

目錄

1.摘要.....	2
2.概論.....	2
2.1 研究目的.....	2.3
2.2 研究設備.....	3
2.2.1 耗材.....	3
2.2.2 設備儀器.....	3
3.研究方法.....	3
3.1 RS232 接線製作（公頭對母頭）.....	4
3.2 訊號測試.....	5
3.3 觸碰電路測試.....	5
3.4 觸碰電路製作.....	5.6
3.5 藍芽控制電路	6
3.6 後端程式開發-取得磁碟序號與標籤建立.....	6.7
3.7 磁碟序號與磁碟標籤加密.....	7.8.9
4.控制外部硬體電路圖及說明.....	9
5.執行結果.....	9.10.11
6.參考文獻.....	11

隨身碟&藍芽門控系統之研發

Flash Drives& Bluetooth gated system of research and development

指導老師：黃俊翔 老師

學號 00305109 郭忠齊

1.摘要

本研究旨在探討整合隨身碟、藍芽、傳統門鎖及數位監控系統之可行性。我們嘗試利用隨身碟本身的磁碟序號、使用者自己建立的磁碟標籤，經過運算及加密後的字串，再搭配One timepassword、時效性等技術當成我們的鑰匙。當隨身碟插入門上的USB 插槽，經過中央控制設備比對並確認後，便能開啟門鎖。當鑰匙判別錯誤時，攝影機將擷取人物影像以作為日後追蹤用。本系統的優點為：鑰匙可由使用者隨時增加或刪除、密碼難以複製、即時影像擷取可嚇阻企圖不良的入侵者。

2.概論

隨著人類生活水平逐漸上升，科技產業迅速發展，生活與科技產生緊密結合，帶來科技的方便性與普及化，帶來更方便的生活。但也帶來不少安全性的隱憂，以致竊盜的案件層出不窮。考量傳統鑰匙安全疑慮問題，以現今鎖匠技術能在一分鐘內可以複製出功能相同的一把鑰匙，所以傳統鑰匙的防盜功能的確有待加強。較現代化的電子密碼鎖，在密碼組數受限之下要找到重複密碼並不困難只需花費時間即可破解；還有現在的RFID 無線射頻辨識系統，以卡片中的線圈接近讀取器，常發生感應異常，或是複製卡片、卡片遺失的服務價格昂貴等問題。

2.1研究目的

1. 抓取磁碟序號

2. 建立磁碟標籤
3. 以演算法轉換磁碟標籤並加密
4. 鑰匙具唯一性
5. 採用揮發性密碼技術
6. 密碼具時效性
7. 磁力鎖動作原理研究
8. 觸碰電路抗靜電力之研究
9. 數位監控設備之控制

2.2研究設備

2.2.1 耗材

1. 電子元件（包含電晶體、電阻、電容、二極體、繼電器）
2. 單心線、錫、PCB板
3. 顯影劑、氯化銅液

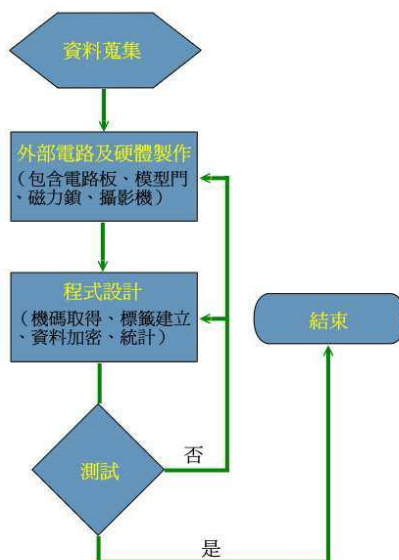
2.2.2 設備儀器

1. 電腦主機（EBOX）（後端程式開發）
2. USB轉RS232傳輸線（硬體與程式訊號傳輸）
3. 電源供應器（提供硬體電源）
4. 示波器（顯示訊號）
5. 電動鑽孔機（架設磁力鎖）
6. 隨身碟（當鑰匙用）
7. 數位監視設備（攝影鏡頭）
8. 電話控制電路板（電話語音控制）
9. 三用電表

10. 電烙鐵

3.研究方法

在實驗計畫進行前，我們先行找了一些資料文獻，除原理說明之外，也給我們一些方向，雖然，每個理論都是獨立的，但我們有信心將這些理論，全部組合在一起，實現我們所要研發的系統，以下是實驗流程圖：



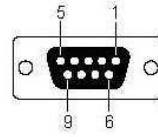
圖五 實驗流程圖

3.1 RS232接線製作（公頭對母頭）

根據圖六，線在製作時，必須跳線，2 3、3 2、4 6、6 4、7 8、8 7，且在焊接時必須注意，因為接腳之間距離很近，因此用錫的量要掌握好，才不會發生短路的現象，下圖七為完成圖。

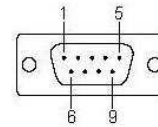
RS-232 — DB9母頭

Pin No.	Signal
1	DCD
2	TxD
3	RxD
4	DSR
5	GND
6	DTR
7	CTS
8	RTS
9	---

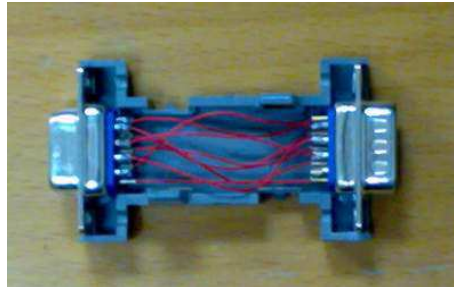


RS-232 — DB9公頭

Pin No.	Signal
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	---



圖六 RS232接線電路圖



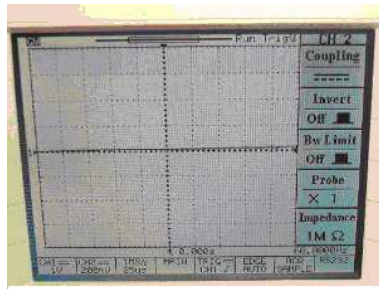
圖七 RS232線路完成圖

3.2 訊號測試

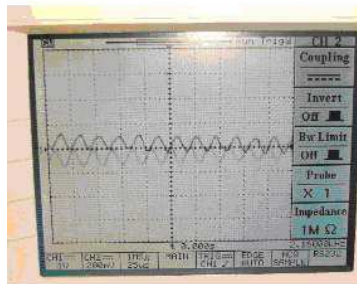
以筆記型電腦連接USB轉RS232之傳輸媒體，連接上述之驅動電路，以自行撰寫之程式測試繼電器是否有動作，若無，則修改電路，可能為電晶體故障，可更換新品或是調整接腳B.C.E後再做測試。

3.3 觸碰電路製作

運用人體靜電力（圖九）來驅動繼電器，在製作時需特別小心，不可在元件上焊接太久。且佈線也要特別注意兩線之間是否太近或重疊，因為可能產生干擾，而讓繼電器不停跳動，無法控制。



手未觸碰電路

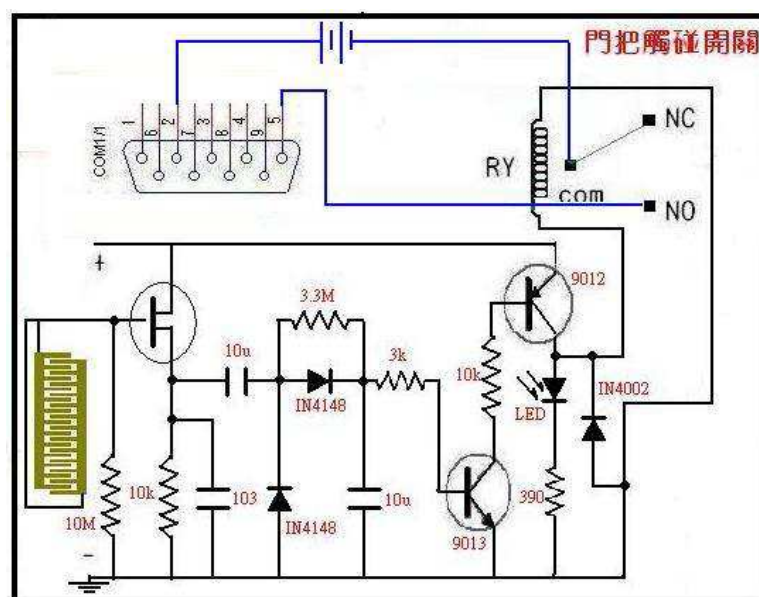


手觸碰電路後

圖九 示波器顯示人體靜電力

3.4 觸碰電路測試

將觸碰電路連接電源，以電腦的「超級終端機」進行測試，設定條件為：鮑率：9600bit/sec，資料位元：8位元，同位檢查：無，停止位元：1位元，若繼電器有動作，且有訊號傳輸進入電腦，則終端機畫面會取的資料（圖九），若無訊號進入，則無資料呈現，必須重新檢修電路。



圖十 觸碰電路製作

3.5 藍芽控制電路

以智慧型手機控制，為考量安全性，僅用於當隨身碟遺失時，透過手機內具有反饋密碼技術功能的自行開發軟體進行開門動作。而反饋技術即是當藍芽取得連線後，由晶片自動回傳一組字串，由軟體進行運算比對，若認證成功後即可開門。

3.6 後端程式開發-取得磁碟序號與標籤建立

後端程式開發-取得磁碟序號與標籤建立在VB下運用API，抓取新增磁碟的機碼，即磁碟序號，運用前後狀態比較，辨識哪一個磁碟槽為新增磁碟，以下列程式直接擷取磁碟序號：

```
GetVolumeInformation strDrive,  
vbNullString, 0, SerialNum, 0, 0,  
vbNullString, 0  
'SerialNum為磁碟序號
```

同時，磁碟序號自動填入程式欄位，也透過讓使用者自行建立磁碟標籤及檢查常數（圖十一），將磁碟標籤存入隨身碟，使用的技術為，讓程式自動產生批次檔，批次檔內容為：

```
@echo off  
d: '新增的磁碟槽  
label 123456  
'「123456」為想建立的磁碟標籤名稱
```

透過存檔的同時，執行檔案，以達到建立磁碟標籤的動作。下式為執行批次檔：

```
nPath = "C:\Test.bat" 'Test.bat為欲開  
啟執行之檔案  
ShellExecute Me.hwnd, "", nPath, "", "",  
vbNormalFocus
```



圖十一 自動填入磁碟序號

3.7 磁碟序號與磁碟標籤加密

在VB中運用API撰寫程式將隨身碟之磁碟標籤取出：

```
GetVolumeInformation strDrive,
DiskLabel, 0, SerialNum, 0, 0,
vbNullString, 0
'DiskLabel為磁碟標籤
```

使用迴圈運算，將隨身碟之磁碟標籤先行轉換成Unicode：

```
For i = 1 To Len(S)
If Mid(S, i, 1) = " " Then
tmp = tmp & Mid(S, i, 1)
Else
tmp = tmp &
Hex(AscW(Mid(S, i, 1)))
End If
Next
```

因Unicode為16位元，故轉換為16進位時會以4位元來表示（圖十二），所以，假設我們以輸入三個中文字為例，那麼會產生12位元的16進位的資料；



圖十二 2進位與16進位轉換

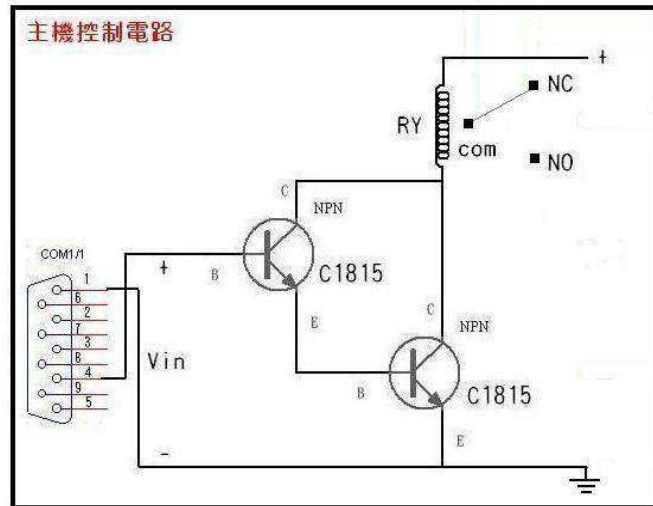
我們將所得的16進位數值的資料字串，再以迴圈轉換成ASCII碼，同時，依使用者一開始建立的檢查常數「C」來進行加密轉換，「C」由使用者自訂0~10，系統會自動記憶，轉換之後，將此數值還原為字元來呈現，程式如下：

```
j=1
while j <= Len(a)
b=b + chr(Asc(Mid(a, i, 1)) + c)
j=j + 1
wend
```

因為磁碟序號為8位元16進位的數值組成，因此，會有 $16^8=4,294,967,296$ 個組合，再加上，若使用者在標籤建立時以自己的姓名來建立，那麼也會有12位元產生，以自己建立的常數來加密，最後可以至少產生12個字元，每一字元有16種符號可以選擇，所以會有 $16^{12}=281,474,976,710,656$ 個組合，如此由磁碟序號與標籤一同運算共有 $16^{20}=1,208,925,819,614,629,174,706,176$ 個組合，其出現重複的機會更是微乎其微，因此，我們將此結果拿來建立私鑰。

4. 控制外部硬體電路圖及說明

主要由達靈頓電路（圖十三）組成，由兩個共集極組態的電晶體直接耦合所組成，以第一級放大器的輸出電流作為第二級放大器的輸入電流，再以第二級放大器的射極作為信號輸出端，如此可將輸入電流放大約 $\beta_1 \times \beta_2$ 倍；因為電腦送出的訊號極小，因此必須搭配達靈頓電路，來驅動繼電器，才能讓磁力鎖有所動作。



圖十三 磁力鎖驅動電路-達靈頓電路

5.執行結果

當硬體設備製作完成並經測試後，我們開始撰寫程式，整個系統花了將近5個月的時間，在多次程式測試錯誤及修改之後，終於可以將程式與硬體連接測試，以下為測試流程：

1. 將硬體電源與電腦連線就緒後，第一個動作便是建立新鑰匙，先將隨身碟插入電腦之後，接著選擇功能列的新增鑰匙功能，會出現如下的畫面（圖十四）



圖十四 新增隨身碟鑰匙

，磁碟序號為自動擷取，使用者只要輸入姓名與標籤，在填完標籤後，必須按下建立，接著，點選「常數」的按鍵，輸入0-9任一數字，並選新增，即完成建立鑰匙的程序；而若是隨身碟已建立過鑰匙，那麼系統會在您點選新增鑰匙之後，自動告知已重複（圖十五）。



圖十五 系統自動辨識是否已建立過鑰匙

2. 將隨身碟拔除之後，將它再次插入，會看到磁力鎖開啟，並有語音自動告知今日異常插入人次。同時，畫面（圖十六）的程式也會多一筆記錄，清楚記載進入時間及姓名，在將門關閉之後，磁力鎖自動鎖上；當我們拿一個未建立的隨身碟插入之後，門不能開啟，系統一樣新增一筆記錄，且系統自動拍照，照片檔名以日期及時間命名，同時畫面上也會有每日異常插入USB槽之次數的長條圖。



圖十六 記載正常與異常插入隨身碟之記錄

3. 當前兩項主要功能測試完畢，接下來是一個創意的發想，我們期望當由內外出時，只要手握著把手，門就自動可以開啟，同時記錄日期與時間，並啟動系統錄影5分鐘，經過測試之後，因為電路的關係，造成繼電器重複動作不停的跡象，但經修改後，我們降低外部靜電的干擾，及修改程式的鮑率定義，最後測

試之後仍然可行。

6. 參考文獻

- 1.林祐廷，民國92年，利用DiskOnKey的金鑰建構企業安全的電子郵件，國立交通大學研究所碩士論文。
- 2.之紹慈、康良三，電子實習（2），台北市，啟台圖書有限公司，42頁，民國85年。
- 3.劉明舜，數位邏輯，台北市，旗立資訊股份有限公司，17頁，民國98年。
- 4.吳進北，程式語言Visual Basic 6一切搞定，台北市，基峰資訊股份有限公司，2頁，民國97年。
- 5.蔡朝洋，電子學實習，台北市，全華科技圖書股份有限公司，215頁，民國86年。
- 6.王旭正、柯宏叡、ICCL-資訊密碼暨建構實驗室，資訊與網路安全-秘密通訊與數位鑑識新技法，台北縣，博碩文化股份有限公司，220頁，民國96年。