A Study of Security on Electronic Payment System

梁道一、顏嵩銘

E-mail: 8809489@mail.dyu.edu.tw

ABSTRACT

As business is moving from face-to-face trading, mail order and phone order to electronic commerce over open networks such as the Internet, crucial security issues are being raised. While Electronic Fund Transfer over financial networks is reasonably secure, securing payments over open networks connecting commercial servers and consumer workstations poses challenges of a new dimension. We believe that will be done which must sign his name on for the same experience. One, your trade under the control of someone. Two, you can’t use credit card to buy a beverage, due to the two point. Maybe you don’t think so, but it have some problem in the viewpoint of privacy and conveniently. Therefore, we will to bring up electronic cash to accomplish anonymous system. It will be include merchant and bank. However, we also added some escrow function in here for the sake of convenient to control disputes or extorts. Otherwise, in this time, it has to use payment systems that only buy a beverage, it have the aid of micropayment. Consequently, we will to discuss and some problem about efficiency of micropayment.

Keywords : Micropayment ; Electronic cash ; Anonymous ; Escrow ; Coin

Table of Contents

封面內頁 簽名頁 授權書 iii 簽署人須知 iv 中文摘要 v 英文摘要 vi 誌謝 vii 目錄 viii 圖目錄 xii 表目錄 xiii 第一章 緒論 1 1.1 前言 1 1.2 研究動機 2 1.3 論文架構 3 第二章 加密技術簡介 5 2.1 RSA公開金匙密碼系統 5 2.2 數位簽章 7 2.3 DES私密金匙加密系統 9 2.4 赫序函數 10 第三章 電子付費系統之回顧 12 3.1 電子商業 13 3.2 電子金錢的觀念、功能與特性 14 3.2.1 電子金錢的主要功能 15 3.2.2 電子金錢的必備特性 15 3.3 電子付費系統的特性與功能 16 3.3.1 電子付費系統的必備特性 16 3.3.2 電子付費系統的操作特性與功能 17 3.4 電子付費系統的模組與作業模式 18 3.4.1 現金式與支票式付費系統的基本流程 19 3.4.2 異線式與連線式 21 3.4.3 支付面額 21 3.4.4 可移轉性 22 3.4.5 防偽硬體 23 3.4.6 清算作業 23 3.5 具代表性的電子付費系統 24 第四章 具匿名功能之電子付費系統回顧 26 4.1 使用符號說明 26 4.2 以假名進行匿名 28 4.2.1 作業流程 28 4.3 具可信賴第三者的匿名 32 4.3.1 作業流程 32 4.4 假名與具有可信賴第三單位之匿名方式比較 35 第五章 具使用者身份匿名與託管之電子現金系統 38 5.1 預設幾個先決條件 38 5.1.1 遺失之補救 38 5.1.2 使用限制 39 5.1.3 重複使用 40 5.1.4 匿名 40 5.2 系統的建構與需求 41 5.3 託管機制 42 5.4 具體的協定內容 44 5.4.1 申請使用證書 44 5.4.2 使用者提領數位現金 47 5.4.3 支付 49 5.5 卡片遺失或其他狀況時的處理原則與方式 51 5.5.1 遺失或被竊 52 5.5.2 求償申請 52 5.5.3 謊稱遺失或被竊 53 5.5.4 託管 54 5.6 安全評估 55 5.6.1 因數分解n值攻擊法 55 5.6.2 密文攻擊法 56 5.6.3 重送攻擊法 56 第六章 改良式小額付費之研究 58 6.1 小額付費的基本觀念與目的 58 6.2 Probabilistic Polling小額付費系統 59 6.3 Lotter Tickets小額付費系統 63 6.3.1 細部協定與兌換方式 64 6.3.2 一個中獎號碼串中的理想中獎號碼個數 68 第七章 結論 75 參考文獻 78 附錄 83

REFERENCES


