網路安全的理論與實務

楊中皇 著

第九章 IC卡

http://crypto.nknu.edu.tw/textbook/

第九章 IC卡

- IC卡概論
- IC卡安全管理機制
- IC卡應用

IC卡與磁條卡

- 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。
- 相較之下，現有一般常用之磁條卡(如信用卡)有兩種缺點：
  - 安全性: 磁卡上沒有保密的技術，故任何人只要拿到磁卡和讀磁卡的機器，此磁卡上的資料便被人一覽無疑了，所以我們常可看到信用卡側錄僞卡的媒體報導。
  - 容量: IC卡記憶容量大，資料可重複多次寫入或更新，具有發展爲多目的、多功能卡的潛力。相對於IC卡，目前市場上較普遍之而磁條卡的記憶容量僅約爲100個位元組，磁條卡無法包含應有的憑證或金鑰資訊，並沒有辦法達到電子商務的用途，所以較難使用。

接觸式與非接觸式IC卡

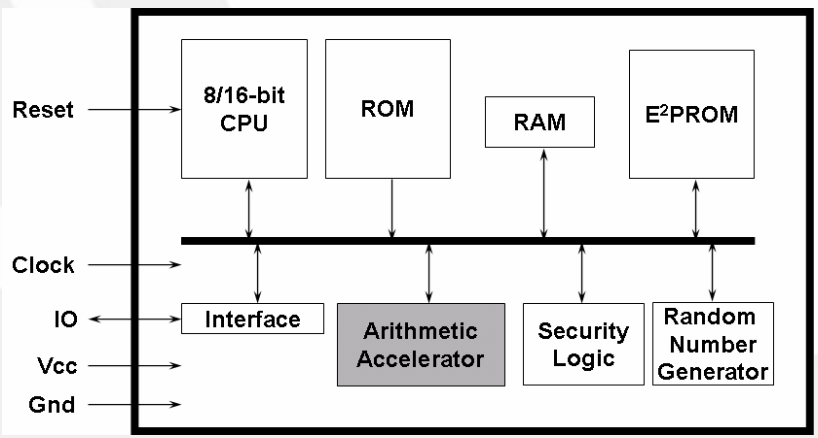
- IC卡可分爲接觸式與非接觸式兩種，前者歷史悠久且功能強大，後者則目前功能較簡單且多爲單一用途
- 國內常見的非接觸式IC卡爲Philips公司的MIFARE非接觸式IC卡，使用感應線圈傳遞資料至讀卡機。晶片內共有1K位元組的記憶體EEPROM，記憶體分成16個相互獨立的區段(sector)，每一個區段由4個區塊(block)組成，每一個區塊的大小是16位元組。MIFARE IC卡不需外加電池，以無線加密傳送資料。

國內常見IC卡之比較

	主要優點	主要缺點
電話IC卡	價格低且技術成熟	安全性低且記憶容量小
金融IC卡	中價位且內含密碼學機制	金鑰管理不易且DES安全性受到質疑
含數位簽章之IC卡	安全性高且記憶容量大	價格高

接觸式IC卡的內部結構

- 接觸式IC卡晶片內部至有包括一個八(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



晶片作業系統(chip operating system，COS)

- IC智慧卡晶片作業系統(chip operating system，COS)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
- 智慧卡核心的COS開發時有賴發展工具，開發時多須以組合語言撰寫COS程式。

智慧卡的種類

種類	說明
軟罩(Soft Mask) IC卡	應用程式放在EEPROM區域執行
硬罩(Hard Mask) IC卡	應用程式放在ROM區域執行
特定(Proprietary) IC卡	針對某一特定系統設計的IC卡
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

IC卡安全管理

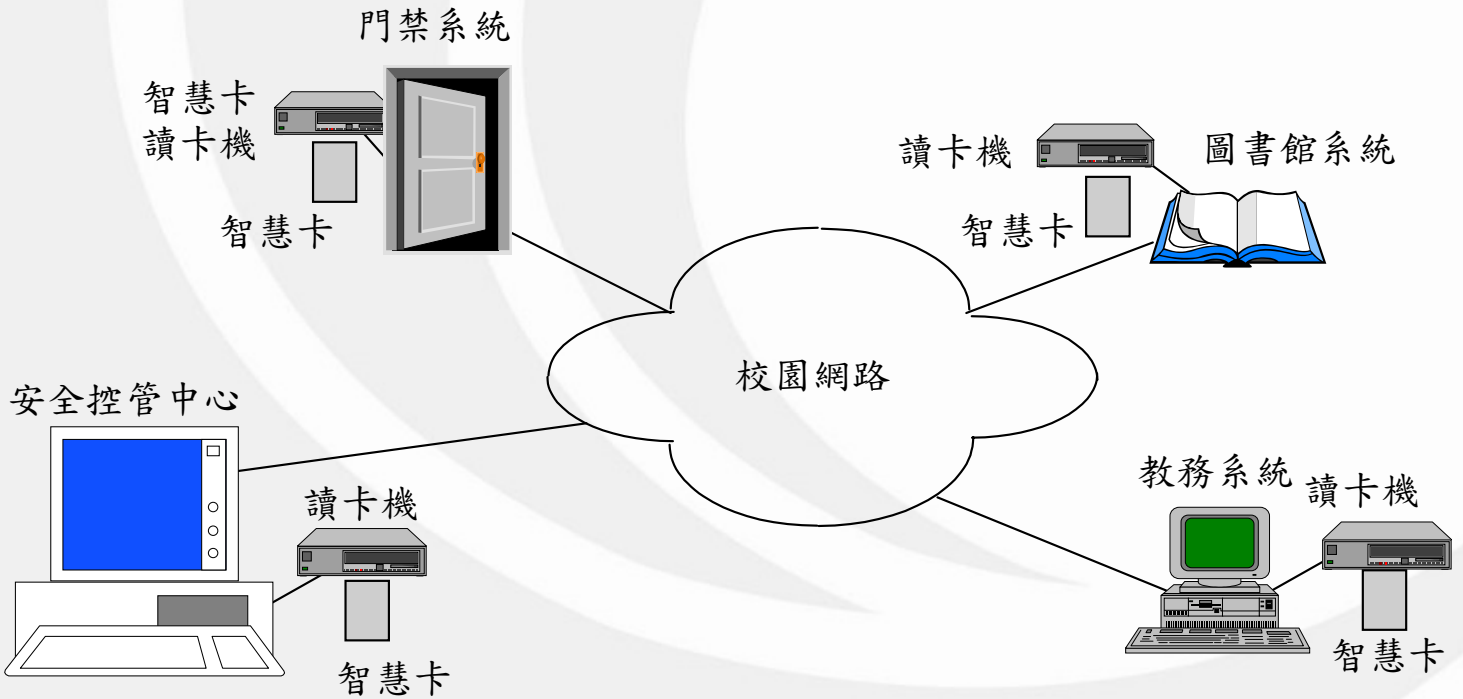
步驟	說明
IC卡描述	微處理器硬體規格 記憶體種類(ROM、EEPROM、RAM等)、大小與位址配置 實體IC積體電路佈局圖 所有啟動與未啟動的硬體安全功能 所有啟動的硬體安全功能 軟體規格 所有啟動與未啟動的軟體體安全功能 所有啟動的軟體體安全功能 狀態圖
安全環境	操作時的環境假設 可能受到的威脅 安全政策
安全目的	保護資料避免被揭露或竄改 使用者與系統管理者身分認證 應用程式的控制管理 ... ...
安全需求	功能需求 安全確保需求

IC卡應用

- 目前(校園)網路的資訊安全措施以使用防火牆爲主，並以通行碼(password)提供使用權限控制(access control)與基本網路稽核控管功能。這可防止未經許可的系統資源被使用，並可管制遠端登錄(telnet)或檔案傳送(file transfer protocol，ftp)的網路服務
- 雖然以防火牆及通行碼(password)可提供基本的資訊安全功能，但仍需要進一步的防護措施。例如遠端登錄或檔案傳送時，使用者須輸入通行碼以驗證身份；但如果網路沒有保密的功能便很容易爲別有用心者在網路傳遞過程中擷取通行碼等相關訊息
- 以硬體做資訊安全控管不但安全性高，且使用方便。在硬體的技術上，當然可將安全系統以傳統式的電腦外加卡(add-on card/board)實現，但其成本高不易大量推廣。新一代的智慧IC卡雖然界面通訊速度仍然偏低，但同時具有成本低及安全性高(內部含有數學運算加速器)優點，我們可將IC卡應用於(校園)網際網路系統內，以低成本高安全性之可攜式硬體裝置來提供校園資訊安全功能。

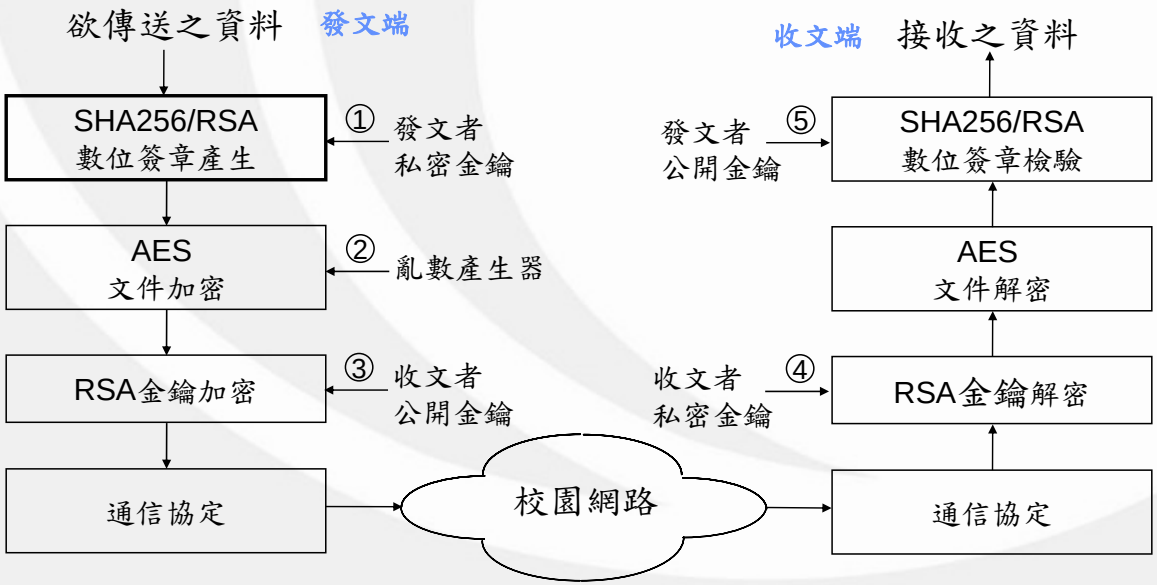
結合IC卡建構校園網路安全系統

- 以端對端安全架構爲主，依據使用的應用軟體進行端對端資訊安全設計
- 使用時每個單位或個人配備IC卡的安全裝置來做身份的認證與數位簽章的產生，用戶端爲配備IC卡讀卡機之個人電腦。在安全控管中心須具備認證中心(certificate authority, CA)與目錄伺服器(directory server)的功能。我們以智慧IC卡爲基礎，採用密碼學的理論，以公開金鑰密碼系統及私密金鑰密碼系統來達成校園網路內如門禁系統、教務系統等的無可爭議、認證、責任性等網路安全功能



網路資料安全通信架構

- 發文單位首先將準備好的資料計算其單向雜湊函數SHA256值，再將此值輸入至已個人化(personalized)的智慧IC卡內，由智慧IC卡根據內存自己單位的私密金鑰計算出1024位元RSA數位簽章(步驟1)。發文單位然後將此資料用AES128私密金鑰密碼演算法予以加密(步驟2)。資料加密時所用到的「加密金鑰」則根據收文單位於1024位元RSA 公開金鑰密碼系統上對外公開的加密金鑰予以加密後(步驟3)與加密資料訊息一起透過校園網路傳送出去
- 在收到加密後之資料時，收文單位先以其於RSA公開金鑰密碼系統上對外不公開之「解密金鑰」加以解密出文件金鑰，再用事先約定好的AES128私密金鑰密碼系統將文件恢復成未經加密前的資料原狀。最後，收文單位根據發文單位的公開金鑰與收到的數位簽章元素值，辨認簽章的真偽。如果它們匹配，收文單位便可確保收到的資料的確來自該發文單位，且在傳送的過程中並未被竄改。



參考資料

- 何大可等，多功能校園卡—IC卡應用系統實例，第五屆中國密碼學學術會議論文集，1998, pp. 155-159。
- 楊中皇，校園IC卡的資訊安全系統設計，第十屆國際資訊管理學術研討會論文集，1999年6月，pp. 614-618。
- 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，2002，8-17。
- 楊中皇，IC卡電子簽章的過去、現在與未來，陸軍軍官學校基礎學術研討會，2004年5月。
- 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.
- W. Rankl and W. Effing, *Smart Card Handbook*, 3rd edition, John Wiley & Sons, (2003).
- M. Hendry， *Smart Card Security and Applications*，Artech House, Inc., 1997.