第二十七章

密碼學機制在電子檔案保護之應用

Cryptology Mechanism for Electronic Records Protection

吳宗成

Tzong-Chen Wu

國立台灣科技大學資訊管理系暨研究所

Professor, Department of Information Management,

National Taiwan University of Science & Technology

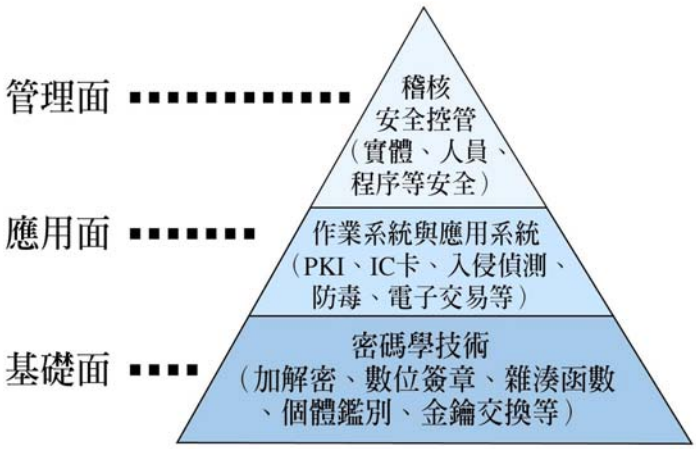
壹、前言

資訊科技(Information Technology, IT)的蓬勃發展，爲個人、企業、政府等相關實務之電子化或資訊化環境帶來催化作用。電子化或資訊化的內涵並非只是將人工作業單純地改由利用資訊科技的自動化作業而已，而是在於能將讓實體文件資料虛擬化或系統化，輔與組織管理及流程再造，促成生產效能的增加、成本的降低與資源的分享，進而達到具整合性與競爭性的策略目標[2]。因此之故，個人、企業、政府機構，每年均投入相當多的經費與人力資源，積極推動電子化或資訊化工作。

建置資訊系統(Information System, IS)以遂行管理實務或提供服務是資訊化的首要步驟。一個資訊系統是由五個基本元件組成[1]：軟體(software)、硬體(hardware)、資料(data)、人員(people)、程序(procedure)，而資料是資訊系統的核心，也是資訊系統的價值所在，而建立安全的傳輸或儲存環境，遂行資料或資源的分享，方能顯現資料的應用價值。一個好的資訊系統應能提供使用者正確、及時、完整、可存取、與具相關性的資料[2]。因此，除了考量運算效能與可靠度之外，

涵蓋技術面與管理面的資訊安全議題更是資訊系統之建置與營運成功與否的關鍵指標。

圖一爲整體資訊安全體系架構圖。

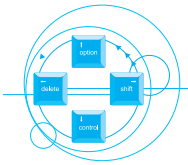


圖一　資訊安全體系架構

在實務應用上，資料通常以電子檔案形式存在。私人企業機構常見的有價值資料有營運計畫書、產品訂單、人事薪資等，政府機構常見的有價值資料有機關往來的公文書與執行業務所需建立的資料庫等[2]。有別於私人企業機構的電子檔案保護工作，政府機構所處理或主管的電子檔案保護機制尚須特別兼具以下幾個特性：

一、開放性：政府機構所擁有的檔案或公文書依資訊公開法相關規定，爲保障民眾權益應可提供調閱服務，而依政府機構電腦處理個人資料保護法規定又需兼顧個人隱私權益。電子檔案保護機制的採用不僅是單純的「保護」而已，尚須兼顧開放式的調閱或查詢服務功能。

二、長期性：政府機構所擁有的檔案或公文書其保存期限可長達一、二十年，但電子檔案保護機制卻往往受限於資訊科技或資訊系統的可用性。從以往實務經驗得知，大多數電子檔案保護機制的存活時間都要比檔案或公文書的保存



期限要來得短。

三、法律性：政府機構的檔案或公文書具有適法性的問題，這些檔案或公文書可回溯作爲爭議或責任歸屬之判定基礎，檔案或公文書的調閱或查詢也需依據相關法律規範（例如檔案法、行政程序法等）加以取用。電子檔案保護機制應能維護原檔案或公文書的適法性，甚至應能提供鑑識證據以作爲適法性的證明。

電子檔案保護或資源分享涉及兩項重要資訊安全技術課題：一、如何保護資料在傳輸或儲存時不會被未授權取用、更改或替代；二、如何控管系統的使用者身分不會被假冒，資料不會被非法運用。從一九八〇年代起，產業界與學術界對密碼學機制的研究發展蔚爲風潮，其應用領域也從原本侷限於國防與軍事活動的封閉用途，推廣到結合電子化政府與電子商務的多元應用。近年來，我國政府推動電子化政府或電子商務相關建設，卓然有成，在資通技術之整備度(readiness)世界評比排名上更是名列前茅。儘管如此，與其他先進國家（諸如美國、英國、法國、德國、澳洲等）相比較之下，我國電子化政府或電子商務在資訊安全技術的發展與應用上，仍存有許多努力空間。基於上述電子檔案保護機制的特性，本文將探討一些密碼學機制的運作原理，並對其在政府機構之電子檔案保護應用議題上提出開放式的討論與建議，以爲各級主管機構擬定資訊安全政策或規劃相關資訊安全系統之參考。

貳、密碼學機制運作原理

密碼學機制(cryptography)是資訊安全技術的基礎，大多是以複雜的數學計算難題（例如因數分解(factorization, FAC)、離散對數(discrete logarithm, DL)、橢圓曲線(elliptic curve, EC)等已知的計算難題）設計而成[3, 13, 15, 22, 23]。以下分別概要說明密碼學機制可達成的安全目標及其運作原理。

一、安全目標

應用適當的密碼學機制可達成機密性(confidentiality)、完整性(integrity)、鑑別

性(authenticity)、不可否認性(non-repudiation)等安全目標，各項安全目標說明如下：

（一）機密性：確保未授權者無法知曉傳輸或儲存資料的內容。透過加解密技術的使用可以達到此目的。

（二）完整性：對資料而言，確保資料在傳輸或儲存過程的正確性，未授權的更改、替代、僞造可以被偵測出來。對系統而言，確保任何使用者的身分不可被假冒，系統程式碼也無法被更改而能成功地通過檢測。透過單向雜湊函數或數位簽章技術的使用可以達到此目的。

（三）鑑別性：確保資料傳送者與接收者的身分可以唯一被識別，傳送者可以確認資料到達所指定的接收者，而接收者可以確認所宣稱的資料來源或擁有者。透過安全通信協定的使用可以達到此目的，甚而可以在開放式系統(open system)環境中建立虛擬私有網路(virtual private network, VPN)，進行秘密傳輸。

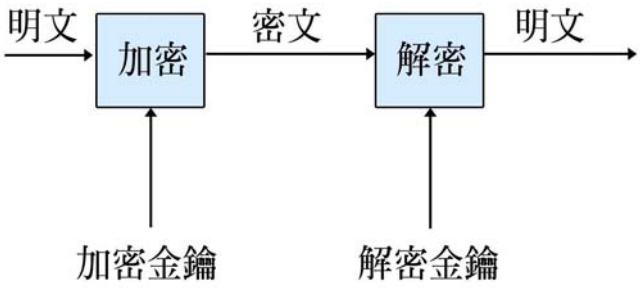
（四）不可否認性：對傳輸資料而言，可以防制傳送者否認曾經傳送過某一訊息，也可以防制接收者否認曾經接收過或知悉該訊息。對系統而言，不可否認機制將自動地留下存取活動的相關證據，以利遂行事後的安全稽核與管理工作。

二、運作原理

密碼學機制涵蓋加解密(encryption/decryption)技術、數位簽章(digital signature)技術、單向雜湊函數(one-way hashing function)、安全通信協定(security protocol)等四大類別。安全通信協定包括個體鑑別(entity authentication)協定、金鑰交換(key exchange)協定、不可否認(non-repudiation)協定等，大多是利用加解密技術、數位簽章技術或單向函數等元件加以整合而成。

- 加解密技術：加解密系統包含五個組件：原文空間(plaintext space)、密文空間(ciphertext space)、加密轉換(encryption transformation)、解密轉換(decryption transformation)、金鑰(key)，如圖二所示。原文空間或稱明文空間爲資料的原形（大多爲有意義的文數字），經過加密轉換後成爲密文空間（大多爲無意義的亂碼字串）；反之，密文空間經過解密轉換後，可以還原成原文。加密轉換與

解密轉換必須透過金鑰來加以驅動，用於加密轉換的金鑰稱爲加密金鑰，用於解密轉換的金鑰稱爲解密金鑰。若加密金鑰與解密金鑰相同，則稱爲對稱式(symmetric)密碼系統；若不同，則稱爲非對稱式(asymmetric)密碼系統。非對稱式系統的加密金鑰是公開的，又稱爲公鑰(public key)，而解密金鑰是秘密的，又稱爲私鑰(private key)，公鑰與私鑰需成對存在，而由公鑰要去推導私鑰是屬於計算不可行的難題[7]。對稱式系統大多基於排列組合難題加以設計，運算速度快，用於大量資料的處理；非對稱式系統大多基於計算難題加以設計，運算速度慢，用於少量資料處理，適合於開放式網路環境。由於運算速度慢，非對稱式加解密系統並不對資料直接加密，而是傳輸端對非對稱式加密系統所需加密金鑰（通常只有 128 或 156 位元）加密後，透過公開通道傳輸給接收端，再將大料資料以該加密金鑰加密後傳輸給接收端。加解密技術的安全度不應取決於演算法是否保密，一般而言，加解密演算法是可以公開並可成爲標準化的，以增加實用性。加解密技術的安全度取決於金鑰的長短，以目前的破解能力，現行對稱式加解密演算法的金鑰長度約爲 128~256 位元應已足夠（例如 Triple DES[16], AES[19]），非對稱式加解密演算法的金鑰長度約爲 1024 位元應已足夠（例如 RSA[21], ElGamal[8]）。隨著破密分析的進步，至少每年應檢討或評估加解密演算法所使用的金鑰長度是否滿足實務安全需求。

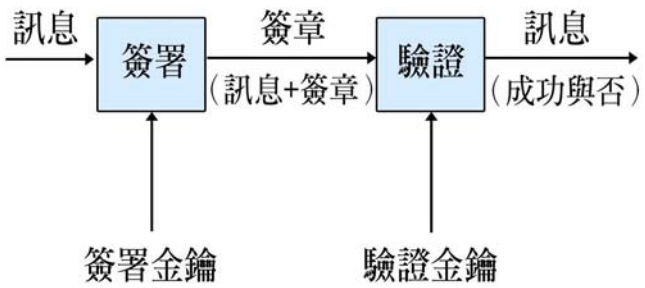


圖二　加解密運作模式

・數位簽章技術：數位簽章可用於提供文件的完整性證明，並可證明文件的擁有

者。數位簽章系統的參與角色包括簽署者、驗證者、及一個可信賴第三者(Trusted Third Party, TTP)，並包含五個組件：訊息空間(message space)、簽章空間(signature space)、簽署 (signature generation)、驗證(verification transformation)、金鑰，如圖三所示。數位簽章系統爲非對稱式密碼系統，用於簽署的金鑰稱爲簽署金鑰（私鑰），要秘密保持；用於驗證的金鑰稱爲驗證金鑰（公鑰），要加以公開，公鑰與私鑰對(key pair)要經過一個 TTP 加以背書認證，並載於憑證(certificate)中，此 TTP 稱爲憑證機構(Certification Authority, CA)[4]。數位簽章技術有兩種運作模式[18]，其一爲具附件(appendix)的簽章，另一爲具訊息復原(message recovery)的簽章。具訊息復原的簽章本身就是一種加密演算法應用，只是用私鑰（亦即簽署金鑰）來加密或簽署本文訊息，而用公鑰（驗證金鑰）來解密或驗證簽章，這種模式所產生的簽章大小與本文訊息的長度一樣。

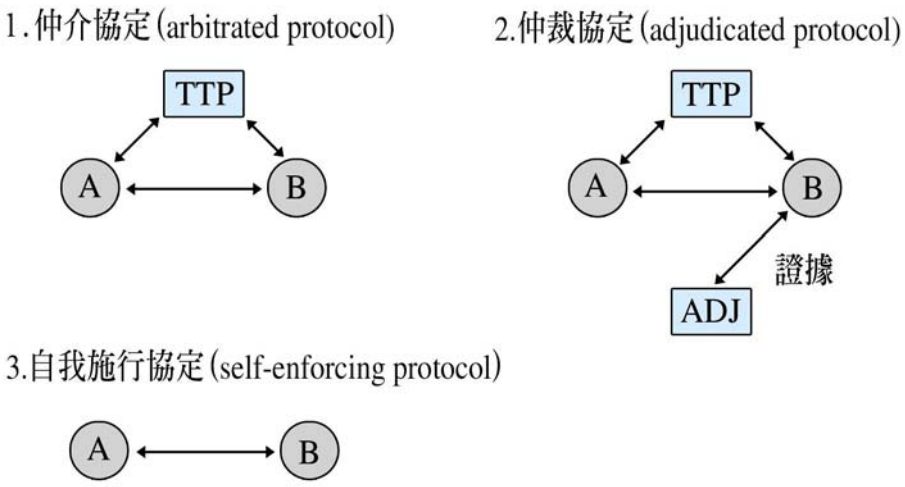
具附件的簽章在簽署時要先利用單向雜湊函數(one-way hashing function)將本文訊息轉換成固定長度的簽體或訊息彙記(message digest)，再對簽體進行簽署，並非直接對本文訊息加以簽署，這種模式所產生的簽章大小遠小於（或可忽略）本文訊息，因此，是實務上最常採用的數位簽章模式。除了一般用於本文簽署外，數位簽章經過改良設計，也可用於一些特別常見的應用。例如：允許簽署者不知簽署之文件訊息的盲目簽章(blind signature)可用於電子現金與電子投票系統[6]；允許簽署者可將他的簽署權力授與他人代行的代理簽章(proxy signature)，可用於公務的代理人制度[14]；允許多人簽署同一文件訊息，而不增加簽章大小與驗證複雜度的多重簽章(multi-signature)[5]。使用數位簽章必須搭配公開金鑰基礎建設(Public Key Infrastructure, PKI)與相關法律規範（例如電子簽章法），驗證簽章時要先驗證憑證的有效性（亦即該公鑰擁有者的身分）與公鑰的正確性，而後再利用此公鑰驗證簽章的有效性。



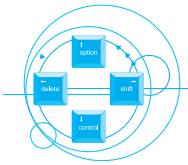
圖三　數位簽章運作模式

- 單向雜湊函數：單向雜湊函數可亦是爲是一種無法還原或不可逆的壓縮(compression)函數，該函數可接受任意長度的輸入訊息，而產生固定長度的輸出結果，此輸出結果又稱爲數位指紋(fingerprinting)。如同人類的指紋，數位指紋可以用來確認訊息在傳輸過程是否遭到更改或替代。一般來說，單向雜湊函數大多搭配數位簽章技術或安全通信協定一起使用。用於數位簽章時，單向雜湊函數具有抵抗選擇密文攻擊的能力，亦即攻擊者無法成功僞造出一個不知內容但又合法（可以通過簽章驗證程序）的簽章，尤其在金融或付款系統上所採用的數位簽章技術，必須具備此能力。用於安全通信協定時，單向雜湊函數所製作出的數位指紋可確保資料在傳輸過程的完整性，甚可提供通信雙方鑑別彼此身分之用。目前知名且安全的單向雜湊函數有 MD5[20]與 SHA-1[17]。前者的輸出長度爲 128 位元，用於產生對稱式加解密系統所需的金鑰；後者的輸出長度爲 160 位元，用於製作數位簽章時所需的簽體或訊息彙記。使用單向雜湊函數時要特別注意其所產生的碰撞(collision)問題，亦即不同的本文訊息會有相同的簽體或訊息彙記。一個實務堪用的單向雜湊函數其所造成的碰撞機率應要小於 10^{-6}。
- 安全通信協定：安全通信協定有三種運作模式：仲介模式、仲裁模式、自我施行模式。在仲介模式中，通信雙方需藉助可信賴第三者 TTP 的參與來建立安全

協定，這種模式常見於網路系統的個體鑑別與金鑰交換協定[4, 7]。透過仲介模式，通信雙方可以在開放式系統中建立具鑑別性的安全通道（亦即虛擬私有網路 VPN）。在仲裁模式中，通信雙方需藉助兩個可信賴第三者 TTP 與 ADJ 的參與，TTP 負責建立安全通道並產生相關的不可否認證據，而當通信雙方對通信內容有爭議時，則必須將不可否認證據送交 ADJ 加以仲裁。仲裁協定常被採用於電子商務或電子公文應用所需的不可否認機制[9, 10, 11]。常見的不可否認證據有來源不可否認(non-repudiation of origin)、遞送不可否認(non-repudiation of delivery)、投件不可否認(non-repudiation of submission)、送達不可否認(non-repudiation of transport)等。來源不可否認證據用於防制傳送端否認曾經傳送某個訊息，遞送不可否認證據用於防制接收端否認曾經收到並知曉該訊息內容。投件不可否認證據用於訊息轉送者(message forwarder)否認曾經接受傳送端的訊息投件，送達不可否認證據用於證明訊息轉送者確實已將該訊息送達接收端。在自我施行模式中，通信雙方必須靠通信的訊息鑑別彼此身分與驗證傳送資料的正確性，這種模式的設計複雜度較高，通常用於封閉(closed)或半封閉(semi-closed)式的嵌入系統(embedded system)。



圖四　安全通信協定示意圖



參、電子檔案保護應用議題

電子檔案保護機制除了須滿足機密性、完整性、鑑別性、不可否認性等資訊安全目標外，尚須兼顧開放性、長期性、法律性等實務應用需求。爲了方便討論起見，本文將政府機構所產出的電子檔案概分成機敏性檔案與一般性檔案。所謂機敏性檔案爲該檔案承辦或製作期間具有機密性，而完成或公佈後雖不具機密性但卻仍具敏感性(sensitivity)或隱私性(privacy)，例如人事任命、懲處等。一般性檔案雖不具機敏性，但政府機構所產出的電子檔案具有適法性與資訊公開的應用需求，仍是要採用適當的保護機制，以確保電子檔案的正確性與完整性。

以下將從政府機構所產出之電子檔案生命週期的角度，亦即製作與傳輸、歸檔與保存、調閱與擷取、銷毀等階段，分別探討這些電子檔案所需採用的保護機制及其欲達成的安全需求。值得注意的是施行非對稱式密碼系統時，公鑰與私鑰對及其公鑰憑證的效力必須經過憑證機構(CA)與電子簽章法相關法律所規範的註冊程序加以認證。

一. 製作與傳輸階段：

對機敏性電子檔案而言，擬稿時必須使用加解密技術加以保護，以確保檔案的機密性，簽辦過程之各級核定者亦需要使用數位簽章技術進行簽核程序，以確保檔案的完整性與不可否認性。傳輸機敏性檔案時，通信雙方必須先執行身分識別或個體鑑別協定，再將該檔案加密與簽署後，才傳輸給接收者。若需要提供傳輸過程的不可否認證據，作爲日後收發兩者的責任歸屬判定，通信雙方需執行不可否認協定。對一般檔案而言。僅需在製作與傳輸過程達成完整性與不可否認性即可，並不需要額外提供機密性與鑑別性的保護機制。

二. 歸檔與保存階段：

在歸檔保存時，不管是機敏性或一般性檔案均需要檔案庫管理者對該檔案進行簽署，以確保檔案的完整性。機敏性檔案的機密性保護是在製作與傳輸階段加

以施行，或另由符合機構組織之安全等級的授權者（例如機構組織內依法授權的行政主管）施以加密保護機制，一般的檔案庫管理者不應具有權力能解密並知曉該機敏性檔案的內容。現行檔案庫管理人員或資訊系統管理者未能遵循資訊安全政策相關授權與規範，大多具有 supervisor 的權力而能讀取機敏性檔案的內容，這並不是適當的作法。屬長期歸檔保存的機敏性檔案，應特別注意或定期評估（一般爲三至四年期間）採行之密碼學機制所提供的保護能力或安全度是否足夠。若發現採行的密碼學機制可能遭受破解之虞，則應立即替換成更具安全強度的密碼學機制。

三. 調閱與擷取階段：

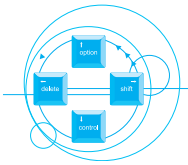
一般性且可公開之檔案調閱與擷取（例如爲民服務需求）僅需確認檔案的完整性即可。調閱或擷取機敏性檔案時，除了需進行調閱者的身分識別或個體鑑別是否滿足解密權限並建立秘密通信管道(VPN)外，尚須對調閱者執行不可否認協定，以確認事後的責任歸屬或安全稽核之用[12]。不管是機敏性或一般性檔案的調閱，當調閱者擷取到檔案時，要驗證該檔案的完整性。

四. 銷毀階段：

爲了釐清責任歸屬，檔案庫管理者與檔案銷毀者應由不同人員擔任。不管是機敏性或一般性檔案的銷毀，均需於銷毀（或刪除）前確認該檔案的內容（亦即驗證檔案庫管理者對該檔案的數位簽章）。銷毀機敏性檔案時，檔案庫管理者與檔案銷毀者應執行不可否認協定，留下銷毀記錄或證據，以確認彼此責任歸屬。

肆、結論與建議

本文從密碼學機制與實務應用的角度探討政府機構所產出之電子檔案或公文書的保護機制，並分別對電子檔案之製作與傳輸、歸檔與保存、調閱與擷取、銷毀等階段，提出可能面臨的資訊安全議題，並初擬解決方案。針對我國推動電子



化政府與施行電子公文政策正值方興未艾之際，提出以下建議以爲未來相關主管機關規劃之參考：

建議一：落實人員與資料的分級制度，尤其是對於處理機敏性檔案或公文書之主管或行政人員的權限，應依據相關法律與規範清楚界定。各項權限之存取行爲應配合適當的電子檔案或公文書的權限控管機制，並建立適當的稽核軌跡，以利事後追蹤與釐清責任歸屬。稽核系統應獨立於作業或應用系統之外，避免系統管理者可以藉由系統權力的行使而逃避稽核[12]。

建議二：涉及系統管理的 supervisor 權力應透過機密共享機制分享給多人。實務上，通常由二至三人共同分享系統管理權力，亦即權力分享者必須全部到場輸入所設定的通行密碼或簽入後，方可啓動與執行系統權力[24, 25]。現行諸多政府機構之管理資訊系統或公文管理系統的系統管理者與其在機構組織內行政職務所賦予的安全等級或權限並不相稱，且通常是由對系統較爲熟悉的系統工程師或操作者擔任，此舉並不適當。以「工程導向」取代「行政導向」的權限管理機制，容易形成機構組織內「權責不符」的現象，應回歸「行政導向」。

建議三：應儘速建立政府機構電子檔案或公文書保護機制標準（含標準作業程序與密碼學技術標準）。各級機構或可依據其單位特性與公務性質，採用不同的保護機制或密碼學機制，但各吹各調的結果容易造成系統整合困難，甚而形成安全漏洞而猶不自知。建立保護機制標準可以增進各級機構間電子檔案或資料的互通性，降低系統整合的複雜度與建置成本，也有利於未來電子檔案集中管理與歸檔作業的進行。

【原刊載於檔案管理局出版之現代檔案管理研討會議題報告彙編（九十三年九月）】

參考資料：

[1] 吳宗成：系統分析與設計，三民書局，民國 84 年。

[2] 謝清佳、吳琮璠：資訊管理 – 理論與實務，智勝文化事業公司，民國 92 年。

[3] 賴溪松、韓亮、張真誠：近代密碼學及其應用，旗標出版公司，民國 91 年。

[4] CCITT, Recommendation X.509, “The directory – Authentication framework”, Consultation Committee, ITU Geneva, 1989.

[5] Chang, Y.S., Wu, T.C., and S.C. Huang, “ElGamal-like digital signature and multisignature schemes using self-certified public keys”, The Journal of Systems and Software, Vol. 50, 2000, pp. 99-105.

[6] Chaum, D., “Blind signatures for untraceable payments”, Advances in Cryptology -- Crypto’82, 1982, pp. 199-203.

[7] Diffie, W. and Hellman, M.E., “New directions in cryptography”, IEEE Trans. Information Theory, Vol. IT-22, 1976, pp. 644-654.

[8] ElGamal, T., “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Trans. Information Theory, Vol. IT-31, 1985, pp. 469-472.

[9] ISO/IEC 13888-1, Information technology – Security Techniques – Non-repudiation – Part 1: General, 1997.

[10] ISO/IEC 13888-2, Information technology – Security Techniques – Non-repudiation – Part 2:Mechanisms using symmetric techniques, 1998.

[11] ISO/IEC 13888-3, Information technology – Security Techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques, 1997.

[12] ISO/IEC 17799, Information technology – Code of practice for information security management, 2000.

[13] Koblitz, N., “Elliptic curve cryptosystems”, Mathematics of Computation, Vol. 48, 1985, pp. 203-209.

[14] Mambo, M., Usuda, K., and Okamoto, E., “Proxy signatures for delegating signing

operation”, Proceedings of the 3rd ACM Conference on Computer and Communication Security, 1996, pp. 48-57.

[15] Menezes, A. and Vanstone, S., “Elliptic curve cryptosystem and their implementation”, Journal of Cryptology, Vol. 6, 1993, pp. 209-224.

[16] National Institute of Standards and Technology, NIST FIPS PUB 46-2, “Data Encryption Standard”, US Department of Commerce, 1993.

[17] National Institute of Standards and Technology, NIST FIPS PUB 180, “Secure Hash Standard”, US Department of Commerce, 1993.

[18] National Institute of Standards and Technology, NIST FIPS PUB 186, “Digital Signature Standard”, US Department of Commerce, 1994.

[19] National Institute of Standards and Technology, NIST FIPS PUB 197, “Advanced Encryption Standard”, US Department of Commerce, 2001.

[20] Rivest, R., “The MD5 message digest algorithm”, RFC 1321, 1992.

[21] Rivest, R., Shamir, A., and Adleman, L., “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, Vol. 21, 1978, pp. 120-126.

[22] Rosen, K.H., Elementary Number Theory and Its Applications, Third edition, Addison-Wesley, 1993.

[23] Schneier, B., Applied Cryptography, John Wiley & Sons, 1996.

[24] Shamir, A., “How to share a secret”, Communications of the ACM, Vol. 24, 1979, pp. 612-613.

[25] Wu, T.C. and Wu, T.S., “Cheating detection and cheater identification in secret sharing schemes”, IEE Proc. Computer and Digital Techniques, Vol. 142, 1995, pp. 367-369.