IC卡電子簽章的過去現在與未來

楊中皇

國立高雄師範大學 資訊教育研究所

摘要

電子簽章泛指以電子方式產生用來取代傳統的簽名或蓋章的識別物。數位簽章是密碼學用於電子簽章的一項成熟技術。數位簽章可確保資料在網路傳輸過程中未被竄改，且能鑑別傳輸者之身分，並防止事後否認傳輸之事實。IC 卡與目前常用的磁條卡比較起來具有難以偽造的優點且可內建電子簽章的功能。本文討論 IC 卡電子簽章的實作歷史，並探討 IC 卡的安全管理。

關鍵詞：電子簽章，數位簽章，IC 卡，智慧卡，認證

一、前言

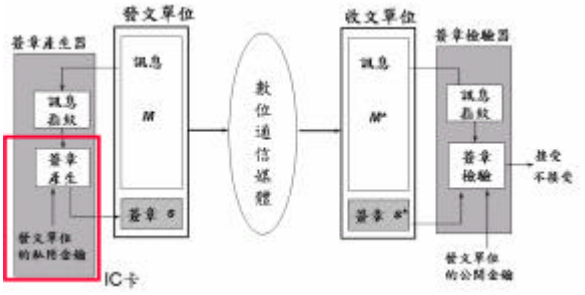
網際網路於近年快速成長，但也隨之產生網路安全的問題。網路安全首要的議題便是如何確認使用者的身分。我國於九十年通過的電子簽章法[1]賦予電子簽章(electronic signature)與數位簽章(digital signature)之法律效力。數位簽章是密碼學(cryptography) [2]中有二十多年歷史的成熟技術，可在網路上提供不可否認的使用者認證功能。

傳統上，密碼學之技術主要用於軍事與外交方面，研究成果也常因所謂的國家安全因素，而無法公開。然而隨著網際網路與全球資訊網(WWW)的極速成長，網路安全問題也一再浮現出來。使用密碼學技術對網路提供最佳的安全防禦，目前電子公文、網路報稅、電子交易等係董皆內含密碼學技術。密碼系統中如果加密金鑰與解密金鑰兩者中有一者可以公開，則稱之公開金鑰密碼系統(public-key cryptosystems)，其中最著名的系統為 RSA [3]。如果加密金鑰與解密金鑰兩者皆須保密，則稱之為私密金鑰密碼系統(private-key cryptosystems)，其中最著名的系統為 AES [4]。

使用者身份認證是資訊或網路應用最基本的安全需求。近年來國內屢次發生的信用卡或銀行提款卡被盜用案件，明顯暴露出磁條卡儲存的資料無法被有效地保護，而磁條卡與個人識別碼(PIN)的結合僅能提供薄弱的單向使用者身份認證(user identity authentication)功能，更不適合在公開網路上提供使用者身份認證功能。IC卡[5]是一個低成本難以仿造的硬體裝置，它可用來儲存密碼學金鑰與公開金鑰憑證，且使用內含電子簽章[1]機

制的 IC 卡更可在網際網路或任何公開網路上提供使用者身份認證及資料認證的功能。

電子簽章可取代傳統的簽名或蓋章，但須確保資料在網路傳輸過程中未被竄改，且能鑑別傳輸者之身分，並防止事後否認傳輸之事實。目前網路電子簽章的使用皆是植基於數位簽章[2]的機制。數位簽章採用公開金鑰密碼系統，它將一串數字(例如 300 位數字) 依附於要保護的資料。數位簽章的運作(參考圖一)是利用每個機構或使用者各自擁有成對的公開金鑰與私密金鑰，而傳輸者根據自己的私密金鑰製造數位簽章。數位簽章檢驗容易，可由任意第三者根據傳輸者的公開金鑰辨認數位章的真偽。

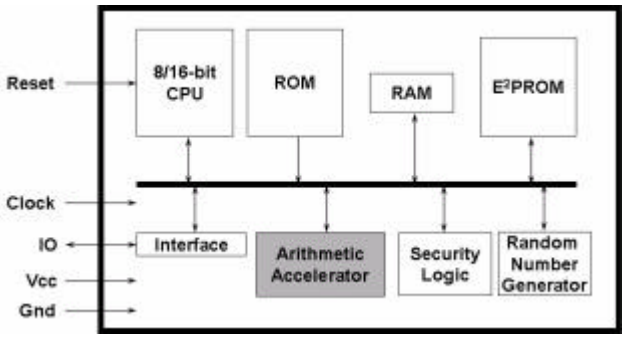


圖一：數位簽章的產生與檢驗

我國政府積極推行 IC 卡已有十多年的歷史，IC 卡在業界的應用也日趨廣泛。然而 IC 卡的晶片猶如電腦，外觀可能相似但實際上有多種差異性極大的規格。IC 卡電子簽章系統設計不善或管理不良時，依舊可能產生弊端。IC 卡可支援多種應用，所以不僅儲存的是一個金鑰(對)而已，不同用途的金鑰與公開金鑰憑證也可事先規劃好空間，放在同一張 IC 卡內，達到一卡多功能的應用。IC 卡讀卡機的介面目前有 RS-232、USB、PCMCIA、3.5 吋磁片等，隨著 Windows2000/XP 的內建 PC/SC 接觸式 IC 卡讀卡機驅動程式庫，同時 IC 卡讀卡機的價格也日益便宜(內政部自然人憑證 IC 卡搭配的 USB 介面接觸式 IC 卡讀卡機一台僅須 NT$350)，這使得 IC 卡越來越適合各種網路安全應用。IC 卡除了資料傳輸速度較慢外，方便性與內部功能都能符合網路安全的要求，且接觸式 IC 卡與讀卡機價格低廉，所以我們以下的討論也將限於接觸式 IC 卡。

二、IC 卡

我國政府積極推行IC卡已有十多年的歷史，IC卡在國內各界的應用也日趨廣泛。IC卡與目前常用的磁條提款卡與信用卡比較起來具有難以偽造與記憶體容量較高的優點。然而如果我們檢視金融IC卡(十多年前的第一代與目前的第二代)、電子公文IC卡、自然人憑證IC卡、以及健保IC卡等的規格，可知IC卡外觀相似但實際上有多種差異性極大的規格，不僅在通信協定與內部密碼學演算法的功能有差異，而且在安全管理等級也有極大的差異。



圖二：接觸式 IC 卡的內部結構

參閱圖二，IC卡晶片內部至少有個八(或十六或三十二)位元中央處理器(CPU)，唯讀記憶體(ROM)、電流可消除可程式唯讀記憶體(EEPROM)、及隨機存取記憶體(RAM)等。晶片的ROM記憶體區域是用來儲存作業系統程式和儲存密碼運算法程式或其他固定的應用程式；EEPROM記憶體區域是用來儲存個人化的資料(如私密金鑰、公開金鑰憑證)或其他易更動的應用程式；RAM則是供暫時性運算變數資料儲存用。算術加速器(arithmetic accelerator)提供快速的數論相關基礎運算，能快速完成數位簽章或公開金鑰演算法。亂數產生器(random number generator)可用在密碼學金鑰產生或用於數位簽章產生。

IC卡晶片作業系統(chip operating system)的功能包括提供外界通信協定(T=0，T=1等)，儲存密碼學金鑰於晶片內部EEPROM記憶區域，接受晶片外部呼叫資料加解密及數位簽章等演算法的命令，監控命令的執行過程，及命令錯誤特殊狀況的處理等。

IC卡有它的生命週期(life cycle)，包括使用者需求、設計、製造、發行、使用、結束等六個階段。每個階段都有個別安全管理[6]的需求，且每個階段的活動與IC卡的種類有關。能執行程式的IC卡(有時稱之為智慧卡)可分為表一所示的四種[7]，每種IC卡有自己的生命週期階段活動也有可能受到攻擊的弱點與安全管理需求。四種智慧卡(以下簡稱IC卡)中，可重組(Reconfigurable) IC卡提供多用途且可在發卡後下載新的應用程式至IC卡EEPROM區域，所以逐漸成為主流。

IC卡可支援多種應用，所以IC卡不僅儲存的是一個金鑰(對)而已，不同用途的金鑰與公開金鑰憑證也可事先規劃好空間，放在同一張IC卡內，達到一卡多功能的應用，而且涵蓋金融(電子商務及付款)、安全電子訊息、身分識別、安全資訊儲存、存取控制等多種應用。

表一：智慧卡的種類

種類	說明
1. 軟罩(Soft Mask) IC卡	應用程式放在EEPROM區域執行
2. 硬罩(Hard Mask) IC卡	應用程式放在ROM區域執行
3. 特定(Proprietary) IC卡	針對某一特定系統設計的IC卡
4. 可重組(Reconfigurable) IC卡	允許高階語言的應用程式於IC卡發行後透過卡片內的虛擬機器(virtual machine)執行。例如：MultOS卡、Java卡、Smart Card for Windows

三、IC卡安全管理

成熟的電子簽章技術須輔以合適的安全管理規範與合適的說明文件，否則就算要求廠商提供(數以千計的)原始程式碼，我們將無法研讀及確保電子簽章技術已在IC卡內適當地實現。雖然資訊技術安全評估共通準則(Common Criteria for

Information Technology Security Evaluation，簡稱CC) [6]安全等級的高低無法用來代表產品的絕對安全性，然而安全等級至少代表產品從設計到製造到安全評估的嚴謹程度。IC卡的CC安全等級可達到EAL 4。表二從IC卡的軟硬體描述開始，簡要說明IC卡安全管理[6,7]的步驟。

表二：IC卡安全管理

步驟	說明
1. IC卡描述	● 微處理器硬體規格 ● 記憶體種類(ROM、EEPROM、RAM等)、大小與位址配置 ● 實體IC積體電路佈局圖 ● 所有啟動與未啟動的硬體安全功能 ● 所有啟動的硬體安全功能 ● 軟體規格 ● 所有啟動與未啟動的軟體體安全功能 ● 所有啟動的軟體體安全功能 ● 狀態圖
2. 安全環境	■ 操作時的環境假設 ■ 可能受到的威脅 ■ 安全政策
3. 安全目的	● 保護資料避免被揭露或竄改 ● 使用者與系統管理者身分認證 ● 應用程式的控制管理 ● ... ...
4. 安全需求	● 功能需求 ● 安全確保需求

表二步驟一的IC卡描述裡的狀態圖包括“電源加入狀態”、"未初始化狀態”、“未定義狀態”、“未認證狀態”、“認證狀態”、“封鎖狀態”等IC卡在與外界聯繫時自我偵測到的狀態。IC卡的某些高安全性功能必須在合適的認證狀態才可被執行。

IC卡安全環境包括對操作環境的假設，例如IC卡的發展工具與生產製造過程可能假設是受到保護不被未授權使用或偷竊，IC卡與外界通信用的交換金鑰的產生也可能假設是安全的，外界傳送到IC卡的資料與程式碼亦可能假設是安全的。IC卡安全環境可能受到的威脅包括實體攻擊(例如利用電子探測棒去更改資料或是操控IC卡輸入的電壓與時鐘脈波)、邏輯攻擊(例如對IC卡輸入不正常的資料)、存取控制(例如試圖使用未經開卡的IC卡)、密碼學功能攻擊(例如以暴力攻擊法或分析加密過的資料)等。IC卡安全環境的安全政策指的是密碼學演算法的金鑰長度與應用程式控制等。

IC卡安全需求的安全功能需求(functional requirements)與安全確保需求(assurance requirements)是取自ISO 15408文件第二部分與第三部分。安全功能需求分為七類；密碼學支援(cryptographic support)、使用者資料保護(user data protection)、身分證明與確認(identification and authentication)、安全管理(security management)、安全功能的保護(protection of the security functions)、資源利用(resource utilization)、可信賴的通道(trusted path/channels)等。進一步的IC卡安全需求可參考ISO 15408 [6]及美國國防部符記保護剖繪(token protection profile) [7]。

為了要確保密碼學演算法的具體實現無誤，便有賴於密碼模組[8]的檢驗。依據NIST的定義密碼模組可以是硬體元件或模組、軟體韌體程式或模組、或它們的組合。美國於於2001年修正通過FIPS 140-2規範[8]，並為目前國際上業界公認的密碼模組標準，用來驗證密碼學演算法的實現。FIPS 140-2標準訂定密碼模組的四種安全等級，從最低要求的第一級到最高階的第四級，每個安全等級各須滿足11個安全要件。每個安全等級的共同基本需求包括模組輸出入及控制與狀態介面的描述、至少須實現一個核定的密碼學演算法、模組啟動時自我測試密碼學演算法、模組安全政策的定義、授權角色與安全服務的說明、驗證機制的選擇、以及模組須以有限狀態機器描述等。IC卡內部密碼學演算法模組也應通過FIPS 140-2的檢測。

四、電子簽章演算法

電子簽章須確保資料在網路傳輸過程中未被竄改，且能鑑別傳輸者之身分，並防止事後否認傳輸之事實。上述圖一數位簽章的產生與檢驗用到兩類演算法：訊息指紋(message fingerprint)演算法與簽章演算法。表三列出目前常用的數位簽章相關演算法。以下我們簡要描述表三的演算法。

表三：IC卡數位簽章演算法

演算法種類	演算法
1. 訊息指紋演算法	MD5、SHA-1、SHA 256、SHA 384、SHA 512
2. 簽章演算法	RSA、DSA、ECDSA

訊息指紋演算法又被稱為單向雜湊函數(one-way hash function)或訊息摘要(message digest)演算法。1990年之前的數位簽章多不採用訊息指紋演算法，而傳輸者將整個訊息用自己的私密金鑰予以加密形成簽章，接收者再用傳輸者的公開金鑰予以解密同時檢驗簽章。如果要簽章的訊息長度較長，則須將訊息切成數個區塊(block)，每個區塊個別以私密金鑰加密，整個數位簽章的產生速度變慢。訊息指紋演算法可將任一長度的輸入訊息計算出一個固定長度的訊息指紋值。設計優良的訊息指紋演算法都有強碰撞抵抗性(strong collision resistance)，也就是說實務上我們找不到兩個不同的輸入訊息而計算出相同的輸出訊息指紋。MD5 [9]為1992年IETF的RFC 1321標準，它的前身為1990年IETF的RFC 1186標準MD4。MD5訊息指紋輸出固定為128位元，目前廣泛用於瀏覽器。

美國國家技術標準局(NIST)於1995年修訂公佈SHA-1 [10]的訊息指紋演算法則可以計算產生160位元的訊息指紋。由於訊息指紋演算法的安全度取決於訊息指紋的長度，128位元的MD5安全度約為2^{64}，160位元的SHA-1安全度約為2^{80}。2002年NIST公佈的FIPS 180-2 [10]提出SHA-256、SHA-384、SHA-512三個訊息摘要長度各為256位元、384位元、512位元的雜湊函數演算法，它們的安全性各約為2^{128}、2^{192}、2^{256}。訊息摘要長度較大時，雖較安全但執行速度會較慢。

表三的三種簽章演算法中，RSA [3]公開金鑰密碼系統可用數位簽章或金鑰交換，但RSA用於數位簽章時速度慢，而NIST於1991年公佈數位簽章專用的DSA (Digital Signature Algorithm) [11]演算法用於數位簽章時速度較快。橢圓曲線密碼系統(Elliptic Curve Cryptosystem, ECC) [12,13]則是近年開始被採用的密碼學演算法技術，且近年

來已被廣泛地制訂於國際標準如ISO 11770-3、ANSI X 9.62、IEEE P1363 等。在相同的安全強度下, ECC的密碼學參數可遠較諸如RSA的其他公開金鑰密碼系統為小，這代表IC卡儲存ECC演算法的金鑰或公開金鑰憑證時能節省EEPROM的空間。ECDSA（Elliptic Curve Digital Signature Algorithm，DSA）[14]是將DSA內部的數學運算改用橢圓曲線的一種數位簽章標準。

RSA公開金鑰密碼系統[3]是1977年美國麻省理工學院三位教授共同發明。在這系統中每個使用個體(entity)有一組成對的金鑰：公開金鑰與秘密金鑰。公開金鑰可以讓大眾知道它的內容，而秘密金鑰則要安全地保管(例如存放在IC卡內)。RSA密碼系統的安全原理是基於兩個大整數相乘得到乘積容易，而去分解兩個大整數的乘積則是很難(美國RSA公司甚至有總獎金超過美金六十萬元的有獎懸賞[15])。RSA公開金鑰系統的使用方式為：

1. 個體首先自行挑選兩個大質數(例如 512 位元，可以用硬體或軟體產生)， p和 q。
2. 個體再選個正整數 e滿足 $\gcd(e,(p-1)(q-1))=1$，意即 e與 $(p-1)*(q-1)$的最大公因數為 1。
3. 最後利用歐基里得輾轉相除法(extended Euclidean algorithm)，計算出一個唯一正整數 d，滿足(符號 mod 代表模運算)

$$d\times e=1 \mod (p-1)\times(q-1)$$

RSA 個體的公開金鑰為 e與 n (= p x q) ，可以到處公開，而私密金鑰為 d與 p及 q由自己保管。RSA不僅能用在數位簽章，也適用在數位信封做金鑰加解密。假設 $H(M)$代表訊息 M 的訊息指紋值，那麼 RSA 數位簽章的產生與檢驗可簡單描述如下

(1) RSA 簽章產生：用私密金鑰 d與公開金鑰 n以下列公式計算簽章 s

$$s = H(M)^d \bmod n$$

(2) RSA 簽章檢驗：將收到的訊息 M重新計算訊息指紋值 $H(M)$。若且唯若下列公式成立則接受簽章，否則拒絕簽章。

$$H(M) \stackrel{?}{=} s^e \bmod n$$

實務上我們可以使用中國剩餘定理(Chinese Remainder Theorem)來加速 RSA 簽章的產生，此時除了金鑰 n、p、q、e、d之外，我們需有 $d \bmod p-1$、$d \bmod q-1$、$q^{-1} \bmod p$。這些數值將儲存於 IC 卡的 EEPROM 區域供數位簽章的產生與檢驗用。

NIST數位簽章專用的DSA演算法使用方式為：

1. 系統首先決定一個 160 位元的質數 q及 512 位元到 1024 位元的質數 p，但是 $p-1$必須是 q的倍數。
2. 系統再找個生成數(generator of a cyclic group) g滿足

$$g^q = 1 \bmod p$$

3. 個體挑選介於 1 與 q-1 的亂數 x當做自己的私密金鑰，再計算公開金鑰 y，

$$y = g^x \bmod p.$$

假設 $H(M)$代表訊息 M 的訊息指紋值，那麼 DSA 中，對應於訊息 M的簽章(r, s)產生步驟如下:

1. 產生介於1與n-1的亂數k.
2. 計算$r = (g^k \bmod p) \bmod q$.
3. 計算$s = k^{-1} \{H(M) + x\ r\} \bmod q$,
4. 如果 $s = 0$，則回到步驟1。

DSA 簽章檢驗的步驟如下:

1. 計算$w = s^{-1} \bmod q$ 及 $H(M)$.
2. 計算$u_1 = h(m)w \bmod q$ 及 $u_2 = rw \bmod nq$.
3. 計算$v = (g^{u_1} y^{u_2} \bmod p) \bmod q$.

若且唯若 $v = r$ 接受簽章，否則拒絕簽章。

橢圓曲線密碼系統其最大優點為可用較其他系統短的位元數，例如 ECDSA 簽章演算法金鑰長度為 160 位元時與 1024 位元 RSA 二者的安全度是相等的。因此在相同的安全強度下，ECDSA 軟體執行速度比 RSA 系統快，同時可節約金鑰儲存空間, 但 ECC 需要較複雜的運算且背後的數學理論不易說明與理解，這是它的缺點。ECC 執行速度快慢的決定因素是在點乘法(Point Multiplication) 的效率上。點乘法是計算 $k \cdot P$, 其中 k 為 160 位元以上之整數而 P 為事先選取的橢圓曲線上的一個點

$$k \bullet P = \overbrace{P + P + \ldots + P}^{k \quad times}$$

ECDSA [12-14]中，系統首先須挑選一條合適的橢圓曲線及選取域 (field)，然後須挑選價(order)為 n 的基點(base point) G。個體自行挑選介於 1 與 q-1 的亂數 d 當做自己的私密金鑰, 再用點乘法計算公開金鑰 Q

$$Q = dG$$

ECDSA 對應於訊息 M 的簽章(r, s)產生步驟如下:

1. 產生介於1與n-1的亂數k.
2. 計算$kG = (x_1, y_1)$ 及 $r = x_1 \bmod n$.
3. 如果$r = 0$, 則回到步驟1。
4. 計算$s = k^{-1} \{H(M) + dr\} \bmod n$,
5. 如果 $s = 0$, 則回到步驟1。

ECDSA 簽章檢驗的步驟如下:

1. 計算$w = s^{-1} \bmod n$ 及 $H(M)$.
2. 計算$u_1 = H(M)w \bmod n$ 及 $u_2 = rw \bmod n$.
3. 計算$u_1G + u_2Q = (x_0, y_0)$ 及 $v = x_0 \bmod n$.

若且唯若 $v = r$ 接受簽章，否則拒絕簽章。

四、IC 卡電子簽章的演進

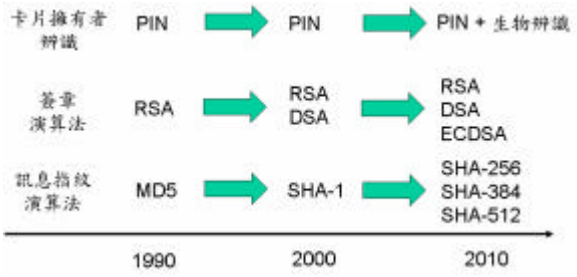
1992 年美國政府正在發展 DSA (簽章演算法時，曾以內含 H8/300 八位元中央處理器的智慧卡晶片(當時 RAM 僅有 256 位元組，ROM 有 10K 位元組，EEPROM 有 8K 位元組，也不具備算術加速器)評估 512 位元 DSS 與 RSA 的效率[16] (雖然目前對 RSA 密碼系統的金鑰長度要求 1024 位元，但十年前 512 位元已經夠安全)。假設 H8/300 晶片內部時鐘假設為 5MHz，表四說明 DSS 由於數位簽章較費時，所以宜採用事先計算(pre-computation)的方式，先將與亂數有關的事先計算處理，而 RSA 不適用此種方式。同年日本 NTT 也在同一智慧卡晶片評估其 ESIGN 演算法的效率[17,18]，結果同列於表四，因為 576 位元 ESIGN 簽章可以快速算出，所以不需要進行事先計算。

表四：1992 年三種不同數位簽章演算法的 IC 卡效率(H8/300 CPU)

公開金鑰演算法	512-bit DSS	512-bit RSA	576-bit ESIGN
事先計算	28 秒	不適用	不需要
簽章產生時間	0.05 秒	25 秒	0.45 秒
簽章檢驗時間	56 秒	5 秒	0.27 秒

過去十年中, 我們看到 IC 卡晶片的功能有顯著的成長，記憶體容量大幅增加，且目前多內建數位簽章演算法能於一秒鐘內產生 1024 位元的 RSA

簽章。然而晶片的大小受限於 IC 卡的規範，長寬皆必須小於 1 公分，這使得它的資源有限，實現演算法時也較個人電腦困難。圖三列出 IC 卡內部電子簽章的發展歷程，在訊息指紋演算法方面目前多已採 SHA-1，且將逐漸改為更安全的 SHA-256/384/512。



圖三：IC 卡電子簽章的發展歷程

DSA/ECDSA 的簽章長度可遠較諸如 RSA 的金鑰密碼系統為小，這代表 IC 卡儲存金鑰或公開金鑰憑證時能節省 EEPROM 的空間，放更多資料。然而由於 DSA/ECDSA 的實現時會用到模運算(modular arithmetic)，這使得開發 DSA/ECDSA 簽章時通常可輕易開發 RSA 簽章，且 RSA 簽章容易理解，所以未來我們應仍將看到 IC 卡內建 RSA 簽章。

目前 IC 卡擁有者使用時需輸入個人識別碼(PIN)作為卡片控管用，然而隨著生物辨識(指紋、顏面、語音等)技術的發達，我們將逐漸看到用生物辨識技術來控管卡片。個人的生物辨識資料可放於 IC 卡內，經過辨識後輔助或取代 PIN 的功用，然後啟動 IC 卡電子簽章的功能。

五、結論

一卡多功能的 IC 卡具有攜帶方便以及安全性高的特性，可以提供電子簽章等的網路安全功能。隨著低廉 IC 卡與讀卡機的逐漸普遍，我們可預見 IC 卡電子簽章的應用將更深入日常生活，帶給我們更方便與安全的網路應用環境。

參考文獻：

[1] 經濟部商業司，電子簽章法，http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm, (2004)

[2] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, http:// www.cacr.math.uwaterloo.ca/hac/, (1996)

[3] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, Vol. 21, No. 2, pp. 120-126, (1978)

[4] NIST, Advanced Encryption Standard (AES), FIPS 197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, (2001)

[5] W. Rankl and W. Effing, Smart Card Handbook, 3rd edition, John Wiley & Sons, (2003).

[6] ISO/IEC 15408 — Information technology — Security techniques — Evaluation criteria for IT security (Common Criteria, CC, Version 2.1) — Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements, (1999)

[7] Department of Defense, Public Key Infrastructure and Key Management Infrastructure Token Protection Profile V3.0, http://www.niap.nist.gov/cc-scheme/PP_PKIKMITKNPP-MR_V3.0.pdf, (2002)

[8] NIST, Security Requirements for Cryptographic Modules, FIPS 140-2, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf, (2001)

[9] R. Rivest, "The MD5 Message-Digest Algorithm," IETF RFC 1321, (1992)

[10] NIST, Secure Hash Standard (SHS), FIPS 180-2, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf, (2002)

[11] NIST, Digital Signature Standard (DSS), FIPS 186-2, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf, (2000)

[12] A. Menezes, Elliptic curve public key cryptosystems, Kluwer, (1993)

[13] I. F. Blake, G. Seroussi and N. P. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series, Vol. 265, Cambridge University Press, (1999)

[14] ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), (1999)

[15] The RSA Challenge Numbers, http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html, (2004)

[16] ISO TC68/SC21 **會議資料，**(1992)

[17] C.H. Yang, "Modular Arithmetic Algorithms for Smart Cards," IEICE Technical Report on Information Security (**日本電子資訊通信學會資訊安全技術報告**), ISEC92-16, August, (1992)

[18] **楊中皇，密碼學演算法於** IC **卡上的具體實現，資訊安全通訊，第八卷第三期，**8-17**，**(2002)

Electronic Signature based on IC Cards: Past, Present and Future

Chung-Huang Yang

Graduate Institute of Information and Computer Education, National Kaohsiung Normal University

Abstract

Electronic signature means an electronic identifier and intended by the party using it to have the same force and effect as the use of a handwritten signature. Digital signature is by far one of the most important cryptographic techniques used in the electronic signature applications. It provides authentication of senders or receivers and offers non-repudiation of transmission. IC cards are much more difficult to duplicate than magnetic strip cards and electronic signature functions can be implemented inside these cards. In this paper, we describe the history of IC card used for electronic signature and discuss the security management issues.

Keywords：Electronic Signature, Digital Signature, IC Card, Smart Card, Authentication