雙重文件混合加密方法之研究

蘇品長[1]　高嘉言[2]　胡智卿[3]　蔡嘉富[4]

[1, 2, 4]國防大學資訊管理學系

[3]國防部後備司令部動員處

摘　要

近年來網路盛行與資訊科技蓬勃發展，為人們帶來生活的便利，然而網路是一個開放式的環境，如何使檔案在傳輸過程中維持其機密性與完整性，成為備受重視的課題。鑑於網路與密碼技術的成熟，如何將國軍機敏資料傳輸作業導入安全的系統運作，值得探討。本研究設計一套植基於橢圓曲線離散對數(Elliptic Curve Discrete Logarithm Problem; ECDLP)及背包問題(Knapsack)的雙重文件加密機制，密文具雪崩效應，增加密文破解的難度，進而提高傳送資料的安全性。

國軍身繫保國衛民、抵抗外侮的使命，掌握敵情及機密防護為其重要之工作，在這個資訊爆炸的數位時代中，軍事資訊的快速取得及如何確保不被有心人士所竊取為其發展的重要關鍵，基於國軍資訊安全考量，遂引發本研究動機，現行國軍所使用的電子公文交換雖說已完成電子化的初步目標，但距離真正的「無紙化」尚有努力的空間，其原因不外乎是安全性的考量，因此密級以上的重要公文大都還是以紙本的方式傳遞，不僅僅浪費寶貴人力及運送的時效性，透過本研究之加密方法，即使資料在公開的網域中，為他人所截取，亦無法成功破解之優勢達到資料安全性；另以雙重文件一次加密之方法提升效率，以背包型態的值作為雙份文件擬亂的效果來增加密碼強度，可使得國軍電子公文交換及各項重要軍事文件的傳輸更加安全及迅速，達成保密及速度雙贏的效果。

關鍵字：橢圓曲線密碼系統、背包理論、雙文件加密、公開金鑰

The research of double-file encryption based on mixed approach

Pin Chang Su[1]　Chia-Yen Kao[2]　Chih-Ching Hu[3]　Jia-Fu Tsai[4]

[1,2,4] Department of Information Management, National Defense University, Taiwan, R.O.C.

[3] Reserve Command Mobilization Service, Taiwan, R.O.C.

Abstract

In recent years, the prevalence and information technology networks to flourish, the convenience of life for people, but the network is an open-like environment, how to make the files in the transmission process to maintain its confidentiality and integrity to become the subject of much attention. In view of the maturity of network and cryptographic techniques, how the military alert data transfer operations into the safety of the system, worth exploring. In this paper, we will present a new double-file encryption design based on Knapsack and elliptic curve discrete logarithm problems (ECDLP), to enhance the security, while maintaining the efficiency of the implementation.

Keywords: Public Key Cryptosystem, Knapsack, Elliptic Curve, Double-file encryption

壹、前　言

密碼技術中，「加密」（Encrypt）就是我們將原來的文件檔案裡的每一個字，透過許多數學公式的運算，產生另一份讓人完全看不懂的文件，且文件內容轉換成不具任何意義的代碼。其主要目的在於提高資訊內容的隱私性，讓要傳遞的資訊在公眾網路傳輸過程中，就像是加了信封的信件，具有保護資訊的外衣，只有特定的人能讀取內文資訊，而非像明信片一樣任何人均可讀到該信件之內容。但究竟什麼樣的密碼系統才是一個安全的密碼系統呢？Shannon[12]提出了密碼系統安全定義中包含兩種，一為理論安全（Theoretical Security），二為實際安全（Practical Security）。所謂的理論安全是指不管破密者截獲多少密文加以分析，其破密的難度和直接猜測明文是一樣的。而 Shannon 所謂的實際安全是假設每一密碼系統在給定 n 位密文時，均有一破解此系統的最少工作次數，稱為此系統的工作特性 $W(n)$（Work Characteristic）。若一系統的 $W(n)$大到使得具有有限計算能力及記憶體的破密者無法在合理的時間內破解此系統，則此系統即可稱為實際安全（Practical Security）或計算上安全（Computational Security）。

加密系統區分為對稱式加密系統與公開金鑰密碼系統，對稱式加密系統以資料加密標準 (Data Encryption Standard, DES) 及進階加密標準(Advanced Encryption Standard, AES)為主，公開金鑰密碼系統以 RSA 密碼系統、ElGamal 密碼系統及橢圓曲線密碼系統(Elliptic Curve Cryptosystem, ECC)，就現今的公開金鑰密碼系統而言，目前都無法滿足理論安全，因此如何設計出符合實際安全與維持良好系統效率的密碼系統則成為密碼學家努力的目標。因此，為強化系統之安全，Harn 年提出一個植基於因式分解和離散對數的簽章系統，Hwang 和 Lee 改進了 Harn 的方法以避免偽造攻擊，之後陸續有專家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，強化系統安全性。但從已發表植基於因式分解和散對數的雙重難題的文章中，可發現多數都只提供強化演算法之安全性，對於演算效率卻有重大影響，因此如何兼具安全與效率，是為本研究積極追求突破的目標。

搜尋全國博碩士論文資訊網網站大多文獻在探討加密、簽章方法與機制，未發現文獻探討雙文件加密方法，而多為研究單一文件，或檔案、資料加密機制。另找尋國內外探討文件加密之網站（軟體）經綜理後，大致上區分為下列 2 種加密及運作方式：

- 似「**7-Zip**」壓縮軟體：其加密方式為針對存放多文件之資料夾進行壓縮，並賦予密碼實施加密，壓縮加密後可呈現單一或分割多個壓縮檔案，需經解密及解壓縮後始能還原。
- 似「檔案守護神」軟體：可針對單一或多文件進行加密，其加密方式為將多個單一文件置放於同一資料夾後進行加密，惟加密後資料夾中仍為多個單一文件加密檔案。

在這個競爭日趨激烈的數位時代，工作的即時性將愈顯重要，速度與保密將成為資訊發展的重要關鍵，建立一個安全及可信賴的網路環境，將是電子商務能否全面普及的關鍵，然而「安全及可信賴的網路環境」是確保資訊在網路傳輸過程中不易遭受偽造、非法存取、竄改、竊取或截聽該內容，並且亦能鑑別傳送及接收雙方的身分，以防止事後否認其行為事實。資訊化的時代所注重的無非是安全及效率，不僅僅在電子商務方面，在戰場上訊息快速且安全的傳遞亦是提升我方勝率的因

素，藉由一次性混合式方法的雙重文件加密機制，降低文件分批加密後特徵值，減少認證頻率、加（解）密次數及傳輸頻寬之需求等優點，以符合各種資訊與網路環境中數位多文件加密傳遞的速度與效能。因此，我們提出一種植基於橢圓曲線離散對數及背包理論之密碼機制運用於雙文件加密上之演算法，主要就是希望藉由結合離散對數與資訊混淆之特點來增加密碼系統之安全性，打破以往檔案單一文件單一加密的方式，將雙文件的資訊藉由混淆機制，將其變成一份密文，並使其密文具有雪崩效應，令竊密者既使截獲部分資訊亦無法得知明文資訊，成為一套能增加文件解密之難度，卻不會降低其演算效率之加密法。

本研究之前言為探討現今社會使用的加解密模式及本研究動機，文獻探討方面針對橢圓曲線觀念、背包理論及橢圓曲線加密方法來做簡介探討，說明上述公開金鑰密碼系統的緣由及發展的歷程，並詳細說明本文所提之雙文件混合加密法，從系統符號說明、系統初始階段、文件加密階段至文件解密階段，詳細介紹各個步驟及方法，並從機密性、完整性及不可否認性等三方面來進行安全性分析與考量，針對本文所具備的特點及效益分析，綜整本研究的創新理念及未來研究方向為結論，對國防領域之應用，可適用於國軍資料傳輸作業，提昇資訊作業之機密性、完整性及可用性等優點。

貳、文獻探討

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。

(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。下表為 RSA 與 ECC 在相同安全度下金鑰長度之比較表。

表 1　RSA 與 ECC 相同安全度金鑰比較表

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

二、背包式公開金鑰密碼系統(Knapsack Cryptosystem)

背包問題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，我們將如何選擇最合適的物品放置於給定背包中。它的數學描述是指給定一個自然數數列 $B=\{b_1,b_2,\text{K},b_n\}$ 及一數S，是否存在一子數列 $B'\subseteq B$，其中 $B'=\{b'_1,\text{K},b'_m\}$，使得 $\sum_{i=1}^{m} b'_i = S$ ？

背包問題已經被證實是一個 NP-Complete 問題。並無法在多項式時間內解決，而且背包式密碼系統的最大優點為加解密(或簽署驗證)速度相當快，故將其套用在密碼系統的設計上有其優點。但是這種密碼系統被發現是不安全的，因為這種密碼系統中的“超增數列”被許多學者發現其弱點並對此展開攻擊，第一位成功攻擊 Merkle-Hellman 背包式公開金鑰密碼系統的學者是 Shamir，在 Shamir 攻擊之後，陸陸續續又有許多學者提出攻擊的方式，其中較為特別的是一位 Brickell[3]的學者所提出的攻擊方式，它的攻擊方式稱為低密度攻擊，只要是背包式密碼系統中的超增數列中的數值，在整個數列中所佔的密度太低，就有可能被猜出來，而背包式密碼系統也就可能因此瓦解。

Diffie 向世人介紹了公開金鑰密碼的概念之後，不久之後就有了公鑰密碼的實作系統被提出，其中一個較著名的為 Merkle-Hellman 的背包式公鑰密碼系統[9]。以下介紹 Merkle-Hellman 的背包式公鑰密碼系統：

給定一正整數集合 $\{b_1,b_2,...,b_k\}$ 及一個和 S，計算 $m_i \in \{0,1\}$ *(for i = 1, 2, ..., k)*，使得 $S=\sum_{i=1}^{k} b_i \times m_i$ 。

超增背包(super-increasing knapsack)：

一數列$<a_i>$，若 $a_{i+1} > \sum_{j=1}^{i} a_j$ ，則$<a_i>$稱為超增數列。

(一)金鑰產生

1.任選一個超增數列$<a_i>$(for i = 1 to k)及一整數 n，其中 $n > \sum_{i=1}^{k} a_i$ 。

2.任選一數 e 滿足 $\gcd(e,n)=1$，並求出 $d = e^{-1} \bmod n$ 。

3. 將 $<a_i>$ 轉換成 $<b_i>$，使得 $b_i = e \times a_i \bmod n$ 。

4.$<b_i>$為公鑰，d 為私鑰。

(二)加密程序

1.令明文 $M = m_1 m_2 \text{L}\ m_k$ (每一個 m_i 為一個位元)。

2.計算密文 $C=\sum_{i=1}^{k} b_i \times m_i$ 。

(三)解密程序

1.計算

$$C' = C \times d \bmod n$$
$$= C \times d = \sum_{i=1}^{k} b_i \times m_i \times d = \sum_{i=1}^{k} a_i \times m_i (\bmod n)$$

2.利用超增數列求解演算法，代入 C' 求出 m_i 。

三、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，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：

(一)系統初始階段

1.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。

2.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]

3.計算簽章者公鑰$Q=n_AG$

4.將(E,G,Q)公開

(二)加密階段

1.令明文m為E上的一點M。

2.加密者任選一個整數$k\in[1,n-1]$

3.計算密文

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

(三)解密階段

計算明文$M=C_2-n_BC_1$，其中n_B為收方私鑰。

參、雙文件混合加密方法

本節將基於橢圓曲線離散對數（ECDLP）及背包問題(Knapsack)設計一個改良式橢圓曲線加密法。方法分為三個階段：系統初始化階段、加密階段、解密階段。我們的加密法在完整性上面，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；本法於橢圓曲線加密過程以背包問題概念另外混入假資料增加破密困難，雖然運算量提高但運算複雜度並未增加。以下對本方法各階段進行說明：

一、系統符號說明

表2為本系統中所使用的符號說明。

表2　系統使用符號說明表

項目	符號	說明
1.	CA	認證中心
2.	$E(F_q)$	有限域F_q中的一條橢圓曲線
3.	G	橢圓曲線中的基點
4.	n	橢圓曲線上基點的秩(order)
5.	q	$q>2^{160}$之質數
6.	ID_A, ID_B	A、B 的ID 資訊
7.	PK_{AS}, SK_{AS}	CA的公私鑰
8.	PK_A, PK_B	使用者 A、B 之公鑰
9.	SK_A, SK_B	使用者 A、B 所選擇之私鑰各為n_A, n_B兩整數
10.	CA_A, CA_B	使用者 A、B 之憑證
11.	$H_{pub}()$	認證中心公開之雜湊函數
12.	$H_{m2p}()$	將訊息轉為橢圓曲線點之函數
13.	$H_{p2m}()$	將橢圓曲線點轉為訊息之函數

二、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(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。

使用者 A、B 分別選擇$n_A, n_B \in Z_q^*$當成私鑰，以親自前往交付CA並計算其相對應之公鑰$PK_A = n_A \cdot G$， $PK_B = n_B \cdot G$，並保留經過認證後的私鑰，選擇的一個單向無碰撞雜湊函數$H_{pub}()$，最後公開$E(F_q), G, n, q, PK_A, PK_B, H_{pub}()$。

在金鑰管理方面，使用者皆必須經過認證中心*CA*的檢驗認證之後，方可擁有自己的公鑰和私鑰來進行加解密動作，因為使用者 A、B 在資料傳遞前，必定先進行使用者身分的認證，利用以達成不可否認性。

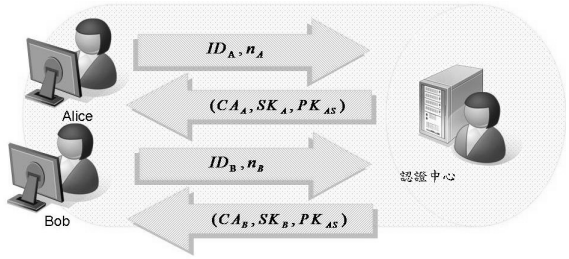

圖 1　金鑰管理認證圖

三、文件加密：

步驟一：使用者 A 將明文作雜湊運算得到明文雜湊值m'如 (1) (2) (3) 式

$$m_1 = H_{pub}(M_1) \quad \text{.....(1)}$$

$$m_2 = H_{pub}(M_2) \quad \text{.....(2)}$$

$$m = H_{pub}(m_1, m_2) \text{.....} \quad (3)$$

步驟二：使用者 A 將明文轉為點座標

A 將兩份訊息拆解成數個區塊如(4)(5)式

$$m_1 = \{m_{11}, m_{12}, ..., m_{1i}\} \quad \text{.....(4)}$$

$$m_2 = \{m_{21}, m_{22}, ...m_{2j}\} \quad \text{.....(5)}$$

步驟三：接著 A 利用$H_{m2p}()$函數將訊息編碼成為橢圓曲線之點，如 (6) (7) 式

$$P_i = H_{m2p}(m_i) \quad \text{.....(6)}$$

$$Q_j = H_{m2p}(n_j) \text{.....} \quad \text{.....(7)}$$

步驟四：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(8)式表示。

$$T_l \in \{[P_i]+[Q_j]\} \text{.....(8)}$$

步驟五：註記訊息位置

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$\bar{x}_l \in \{0,1\}$數列如(8)式

$$\text{if } T_l \in P_l, x_l = 1 \; else \; x_l = 0 \text{.....(9)}$$

步驟六：計算訊息所在之背包值

$$W = \{x_1.2^{l-1} + x_2.2^{l-2} + ...x_l.2^0\} \text{....} \quad (10)$$

步驟七：加密運算

A 將點序列T_l進行下列式(11) (12) (13)運算

$$C = \{C_0, C_1, C_2, .., C_l\} \text{.....(11)}$$

$$C_0 = [H_{m2p}(W, m) + n_A.n_B G] \text{.....} \quad (12)$$

$$C_l = [T_l + x_l \cdot C_{l-1} + n_A.n_B G], 2 \le l \text{.....(13)}$$

步驟八：A 將 C 送出給 B

四、解密

步驟一：當 B 收到 A 所傳送過來的C之後，按以下步驟解密。

$$H_{m2p}(W, m) = C_0 - n_B.n_A G \text{.....} \quad (14)$$

$$(W, m) = H_{p2m}[H_{m2p}(W, m)] \text{.....(15)}$$

步驟二：接著將 W 還原成$\bar{x}_l$數列，還原方式如(16)。

$$W = \bar{x} = (x_1 x_2 .. x_l)_2 \text{.....} \quad (16)$$

步驟三：B 進行點序列T_l解密，運算方式如(17)(18)(19)：

$$T_1 = C_1 - x_l \cdot C_0 - n_B.n_A G \text{.....} \quad (17)$$

$$T_l = C_l - x_l \cdot C_{l-1} - n_B.n_A G \text{ ……..…...(18)}$$

$$\text{If } x_l = 1 \text{ then } P_l = T_l \text{ else } \mathrm{Q}_l = T_l \text{ …..(19)}$$

步驟四：還原明文

利用 (20) (21) (22) (23)將所有點資訊還原成訊息區塊，再將所有的訊息區塊組合成明文。

$$m_i = H_{p2m}(P_i) \text{ ……...(20)}$$

$$m_j = H_{p2m}(Q_i) \text{ ……(21)}$$

$$m_1^{'} = \{m_{11}, m_{12} ... m_{1i}\} \text{ ……(22)}$$

$$m_2{'} = \{m_{21}, m_{22} ... m_{2j}\} \text{ …… (23)}$$

步驟五：驗證明文正確性

收方 B 計算

$$m_1{'} = H_{pub}(M_1{'}) \text{ ……..…(24)}$$

$$m_2{'} = H_{pub}(M_2{'}) \text{ ……..……(25)}$$

$$m^{'} = H_{pub}(m_1{'}, m_2{'}) \text{ ……..(26)}$$

$$m^{'} \overset{?}{=} m \text{ …… (27)}$$

(27)等式成立則收方所收之訊息正確無誤本系統之加密及密解密運作示意圖，如圖 2、3 所示：

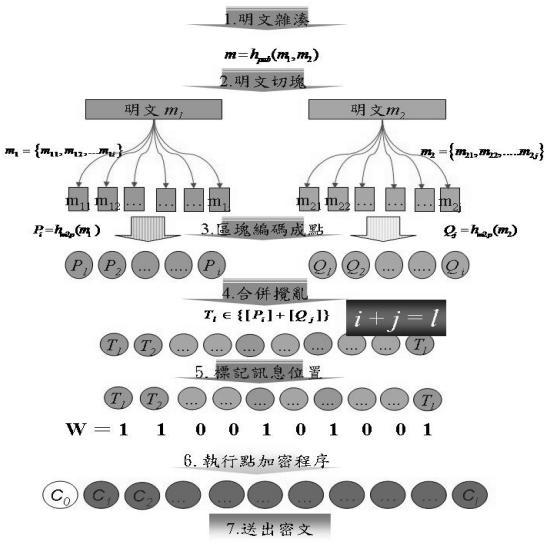

圖 2　系統加密運作示意圖

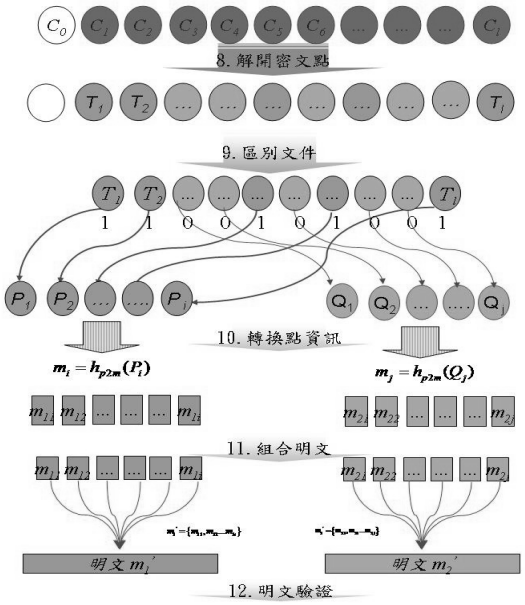

圖 3　系統解密運作示意圖

肆、安全性分析

本研究所提之加密機制，其安全性植基於 ECDLP、Knapsack 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，一個安全的資訊應用系統必須達到機密性、完整性及鑑別性等特性，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)：

對電子商務來說所謂機密性是指交易不能經由公共網路來追蹤，未經授權的中間人無法取得交易複本。電子商務的環境中所有的訊息交換都是保密的，訊息在成功地送達目的地之後，除了稽核資訊外，所有存在於公共環境中的相關資訊會被刪除，且訊息的儲存必須在具備完善保護的系統下進行。本方法於網路中傳送之資料為 C，如第三方於通訊過程中竊聽，則他必須面對(13)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 及 Q_j 散佈於 T_l 中，要分別 T_l 中的 P_i 及 Q_j，必須破解

(12)同樣必須面對破解橢圓曲線離散對數之困難。

二、完整性(Integrity)：

交易一定不能被破壞或干擾。電子交易的內容在用戶端和伺服器間傳遞的過程中確認沒有被改變，也就是訊息在交易的處理過程中不能被任意地加入、刪除或修改。在本方法中(3)為傳送方對明文進行雜湊運算得 m ，並將 m 放入(12)中，若第三方想要竄改明文偽造 m 而不被發現，則他必須面對(1) (2) (3)破解單向雜湊函數的問題及面對(12)橢圓曲線離散對數問題，這使得系統之完整性得以確保。

三、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。系統中密文如(12) (13)式使用傳送方之私鑰 n_A 加密，接收方未來必須利用傳送方之公開金鑰才能將密文解開。對於公開金鑰密碼系統來說，公鑰及私鑰是成對的，而且是具有唯一性的，也就是說使用者 A 用其私鑰加密日後也僅能以其公鑰進行解密。故當使用者 A 將明文加密傳出後，他便無法否認密文是經由他加密的，若第三方想要藉由傳送方使用者 A 之公鑰 n_AG 推斷其私鑰 n_A ，則破譯者會面對橢圓曲線離散對數之問題，這使得傳送方發出密文具有不可否認性。

伍、效益評估

一、系統的安全性

本方法之密文具雪崩效果，先將明文在加密前分割成若干點，求算密文時將每一點導入後一點作橢圓曲線點相加運算如(13) $C_l=[T_l+x_l\cdot C_{l-1}+n_A.n_BG],2\le l$ ，使得連續的兩點間具有依存關係。而且每一點都使用收方的通信公鑰來作加密，每一個點都擁有不同的加密密鑰，因此在傳送過程中若遭部分截獲，第三方並無法由部分密文解讀任何資訊。

二、執行的效率性

要破解本方法之密文除了必須面對橢圓曲線離散對數之難題外，同時還必須猜測明文所在位置如(12)式才有辦法成功破解密文還原明文。也就是對每一密文點來說，竊聽者將會面對解橢圓曲線離散對數的困難。竊聽者若要判斷原文之密文點藏身處則他將會面對解背包問題。經由結合橢圓曲線與背包問題，使得本加密機制擁有更高的安全性，表 3 為本研究與 Elgamal 橢圓曲線加密法之分析比較表，本研究以橢圓曲線密碼系統為主體，與現今所使用的 Elgamal 與 RSA 等等非對稱式加密系統比較，在相同安全度下，不僅僅在金鑰長度上占優勢，加解密的速度更是具備效率，結合雙文件的一次加密，作業速率更比傳統單一文件單一加密更快，表 4 為本篇研究與 Elgamal 的運算速率比較表，從表 4 中可以明顯的比較出本篇研究實施雙份文件一次加密的運算複雜度與 Elgamal 進行兩份文件的加密運算複雜度還要低，因此效率更佳。

表 3　本研究與橢圓曲線加密法之分析比較表

比較項目	Elgamal 橢圓曲線加密法	雙文件加密機制
密文完整性	未進行完整性檢查。	密文具有雪崩效應，若有一個位元遭到竄改可能會造成整體密文無法解密的狀況。
密文機密性	植基於橢圓曲線離散對數。	植基於橢圓曲線離散對數。

不可否認性	具不可否認性，但有漏洞。	具不可否認性。
密文通訊量	僅有橢圓曲線密碼系統密文擴充現象。	除有橢圓曲線密碼系統密文擴充現象外，以雙文件混合，有不同密文擴充現象。
加密金鑰	收方公鑰。	會議公鑰。
明文拆解	拆解成一個點。	拆解成為多個點。
加密程序	以收方公鑰加密。	除以雙方會議金鑰加密外，且密文點之間相互進行點加運算。
解密程序	以橢圓曲線點減法解密。	以橢圓曲線點減法解密。
密文種類	機率式。	機率式。
加密次數	單一文件單一加密。	雙文件一次加密。

表4　Elgamal加密兩份文件與本研究方法運算時間複雜度比較

演算法	Elgamal 加密兩份文件		本研究方法	
比較項目	時間複雜度	概估	時間複雜度	概估
金鑰產生	T_{EXP} x2	$\approx 480T_{MUL}$	T_{ECCMUL}	$\approx 29T_{MUL}$
加密運算	$(T_{EXP}+T_{INVS}+T_{ADD}+3T_{MUL})$ x2	$\approx 480T_{MUL}+(6.94+(1.686\ln(p))T_{DIV})$	$T_{ECCADD}+2T_{ECCMUL}$	$\approx 58.12T_{MUL}$
解密驗證	$(3T_{EXP}+T_{MUL})$x2	$\approx 1440T_{MUL}+6T_{DIV}$	$T_{ECCADD}+2T_{ECCMUL}$	$\approx 58.12T_{MUL}$
	T_{ECCMUL}：進行一次ECC乘法運算所需時間 $\approx 29T_{MUL}$		T_{INVS}：進行一次模式乘法反元素運算所需時間 $\approx (0.843\ln(p)+1.47)T_{DIV}$	
	T_{EXP}：進行一次模式指數運算所需時間 $\approx 240T_{MUL}$		T_{ECCADD}：進行一次ECC加法運算所需時間 $\approx 0.12T_{MUL}$	
	T_{ADD}：進行一次模式加法運算所需時間(可忽略不計)		T_{MUL}：進行一次模式乘法運算所需時間 $\approx T_{DIV}$	

陸、結　　論

本研究提出以橢圓曲線為基礎所設計的一個橢圓曲線雙文件加密法，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，運用在適合以公開金鑰加密之機制。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，為本實驗室另一積極追求的目標，未來將結合對稱金鑰快速運算的特性，實作為認證模組，產生對稱金鑰後再行加密，並期待可以完成多重文件進行一次加密及簽章的構想，未來可適用於國軍無線通訊上藉由一次性混合式方法的多檔案加密機制，降低檔案分批加密後特徵值，減少認證頻率、加（解）密次數及傳輸頻寬之需求。縱整本研究，達成貢獻如下：

- 滿足機密性、完整性及不可否認性之安全需求。
- 結合背包問題，將欲加密之雙份文件進行混合，增加破密困難亦可視為橢圓曲線密碼加密的一種變形。

- 密文部分具有雪崩效果，即使遭受部分截獲第三方將無法藉由片段密文進行破密工作，此 一特徵可提供更安全的機密性及完整性。

捌、參考文獻

肖攸安，2006。橢圓曲線密碼體系研究，華中科技大學出版。

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。

Brickell, E. F., 1985, Breaking Iterated Knapsacks, Advances in Cryptology: Proceedings of Crypto84, G.R. Blakely and D. Chaum. eds., Springer-Verlag,pp. 342-358.

Diffie, W. and Hellman, M., 1976, New Directions in Cryptography, IEEE Trans. Inform. Theory, Vol. IT-22, 644-654.

Harn, L., 1994, Public-key cryptosystem design based on factoring and discrete logarithms, Computers and Digital Techniques, IEEE Proceedings, Vol. 141, Issue 3, 193-195.

Hwang, T. and Chen J. L., 1994, Identity-based conference key broadcast system, Computers and Digital Techniques, IEEE Proceedings, Vol. 141, Issue 1, 57-60.

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

Koblitz, N., 1987, Elliptic Curve Cryptosystems, Mathematics of Computation American Mathematical Society, Vol. 48, 203-209.

Merkle, R.C. and Hellman, M., 1978, Hiding Information and Signatures in Trap-door Knapsacks, IEEE Trans. Inform. Theory, Vol. IT-24, 525-530.

Miller, V. S., 1985, se of Elliptic Curve in Cryptography Advance in Cryptography-Crypto ’85, New York: Spring-Verlag, 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, 145-152.

Shannon, C.E., 1949, Communication Theory of Secret Systems, Bell System Technical Journal, Vol.28, No.4, 656-7153.