

使用FPGA實作智慧型IC卡之介面模組

呂良德、洪進華 程仲勝

E-mail: 9314953@mail.dyu.edu.tw

摘要

IC 卡 (Integrated Circuit Card) 科技的問世，將金融交易帶入了另一個新的境界。就整體而言，IC 卡不同於傳統磁卡，其最大的差異就是擁有記憶容量大、安全性佳、具有內部控管能力與可離線作業等優點。有鑑於IC 卡如此龐大之系統效益，目前已有許多先進國家均積極地投入人力與物力在其相關之應用發展。本論文使用Altera NIOS FPGA 晶片 (Stratix-EP1S10)，來實現IC 卡介面模組並執行IC 卡與卡片讀卡機在傳輸介面上之存取機制。我們以IC 卡之基本功能來說明與驗證我們的設計電路，其功能包含「電子錢包」、「門禁管理」、「會員管理」..等。

關鍵詞：IC 卡，資訊安全，電子商務，電子錢包

目錄

封面內頁 簽名頁 授權書.....	iii	中文摘要.....
.....iv 英文摘要.....	v 誌謝.....
.....vi 目錄.....	vii 圖目錄.....
.....x 表目錄.....	xiv 第一章 緒論.....
.....1 1.1 IC Card 的介紹.....1 1.2 IC Card 的歷史簡介.....
.....2 1.3 IC Card 的優勢.....3 1.4 IC Card 的應用.....
.....4 第二章 IC 卡的介紹.....8 2.1 IC Card 的概述.....
.....8 2.2 基本的卡片型式.....9 2.2.1 記憶卡與微處理器卡片.....
.....9 2.2.2 接觸式卡片與非接觸式卡片.....11 2.3 IC Card 的標準與規格.....
.....13 2.3.1 ISO 7816 標準.....13 2.3.2 GSM.....
.....14 2.3.3 EMV.....15 2.3.4 開放式平台.....
.....16 2.3.5 PC/ SC.....16 第三章 IC Card 的電器特性.....
.....18 3.1 IC Card 的裝置接觸點.....18 3.2 IFD 與IC Card 介面之訊息傳輸.....
.....22 3.2.1 傳輸字符框架.....24 3.2.2 ATR 封包之格式.....
.....26 3.2.3 IFD ASM Chart 之介紹.....29 3.2.4 IC Card ASM Chart 之介紹.....
.....31 3.3 IC Card 的檔案系統.....32 3.4 APDU 協定.....
.....34 3.4.1 APDU 指令說明.....38 3.4.2 回應代碼說明.....
.....47 3.4.3 TPDU 協定.....49 第四章 認證過程.....
.....51 4.1 資訊安全.....51 4.2 資料加密標準 (DES).....
.....54 4.3 IFD 與IC Card 的認證流程.....64 4.3.1 終端機認證卡片.....
.....64 4.3.2 卡片認證終端機.....66 4.3.3 持卡人身分核驗.....
.....67 第五章 硬體設計與實作.....68 5.1 電子錢包之介紹.....
.....68 5.1.1 信用卡交易的問題.....68 5.1.2 以國內業者為例.....
.....69 5.2 IC Card 的運作程序.....70 5.3 IFD ASM Chart 之介紹.....
.....72 5.4 IC Card ASM Chart 之介紹.....75 5.5 電子錢包之溝通訊息.....
.....77 5.5.1 「交易」作業.....77 5.5.2 「增值」作業.....
.....79 5.5.3 「查詢」作業.....81 5.5.4 「更改密碼」作業.....
.....83 5.5.5 「門禁」之溝通訊息.....85 5.6 電路架構.....
.....86 5.7 電路模擬.....92 5.8 電路的Place & Rount.....
.....100 5.9 FPGA Download 實作.....102 5.9.1 FPGA 介面硬體架構圖介紹.....
.....102 5.9.2 FPGA 晶片內部區塊規劃介紹.....106 5.9.3 FPGA 實作硬體與量測.....
.....112 第六章 結論與討論.....123 參考文獻.....
.....124

參考文獻

- [1] 周利欽, 翁御舜, “智慧卡技術實務-使用JavaCard (技術架構與程式設計指南),” 碁峰圖書, 2002年四月.
- [2] 葉俊麟, “ISO-IEC 1443 非接觸式智慧型IC卡多元應用之整合研究,” 國立成功大學工程科學研究所所碩士論文, 台灣台南, 2001年.
- [3] 陳憲禹, “兩代醫療網之醫師卡安全作業之研究,” 國立成功大學工程科學研究所所碩士論文, 台灣台南, 2001年.
- [4] ISO 7816. Identification cards – Integrated Circuit(s) cards with contacts.
- [5] 林炳奇, “IC卡結構與應用,” 第二版, 全欣科技圖書, 1993.
- [6] 翁竟翔, 虞孝成, “IC卡在校園中應用之個案研究,” 1992 中華民國科技管理研討會論文集, p.p. 147-152.
- [7] 黃朝義, “健保IC金融卡系統建置及安全架構之研究,” 國立成功大學工程科學研究所所碩士論文, 台灣台南, 1996年.
- [8] 廖英首, “雙智慧卡PCMCIA讀卡機設備應用之研究,” 國立成功大學工程科學研究所所碩士論文, 台灣台南, p.p. 24, 1999年.
- [9] 陳曉開, “智慧e卡,” 全球智慧中文化, 2000.
- [10] 工業研究院, “Baseline Privacy Plus Interface Specification” .
- [11] 吳儀隆, “電子錢包IC加值技術,” 電信研究雙月刊第31卷第2期, 民國90年四月, p.p. 115-125.
- [12] W.Ranki, W.Wffing, “SMART CARD HANDBOOK,” Wiley, 1997.
- [13] 碩良科技, “Microsoft Windows Smart Card Toolkit, Version 2.0,” user manual.
- [14] 潘同泰, “16位元介面原理與控制實習,” 長高電腦圖書, 民國86年, p.p.2-62.
- [15] William Stallings, “Cryptography and Network Security,” Third Edition, Pearson education, 2000.
- [16] http://www.cardweb.com.tw/card/card/ic_EC.htm , IC智慧卡 (Smart card) 與電子商務.
- [17] <http://www.lib.fcu.edu.tw/information%20literacy/%B4%AD%AF u%B2%D5/outline.htm> , 電子商務.
- [18] S. Makino, M. Akita, Y. Asashiba, T. Chikazawa, F. Hidani, and K. Ito, “Key technologies for passive double star system,” in proc. 5th Optical/Hybrid Access Networks, pp. 4.18/01 - 4.18/06, Sept.1993.
- [19] H. Ploog, D. Timmermann, “FPGA based architecture evaluation of cryptographic coprocessors for smartcards,” in Proc. IEEE Symposium on FPGAs for Custom Computing Machines, pp. 292 – 293, April 1998.
- [20] Won Jay Song, and Byung Ha Ahn, “Secure transmission of the prescription order communication system based on the internet and the public-key infrastructure using master smart cards in the 2-way type terminal,” in Proc. 35th Annual Hawaii International Conference on System Sciences, pp. 2035 – 2042, Jan. 2002.
- [21] A. Wahab, E.-C. Tan, and S. -M. Heng, “Biometrics electronic purse,” in Proc. IEEE Region 10 Conference TENCON 99, Vol.2, pp. 958 – 961, Sept. 1999.
- [22] W.-P. Choi, and I.-M. Cheng, “A proposal of an algorithm for DES applications in IC cards,” in Proc. European Conference on Security and Detection, pp.87-90, April 1997.
- [23] B. Arazi, “Interleaving security and efficiency considerations in the design of inexpensive IC cards,” IEE Trans. Computers and Digital Techniques, Vol.141, pp. 265 – 270, Sept. 1994.
- [24] C.-C Chang, T.-C. Wu, “Remote password authentication with smart cards,” IEE Trans. Computers and Digital Techniques, Vol.138, pp. 165 – 168, May 1991.
- [25] E. Trichina, M. Bucci, D. De Seta, and R. Luzzi, “Supplemental cryptographic hardware for smart cards,” IEEE Trans. Micro, Vol. 21, pp. 26 – 35, No. 6, Nov.-Dec. 2001.