專題報告

基於藍牙 BLE 與對稱加密的智慧無鑰鎖

專題成員:高司玹
指導教授:李皇辰 教授

目錄

研究動機和目的

在現代生活中，我們不斷尋求方法來提高生活品質，並使日常活動更為便捷。其中之一是簡化常見的任務，例如開門或付款。原因是現代人生活節奏快，人們常常身上攜帶著多種物品，例如手機、錢包、購物袋等等。在這樣的情況下，需要尋找鑰匙或處理現金交易可能會導致不必要的延誤和不便。這就是為什麼自動化開門和無現金支付方式變得越來越受歡迎的原因之一。這不僅提高了生活品質，還有助於節省寶貴的時間和精力。

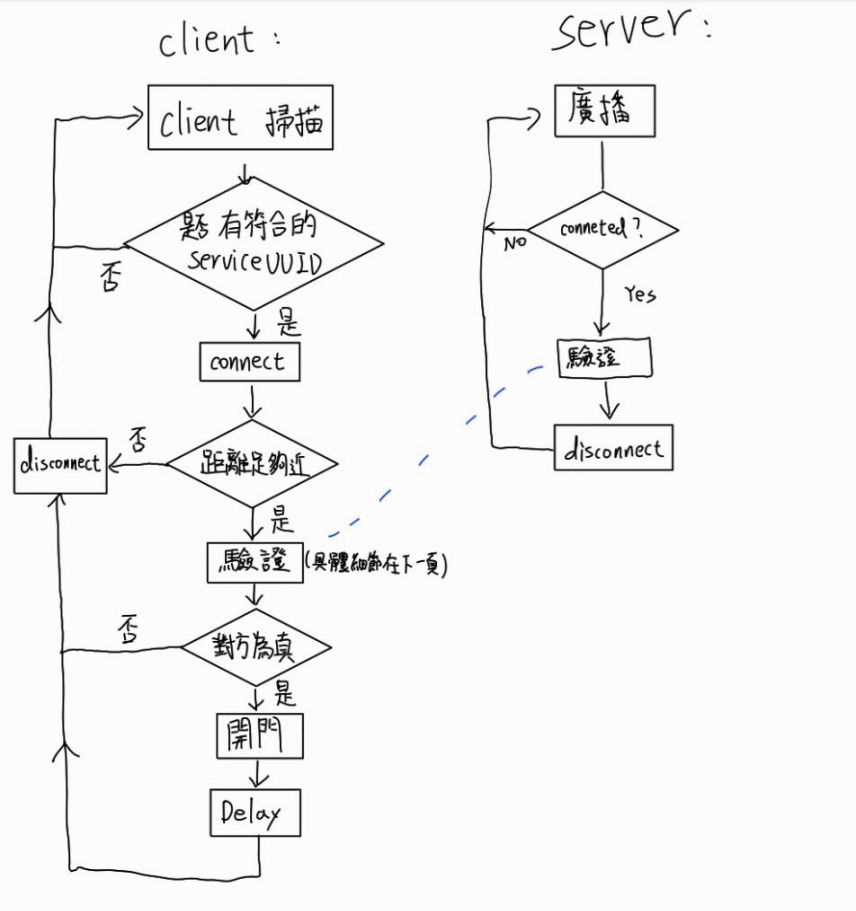
而付錢或是近距離開門的自動化由於都是近距離的動作，即當在主人在周圍時，裝置才可以做相對應的動作，因此就須仰賴無線測距的功能來協助完成，因此我想要借用 BLE 無線測距功能來實現。

此外付款或開門的自動化不僅僅是關於便利性，還關係到個人隱私和財務安全。因此，本研究除了要結合 BLE 無線測距技術實現近距離操作，同時還要包括身份驗證機制，確保只有授權用戶能夠執行這些操作。

在本專題中，我們將以 Keyless 門鎖作為目標示例，採用 ESP32 作為實現的平台。不僅要實現無線測距功能，還要設計一個安全的驗證系統，以確保只有合法的使用者可以啟動門鎖。

設計方法

- 兩塊 esp32，一個做為門鎖(client)，另一個做為鑰匙(server)，彼此以 BLE 溝通。
- 當鑰匙靠近門鎖一定距離後，會驗證鑰匙的身分，若正確則開門。



圖(一)

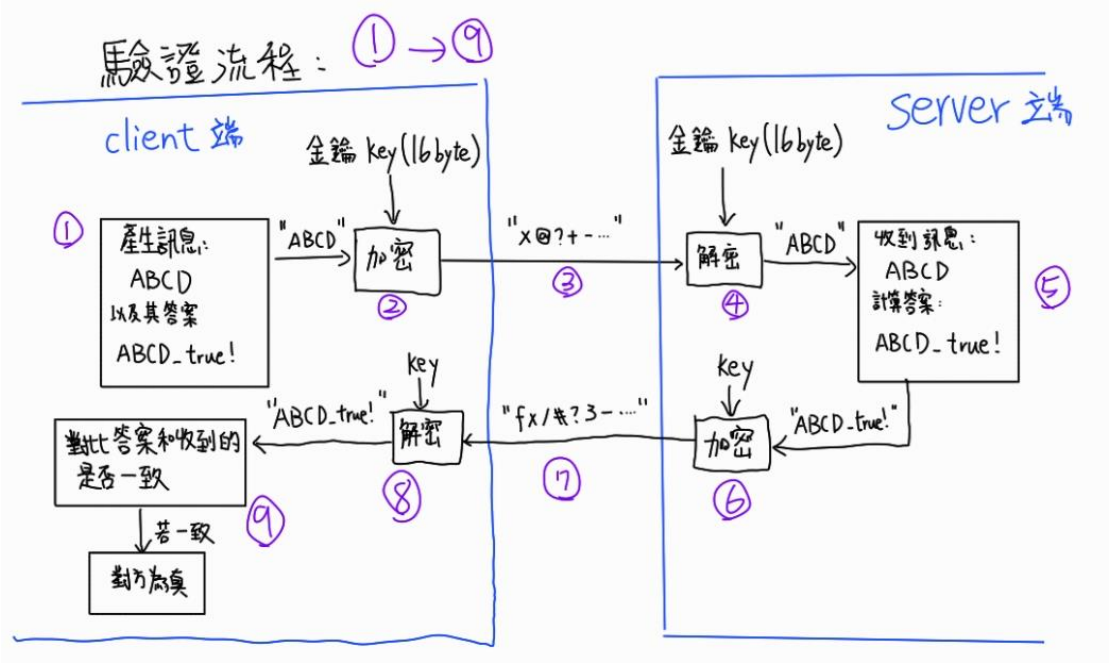
Client 端不斷掃描，Server 是不斷廣播，當雙方的 UUID 是對的便會連接(connect)，連接後便會檢查彼此距離，必須距離接近一定數值時才會後才會進入下一步，如圖(一)

驗證方法如下:

雙方透過對稱式加密 AES 溝通，雙方擁有同一筆金鑰(16byte)(事先寫好在雙方程式內，因此除非記憶體洩漏等因素，不然只有溝通的雙方知道)，client 隨機產生一段訊息(<=16byte)並加密傳給 server，serve 收到後便根據訊息產生一段對應的答案，唯有當 server 能夠正確解密這段訊息才能產生正確的答案，因此 client 只要確認對方的回覆的答案是否正確，就能證明對方是不是假冒的。

而此時會有個問題，若每次的訊息都是一樣的，則每次傳回的答案都會是固定的，那麼入侵者將可以模仿(流程 7)中帶的加密的答案通過，即便入侵者看不懂這串加密文字的涵義。

因此為了避免此情況，client 端每次產生的訊息是隨機的，所以每次的答案也不會固定。



圖(二)

根據圖(一)可知運行過程中，Client 和 server 連接後在驗證前會先確認對方距離是否足夠接近，接著在 loop 內不斷收、發訊息(透過 charcteristic)以進行驗證，若 client 發現在迭代次數到達前 server 無法回傳正確答案則斷開，因此會有三個階段:

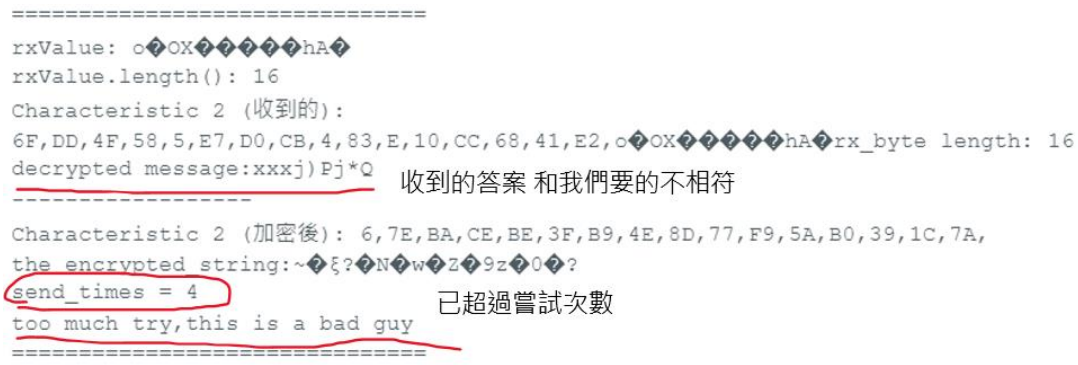
Case 1: 距離夠近且驗證正確

```
random originalString:4Lr94s        隨機產生的訊息
Characteristic 2 (加密後): D3,76,3B,80,AC,6D,A9,1D,1D,10,A6,D1,41,D8,C5,46,
the encrypted_string:v;mA8F8?
send_times = 0                       加密後
==============================
rxValue: In]kd6]h                    對方回傳
rxValue.length(): 16
Characteristic 2 (收到的):
49,C9,B2,ED,E3,15,6F,83,BD,5D,E5,6B,64,36,5D,68,In]kd6]hrx_byte length: 16
decrypted message:true!_4Lr94s       解密後
------------------                   這裡設正確答案為"true!_" + "原本訊息"
Characteristic 2 (加密後): D3,76,3B,80,AC,6D,A9,1D,1D,10,A6,D1,41,D8,C5,46,
the encrypted_string:v;mAF ??
correct !
onDisconnect                         正確 並 退出連接
send_times = 1
==============================
```

圖(三)、Client 端

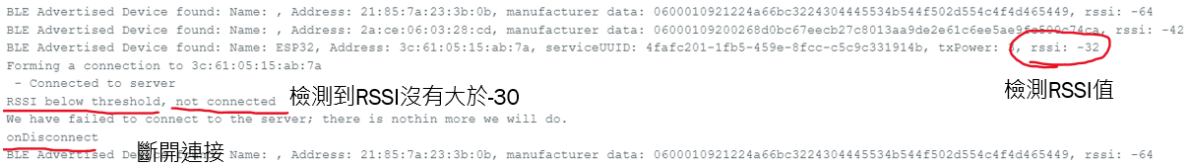
圖(四)、Server 端

Case 2: 超過迭代次數，仍未收到正確答案



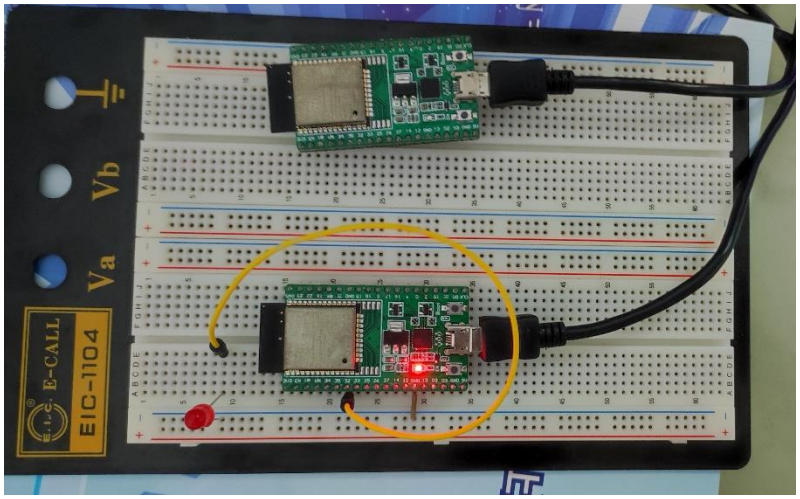
圖(五)、Client 端

Case 3: 距離不夠近



圖(六)、Client 端

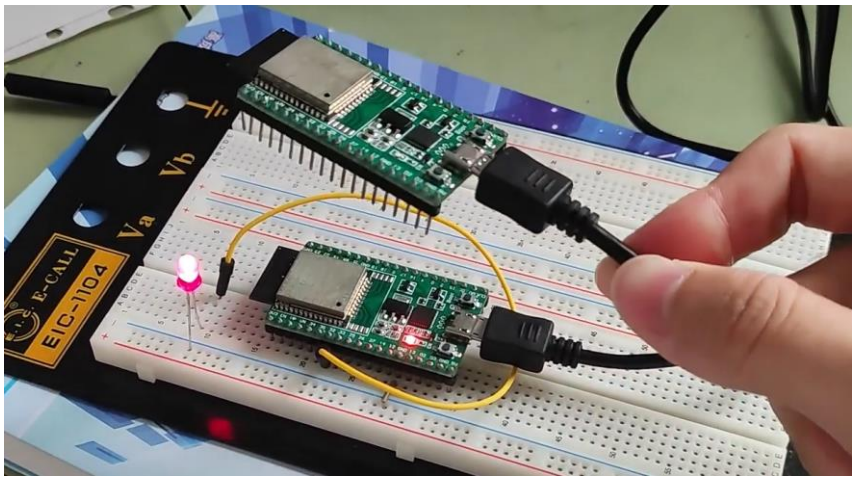
成果展示



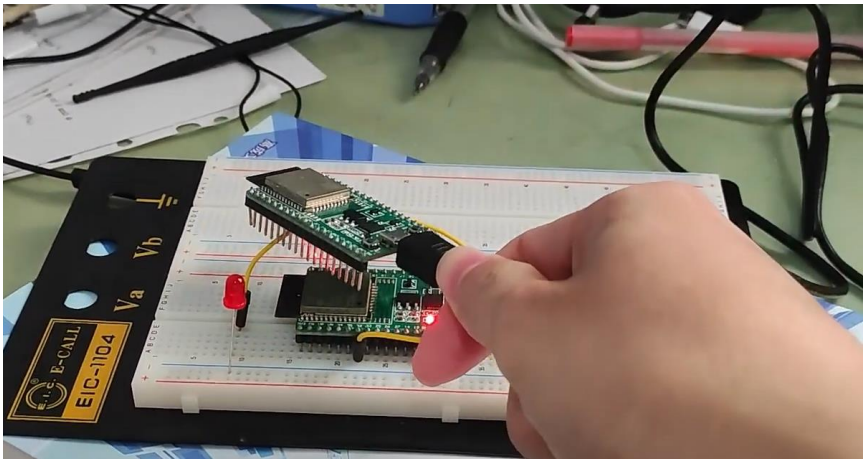
圖(七)、上方為鑰匙，下方為門鎖。

這邊以紅色 LED 亮來表示解鎖。

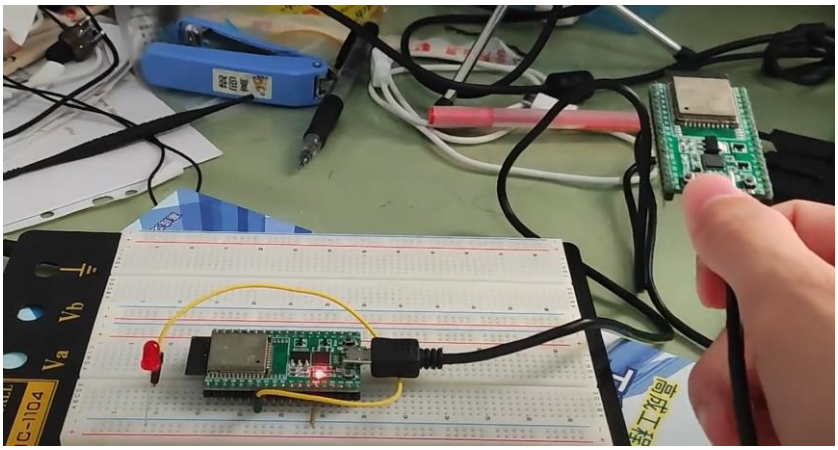
Case 1: 正確密碼且距離足夠接近設定的值。



Case 2: 如果是錯誤的密碼，即便距離夠近也不會解鎖。



Case 3: 正確密碼但距離過遠。



實驗 DEMO 影片：

問題與討論

可以改進的方向:

1. 在此實驗，訊息和金鑰皆為 16byte，因此有心人可以花時間破解，若要提高安全性則要提升金鑰的長度。
2. 因為是使用 RSSI 來進行距離的判定，但 RSSI 數值不會非常穩定，會因為環境的各種因素而浮動，因此還有待研究與改進。
3. 延遲較高，需要優化程式。

總結

在這份專題報告中，我們探討了現代生活中追求便捷性和安全性的需求，特別是在開門和付款等日常任務中可能導致不必要的不便。因此我們想要設計一個可以實現自動化開門或無現金支付的裝置。
因為距離要求短且需要省電的功能，我們採用藍芽的 BLE 來實現。

除了無線測距外，**此專題的重點著重在驗證身分這一部分**。

具體方法中，我們使用了兩塊 ESP32，一個充當門鎖（client），另一個充當鑰匙（server），通過 BLE 通信進行互動。鑰匙在靠近門鎖一定距離後，使用 AES 對稱加密進行通信，為確保通信的安全性。設計了一套簡易的流程避免被入侵者仿冒其為主人，用**簡單的對答機制確保只有授權的鑰匙可以產生正確的回應以成功驗證**。

接著，我們也討論了一些改進的方向和問題，包括提高金鑰長度以增強安全性、以及待克服的難點，如透過 RSSI 判斷距離的穩定度等等。

總結來說，這份專題報告強調了在現代生活中提高便捷性和安全性的需求，並提供了一個有前景的解決方案，通過無線測距技術實現自動化操作，同時確保通信的安全性。這個研究為未來的相關研究和實際應用提供了重要參考和啟示。

以加油站為例，此裝置若運用在加油站，加油站掏錢是很不方便的，因此若將此系統設計在加油站的油槍和車子油箱蓋附近，當加油時兩者會足夠靠近並經驗證通過後，便會計算加油量並自動扣款向該車駕駛或該系統設定的扣款人扣款。

參考資料

1. https://www.youtube.com/watch?v=0Yvd_k0hbVs&t=330s&ab_channel=MoThunderz
2. https://www.youtube.com/watch?v=7mkTBgVfg3w&ab_channel=%E6%9E%97%E6%B8%85%E6%98%80
3. http://wywiot.com/blenote-whatisuuid/