設計植基於混合難題的認證及簽密機制適於軍事應用之方法

作者/蔡嘉富 上尉、蘇品長 中校、胡智欽 上尉

提要

戰場指揮是否可以順利通達，端視命令是否可以安全地傳達。在某些場合中指揮官希望在他傳送訊息時能達到命令可認證及訊息安全的要求，也就是命令能夠接受驗證真偽外，並且還希望命令傳遞的同時能夠對訊息進行加密。「戰爭中許多情報往往是矛盾的，甚至有許多是虛假的，更多則是不確實的。」這是西方兵聖克勞塞維茲在其鉅著《戰爭論》中所揭示「戰爭之霧」的概念。若想要解決「戰場之霧」的迷況下就必須將認證及加密的技術結合在一起，才能夠達成這樣的要求。本文中我們提出一個利用橢圓曲線密碼及背包問題為概念的一個新方法。我們的方法除了符合機密性、完整性、鑑別性及不可否認性的基本安全需求之外，同時密文具備雪崩效應效果，另背包問題概念的導入也是簽密方式的一種靈活運用。本方法可適用於人員身分認證識別及訊息加密簽章之軍事應用，期望能夠成為戰場上電子資料簽密及識別方式的參考，解決「戰場之霧」所造成的戰場資訊不透明的狀況。

關鍵詞：橢圓曲線、背包問題、簽密法

前言

一九九三年托夫勒出版「新戰爭論」一書，開始將資訊科技的視野，由社會移向軍事領域。他所要傳達的觀點是，資訊科技的發展，不僅造成社會變遷、影響國家競爭力，也帶動新的戰爭型態出現，資訊科技將在作戰中扮演一項極為重要的角色[1]，那如何利用資訊技術讓所有部隊能達成協同作戰數位化、行動化，保持資傳通聯，小至單兵或武器載台，大至後勤補給，完全在數位鏈路中，不管是定點或是行動，隨時連網，命令下達沒有延遲，達到網狀作戰之目標。欲達成此目標，首先我們必須先要解決西方兵聖克勞塞維茲在其鉅著《戰爭論》中提出「戰爭之霧」的存在問題，他認為：「在戰爭中許多情報往往是矛盾的，甚至有許多是虛假的，更多則是不確實的。」這些存在資訊理論中所謂的「噪音」與不確定的要素，在戰場上融合成了遮蔽指揮者與士兵的迷霧，此即「戰爭之霧」。但「戰爭之霧」並不只是影響部隊敵情的判斷與作戰的遂行，甚至是

[1] 黃志泰，〈戰場覺知-戰場即時共通圖像系統〉，台灣地理資訊學會年會暨學術研討會，民國94年，頁1。

戰爭成敗的關鍵因素。在戰場通訊時雙方往往不知道對方的真實的身分，通訊雙方可能會對於訊息內容產生懷疑，亦或指揮官命令下達之後其下屬部隊無法完整接收訊息，這些都會使得戰場指揮無法遂行。如果不能提供一個安全又可確認對方身分的通信方式，也就無法遂行戰場管理機制，形成戰場上戰爭機器無法指揮的狀況。解決的辦法必須要確保戰場資訊不會洩漏，並且可驗證通訊雙方的身分。本文中所提出之身分認證是指交談的雙方僅需要靠彼此傳送一些公開的資訊，即可達成雙方身分的確認，而不需透過第三者來做保證或協調。如此可在混亂的戰場環境之下，增加溝通的效率以及提升訊息來源的可信程度。

自古以來，人們一直有隱藏與交換秘密的需求，小至個人的隱私，大到國家軍事機密，都需要「安全的」方法隱藏與交換秘密。為了保護秘密，人們想盡了各式各樣保護秘密的方法；相對地，人們也無所不用其極地，使用各種手段，就是為了竊取機密。因為有了千奇百怪的方法，所以密碼學不只是一門古老的學問，也是一門包羅萬象的學問。經歷了數千年的發展，保護秘密的方法與觀念，也隨著人類科技的進步而有所演化，尤其是電腦科技的出現，更讓密碼學出現了與之前完全不一樣的風貌。在二次世界大戰之前，密碼學的先進技術與觀念，大都應用於國家機密與軍事戰爭的用途，隨著網際網路的興起，人們生活中出現大量各式各樣的資訊科技應用，這些資訊科技的應用同時也將資訊安全的問題，帶進了每個人的日常生活中，因此密碼學的應用，就這樣地隨著網際網路的網路線，進入到我們的日常生活中。密碼學應用對象的改變，也改變了密碼學的研究內涵，不再侷限於為國家與軍事服務，密碼學服務的範圍擴及商業應用，服務的對象也小至個人[2]。

現行實際的公開密碼系統，均無法歸屬於理論安全系統，僅能以目前最好的破解技術來計算。由於計算機計算技術不斷提昇，當破密者可突破的範圍或找到破解方法時，稱此系統被破解，這也說明了不斷有系統被認定為不安全的原因。自 1970 年代以來，許多公開密碼系統被提出，安全屏障不外乎植基於因式分解或離散對數的單一難題上，藉由不斷的增加金鑰長度來確保系統的安全，已造成系統執行效率的取捨難題，以科技發展的速度，這些安全的假設，在相同的加密條件下，預期在未來將成為系統致命的傷害。環視全球科技發展，尚未有一個安全機制是可以同時滿足所有安全考量（諸如：識別、認證、授權、加密、簽章...等等），在這些安全考量下確實有一個資訊安全的最底線，就是編碼技術，亦即大家在資訊傳遞時所熟悉的安全基本觀念。

[2] 胡智卿，〈混合式公開金鑰密碼系統之設計〉《國防大學管理學院資訊管理學系碩士班碩士論文》，民國 98 年 6 月)，頁 1-2。

不利公開金鑰密碼學發展的最大因素是速度,因為現有的公開金鑰加密法計算量遠比傳統加密法大且耗時，且無從比較兩者演算法的安全程度，端視金鑰的長度及破解密所需的計算量；此外，使用公開金鑰加密法未必讓金鑰分送變得簡單，事實上，取決於金鑰（集中代理）協定機制設計之良莠。所以公開金鑰密碼學無法取代或淘汰傳統密碼學，而是截長補短、兼容並蓄，結合對稱和不對稱金鑰系統，以建立系統的安全性及加解密的快速性等優點。Harn於 1994 年提出一個植基於因式分解和離散對數的數位簽章系統[3]，之後陸續有學者針對不同的因式分解與離散對數問題設計不同的演算機制。從已發表的論文中，都只強調演算法的安全性，因此如何兼具安全與效率，遂成為本研究積極追求突破的目標。本研究首先將提出植基於同時解因式分解及離散對數困難度的密碼機制，適用於使用者身分認證、加解密、數位簽章、金鑰交換及分配等應用機制。自從 80 年代中期被發表以來,橢圓曲線密碼系統(Elliptic Curve Cryptography, ECC)已成為一個十分令人感到興趣的密碼學分支，1997 年以後更形成了一個研究重點。這種密碼系統的誘人之處在於安全性相同的前提下，可使用較短的私密金鑰，一般認爲，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。私密金鑰較短意味著所需要電腦網路的頻寬和記憶體較小，這在電腦網路應用中是個決定性的關鍵。

密碼領域所討論的系統，其安全性為最高的評價標準。一個密碼系統的安全性很難用理論證明（證明系統安全：難；證明系統不安全：易），因此，新的密碼系統被提出後，就會引起專家學者的研究，試圖提出破解方式證明系統為不安全。而密碼系統設計者就會對破解方法進行圍堵與改良，而破密者也虎視眈眈的等著研究，密碼學領域就在如此反覆挑戰與改進的環境中成長。Shannon 在 1949 年提出了密碼系統的安全性考量：

一、 當破密者擁有無限制的時間與計算能力時，對密碼系統所保護的密文加以分析，最多能有多少的安全性？

二、 當破密者在有限的時間與計算能力對密文加以分析時，密碼系統是否足夠安全？

此即 Shannon 著名的系統安全定義；理論安全（Theoretical Security）及實際安全（Practical Security）。所謂理論安全（或稱「絕對安全（Perfect Security）」）是指不管破密者截獲多少密文，並加以分析，其結果和直接猜測明文是一樣的。密碼系統欲達到理論安全必須使加密金鑰的長度大於或等於明文的長度，而且

[3] 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》，民國 96 年 6 月，頁 35-37。

金鑰祇用一次，用完即丟棄，不重複使用。一般而言，明文長度通常很長，如何獲得比明文長度相等或更長的金鑰是一大難題，專家學者以設計適當的亂數產生器，使其滿足一些特性以達到一定的安全性，稱為串流密碼系統（Stream Cryptosystem），此類系統廣泛應用於軍事保密事務。

密碼系統並非一定滿足理論安全才是安全的系統。Shannon 假設每一個密碼系統在給定 n 位元密文時，均有一破解的最少工作次數（稱為「工作特徵 $W(n)$（Work Characteristic）」），$W(n)$定義為所有破解此密碼系統方法中最佳解的最少次數。若系統之 $W(n)$大到破密者所具有的有限計算能力無法在合理的時間內破解，即稱此系統為實際安全（或稱「計算上安全（Computational Security）」）。

現行實際的公開密碼系統，均無法歸屬於理論安全系統，僅能以目前最好破解技術（稱為「歷史工作特徵 $W_h(n)$（Historical Work Characteristic）」）來計算。當密碼系統的 $W_h(n)$大到無法在合理的時間內被解時，我們稱此系統為實際安全。由於計算機計算技術不斷提昇，當 $W_h(n)$變小到破密者可突破的範圍或找到破解方法時，稱此系統被破解，這也說明了不斷有系統被認定為不安全的原因。不斷地設計及驗證具安全性且符合潮流需求之公鑰密碼系統，便成為密碼領域之專家學者努力突破的目標。綜整研究分析，本論文將以研究橢圓曲線快速運算為基礎，提出不同於以往學者所提的應用方法，並結合背包理論(是一種組合優化問題，假設我們有一個背包它所能裝載的物品重量是固定的，但現在我們有非常多的物品，每個物品的重量都不一定相同，我們將如何選擇物品放置於給定背包中是不易猜測出的。)，設計一套植基於背包問題(Knapsack)及橢圓曲線離散對數(Elliptic Curve Discrete Logarithm Problem, ECDLP)難題可適用軍事應用於人員身分認證及電子文件簽密機制，期許能在浩瀚的密碼學研究裡，對國防基礎訓練及建軍備戰有所貢獻。

本文

加密演算法(Encryption Algorithm)可以達到機密性的需求，而數位簽章演算法(Digital Signature Algorithm,DSA)可以達到完整性、鑑別性及簽署的不可否認性之需求。為了同時達到上述的需求，傳統的作法是採用兩階段作法。為了改進兩階段作法的效率，Zheng[4]在 1997 年提出簽密法(Signcryption Scheme)的技術。這個方法的特性是同時達到簽署及加密的功能，而此簽密法比傳統兩階段作法[5]來得更有效率，這也是簽密法的濫觴，之後陸續有學者提出新的簽密法技

[4] Yuliang Zheng , “Digital Signcryption or How to Achieve Cost (signature & encryption) << cost (signature) + cost (encryption),” CRYPTO'97, LNCS 1294, Springer-Verlag, pp.165-179, 1997.

[5] Jee Hea An, Yevgeniy Dodis and Tal Rabin, “On the security of joint signature and encryption,” In Advances in

術。而Zheng 和 Imai[6] 也曾提出過一種基於橢圓曲線密碼系統下的簽密方法，下面將針對橢圓曲線之簽章、加密以及簽密等方法進行介紹。

橢圓曲線公開金鑰密碼系統

Miller[7]首先提出將橢圓曲線用來實作公開金鑰密碼系統的技術。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。

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， ECC 僅需要較小的密鑰長度，相同地，在同樣的密鑰長度下，ECC 卻擁有更高的安全性。RSA 與 ECC 之金鑰長度與安全性比較如表一所示 (RSA 為目前普遍的公開金鑰演算法，是由 R. Rivest、A. Shamir 與 L. Adleman 三人於 1977 年所發表。)：

表一 RSA 與 ECC 在相同安全度下金鑰長度之比較表

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

(資料來源：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 6 月。)

橢圓曲線加密方法

橢圓曲線加密一般使用ElGamal的橢圓曲線加密法[8]，方法總共分為三部分，系統初始階段、加密階段及解密階段，各階段分述如下：

Cryptology-EUROCRYPT '02, LNCS Vol.2332, pp.154-159,2002.

[6] Yuliang Zheng and Hideki Imai, "How to construct Efficient Signcryption Schemes on Elliptic Curves," Information Processing Letters 68, pp.227-233, 1998.

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

[8] Darrel Hankerson, Alfred Menezes, and Scott Vanstone, "Guide to Elliptic Curve Cryptography," ISBN: 0-387-95273-X, pp.15-16, 2004.

一、系統初始階段

(一)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。

(二)簽章者隨機選擇一整數n_A當成私鑰，其中n_A介於[1, n-1]

(三)計算加密者公鑰$Q = n_A G$

(四)將(E, G, n_A, Q)公開

二、加密階段

(一)令明文 m 為 E 上的一點 M。

(二)加密者任選一個整數$k \in [1, n-1]$

(三)計算密文$(C_1, C_2) = (kG, M + kQ)$，其中 Q 為收方之公鑰。

三、解密階段

解算出明文$M = C_2 - n_B C_1$，其中n_B為收方私鑰。

橢圓曲線簽章方法

橢圓曲線簽章演算法(Elliptic Curve Digital Signature Algorithm, ECDSA)，是一種標準的橢圓曲線數位簽章演算法，方法總共分為三部分，系統初始階段、簽章階段及驗證簽章階段，各階段分述如下。

一、系統初始階段

系統所使用參數如下：

(一)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$E(F_q)$上選一階數為 n 的基點 G ，使得 $nG=O$，其中 O 為此橢圓曲線之無窮遠點。

(二)簽章者隨機選擇一整數n_A當成私鑰，其中n_A介於[1,n-1］。

(三)計算簽章者公鑰$Q = n_A G$

(四)將(E, G, n_A, Q)公開

二、簽章階段

(一)假設欲簽章之訊息為 m，$h(m)$為雜湊值。

(二)隨機選擇一整數 k 介於[1, n-1]

(三)計算$R = kG = (x, y)$ ……(1)

(四)計算$r = x \bmod n$ ……(2)

(五)計算$s = k^{-1}(h(m) + n_A r) \bmod n$ ……(3)

(六)訊息 m 的簽章為(r,s)

三、驗證簽章階段

(一)取得簽章者之公鑰及系統公開訊息(E,G,n_A,Q)

(二)檢驗 r 及 s 是否介於[*1,n-1*]，若不在範圍內則否定其簽章。

(三)計算 $w=s^{-1} \bmod n$ 及 $h(m)$ ……(4)

(四)計算 $u_1=h(m).w$ 及 $u_2=rw(\bmod n)$ ……(5)

(五)計算 $V=u_1G+u_2Q=(x_v,y_v)$ 和 $v=x_v \bmod n$ ……(6)

(六)若 $v=r$ 則接受為正確簽章

橢圓曲線簽密方法

ZHeng 在 1998 年提出以橢圓曲線為基礎之簽密法，以下為此簽密法的描述，假設送方 A 欲對明文 M 產生簽密文並將簽密文傳給收方 B 作解密與驗簽。ZHeng 的方法分成「系統初始階段」、「送方簽密階段」、「收方解密及驗簽階段」。

一、系統初始階段

系統在有限域 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 $E(F_q)$ 上選一階數為 n 的基點 G ，使得 $nG=O$，其中 O 為此橢圓曲線之無窮遠點。選定一單向無碰撞雜湊函數 $H(\,)$ 及一組對稱式加解密函數，令其加密函數為 $E(\,)$，解密函數為 $D(\,)$，系統公開 $E(F_q),G,n,q,H(\,),E(\,),D(\,)$，使用者 A、B 依系統參數分別選擇 $n_A,n_B \in Z_q^*$ 當成私鑰，並計算其相應之公鑰 $PK_A=n_A \cdot G$，$PK_B=n_B \cdot G$ 。

二、送方簽密階段

(一)在送方 A 使用以下步驟產生簽密文(C,h,s)，以收方之憑證驗證其公鑰 PK_B 正確性。

(二)選取一亂數 $r \in Z_n^*$

(三)計算 $B=H(r.PK_B)=(x_B,y_B)$ ……(7)

(四)計算密文 $C=E_{x_B}(M)$，計算雜湊值 $h=H(M)$ 。

(五)計算 $s=r/(h+n_A) \bmod q$ ……(8)

(六)將簽密文(C,h,s)送出

三、收方解密及驗簽階段

(一)以送方之憑證驗證其公鑰正確性，計算 $u=s \cdot n_B \bmod q$ 。

(二)計算 $B'=(u \cdot PK_A+u \cdot h \cdot G)=(x_{B'},y_{B'})$ ……(9)

(三)以 $x_{B'}$ 進行解密得到明文 $M'=D_{x_{B'}}(C)$

(四)驗證 $h \stackrel{?}{=} H(M')$，若等式成立則收方接受送方訊息，並且表示簽密文確為送方所產製，反之，收方拒絕送方之簽密文。

設計植基於混合難題的認證及簽密機制適於軍事應用之方法(本方法)

本節將基於ECDLP及 Knapsack建立一個具有公開驗證功能的簽密方法。方法分為四個階段：系統初始化階段、使用者註冊階段、文件簽密階段以及解密及驗簽階段。我們的簽密法與Zheng [9]所提的方法，在完整性上面，我們的方法收方訊息檢查方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，何謂雪崩效果，就是一種加密演算法的特徵，它是指明文或密鑰的少量變化會引起密文的很大變化，亦可當成完整性檢查的一環；本法於橢圓曲線加密過程以背包問題概念另外混入擬亂資料增加破密困難，雖然運算量提高但運算複雜度並未增加；另外本法之送方將簽章嵌入密文當中可有效減少簽章於傳送過程中遭受偽冒之風險。以下對本方法各階段進行說明。

一、系統符號說明

系統中使用的符號說明如表二所示。

表二 系統使用符號說明

項	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.	n	橢圓曲線上基點的秩(order)
4.	q	$q > 2^{160}$之質數
5.	x_Z, y_Z, x_R, y_R	為橢圓曲線上的點座標
6.	PK_A, PK_B	使用者 A、B 之公鑰
7.	SK_A, SK_B	使用者 A、B 所選擇之私鑰各為n_A, n_B兩整數
8.	$H_{pub}()$	認證中心公開之雜湊函數
9.	CA_A	使用者 A 之身分憑證
10.	$F_{m2p}()$	將訊息轉為橢圓曲線點之函數
11.	$F_{p2m}()$	將橢圓曲線點轉為訊息之函數
12.	w	計算訊息所在之背包值

(資料來源：作者整理）

二、系統初始階段

系統之認證中心(Authentication Server, AS)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$E(F_q)$上選一階數為 n 的基點 G ，使得 $nG = O$，其中 O 為此橢圓曲線之無窮遠點。使用者 A、B 及認證中心

[9] Y. Zheng and Hideki Imai, "How to construct Efficient Signcryption Schemes on Elliptic Curves," Information Processing Letters 68, pp.227-233, 1998.

分別選擇 $n_A, n_B, n_{AS} \in Z_q^*$ 當成私鑰，認證中心選擇的一個單向無碰撞雜湊函數 $H_{pub}()$，最後認證中心公開 $E(F_q), G, n, q, PK_A, PK_B, H_{pub}()$。

三、使用者註冊階段

系統使用者將其私鑰 SK_A 及帳號 ID_A 親自持往認證中心辦理或使用其他安全之方法向認證中心辦理註冊（這裡以使用者 A 為例說明，B 之操作步驟同 A），用者註冊階段示意如圖一。

(一)認證中心完成使用者身分確認後，求算使用者公開金鑰 PK_A

$$PK_A = n_A \cdot G \quad \text{.....(10)}$$

(二)認證中心將使用者帳號及其公鑰進行關聯運算求得關聯值 e_A

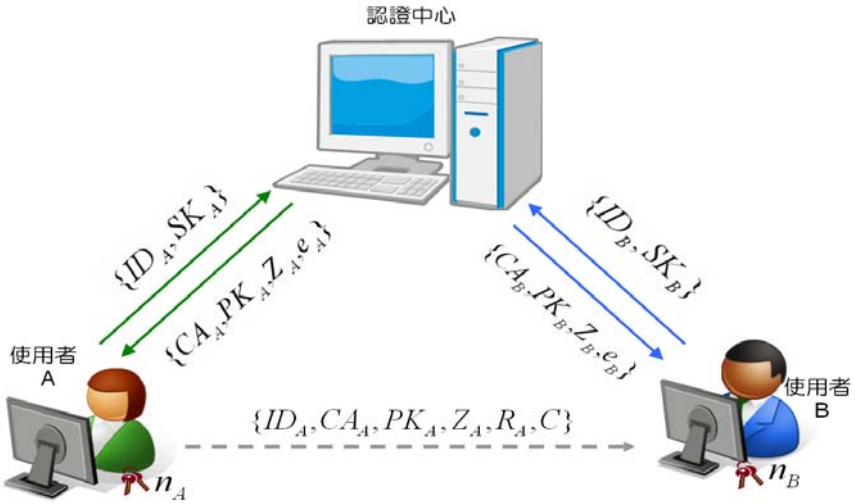
$$e_A = H_{Pub}(PK_A, ID_A) \quad \text{.....(11)}$$

(三)認證中心為 A 選擇一隨機整數 $l_A \in [1, n-1]$，並計算

$$Z_A = l_A \cdot G = (x_Z, y_Z) \quad \text{.....(12)}$$

(四)認證中心製發使用者身分憑證計算

$$CA_A = l_A(e_A + x_Z \cdot n_{AS})^{-1} \quad \text{.....(13)}$$



圖一 使用者註冊示意圖
(資料來源：作者繪製)

四、文件簽密階段

(一)使用者 A 選擇一隨機整數 $k_A \in [1, n-1]$，並計算

$$R_A = k_A \cdot G = (x_R, y_R) \quad \text{.....(14)}$$

(二)使用者 A 計算(15)式，若 $r_A = 0$ 則重新選擇(14)式之 k_A

$$r_A = x_R \bmod n \quad \text{.....(15)}$$

(三)使用者 A 將明文作雜湊運算得到明文雜湊值 m' 如(16)式

$$m' = H_{pub}(M) \quad \text{.....(16)}$$

(四)使用者 A 利用其私鑰SK_A進行式(17)運算得S_A

$$S_A = k_A^{-1}(m' + n_A r_A) \bmod n \quad \text{.....(17)}$$

(五)將明文轉為點座標，A 將訊息拆解成 n 個m_i區塊如(18)式

$$M = \sum_{i=1}^{i=n} m_i \quad \text{.....(18)}$$

(六)接著 A 利用$F_{m2p}(\,)$函數將訊息塊m_i編碼成為橢圓曲線之點，得到如下訊息：

$$T_l \in \{P_i, Q_j\} \quad \text{.....(19)}$$

(七)隨機產生一組之亂數，並以此組亂數產生一組橢圓曲線上之點

$$\bar{v} = \{v_1, v_2, ...v_j\}, 1 < v_j < n-1 \quad \text{.....(20)}$$

$$Q_j = v_j G \quad \text{.....(21)}$$

(八)混合攪亂兩組訊息點，將P_i點依序按任意間隔插入Q_j點序列中成為T_l點序列，混合完成後之點序列以(22)式表示。

$$T_l \in \{[P_i] + [Q_j]\} \quad \text{.....(22)}$$

(九)註記訊息位置

A 將點序列T_l進行式(23) (24)運算

對應T_l點序列，若T_l點屬於P_i，則x_l=1，否則x_l=0。製造$\bar{x}_l$數列如式。

$$\text{if } T_l \in P_i, x_l = 1 \; else \; x_l = 0 \quad \text{.....(23)}$$

(十) 計算訊息所在之背包值

$$W = \{x_1.2^{l-1} + x_2.2^{l-2} + ...x_l.2^0\} \quad \text{.....(24)}$$

(十一) 簽密運算

A 將點序列T_l進行式(25) (26) (27) (28)運算

$$C = \{C_0, C_1, C_2, .., C_l\} \quad \text{.....(25)}$$

$$C_0 = [F_{m2p}(W, S_A) + k_A.n_B G] \quad \text{.....(26)}$$

$$C_1 = [T_1 + C_0 + k_A.n_B G] \quad \text{.....(27)}$$

$$C_l = [T_l + T_{l-1} + k_A.n_B G], 2 \le l \quad \text{.....(28)}$$

A 送出下列資料給 B，

$$\{ID_A, CA_A, PK_A, Z_A, R_A, C\} \quad \text{.....(29)}$$

五、解密及驗簽階段

(一)當 B 收到 A 所傳送過來的C之後，按以下步驟解密。

$$F_{m2p}(W, S_A) = C_0 - n_B.R_A \quad \text{.....(30)}$$

(二) 解T_l點序列，運算方式如下：

$$T_1 = C_1 - C_0 - n_B.R_A \quad \text{.....(31)}$$

$$T_l = C_l - T_{l-1} - n_B.R_A \quad \text{.....(32)}$$

(三)解開明文位置及簽章值，B 將(W, S_A)解出。

$$(W, S_A) = F_{p2m}[F_{m2p}(W, S_A)] \quad \text{.....(33)}$$

(四)再將 W 還原成 2 進位數，對應 i 的位置即為 P_i 存放位置，挑出所有 P_i。

(五)還原明文，利用(34)將所有 m_i 還原，再將所有的 m_i 區塊組合成明文 M。

$$m_i = F_{p2m}(P_i) \quad \text{.....(34)}$$

(六)在身分驗證程序中，使用者 B 計算如下:

$$e_A = H_{Pub}(PK_A, ID_A) \quad \text{.....(35)}$$

$$I_A = CA_A(e_A G + x_z . PK_{AS}) \quad \text{.....(36)}$$

若 $I_A = Z_A$，則確認本訊息確實為使用者 A 所發送。

(七)檢驗簽章，使用者 B 計算如下:

$$m_B' = H_{pub}(M) \quad \text{.....(37)}$$

$$Y = S_A^{-1} \bmod n \quad \text{.....(38)}$$

$$r_R = x_R \bmod n \quad \text{.....(39)}$$

$$u_1 = m_B' Y \bmod n \quad \text{.....(40)}$$

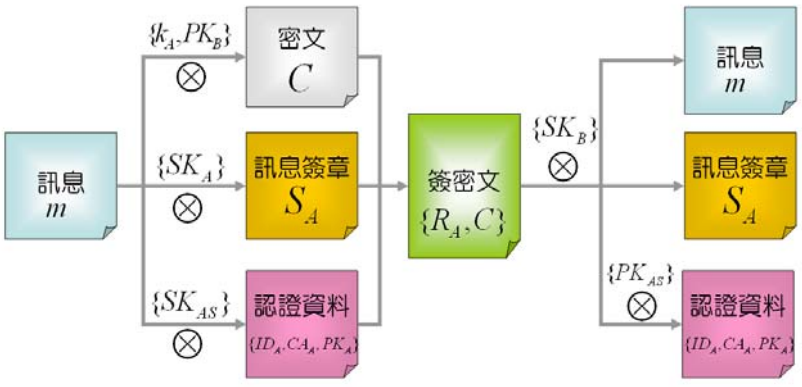
$$u_2 = r_A Y \bmod n \quad \text{.....(41)}$$

$$F = u_1 G + u_2 . PK_A = (x_F, y_F) \quad \text{.....(42)}$$

$$r_F = x_F \bmod n \quad \text{.....(43)}$$

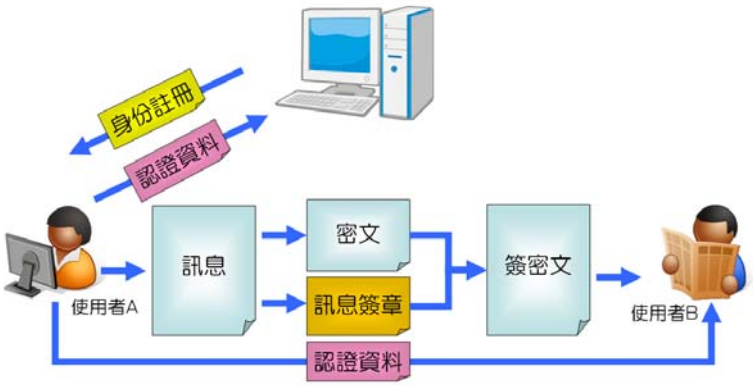
若 $r_F = r_R$， 則確認本訊息為 A 所簽署。

下圖二為簽密及解簽密示意圖，線上的符號代表所使用來進行加密運算的密鑰值。圖三為本系統成員間訊息傳遞關係圖，箭號表示資料的流向。



圖二 簽密及解簽密示意圖

(資料來源：作者繪製）



圖三 系統成員間訊息傳遞關係圖
(資料來源：作者繪製)

安全性及效能分析

一、安全性分析

本研究所提之加密機制，其安全性主要植基於橢圓曲線離散對數問題、背包問題及單向雜湊函數(One-Way Hash Function, OWHF)，根據ISO組織所提之資訊系統安全管理需求[10]，一個安全的資訊應用系統必須達到機密性、完整性、鑑別性及不可否認性等特性，以下針對本系統之安全需求滿足狀況進行探討：

(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。本方法於網路中傳送之資料為$\{ID_A, CA_A, PK_A, Z_A, R_A, C\}$，如第三方於通訊過程中竊聽上述資料，則他必須面對式(28) $C_l = [T_l + T_{l-1} + k_A.n_B G], 2 \le l$ 破解橢圓曲線離散對數之困難。並且因為$T_l \in \{P_i, Q_j\}$，P_i散佈於T_l中，要找出T_l中的P_i，必須破解式(26) $C_0 = [F_{m2p}(W, S_A) + k_A.n_B G]$同樣必須面對破解橢圓曲線離散對數之困難。

(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。在本方法中式(16) $m' = H_{pub}(M)$ 為傳送方對明文進行雜湊運算得m'，並將m'放入式(17) $S_A = k_A^{-1}(m' + n_A r_A) \bmod n$ 中之S_A，然後再將S_A放入式(26) $C_0 = [F_{m2p}(W, S_A) + k_A.n_B G]$，若第三方想要竄改明文$M$偽造簽章$S_A$而不被發現，則他必須一樣得面對橢圓曲線離散對數問題，這使得系統之完整性得以確保。

(三)鑑別性(Authenticity)

指的是訊息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。在本方法中有關使用者認證之參

[10] ISO, Information technology – Security techniques - Code of practice for information security management, ISO/IEC 17799:2005-06-15, 2.6,pp.1.

數為式(29)中之$\{ID_A, CA_A, PK_A, Z_A\}$，而認證之方式如式(35) $e_A = H_{Pub}(PK_A, ID_A)$及式(36) $I_A = CA_A(e_A G + x_z.PK_{AS})$，對式(35)來說他必須面對破解單向雜湊函數之問題，對式(36)來說則是必須面對橢圓曲線離散對數問題，若第三方無法破解式(35)(36)則鑑別性可以確保。

(四)不可否認性(Non-repudiation)

指的是訊息在傳送後，送方不能否認曾經送過此訊息，或收方也不能否認已收到此訊息。有了上述這些特性，一個安全的電子交易行為才有辦法進行。本方法具有送方不可否認性，系統中若非送方本人則無法完成式(17) $S_A = k_A^{-1}(m' + n_A r_A) \bmod n$ 簽章S_A，若無法完成簽章S_A則式(38) $Y = S_A^{-1} \bmod n$ 式(40)$u_1 = m_B' Y \bmod n$及式(41) $u_2 = r_A Y \bmod n$都無法完成，收方在檢驗送方簽章時式(42) $F = u_1 G + u_2.PK_A = (x_F, y_F)$，必須利用送方之公鑰$PK_A$進行檢驗，故若式(42)可完成驗證則可證明式(17) $S_A = k_A^{-1}(m' + n_A r_A) \bmod n$確實由送方 A 所簽署送出。

二、與 Zheng 方法的比較

(一)本方法之加密方法如式(26) $C_0 = [F_{m2p}(W, S_A) + k_A.n_B G]$ 式(27) $C_1 = [T_1 + C_0 + k_A.n_B G]$及式(28) $C_l = [T_l + T_{l-1} + k_A.n_B G], 2 \le l$，故密文若遭受竄改，整個解密過程便無法完成，此一特點亦可作為拒絕送方簽密文的依據，故較 Zheng 僅使用單向雜湊函數檢查訊息完整性有較高的完整性機制。

(二)本方法之加密過程以背包問題概念混入擬亂資料如式(22) $T_l \in \{[P_i] + [Q_j]\}$，破密方除了必須破解密文外，還必須判斷真實明文藏身位置才有辦法正確解密文訊息，故本加密法密文較 Zheng 的方法有較高之機密性，不過也因為於密文中混入擬亂資料，造成密文的資料量變大，因此導致密文的通訊量變大的問題無法避免。

(三) Zheng 方法中之簽章資訊以明文傳遞，而本方法之簽章直接置入密文中，故本方法之簽章有較高之機密性。綜整比較表如表三所示。

表三 本研究與 Zheng 方法比較表

比較項目	Zheng 的方法	本研究
密文完整性	僅使用摘要值檢查	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	以對稱式方法加密	以橢圓曲線密碼系統加密
密文擴增量	因以對稱方法加密，故密文資料量約等於明文。	視加入擬亂資料的多寡而變化，有密文擴充之現象。
簽章機密性	明文傳遞，易遭竄改。	加密後傳遞，偽冒不易。

(資料來源：作者整理）

結論

不斷地設計及驗證具安全性且符合潮流需求之密碼系統，一直是密碼領域研究者努力突破的目標，在強調資訊安全的現實生活中，能提供安全且不影響執行效率的演算法並能導入國防實務領域內，為本研究另一積極追求的目標。本研究提出以橢圓曲線為基礎，設計植基於混合難題的認證及簽密機制適於軍事應用之方法，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，可運用在作戰指揮之場合下，針對戰場環境之特殊限制，身分認證、訊息安全、連線不穩定、頻寬不高及命令下達迅速等要求將可有效改善，綜整本研究，達成貢獻如下：

一、簽章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、認證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、本篇研究方法滿足了 ISO 組織所提之資訊系統安全管理需求，確保了機密性、完整性、鑑別性及不可否認性等基本安全要求。

四、背包問題，於密文中混入擬亂資料，增加敵方或是不法人士破解密文困難亦可視為橢圓曲線密碼加密的一種變形。

五、部分具有雪崩效果，即使遭受敵方或是不法人士部分截獲，其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及完整性。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。