

中國文化大學商學院資訊管理學系研究所

碩士論文

Graduate Institute of Information Management

College of Business Chinese Culture University

Proposal of Thesis

Mifare Classic 模擬及安全性改良之研究

A Study on the Improvement of Mifare Classic Simulation and Security



Lee, Kuei Yuan

指導教授：周立平 博士

孫振東 博士

Advisor: Chou, Li-Ping PhD

Sun, Jenn-Dong PhD

中華民國 101 年 1 月

January, 2012

論文名稱：Mifare Classic 模擬及安全性改良之研究 總頁數：102

校(院)所組別：中國文化大學資訊管理學系碩士在職專班

畢業時間及提要別：一百學年度第一學期碩士學位論文提要

研究生：李魁元

指導教授：周立平

論文提要內容：

本研究主要探討「非接觸式」的智慧卡，因為「非接觸式」智慧卡溝通是透過無線電的方式做傳送，因此很容易讓攻擊者以側錄的手段，獲取相關的資訊，造成安全上的問題，例如：複製卡片，竄改卡片的資料…等。

目前使用最廣泛的智慧卡是 Mifare Classic 卡，Mifare Classic 卡是一種可在同一張卡片處理多種不同應用的卡片，因此，本研究以 Mifare Classic 卡為對象。

2008 年開始有許多對 Mifare Classic 卡之安全性的研究被提出，這些研究發現有許多弱點並透過某些攻擊 可以取得卡片的金鑰，藉以更改卡片的資訊，本研究會對這些方式做相關實驗，驗證其可行性。本研究成功利用 proxmark3 設備去模擬 Mifare Classic 卡片，與相關讀卡機實驗，可通過門禁與餘額查詢機。

透過實驗了解到 Mifare Classic 卡鑑別上安全性之弱點，並從這些弱點中，提出改進的方式。對攻擊者可能產生的行為中，尋求因應的方法，能提高 Mifare Classic 卡安全性，減少被攻擊的機會，本研究提出相關的防禦方法能抵禦大部份現有攻擊方式。

關鍵字：非接觸式、智慧卡、Mifare Classic

# A Study on the Improvement of Mifare Classic Simulation and Security

Student: Kuei-Yuan Li

Advisor: Prof . Li-Ping Chou

Prof . Sun, Jenn-Dong

Chinese Culture University

## ABSTRACT

This study focused on the simulation and security problems of contactless smart card. Since contactless smart cards communicate through radio, it is easy for an attacker to eavesdrop and obtain the card related information. This causes security problems such as card duplicating and card data tampering.

Currently, the most widely used smart card is Mifare Classic card, which is used in a broad range of applications including transport ticketing, access management, e-payment, etc. Therefore, this study targets Mifare Classic card.

In the last few years, many articles have been devoted to the study of Mifare Classic card security. Their studies found that due to many weaknesses in Mifare Classic card the card key can be retrieved by certain attacks and accordingly the card data can be changed. According to their methods, this study conducts experiment to verify their feasibility. This study makes use of Proxmark3 device to read and emulate Mifare Classic card. In the card emulation experiments, the emulation card can be read by building access control reader and MRT balance inquiry machine, successfully.

According to the security weakness of Mifare Classic card authentication learned through experiments, an improved method is proposed to increase the security of Mifare Classic card. Since the proposed method aimed at possible attacker behaviors, it can defend against most existing attacks.

Keywords: contactless, smart card, Mifare Classic

## 誌 謝 辭

本論文幸蒙恩師周立平老師、孫振東老師之悉心指導，在恩師的諄諄教誨下，及在楊博宏、邱乙城、邱奕豪各位學弟的支持與幫助下，才能順利完成，師恩浩翰，無以回報，在此謹向恩師致上最高的敬意！



# 目錄

第一章	緒論	1
第一節	研究背景	1
第二節	研究目的	2
第三節	研究限制	3
第二章	Mifare Classic Card 介紹	4
第一節	Mifare Classic Card 規格與結構	4
第二節	Mifare Classic Card 鑑別協定	8
第三節	Crypto-1 加密演算法	11
第四節	Mifare Classic Card 弱點	20
第三章	Mifare Classic Card 之已知攻擊方式	23
第一節	Mifare Classic 之反向工程	23
第二節	密鑰串流還原攻擊法	24
第三節	側錄攻擊法	25
第四節	同位元攻擊法	26
第五節	Nack 攻擊法	28
第六節	已知明文攻擊法	29
第七節	小結	35
第四章	研究方法	36

第一節	研究工具.....	36
第二節	Mifare Classic 安全性之改良.....	47
第三節	Mifare Classic 模擬.....	66
第五章	結論與未來研究.....	85
第一節	結論.....	85
第二節	未來研究.....	85
參考文獻	.....	87
索引表	.....	89
修讀碩士期間所發表相關之論文	.....	91



## 表目錄

表 2-1	Mifare Classic 卡資料儲存結構.....	5
表 2-2	讀卡機與卡片通訊範例.....	9
表 3-3	線性反饋位移暫存器差距變化表.....	29
表 3-4	Mifare Classic 指令分類.....	31
表 3-5	指令種類及長度.....	35
表 3-6	各類攻擊方法比較表.....	35
表 4-7	各種攻擊方式之防禦.....	48
表 4-8	各種防禦方式傳送資料比較表.....	64
表 4-9	各項指令傳送資料比較表.....	65
表 4-10	學生證與門禁讀卡機溝通資料.....	76
表 4-11	學生證與捷運站餘額查詢機之間溝通的訊息.....	79
表 4-12	模擬卡片成本統計.....	84
表 5-1	本研究所提之改良方法.....	86

## 圖目錄

圖 2-1	Mifare Classic 卡記憶體結構.....	6
圖 2-2	Mifare Classic 卡通訊流程 .....	7
圖 2-3	Mifare Classic 卡鑑別流程 .....	8
圖 2-4	PRNG 演算法.....	12
圖 2-5	Filter Function .....	13
圖 2-6	同位元加密 .....	14
圖 2-7	Crypto-1 初始狀態設定 .....	15
圖 2-8	Nr 加密.....	15
圖 2-9	Tag 產生 Ar、At 前的 Crypto-1 初始狀態 .....	16
圖 2-10	產生 Ar、At 的密文 .....	17
圖 2-11	線性反饋位移暫存器狀態表示 .....	18
圖 2-12	密鑰串流狀態表示.....	18
圖 2-13	加密的 Nr、加密的 Ar 與加密的 At 表示 .....	20
圖 3-14	鑑別指令示意圖 .....	32
圖 3-15	讀指令 .....	33
圖 3-16	寫指令 .....	33
圖 3-17	值運算指令 .....	34
圖 4-18	CRYPTO1 範例 1 .....	36



圖 4-19	CRYPTO1 範例 2.....	37
圖 4-20	MFCUK 測試畫面.....	38
圖 4-21	Ubuntu10.10 測試畫面.....	39
圖 4-22	Ubuntu10.10 測試畫面.....	40
圖 4-23	Ubuntu10.10 測試畫面.....	40
圖 4-24	Mfoc 測試畫面 1.....	42
圖 4-25	Mfoc 測試畫面 2.....	42
圖 4-26	查詢卡片資訊.....	43
圖 4-27	防碰撞測試.....	44
圖 4-28	Proxmark 3 之主機.....	48
圖 4-29	Proxmark 3 之天線.....	46
圖 4-30	NFC 的讀卡機及卡片.....	47
圖 4-31	本研究所提之鑑別流程.....	49
圖 4-32	鑑別流程圖.....	51
圖 4-33	使用 Key0 做初始設定.....	52
圖 4-34	{Nt0}.....	52
圖 4-35	{Nr0}.....	53
圖 4-36	{Ar0}.....	54
圖 4-37	{At0}.....	55



圖 4-38	{Command0} .....	56
圖 4-39	{Nt1} .....	57
圖 4-40	{Nr1} .....	58
圖 4-41	{Ar1} .....	59
圖 4-42	{At1} .....	60
圖 4-43	{Command1} .....	61
圖 4-44	{data0} .....	62
圖 4-45	卡片記憶體配置 .....	67
圖 4-46	proxmark3 軟體架構 .....	68
圖 4-47	主程式及副程式架構 .....	69
圖 4-48	iso14443a 程式架構 .....	69
圖 4-49	模擬卡片程式架構 .....	71
圖 4-50	proxmark3 模擬卡片程式流程 .....	72
圖 4-51	proxmark3 模擬卡片實驗流程 .....	73
圖 4-52	proxmark3 連接電腦 .....	74
圖 4-53	proxmark3 模擬卡片 .....	75
圖 4-54	proxmark3 運作時設備會亮橘燈 .....	75
圖 4-55	讀卡機與卡片溝通流程(學生證) .....	76
圖 4-56	Libnfc 讀卡機與合法卡片測試畫面 .....	77

圖 4-57	合法卡片與討論小間讀卡機.....	77
圖 4-58	proxmark3 與討論小間讀卡機.....	78
圖 4-59	側錄(snoop)學生證與捷運站餘額查詢機之間溝通的訊息	79
圖 4-60	模擬卡片程式架構.....	81
圖 4-61	Libnfc 讀卡機與合法卡片測試畫面.....	82
圖 4-62	合法卡片與餘額查詢機.....	83
圖 4-63	proxmark 模擬卡片與餘額查詢機.....	83

