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

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.