IC 卡安全電子郵件系統

葉杰榮、謝祥尹、謝劭杰、楊中皇
國立高雄第一科技大學資訊管理系
chyang@ccms.nkfu.edu.tw

摘　要

本研究中我們製作了一個安全電子郵件收發系統，在現有的電子郵件協定中，使用 IC 卡管理個人憑證，並且搭配自行製作的憑證管理中心，建製一個完整的安全電子郵件系統。

在系統中，我們結合私密金鑰系統（本研究採用 Triple-DES）以及公開金鑰系統（本研究採用 RSA）來確保郵件的私密性、完整性、防止偽造以及無可否認性。在憑證管理中心方面，我們使採用 2048 位元的金鑰來製作憑證管理中心的數位簽章，郵件使用者的數位簽章則採用 1024 位元的金鑰來製作，我們也採用 IC 卡來儲存與管理認證中心與個人的憑證以及私密金鑰。。

關鍵字：*安全電子郵件*、*IC 卡*、*憑證管理中心*

壹、前言

Internet 的興起讓我們的生活上方便了許多，電子郵件更是讓我們可以用方便、快速、低成本的方式交換訊息。但是一般人甚少在電子郵件中加上安全機制。網際網路這樣透明的環境中，電子郵件在方便、快速、低成本之餘，一點都不安全。

資訊安全領域的技術與理論，可以讓我們的機密資料得到保障，而且保護我們在網路上的隱私權；在更積極的來說，它也保護了我們的財產安全。

若電子郵件可以提供某種程度的安全性，那麼我們便可以利用電子郵件來作更多的事情。例如配合特定格式，可以利用 Internet 來作為 EDI 的媒介，便省去了鋪設專線的成本。配合信用卡交易程序，我們可以更安心的在網路上購買商品。這些好處都一再地刺激我們將『安全電子郵件』化為實際成品的渴望。

貳、以 IC 卡為安全機制的電子郵件系統

根據『Network Security Private Communication in a Public World』[1]一書中所述，安全電子郵件可具備下列特性：

(一)隱私權（privacy）
(二)身份證明（authentication）
(三)無可否認（non-repudiation）
(四)寄信證明（proof of submission）
(五)收信證明（proof of delivery）
(六)寄信過程的保密（message flow confidentiality）
(七)可匿名性（anonymity）
(八)圍堵（containment）
(九)稽核（audit）
(十)記帳（accounting）
(十一)自我破壞（self destruct）
(十二)訊息順序的完整（Message sequence integrity）

很明顯的，以上幾項功能之間有互相抵觸。因此大部分的安全電子郵件系統並無法提供以上全部的功能。

IC 卡就是在塑膠卡片上裝置積體電路（IC)。IC 卡上的 IC 可以包含記憶體與微處理機；因此 IC 卡除了儲存資料還具有處理資料的能力。IC 卡在外觀上跟一般磁條卡很類似，IC 卡依照其封裝的 IC 可分成兩大類；在 IC 中只有記憶體的稱為記憶卡（Memory Card)，IC 中有微處理機的卡，因其具有資料處理的能力，又叫做主動卡（Active Card)。

傳統的磁條卡（如信用卡、提款卡）容量小，且資料容易讀取、安全措施薄弱，很容易遭不法之徒偽造，因此很多犯罪行為的產生。目前半導體封裝技術成熟，可以很容易將 IC 裝置在塑膠卡片上，因此卡片可以藉著 IC 提高儲存容量，若內建微處理器還可以增加資料處理能力，更可以提供多種層次的密碼保護。在未來的應用上可以搭配磁條卡使用或是全面替代磁條卡。根據 ISO 制訂的標準，IC 卡上面有八個接點作為外界提供電源、控制信號和資料傳輸的介面，而 IC 卡可以依照使用上的需求決定要不要內建微處理器。

IC 卡的主要優點如下：

(一)記憶容量大，資料可重複多次寫入或更新

目前磁條卡的記憶容量約為 110個英文及數字，本研究中使用容量為 6K 的 IC 卡；而 16K 位元組的卡片也已經進入量產階段。IC 卡的資料可重複多次的寫入或更新，使其應用領域大增，具有發展為多目的、多功能卡的潛力。

(二)具備 CPU 可執行各種邏輯運算，利用 CPU 的指令組合成各種不同功能。

(三)資料控管功能

利用 CPU 的邏輯運算能力，使檔案各具不同屬性、達到多層資料存取控制功能。

(四)安全性高

利用 CPU 的指令實現所想要的各種安全演算法，達到安全無慮的要求。可執行驗證、認證等演算法，確認使用者、傳輸資料及介面裝置（讀寫機）的正確性。執行加密、解密等演算法達到安全通訊的目的。執行電子簽章演算法，達到交易保證功能。

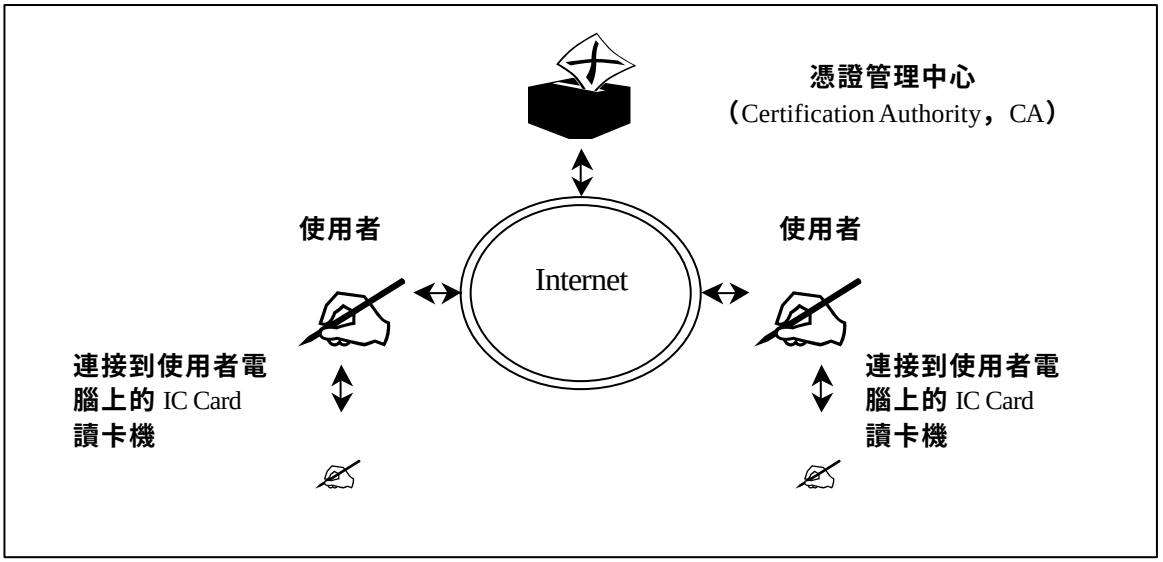
(五)安全性高不易偽造，防止卡片犯罪的損失

由於 IC 卡從製造到發卡的過程相當嚴謹；且 IC 卡是屬高科技的產品，一般人能偽造的機會不高，且其內部資料也是層層保護不易竊讀。因此從安全性的觀點而言，IC 卡實是比磁條卡安全多了，而這也正是 IC 卡吸引人的特點。

(六)可採離線（off-line）作業，減少通訊成本

因為通訊成本的高漲及通訊不良，造成連線（on-line）作業越來越不受歡迎。而由於 IC 卡對於卡片資料的保護較為嚴謹，使其可適用於離線作業系統的使用，利用離峰時間整批傳輸資料。如此可節省連線系統中通訊網路、硬體、軟體人力及時間的成本，使整體系統的表現更有效率，安全性更高。

基於以上幾點，我們可以利用 IC 卡特性，保護個人的憑證資料，增加系統的安全功能。



圖一：系統架構圖

參、系統架構

本系統是由憑證管理中心、安全電子郵件系統、與 IC Card 這三個部份所組合而成，其架構如圖一所示，IC 卡與安全電子郵件在上一節已經說明過，在此不加贅述，針對憑證管理中心功能描述如下：

憑證管理中心（Certification Authority, CA）為具公信力第三者（Trusted Third Party），對使用者提供認證及憑證簽發管理等服務，以建立具有機密性、完整性、防止偽造、不可否認性的通信安全環境與機制。

憑證管理中心提供下列的功能：

(一)憑證申請

提供用戶申請其所屬的電子憑證。憑證是以 X.509[2]的格式儲存。

(二)憑證註銷

註銷尚在有期間內用戶憑證。

(三)憑證查詢

可以查詢自己或他人的憑證資料，以便得到他人的公開金鑰檔案。

(四)憑證展期

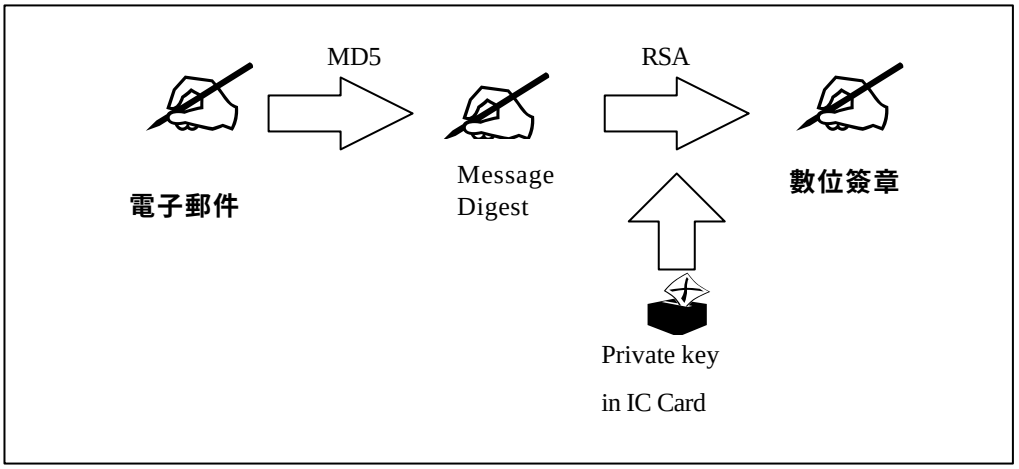
若因為其他因素必須延長有效期限，CA 也提供憑證延期的服務。

(五)CRL 列表

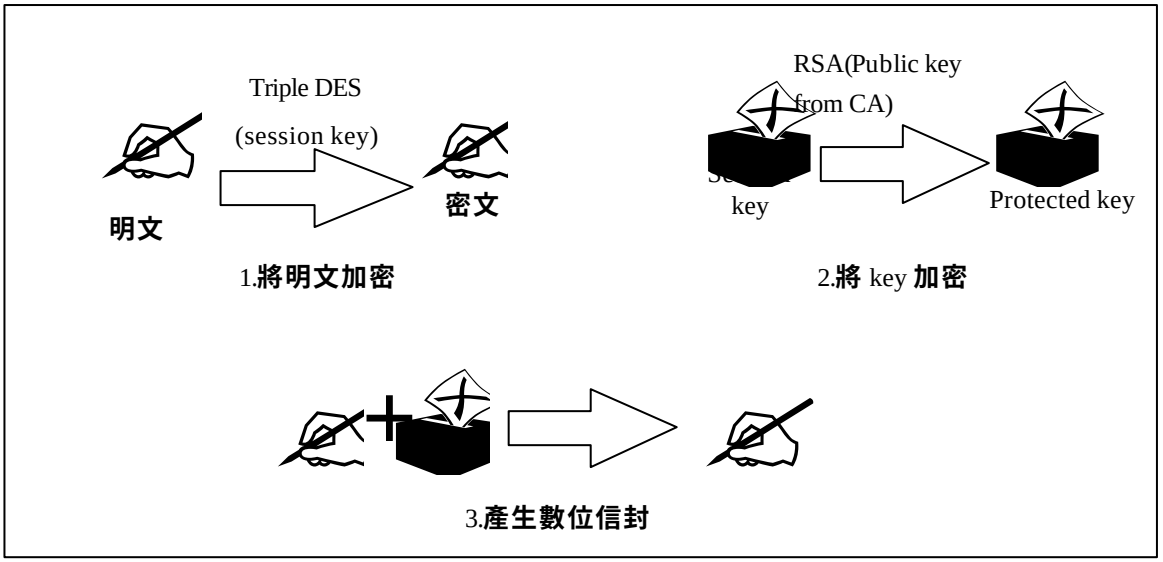
當憑證註銷後，系統便會將憑證資料轉入此表中，讓使用者可以查詢。

肆、系統安全機制說明

電子郵件的收件人和寄件人都必須



圖二：數位簽章產生的流程



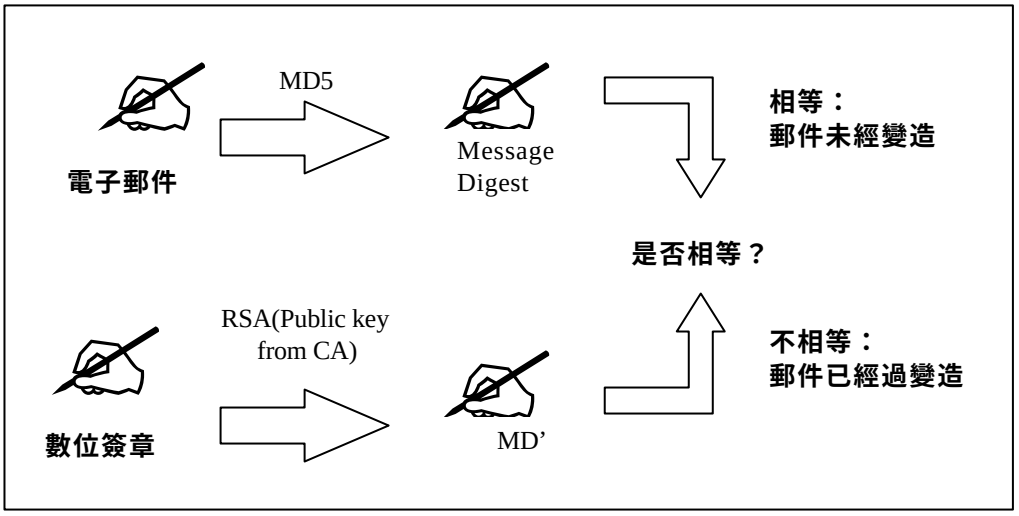
圖三：數位信封產生流程

先在認證中心上面註冊自己的個人資料和自己的公開金鑰[3,4]。註冊成功之後認證中心會發給申請人一個憑證。

在信件寄出之前，系統會對郵件產生數位簽章（Digital Signature）[1,3,4]用以防止郵件內容遭到修改或仿造且提供寄信的證明。為了產生此數位簽章，使用 MD5[1,5]演算法產生該郵件的單向雜湊函數值（One-way hash value）並使用寄件人的 RSA 私密金鑰（private key），，產生數位簽章，附加於此郵件。其流程如圖二所示：

為了提供郵件在傳輸時的隱密性，本系統在傳送端會產生一串 112 位元的隨機字串作為將郵件做 Triple-DES[1,6]加密的金鑰（Session Key），然後使用從憑證管理中心取出收件人的公開金鑰對 Session Key 作加密；最後藉由簡易郵件傳輸協定（SMTP [7]）將加密過的郵件和金鑰傳送給所指定的接收者，而此加密過的文件和金鑰則稱為數位信封（Digital Envelope）。加密過程如圖三所示。

當收件人收到數位信封時，先利用收件人的私密金鑰來對 Session Key 解密，然後利用解密後的 Session Key 將被 Triple-Des 所加密的郵件予以解密，最後將利用 MD5 演算法對解密過的郵件產生其單向雜湊涵數值和使用寄件人的 RSA 公開金鑰對所接收到數位簽章予以解密所得到的值比較，看是否互相符合，如果是相同的，則表示所接收到郵件的確是由



圖四：數位簽章檢驗的流程

被認證過的寄信人所傳送出的而且在傳輸的期間未遭到他人竄改。（如圖四所示）

我們採用Fischer公司的IC Card讀卡機－－『ECMaster/Anywhere』作為使用者保管個人憑證工具。它在形狀大小上跟3.5吋磁碟片一樣，但是它是一個IC卡讀卡機。可將IC卡置入讀卡機後，再將此讀卡機插入電腦軟碟位置即可透過PC操作。

其部分規格如下：

(一)適用於任何符合ISO 7816及7810標準尺寸大小的IC卡。

(二)使用本身的水銀電池，可以防止來自PC電源的波動，或靜電荷對讀取品質的影響。

(三)支援所有IC Card的傳輸協定，包括ISO 7816。

(四)支援Windows 3.x，Windows 95/98，Windows NT，DOS

其提供的發展軟體在IC Card上定義了幾個運算：

(一)建立檔案

可以在IC Card上建立16個檔案，16個檔案的大小總和不超過6K bytes。

(二)寫入資料

(三)讀取資料

(四)建立讀寫密碼

讀與寫的密碼可以不同。

(五)更改密碼

(六)讀取卡片序號

每一張IC Card出廠皆內建一個序號，這個序號每一張卡都是唯一。

啟動CA伺服器的卡片(簡稱CA卡)與使用者使用來存憑證的卡片（簡稱user卡）在內容的規劃上不同。

IC Card內部檔案結構規劃如表一。

伍、系統功能簡述

本系統的三個子系統：安全電子郵件系統、資訊認證Server端系統與資訊認證Client端系統皆是在Windows 98平台下發展，而且可以在Windows 95/98/NT平台執行的應用程式。

利用安全電子郵件收發系統收發郵件之前，使用者必須先用『資訊認證Client端系統』連線到『NKFU資訊認證Server端系統』申請個人的憑證。使用者利用Client端系統輸入名字、身份證號碼、電子郵件…等資訊，並將自己的公開金鑰上傳給Server端系統，申請通過後即可下載憑證。

憑證採用符合X.509的格式儲存，憑證內含有憑證所有人的姓名，電子郵件等資料，其中最重要的是憑證所有人的公開金鑰。

表一：IC Card內部規劃方式

	CA卡	User卡
用途	啟動、管理認證伺服器。	讓使用者可以儲存個人資料、private key與憑證。
內含檔案數目	四個	四個
第一個檔案大小、用途	80 bytes 開啟CA伺服器的的辨識值	10 bytes 儲存IC卡DEMO程式所使用的資料，即是作DES加解密的key。
第二個檔案大小、用途	1024 bits RSA中的『D』	128 bytes 持卡人的個人資料，用以驗證持卡人身份的真實性
第三個檔案大小、用途	80 bytes RSA中的『E』	128 bytes 保留供未來使用
第四個檔案大小、用途	1024 bits RSA中的『N』	400 bytes RSA中的『D』

圖五：資訊認證 Client 端系統

在下載憑證之後，使用者就可以透過『安全電子郵件收發系統』來為電子郵件加上安全機制了。本系統有三種郵件傳送的方式：

(一)不加密但加數位簽章

這種方式不對郵件內容做加密的保護，但是數位簽章可以確保寄件人的身份。並且寄件人無法否認曾經寄過這一封電子郵件。這方法適用於欲傳郵件不具私密性，但是郵件內容正確與否非常重要的郵件，例如：某一公告。

(二)加密而且加數位簽章

這是一種保護郵件內容的方式。郵件加密以後雖然每個人都可以檢驗郵件，但卻只有合法的收件人可以開啟郵件。除了可以確保寄件人的身份外，寄件人也無法否認曾寄出信件。這個方法適用於具有私密性的郵件，加上數位簽章後還可以確保郵件的來源是否正確。

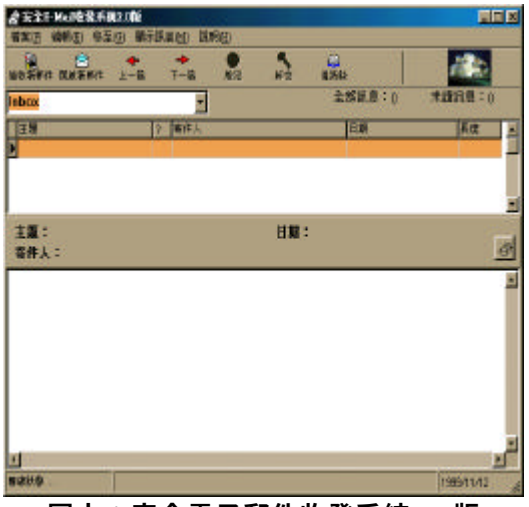
(三)不加密也不加數位簽章

這種方式是最簡單的傳送方式。不對郵件加密，也無法確定寄件人的身份，寄件人可以否認。系統會直接傳送這樣的電子郵件內容。

寄出加密的郵件之前，寄件人必須先要擁有收件人的公開金鑰，因此安全電子郵件收發系統會先到個人通訊錄中查詢是否有該收件人的憑證，若通訊錄中沒有該收件人的憑證，則進一步向 NKFU 資訊認證 Server端系統查詢是否有收件人的憑證。若有收件人的憑證則下載到（寄件人的）個人通訊錄中；若沒有收件人的憑證則無法傳送加密的郵件，只能傳送具有寄信人數位簽章的郵件。

安全電子郵件收發系統發出郵件時，會將寄信人的憑證一併傳送給收件人。因此收件人在向認證中心確認寄信人的憑證有效之後，便可以利用憑證中所記錄的寄件人公開金鑰檢驗該郵件的數位簽章，以檢驗郵件是否曾遭竄改。若該封郵件是經過加密的郵件，收信人則利用自己的私密金鑰將郵件解密。

寄件人的憑證是儲存在自己的電腦裡；而產生數位簽章所需要的寄件人的私密金鑰是儲存在個人的 IC 卡或軟碟片中；檢驗數位簽章要用到寄件人的公開金鑰，則是儲存在寄件人的憑證檔中（該憑證會在郵件傳送時一併傳送給收件人）。



圖六：安全電子郵件收發系統 2.0 版

安全電子郵件收發系統收信時，系統會一併儲存郵件內容與進信人的憑證檔（因此個人通訊錄中的記錄來源有二：一為與寄件人的郵件一併寄來，另一為向 NKFU 資訊認證 Server 端系統查詢得到）。

收信時，系統會對有加上數位簽章的郵件做雙掛號處理，使用者可以決定是否要有雙掛號的處理。而該封雙掛號的回復信件，只對郵件做數位簽章，其餘的與前述發信流程相同。

安全電子郵件收發系統當然也要也可以驗證或是解密郵件內容。當收件人執行驗證功能時，系統會讀取依附在郵件內容的寄信人憑證，依憑證序號連線到憑證中心檢驗此憑證是否合法，當憑證合法時，系統才會進一步驗證信件或是將信件解密。我們的系統採用及時的連線驗證，這與一般不及時連線驗證的系統有所區別。

當收件人針對加密郵件執行解密動作時，系統會要求讀取收件人的 Private Key，系統可以透過 IC 卡或是軟碟片的方式讀取 Private Key。

透過 IC 卡讀取 Private Key 時，系統會要求使用者輸入 IC 卡密碼，密碼正確時才能獲得授權進入 IC 卡讀取資料。驗證密碼的工作由 IC 卡內部完成，因此駭客無法單純的經由破解安全電子郵件收發系統來取得 IC 卡密碼以及使用者的 Private Key。

陸、結論

本研究中實作了一個憑證管理中心，其具有憑證申請、憑證註銷、憑證查詢、憑證展期與黑名單查詢功能。

安全電子郵件的用戶端使用了 Tripple-DES 與 RSA 等密碼學技術而且搭配憑證管理中心，提供了保障隱私權、寄件人身份證明、寄件人無可否認、郵件雙掛號與保障郵件內容完整性幾項功能。

對於使用者憑證的管理則採用 IC 卡作為管理與儲存的工具。將用戶憑證儲存在 IC 卡中，提供周全的保密措施，免去使用者保管憑證的麻煩。

在這個架構之下，我們提供了使用者一個更加安全且方便的電子郵件環境，而且不再需要擔心憑證管理與儲存的問題。我們也期待公開金鑰的系統可以應用在更廣的範圍，例如電子商務、電子資料交換…等。為國人帶來更方便、更安全的網路環境。

柒、參考文獻

1. Charlie Kaufman, Radia Perlman, Mike Speciner, *Network security, Private Communication in a Public World*, Prentice Hall
2. ITU-T Recommendation X.509 *Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*, 1993.
3. R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Crypto systems”, *Communications of the ACM*, Feb. 1978, Vol. 21, No. 2, pp. 120-126.
4. RSA Labs Frequently Asked Questions on Cryptography, http://www.rsasecurity.com/rsalabs/faq/questions.html
5. National Institute of Standards and Technology, “Secure Hash Standard”, Federal Information Processing Standard, FIPS PUB 180-1, April 1995.
6. National Institute of Standards and Technology, “Data Encryption Standard”, Federal Information Processing Standard, FIPS PUB 46-2, December 1993.
7. Jonathan B. Postel, *Simple Mail Transfer Protocol*, RFC 821, 1982.
8. Chung-Huang Yang, Shy-Ming Ju, and T.R.N. Rao, "A Smartcard-based Framework for Secure Document Exchange, " *Proc. IEEE 32nd Annual 1998 International Carnahan Conf. On Security Technology*, Washington D.C.,

USA, October, 1998, pp. 93-96.

作者簡介

葉杰榮

國立高雄第一科技大學資管系學士，現就讀於高雄第一科技大學資管系碩士班。

謝劭杰

國立高雄第一科技大學資管系學士，現服役於軍中。

謝祥尹

國立高雄第一科技大學資管系學士，現服役於軍中。

楊中皇

美國西南路易斯安那州立大學電腦工程博士，現任國立高雄第一科技大學資管系系主任。研究領域為密碼學、資訊安全、IC 卡、電腦算術與電子付款。