 O 點為本研究選用之橢圓曲線系統之無窮遠點，另外在憑證中心 K 中再選擇一個單向無碰撞雜湊函數 $h(\ )$，並計算公開金鑰 Q_{KGC}，及公開 $E, P, n, Q_{KGC}, h(\ )$。

$$Q_{KGC} = d_{KGC} \cdot P \qquad \text{(Eq. 3-1)}$$

(2) 註冊與取得公鑰階段

STEP 1：

用戶端 A 使用自己的 id_a 及隨機選取一個參數 $d_a \in [2, n-2]$，計算(Eq. 3-2)，產生簽章 V_a（應用程式 B 簽章產生方式同用戶端 A）。

$$V_a=h(id_a \,||\, d_a) \qquad \text{(Eq. 3-2)}$$

STEP 2：

用戶端 A 攜帶身分識別碼及簽章（id_a, V_a），親自或視軍種作業規定，運用安全通道的管道向憑證中心 K 辦理登錄註冊（應用程式 B 於本步驟操作方式同用戶端 A）。

STEP 3：

憑證中心(K)取一隨機參數 $k_a \in [2, n-2]$，計算(Eq. 3-3)及(Eq. 3-4)，得出用戶端 A 的公開金鑰 Q_a 及簽章 w_a。

$$Q_a=V_a+(k_a h(id_a)) \cdot P=(q_{ax}, q_{ay}) \qquad \text{(Eq. 3-3)}$$

$$w_a=k_a+d_{KGC} \cdot (q_{ax}+h(id_a)) \bmod n \qquad \text{(Eq. 3-4)}$$

STEP 4：

用戶端 A 計算(Eq. 3-5)，產生驗證值，並運用(Eq. 3-6)驗證之正確性。

$S_a=w_a+(h(id_a \| d_a)) \bmod n$ (Eq. 3-5)

$S_a=s_a \cdot P$
$=Q_a+h(id_a) \cdot P+[(q_{ax}+h(id_a))] \cdot Q_{KGC}$ (Eq. 3-6)

一旦各用戶端及應用程式均完成上述註冊程序，並取得自己本身的（w_a, Q_a）後，爾後在後續任何通訊階段下，均能夠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，即可大幅減輕憑證中心頻於處理來自各用戶端及應用程式提出之驗證次數。

(3) 共同金鑰產生階段

假設此階段為用戶端 A 向應用程式 B 提出要求線上存取機敏影音資料瀏覽權限：

STEP 1：

用戶端 A 將識別碼、驗證值及公鑰（id_a, S_a, Q_a）傳送給應用程式 B；收到傳遞值後，應用程式 B 亦將識別碼、驗證值及公鑰（id_b, S_b, Q_b）傳送給用戶端 A。

STEP 2：

應用程式 B 必須以下列運算式，如(Eq. 3-7)、(Eq. 3-8)，檢查用戶端 A 之（id_a, S_a, Q_a）是否為合法使用者（用戶端 A 驗證方式相同）：

$\overline{S}_a=Q_a+h(id_a) \cdot P+[(q_{ax}+h(id_a))] \cdot Q_{KGC}$ (Eq. 3-7)

$\overline{S}_a=S_a$ (Eq. 3-8)

假如(Eq. 3-8)不成立，即停止通訊並依國軍安全處理機制回報。

假如(Eq. 3-8)成立，接續計算出用戶端 A 與應用程式 B 之共同金鑰 K_{ab}，如(Eq. 3-9)。

$K_{ab}=s_a \cdot S_b=s_b \cdot S_a$ (Eq. 3-9)

(4) 認證及會議金鑰產生階段

用戶端 A 及應用程式 B 計算出一把彼此相同的共同金鑰 K_{ab} 後，使用「挑戰及回應」驗證式來使雙方互相驗證，步驟描述如下：

STEP 1：

用戶端 A 取一隨選亂數 $T_a \in Z_n$，並計算出(Eq. 3-10)、(Eq. 3-11)。

$T_a=t_a \cdot P$ (Eq. 3-10)

$R_a=K_{ab}+T_a$ (Eq. 3-11)

將（id_a, R_a）之訊息傳送給應用程式 B。

STEP 2：

應用程式 B 收到用戶端 A 之請求後，也與用戶端 A 相同取一隨選亂數 $T_b \in Z_n$，並計算出(Eq. 3-12)、(Eq. 3-13)。

$T_b=t_b \cdot P$ (Eq. 3-12)

$R_b=K_{ab}+T_b$ (Eq. 3-13)

應用程式 B 將收到之 R_a 及 K_{ab} 計算出(Eq. 3-14)。

$\overline{T}_a=R_a-K_{ab}$ (Eq. 3-14)

因 A、B 之 K_{ab} 為共同金鑰，所以應用程式 B 計算(Eq. 3-15)。

$W_b=T_b \cdot \overline{T}_a$ (Eq. 3-15)

完成上述計算後，接續將產生本次之連線之會議金鑰 G_{ab} 及認證用之 $Auth(B)$及 $\overline{Auth(A)}$，計算運算式如(Eq. 3-16)、(Eq. 3-17)。

$Auth(B)=h(id_a, id_b, W_b)$ (Eq. 3-16)

$\overline{Auth(A)}=h(id_a, id_b, G_{ab})$,
$G_{ab}=W_b+K_{ab}$ (Eq. 3-17)

再由應用程式 B 將（$id_b, R_b, Auth(B)$）傳送給用戶端 A。

STEP 3：

用戶端 A 收到訊息後，首先先檢查收到之 $Auth(B)$ 是否與自行計算出之 $\overline{Auth(B)}$ 相等，如(Eq. 3-18)、(Eq. 3-19)、(Eq. 3-20)。

$\overline{T}_b=R_b-K_{ab}$ (Eq. 3-18)

$\overline{W}_b=t_a \cdot \overline{T}_b$ (Eq. 3-19)

$\overline{Auth(B)}=h(id_a, id_b, \overline{W}_b)$ (Eq. 3-20)

假如不相符，立即中止連線。

如相符，才接續計算會議金鑰與 $Auth(A)$，如(Eq. 3-21)、(Eq. 3-22)。

$\overline{G}_{ab}=\overline{W}_b+K_{ab}$ (Eq. 3-21)

$Auth(A)=h(id_a, id_b, \overline{G}_{ab})$ (Eq. 3-22)

完成後，再將 $Auth(A)$傳至 B 應用程式，再由 B 以上述相同方式驗證 $Auth(A)$是否與自行計算出之 $\overline{Auth(A)}$ 相等，相等則本階段驗證程序完成。

(5) 串流金鑰產生階段

為使得串流金鑰符合隨機選取要求，將雙方經認證所產生的會議金鑰 G_{ab} 作為種子，傳送至 LFSR 轉換為串流金鑰 S_S，

並將該金鑰逕行混淆運算後，產生新的種子，假設應用程式可產生機敏資料，提供線上用戶端 A 使用，為了達理論安全機制，串流式金鑰種子 S_S 再與選隨機亂數 π（PI），經由無限循環的運算，產生不會重覆的金鑰長度，再利用此把金鑰進行串流加密及解密。各子階段說明如后：

·產生串流式金鑰種子階段

STEP 1：

接收自上一階段之會議金鑰 G_{ab}。

$$G_{ab} = S_B \qquad \text{(Eq. 3.23)}$$

STEP 2：

選擇一反饋多項式（Feedback Polynomial）：

$$f(x)=1+C_1x+C_2x^2+\ldots+C_{L-1}x^{L-1}+C_Lx^L$$
$$C_L=1 \qquad \text{(Eq. 3-24)}$$

其中 L 稱為反饋多項式的級數(Degree)，而反饋係數 Ci $(1 \leqq i \leqq L-1)$ 中不為 0 的個數稱為反饋多項式之項數（Tap），並令 L=256、C_{17}、C_{47}、C_{197} 及 C_{215}、C_{219}、C_{256}=1，餘均為 0，可得下列運算式：

$$f(x)=1+x^{17}+x^{47}+x^{197}+x^{215}+x^{219}+x^{256} \qquad \text{(Eq. 3-25)}$$

本階段可得到一陣列 $S_S\{i\}$，並傳送至下一階段。

$$f(x)=S_S\{i\} \qquad \text{(Eq. 3-26)}$$

·金鑰加長階段

A 接收到(Eq. 3-26)後，將金鑰視為初始向量，經混淆與排列組合運算，使得自選隨機數 π（PI）(無限不循環小數)能與金鑰結合並產生無限長且不重覆的串流金鑰，使加解密金鑰長度恆大於訊息長度。每次運用 π 需經由混淆與擴散運算，達到排列組合的變化，以一函式 π(i)表示取數之起始位置為例，說明如后：

i = 0：$\pi(L+i)=\pi(256)=(5)_{10}=(0101)_2$

i = 1：$\pi(L+i)=\pi(257)=(6)_{10}=(0110)_2$

…

i = Len(M)-1：$\pi(L+\text{Len}(M)-1)$ (Eq. 3-27)

並將(Eq. 3-26)及(Eq. 3-27)進行 XOR 運算，再經選一 LFSR，得串流加密金鑰 K_S。

$$K_S = S_S\{i\} \oplus \pi(L+\text{Len}(M)-1) \qquad \text{(Eq. 3-28)}$$

(6) 串流加解密階段

· 串流加密階段

為強化加密速度，採一次性的 XOR 金鑰加密運算，說明如后：

$$C = M \oplus K_S \qquad \text{(Eq. 3-29)}$$

· 串流解密階段

用戶端 A 接收來自 B 之機敏資料，僅需運用一次性的 XOR 運算，即可完成解密運算，說明如后：

$$M = C \oplus K_S \qquad \text{(Eq. 3-30)}$$

四、安全性分析及效益評估

本章將分析國軍智慧卡身分認證及加解機制的安全性及執行效益，分述如后：

4.1 安全性分析

根據國際標準化組織（International Organization for Standardization, ISO）等所提之資訊系統安全性管理需求，應該要達到機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）及不可否認性（Non-repudiation）等特性，評估國軍智慧卡身分認證及機密系統[18][19][20]導入後是否符合安全規範，另考量實際上的應用需求[21][22]，需避免共謀攻擊，相關說明如后：

(1) 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，資料在成功抵達目的地之後，所有的資料交換都是保密的。國軍某單位內部應用程式 B，將資料傳送給之用戶端 A，若秘密破譯者竊取這些加密資訊，因未經合法授權，無法取得會議金鑰 G_{ab}，則無法產生串流加密金鑰 K_S，如運算式(Eq. 3-28)：

$$K_S = S_S\{i\} \oplus \pi(L+\text{Len}(M)-1)$$

將面臨只能使用暴力破密方式解密，因本研究將加解密金鑰轉換成串流方式，如運算式(Eq. 3-28)，相對破密所需之時間也越長，無法於短期內將單位內部機敏資訊解出，故本系統內資料傳輸時將具有機密性。

(2) 完整性（Integrity）

完整性指的是確保本系統各項資料處理

與傳遞是完整且正確的特性，也就是資料在處理的過程中確認沒有被加入、刪除或修改。假若國軍某單位網路內之秘密破譯者想偽冒合法使用者身分發送訊息給管理者，除非獲得原合法使用者個人申請認證之資訊或共同金鑰，如（id_a, S_a, Q_a）及運算式(Eq. 3-7)，否則傳送至系統中心之存取權限是無法被更改的，故資料傳遞時具有完整性。

$$\overline{S}_a = Q_a + h(id_a) \cdot P + [(q_{ax} + h(id_a))] \cdot Q_{KGC}$$

(3) 鑑別性（Authenticity）

鑑別性是指交易資訊的接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。在本研究中，接收方為用戶端 A，可使用運算式(Eq. 3-7)與(Eq. 3-8)驗證應用程式 B 的身分，而認證方式為：

$$\overline{S}_a = Q_a + h(id_a) \cdot P + [(q_{ax} + h(id_a))] \cdot Q_{KGC}$$

$$\overline{S}_a = S_a$$

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難題，若破譯者無法破解運算式(Eq. 3-7)則鑑別性就能夠有效確保，故資料傳送時具有鑑別性的保障。

(4) 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。在本研究應用程式 B 傳送給用戶端 A 之串流加密所用的金鑰 K_S，如運算式(Eq. 3-28)：

$$K_S = S_S\{i\} \oplus \pi(L + \mathrm{Len}(M) - 1)$$

因為 K_S 為雙方經認證後所產生之會議金鑰 G_{ab} 所生成，只有連線的雙方才會共同擁有，其他任何第三方均無法獲取這把金鑰，若其破譯者想由傳送者應用程式 B 之公鑰來推算私鑰，則破譯者將面臨橢圓曲線離散對數之難題，這使得由傳送方送出之串流影音密文，具有不可否認性。

(5) 共謀攻擊（Collusion Attack）

合法使用者 A 用戶端及 B 應用程式註冊階段時，會將自己的身分識別碼及簽章（id_a, V_a），以安全管道傳送給認證中心 KGC，如運算式(Eq. 3-2)：

$$V_a = h(id_a \,||\, d_a)$$

不同使用者或應用程式持有不同的加密金鑰，可有效避免後端管理者藉由管理之便，進而盜用使用者權限，從事非法行為，造成個人或國軍更嚴重的傷害，故本系統可避免有心人士，經由認證中心進行共謀攻擊。

(6) 資訊理論安全（Information Theoretical Security）

資訊理論安全並非指絕不會被破解的密碼系統，而是指無論你做了多少的分析，在破密時間與亂猜機率相等，亦即花費時間大於或等於猜明文時間。本研究運用串流加密金鑰設計，使得長度恆大於欲瀏覽之訊息，運算式(Eq. 3-28)：

$$S_S\{i\} \oplus \pi(L + \mathrm{Len}(M) - 1)$$

使得金鑰長度會大於加密訊息，達到資訊理論安全的規範。

4.2 效益評估

本研究主要植基於橢圓曲線的密碼系統，導入自我認證機制後，可免去頻於向認證中心身分確認及訊息傳遞時間，且運算速度因金鑰所需長度更短，較傳統 RSA 演算法來的快，降低系統負荷並提升效率及安全性。與國軍智慧卡系統現得運行之簽章機制進行比較，分析結果詳如表 5。另接續上述評估方法，逕行量化分析，首先定義分析中所需的符號[8][23]，詳如表 6，各種運算間的時間量化關係如表 7，本研究與國軍現行架構之時間計算成本比較如表 8。

表 5. 現行簽章及加密機制與本研究之比較表

比較項目	現行運作機制	本研究
簽章方式	非對稱式	非對稱式
加密方式	非對稱式。	對稱式。
核心原理	RSA 簽章機制 RSA 加密機制	橢圓曲線簽章機制 自我認證機制 串流加密機制 金鑰加長機制
運算速度	相對較慢	簽章快、加密快且認證次數少

不可否認	透過 RSA 來進行簽章與加密，均可達成不可否認性之要求，惟其速度相對較慢。	透過橢圓曲線離散對線演算法進行簽章驗證，並運用會議金鑰產生串流加解密金鑰，均可達成不可否認性之要求。
使用者認證	僅透過設定值設定辨識使用者身分，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，且僅第一次需要與認證中心進行驗證，爾後階段均不需要認證中心。
自我認證	無	有
可離線之身分認證	無	有
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，尚有金鑰加長機制需解決，才有辦法成功破解密文還原明文。

表 6. 運算符號定義表

符號	定義
p	一個任意大小的有限場。
T_{MUL}	進行一次模數乘法運算所需花費的時間。
T_{EXP}	進行一次模數指數運算所需花費的時間。
T_{ADD}	進行一次模數加法運算所需花費的時間。
$T_{(ECC,\ MUL)}$	進行一次 ECC 乘法運算所需花費的時間。
$T_{(ECC,\ ADD)}$	進行一次 ECC 加法運算所需花費的時間。
T_H	進行一次單向雜湊函數運算所需花費的時間。
T_{INVS}	進行一次模數乘法反元素運算所需花費的時間。
$T_{\oplus}$	進行一互斥或運算所需時間(可忽略不計)

表 7. 各種運算與時間計算成本之關係表

$T_{EXP} \approx 240T_{MUL}$
$T_{(ECC,\ MUL)} \approx 29T_{MUL}$
$T_{(ECC,\ ADD)} \approx 0.12T_{MUL}$
$T_{MUL} \approx T_{DIV}$
$T_{INVS} \approx (0.843\ln(p)+1.47)\ T_{DIV}$
T_{ADD} 可忽略不計
$T_H \approx 0.4T_{MUL}$
$T_{\oplus}$ 可忽略不計

表 8. 本研究與國軍現行架構之時間比較表

系統各階段	國軍現行架構		本研究	
	時間計算成本	概估	時間計算成本	概估
系統起始	$1T_{EXP}$	$240T_{MUL}$	$1T_{(ECC,\ MUL)}$	$29T_{MUL}$
註冊與取得公鑰			$2T_H+$ $2T_H \times T_{(ECC,\ MUL)}+$ $1T_{(ECC,\ MUL)}$	$53T_{MUL}$
共同金鑰產生	無		$2T_H+$ $2T_H \times T_{(ECC,\ MUL)}+$ $1T_{(ECC,\ MUL)}$	$53T_{MUL}$
認證及會議金鑰產生	無		$2T_{(ECC,\ MUL)}$	$58T_{MUL}$
加解密階段	$2T_{EXP}$	$480T_{MUL}$	$3T_{\oplus}$	$0T_{MUL}$
總計		$720T_{MUL}$		$193T_{MUL}$

五、結論

網路基礎建設的進步及電腦計算能力的提升，建置於國軍網路上的各類網站及應用程式蓬勃發展，身分驗證已成各應用程式於國軍網路使用上的關鍵性問題，建置更快速及安全的認證機制及整合軍人智慧卡應用，已成為建軍備戰之當務之急。本研究為強化現行國軍智慧卡身分認證系統及設計模擬串流加解密系統架構，可應用於國軍智慧卡系統。此外，本研究也導入自我認證機制，避免在網路使用時頻於向認證中心(KGC)提出身分認證，使用者亦僅需要於第一次向認證中心(KGC)提出認證申請及運算，其餘各階段均毋須透由認證中心(KGC)，有效節省網路頻寬。國軍智慧卡身分認證系統導入本方法後，將能有效提昇作業效率，以更少的金鑰位元達到 RSA 相同的安全強度，將可減少公文交換次數、節省軍網可貴的頻寬及節省文件加解密時間；另外，本研究除符合保密需求外，亦滿足機密性、完整

性、鑑別性等功能，實為國軍後續所追求的最高目標，綜整本研究，達成貢獻如下：

(1) 運用橢圓曲線離散對數具難以逆向求解之困難性，擁有相同安全性強度下較短長度之金鑰、更快的運用速度及更高的安全性等優點，強化國軍智慧卡的安全機制設計。
(2) 軍網頻寬受限制的狀態下，採取本研究之自我認證系統，僅需首次由各軍種向認證中心註冊，爾後各階段認證均不再需要認證中心參與認證。
(3) 本研究方法除了符合機密性、完整性、鑑別性及不可否認性等基本安全需求外，並且可避免共謀攻擊及強化加密演算法的安全設計。
(4) 確保資訊維管單位在維護內部機敏性高的資時，滿足國軍對機密性之嚴格要求及防範身分遭竄改或冒用之可能性。

參考文獻

[1] 陳柏諭，強化國軍智慧卡身分認證及串流加密機制之設計，國防大學管理學院資訊管理所碩士論文，2014。
[2] 林則孟，系統模擬：第六章隨機亂數與隨機變數，清華大學工業工程與工業管理系電腦整合製造研究室，2001。
[3] 肖攸安，橢圓曲線密碼體系研究，華中科技大學出版，武漢市，2006。
[4] 李南逸、王智弘、林峻立、張智超、溫翔安、葉禾田，網路安全與密碼學概論，滄海書局出版，台中，2008。
[5] 林威廷，基於信用卡服務之多銀行付費系統，朝陽科技大學資訊工程系碩士論文，2014。
[6] Miller, V. S., “Use of elliptic curve in cryptography,” Proc. Adv. Cryptography (Crypto), pp. 417-426, 1986.
[7] Koblitz, N., “Elliptic curve cryptosystems,” Math. Computation, Vol. 48, pp. 203-209, 1987.
[8] 蘇品長，植基於 LSK 和 ECC 技術之公開金鑰密碼系統，長庚大學電機工程系研究所博士論文，2007。
[9] Girault, M., “Self-Certified Public Keys,” *Proceedings of Eurocrypt*, LNCS 547, 1991.
[10] Chang, Y. F., Chang, C. C., and Huang, H. F., “Digital signature with message recovery using self-certified public keys without trustworthy system authority,” *Applied Mathematics and Computation*, Vol. 161, pp. 211-227, 2005.
[11] Shao, Z.**,** “Cryptographic systems using a self-certified public key based on discrete logarithms,” *IEE Proceedings-Computers and Digital Techniques*, Vol. 148, No. 6, pp. 233-237, 2001.
[12] Tseng, Y. M., Jan, J. K., and Chien, H. Y.**,** “Digital signature with message recovery using self-certified public keys and its variants. *Applied Mathematics and Computation*,” Vol. 136, pp. 203-214, 2003.
[13] Wu, T. S., and Hsu, C. L., “Threshold signature scheme using self-certified public keys,” *Journal of System and Software*, Vol. 67, pp. 89-97, 2003.
[14] Shao, Z.**,** “Self-certified signature schem from pairings,” *Journal of Systems and Software*, Vol. 80, No. 3, pp. 388-395, 2007.
[15] Su, P.C., and Tsai, C.H., “Self-Certified Key Exchange Scheme Based on Hybrid Mode Problems,” *Journal of Chung Cheng Institute of Technology*, Vol. 39, No. 1, pp. 123-135, 2010.
[16] Tsaur, W. J., “Several security schemes constructed using ECC-based self-certified public key cryptosystems,” *Applied Mathematics and Computation*, Vol. 168, pp. 447-464, 2005.
[17] Wu, L., Zhang, Y., & Wang, F.**,** “A new provably secure authentication and key agreement protocol for SIP using ECC,” *Computer Standard & Interfaces*, Vol. 31, No. 2, pp. 286-291, 2009.

[18] ANSI, Public-key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998.
[19] IEEE, Standard Specifications for Public Key Cryptography, IEEE Std 1363-2000:2000, 2000.
[20] NIST, Digital Signature Standard (DSS), FIPS PUB 186-3:2009, 2009.
[21] 蘇品長、邱謙忠、李明忠、廖家宏、黃棠建，“設計具機密性及可自我認證之海巡通訊網”，國防管理學報，第三十三卷．第一期：30～44 頁，2012。
[22] 梁榮哲，多重文件盲簽章機制之設計，國防大學資訊管理學系研究所碩士論文，2012。
[23] Tsai, C. H. and Su, P. C., “ECC-Based Cryptosystem for Multi-Document Fail-Stop Signature with Encryption Scheme,” Journal of Internet Technology (16: 3), pp. 462-475, 2015.