明新科技大學　校內專題研究計畫成果報告

藍牙無線通訊技術的安全機制

The Security Mechanisms of Bluetooth

計畫類別：□整合型計畫　■個人計畫

計畫編號：MUST -97 -資管- 05

執行期間：97 年 1 月 1 日 至 97 年 9 月 30 日

計畫主持人：葉慈章

共同主持人：

計畫參與人員：

處理方式：除涉及專利或其他智慧財產權外得立即公開，

唯必要時本校得展延發表時限。

√可立即對外提供參考

（請打√）□一年後可對外提供參考

□兩年後可對外提供參考

執行單位：管理學院資管系

中　華　民　國　九十七 年 九 月 三十 日

摘要

藍牙是一種短距離無線通訊技術，使各種數位裝置間的連接與資料傳輸，擺脫了電纜的束縛。藍牙原先多應用於手機、耳機間，目前已普遍應用於 PDA 與個人電腦上；隨著機密資料傳輸的增加，藍牙安全的重要性也隨之提升。然而，由於藍牙的身分鑑別和金鑰的建立過程中，許多資訊是以明文方式傳遞，所以惡意的第三者因此可以假冒藍牙裝置通過鑑別，也可推導出通訊的加密金鑰，進而監聽傳送的資料。2007 年藍牙 V2.1 新標準 Secure Simple Pairing，雖然改善了過去配對問題（如，假冒攻擊和竊聽攻擊），但由於藉由六位數字的視覺比對來解決中間人攻擊的鑑別方式，可能因人為操作錯誤導致安全隱私上的疑慮。

本研究將先介紹並仔細分析藍牙現有的安全機制，接下來探討其安全上的問題，最後並提出我們的改善機制，以有效提升安全性，讓藍牙技術可以安心地被應用於安全需求性較高的應用上。

關鍵詞：藍牙，隱私，安全

Abstract

Bluetooth, a short range wireless communication standard, has made possible a number of digital devices totally free from being bonded to wires and cables. Its application which used to serve mostly cell phones and headsets has widely extended to PCs and PDAs. Given the data transferred has come to a greater degree of sensitivity, security issues involving Bluetooth transmission have raised many concerns. However, during the authentication and key exchange process of Bluetooth communication, a lot of information is transferred in plaintext, which allows a malicious third party to spoof the legal Bluetooth device to make it through the authentication, or to deduce the encryption key to eavesdrop the transferring data. The revised version of standard, Bluetooth V2.1, came forth in 2007 with a new security mechanism, Secure Simple Pairing, which seemly eradicated the problems legacy pairing had missed out such as spoofing attacks and eavesdropping attacks. However, as authentication is done by visual confirming on displayed 6-digit numbers to avoid man-in-the-middle attacks, there are quite a few instances of user error that will result in security and privacy breaches.

This paper will introduce and analyze the security mechanism of Bluetooth first, then discuss the security drawbacks on this mechanism, and finally an improved scheme is proposed that could be applied in high security demanding applications.

Keywords：Bluetooth, Privacy, Security

目錄

1. 前言

藍牙[3-6, 38, 41]是一種短距離的無線技術，使用頻段 2.4GHz 的射頻（RF），可穿透大部分障礙的物體，也不用像紅外線受限於可直視（line-of-sight）的讀取範圍，傳送距離可達 10 公尺以上，傳輸速率一般最高可達 3Mbps；使用跳頻方式避免碰撞 IEEE 802.11、 HomeRF、微波爐、其它的藍牙裝置等。

藍牙源自於 1994 年易利信公司為了讓所生產的行動電話與其它鄰近週邊產品能夠不受纜線束縛的通訊，所開發出來的一種無線傳輸技術。1998 年 5 月 Intel、Ericsson、Nokia、IBM 及 Toshiba 五家廠商成立了「藍牙技術聯盟（Bluetooth Special Interest Group；Bluetooth SIG）」，後來陸續加入許多通信、電子、電腦等各領域重量級業者，如：Compaq、Dell、Motorola、3Com、HP、Lucent 及 Samsung，共同訂定藍牙的標準以期降低技術成本，加速應用普及，2008 年 Bluetooth SIG 會員已增加到 10,000 個以上[12]。

IEEE 於 2002 年時已正式將藍牙技術加入 IEEE 802.15.1 的標準，由 IEEE802.15 工作小組訂定標準，並且於 2005 年發表 802.15.1 的修訂版本；目前 Bluetooth SIG 所訂定的協定標準，多已被 IEEE 所採納 [14]。

藍牙基本上有下列三種通訊方式，同一時間只能選擇一種：

1. 一組非同步數據通訊。
2. 三組同步語音通訊。
3. 一組非同步數據通訊，加上一組同步語音通訊。

藍牙支援多個裝置互相連接方式（見圖1）。

- 微網（Piconet）：指的是 2 至 8 台藍牙裝置（電腦、行動電話、數位相機、無線滑鼠、印表機等）的集合體，1 個主裝置（Master device）同時最多能與 7 個 Active 狀態或是 255 個 Standby 狀態的從屬裝置（Slave device）連接，讓眾多的藍牙裝置間可以互相通訊。
- 擴散網（Scatternet）：兩個以上獨立的微網集合所形成的藍牙無線網路。

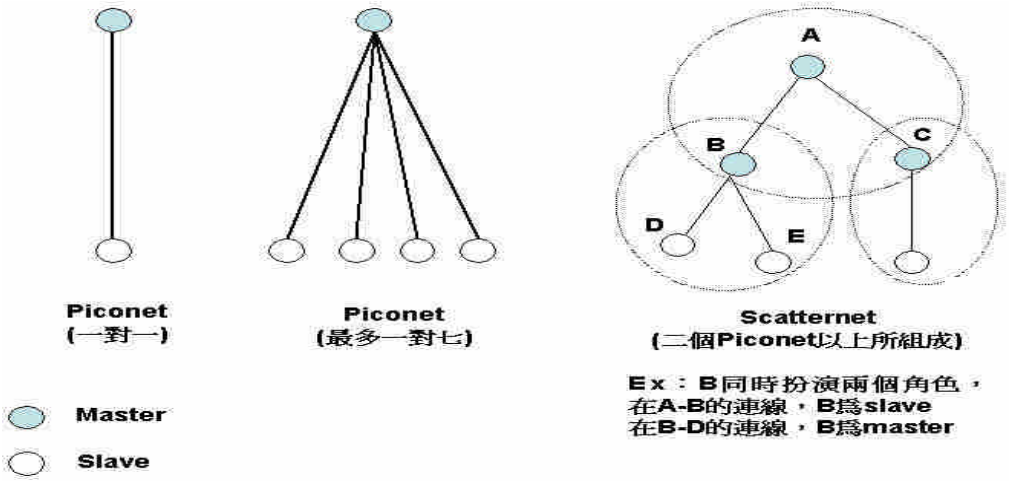
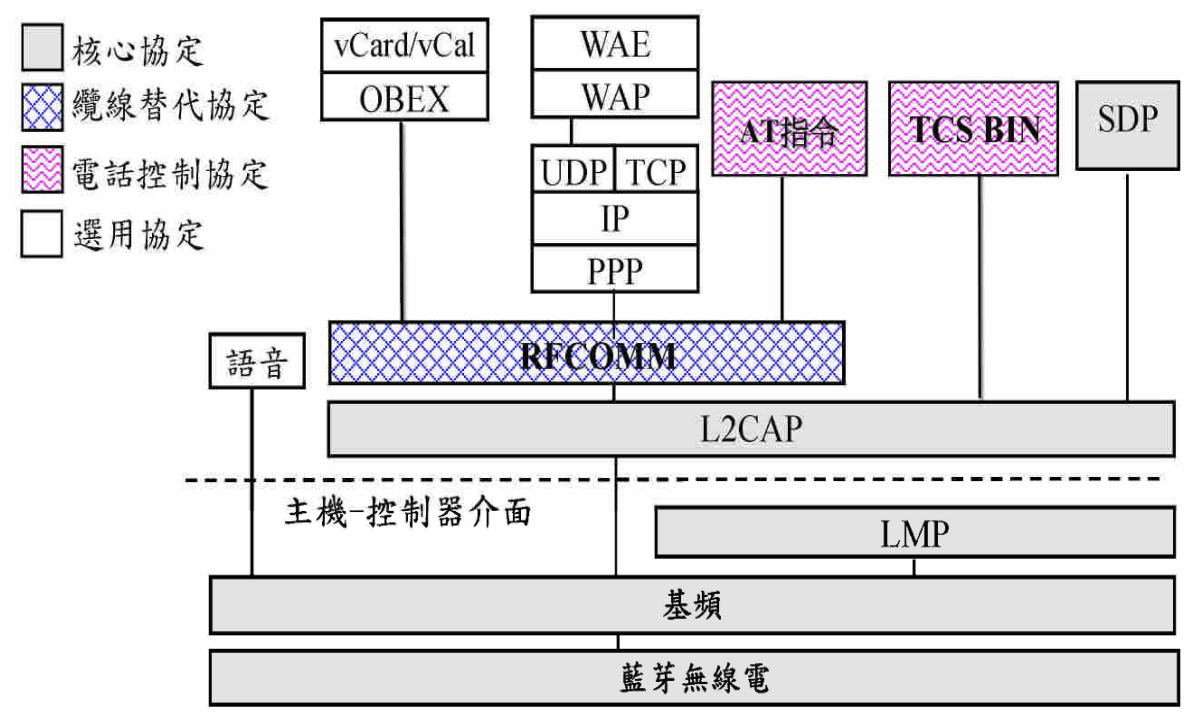


圖 1　微網與擴散網 [**9**]

每個藍牙裝置和網路卡一樣，都有一個唯一的識別碼（裝置位址），藍牙的無線通訊因此可以指定特定的裝置進行配對，以增加通訊的安全性。藍牙的優點有便宜、省電、操作容易、全方位傳輸、具可穿透性與行動性。然而，傳輸速率慢、傳輸距離短則是其缺點。

藍牙通訊協定架構

藍牙通訊協定架構（圖2），包含核心協定（Core Protocol）、纜線替代協定（Cable Replacement Protocol）、電話控制協定（Telephony Control Protocol）以及選用協定（Adopted protocol）協定。可區分為兩個部分，在主機控制器界面（HCI，Host Control Interface）之下為硬體，包括射頻、基頻與鏈結管理；在HCI之上為軟體，包括了L2CAP（Logical Link Control & Adaptation Portocol）以及其它上層協定所組成 [**17**]。



注意序列(Attention Sequence, AT)
網際網路協定(Internet Protocol, IP)
物件交換協定(Object Exchange Protocol, OBEX)
點對點協定(Point-to-Point Protocol, PPP)
射頻通訊(Radio Frequency Comm., RFCOMM)
服務發現協定(Service Discovery Protocol, SDP)
傳輸控制協定(Transmission Control Protocol, TCP)
電話控制規格--二進制(Telephony Control Specification—binary, TCS BIN)
使用者數據電文協定(User Datagram Protocol, UDP)
虛擬行事曆(virtual Calendar, vCal)
虛擬名片(virtual Card, vCard)
無線應用環境(Wireless Application Environment, WAE)
無線應用協定(Wireless Application Protocol, WAP)

圖 2　藍牙通訊協定架構 [**17**]

藍牙成本分析

目前藍牙所使用的頻帶為公開無需付費授權的 2.4G Hz 的 ISM(Industrial、Scientific 與 Medical）頻段，不會增加使用者負擔。隨著藍牙技術的成熟，藍牙晶片的出貨量呈現穩健成長， 2001 年的價格為 150 美元， 2008 年降至低階晶片的成本約為 1~2 美元，中高階晶片約 5~10 美元 [5, 10]。圖 3 為全球藍牙晶片市場規模。

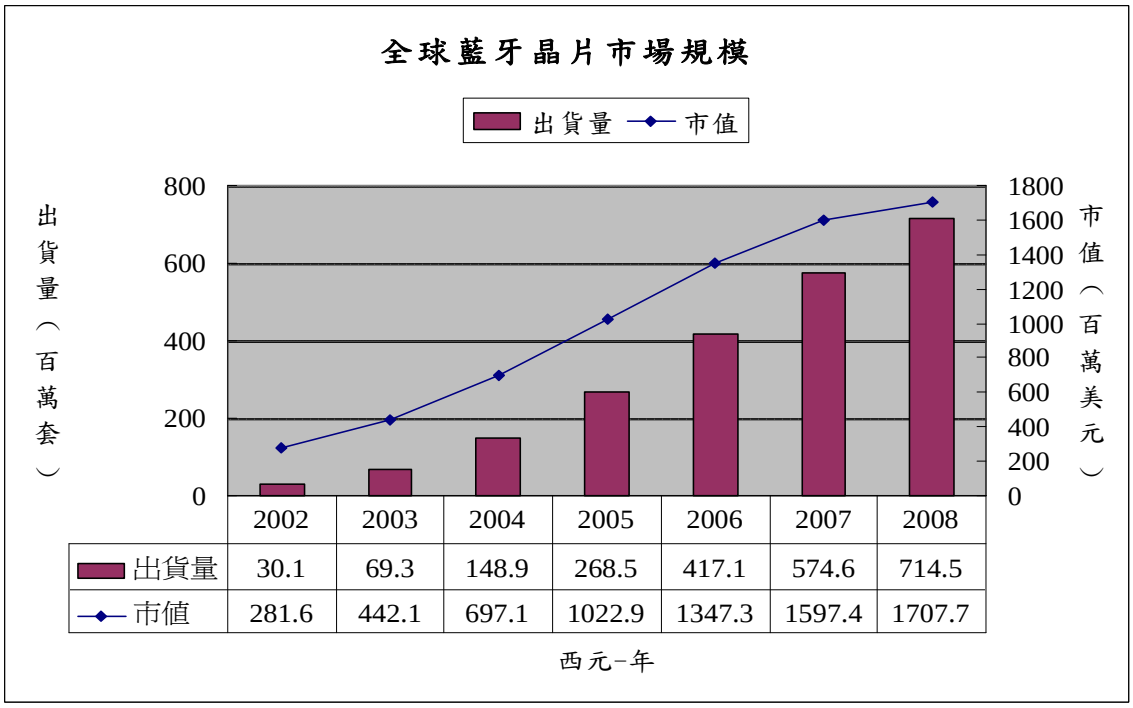


圖 3　全球 Bluetooth 晶片市場規模 [2]

藍牙應用現況

由於藍牙晶片容易嵌入可攜式裝置，除了最先採用藍牙技術的行動通訊裝置外，延伸應用至資料處理裝置，如：滑鼠、印表機、個人電腦、PDA、數位相機、電玩、手錶、汽車、金融付款、家庭感測網路及醫療監控等。

金融領域

藍牙技術已成功跨足小額付款，從瑞典 Ericsson 公司與 Eurocard 合作的 POS 付款實驗 [23]、韓國 LG 公司的汽車匝道收費 [35]，到 ROLLCOMM 公司所推出的 ROLLPAY 付款平台 [15]，ROLLPAY 可使用於 POS 銷售點系統、道路匝道收費、販賣機、網路付款等。

醫療監控領域

結合藍牙技術於醫療監控可有效解決過去因使用有線纜線的缺點與地域限制，且能容易與其它設備溝通，目前常見應用於下面兩方面 [7, 49]：

- **動態監護**：有些病症在平常生活與工作之下需要進行長時間的連續監測，以儘早準確地診斷出重要疾病。此類動態監護的病人需隨身攜帶能連續記錄相關參數的記錄盒。如果利用藍牙技術使傳感器與記錄盒分離，記錄盒放置在衣服口袋或隨身攜帶的公事包中，傳感器利用藍牙點對點無線傳輸技術將數據傳送給記錄盒，免除了各種線材在病人身上纏繞所帶來的不便。

- **遠程監護**：遠程監護和家庭保健監護在遠程醫療領域中是發展最快速、最實用的，不僅為患者帶來方便也減少住院醫療費用。如：病房監護，只需在家中安裝嵌入藍牙晶片的室內探測器，其餘各種醫療設備將數據透過藍牙晶片傳輸到室內探測器，室內探測器再與 Internet 連接將資料傳送到醫院或社區保健中心，達到遠程監護的目的。

藍牙安全架構

藍牙安全主要可分為由鏈結層與服務層提供。此外，藍牙使用跳頻機制，每秒可跳躍高達 1600 次，如此可避免與附近其它微網的藍牙裝置互相干擾；藍牙能根據使用需求，降低無線電波功率並精確的傳送到涵蓋範圍，可使惡意第三者攻擊更加困難。

藍牙的安全需求

藍牙的四個安全需求 [**18**]：

1. 機密性（Confidentiality）：資料只可由經授權的使用者與裝置使用。
2. 真確性（Integrity）：資料在傳送儲存過程中，不能被攻擊者竄改。
3. 可用性（Availability）：獲得授權的使用者在需要的時候，隨時能使用資訊。
4. 身份鑑別（Authentication）：確認使用者的身份。

一般無線網路攻擊包括阻斷服務（DoS，Denial-of-Service）、中間人攻擊（MiTM，Man-in-The-Middle）、欺騙（Spoofing）、假扮（Impersonating）、訊息攔劫（Session Hijacking）、竊聽（Eavesdropping）等。

藍牙主要使用下列三個技術來達成安全性：

- 加密：藍牙裝置使用 Linear Feedback Shift Registers（LFSR）為基礎的 Safer^{+} 加密法（Secure and Fast Encryption Routine）對所傳送的資料與控制訊息加密。
- 身分鑑別：連結時雙方互相驗證對方裝置或是使用者的身分。
- 授權：決定裝置是否允許存取資料或服務的過程，一般多與身分鑑別同時進行。

藍牙安全模式

在藍牙 V2.0 之前的規格，每個藍牙裝置均有三種安全模式[**8**]（圖 4）：

- Security Mode 1 （Non-Secure）：在通訊協定內沒有加入任何的安全保護機制。
- Security Mode 2 （Service Level Enforced Security）：從高層的服務層（應用層）加入安全保護的機制，像是設定權限、安全等級、及驗證時可失敗的次數。
- Security Mode 3 （Link Level Enforced Security）：由底層的鏈結層負責安全保護的工作，包括驗證和編碼。在此模式中兩個藍牙裝置會自動建立通道進行連結的建立，此屬於內建的機制。

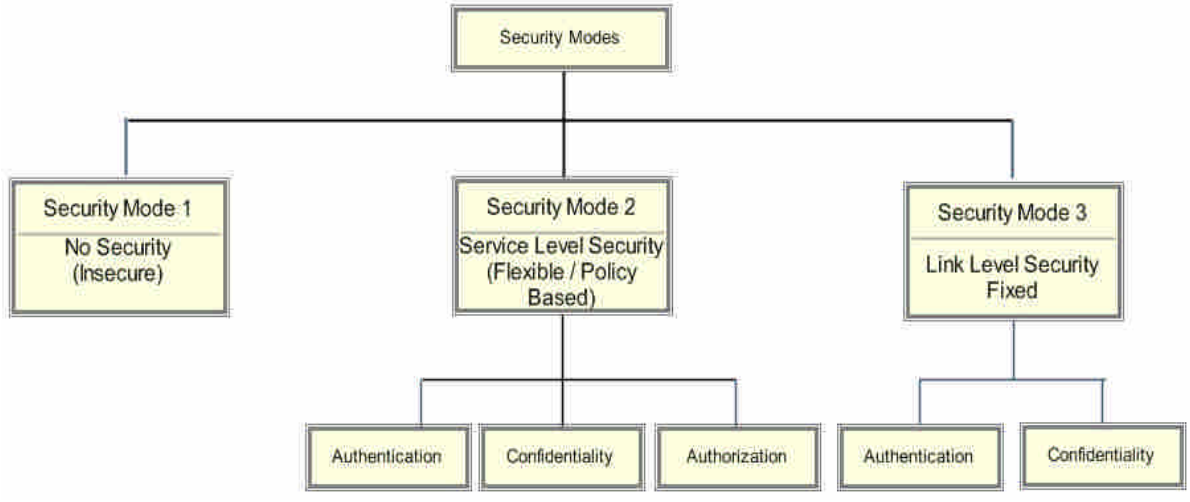


圖 4　藍牙安全模式 [**31**]

在藍牙V2.1新標準中，為滿足使用者的不同安全需求，新增了第四種模式，Security Mode 4 （Service level enforced security）。

又可分為下列4種等級：

Level 0：無安全性，使用 SDP（Service Discovery Protocol）發現對方藍牙裝置即可連線。

Level 1：適用於低安全性，此層級會要求雙方交換藍牙裝置位址。

Level 2：適用於中安全性，需加密，但毋需滿足防止中間人攻擊（如：Just Work）。

Level 3：適用於高安全性，需加密，亦需滿足防止中間人攻擊（如：Numeric Comparison、Out of Band、Passkey Entry）。

2. 藍牙的安全與隱私問題

藍牙技術發展至今，已成功地走入人們的日常生活，如：通訊、電腦、汽車、醫療、影音、金融付款產業等，根據 Bluetooth SIG 於 2007 年的統計 [24]，全球已有超過 10 億個藍牙裝置，數量仍快速增加中。無線技術為人類帶來許多便利性與可能性，然而因使用無線射頻（RF），訊號容易遭受惡意人士竊聽，伴隨而來的安全隱私問題，值得深入探討。

我們將藍牙可能產生的問題舉例說明如下:

隱私（Privacy）

電子裝置一旦全面導入藍牙，消費者可能在不知情的狀況下遭有心人士透過藍牙特殊讀取器蒐集個人產品、信用卡等資訊。即使藍牙裝置內存之資料無機密性或經過加密無法辨識，但透過具唯一性的藍牙裝置位址，將使得消費者的所在位置可以被追蹤。

地點隱私攻擊（Location Privacy Attack），為隱私問題的特殊型態，定義為藍牙裝置不論是否在可發現模式（Discoverable Mode），第三者透過與藍牙裝置進行詢問回應（Inquiries/Response），具有可辨識藍牙裝置身分與是否在某個區域，可推算出藍牙裝置當時或過去的地點，此種攻擊方式屬於新的隱私問題，因此為解決被發現（Discoverability）的問題，建議使用藍牙裝置設為不被發現的模式（Non-Discoverable mode）[30, **48**]。

竊聽攻擊（Eavesdropping Attack）

攻擊者在藍牙網路不像有線網路必須使用實體入侵的方式才能進行竊聽，任何近距離的攻擊者，皆可透過特殊的接收器接收藍牙訊息 [31]。

假冒攻擊（Impersonation Attack）

傳統藍牙透過使用者輸入 PIN 碼作為鑑別鏈結裝置的依據，由於藍牙的許多資訊是以明文方式傳送（例如：藍牙裝置位址、亂數值等），使攻擊者可以透過監聽的方式蒐集資訊 [30, 39]，並進行離線字典攻擊，確認出 PIN 碼或金鑰資訊以進行身分假冒。

重送攻擊（Replay Attack）

攻擊者竊聽與接收藍牙裝置所傳送的封包訊息，並將收到的封包非法重新傳送給接收端，藉此通過鑑別而存取服務 [42]。

阻斷攻擊（Denial-of-Service Attack）

阻斷攻擊（DoS attack）[1, 25, 31, 40, 42]為攻擊者企圖阻止合法的使用者存取藍牙裝置中資訊與服務的方式，常見的攻擊方式有下面三種：

1. 攻擊者可能經由瀑布法（flooding）癱瘓藍牙網路。
2. 透過不斷的傳送假冒資訊或是連結請求，來降低系統的服務能力。
3. 攻擊者假裝成可信任的藍牙裝置（trusted devices），使其它藍牙裝置拒絕真正的可信任的藍牙裝置。

中間人攻擊（Man-in the-Middle Attack）

攻擊者位於合法藍牙裝置間的節點，在不被合法藍牙裝置發現下，進行竊聽、假冒、竄改等攻擊 [29, 30]。一般原因為：

1. 部分重要訊息以明文方式傳遞導致鏈結金鑰被破解。
2. 在微網的所有裝置皆使用相同鏈結金鑰或是無需安全保護模式（安全模式一）。
3. 加密演算法本身有漏洞。

電源消耗攻擊（Battery Exhaustion Attack）

Buennemeyer 等人 [21]所提出的電源消耗攻擊，企圖利用不斷的請求交換訊息方式，消耗藍牙行動裝置中有限的電力。

偷取攻擊（SNARF Attack）

當參加會議、餐廳吃飯、搭乘公共運輸工具旅行時，附近的惡意第三者侵入使用者的手機並更改設定，甚至偷取敏感的資料 [27, 42]，如：電話簿、名片、照片、簡訊和音效檔，事後使用者也無法發覺。

後門攻擊（Backdoor Attack）

藍牙裝置透過「配對」的機制互相通訊。部分電話有功能上的瑕疵，允許它們和之前授權過的裝置做配對，即使此裝置已從授權清單上移除。這個裝置仍可連結你的手機，且有使用你手機所有功能的權限 [37, 42]。

藍蟲攻擊（Bluebug Attack）

惡意第三者可以透過程式的漏洞，連結行動電話的基本「命令集」，可以轉接你的電話，監聽你的對話 [37, 42]。

藍劫攻擊（Bluejacking Attack）

藍劫大部分是無害的，惡意第三者發送惱人的簡訊至附近使用者的手機，就如同垃圾郵件一樣，令人擔心的是，它可能快速地從輕微的騷擾行為演變成危險事件。舉例來說，寄來的文字訊息要求使用者輸入 4 個數字，若照做可能使手機和犯罪者的裝置配對，進而給予他們完全使用你手機的權利，包括連結至儲存的資料。因此，永遠不要回覆這種型式的訊息 [31, 37, 42]。

遠距離攻擊（Long-Distance Attack）

透過指向天線（directional antenna）增加可接觸通訊之距離，使攻擊者不在侷限於 100 公尺之內，就可進行攻擊 [28]。例如：Bluetooone、BlueSniper、Rifle 等。

猜測攻擊（Guess Attack）

利用字典或暴力攻擊法，猜出 PIN 碼或是利用明文傳送的資訊，推導出初始金鑰或鏈結金鑰 [31]。

業界針對藍牙安全弱點常使用的保護策略有下列幾種：

- **選擇沒有安全疑慮的藍牙手機和裝置**

  裝置製造商通常會持續改善產品的問題，也常發佈「修補程式」（patch）來解決現有裝置上的問題。沒有技術能力的人也許會覺得將修補程式安裝到手機很困難，再買一隻不受攻擊的手機較為容易。此保護策略可避免由手機的缺陷所造成的偷取攻擊、後門攻擊、藍蟲攻擊、藍劫攻擊。

- **將手機保持在「隱藏」模式**

  將手機保持在隱藏模式，確保未授權的人無法發現藍牙裝置的存在，而試著連結裝置 [33, 44]。此保護策略可避免攻擊者藉由唯一性的藍牙裝置位址進行追蹤，影響隱私。

- **當不使用藍牙時，關閉此功能**

  在不使用或不需要時關閉藍牙功能，為避免遭受竊聽攻擊，也應避免藍牙裝置在公開環境配對 [33, 44]。此保護策略可減少攻擊的機會。

此研究主要針對眾多學者認為藍牙安全機制中安全性最弱的部分-首次連線需進行的配對過程作探討分析，由於藍牙 V2.0 之前的安全機制-Legacy Pairing 在身分鑑別和金鑰的建立過程中許多資訊是以明文方式傳遞，所以惡意的第三者因此可以假冒藍牙裝置通過鑑別，也可推導出通訊的加密金鑰，進而監聽傳送的資料；雖然藍牙 V2.1 新標準安全機制-Secure Simple Pairing 已解決上述問題，但 Diffie-Hellman 金鑰交換有中間人攻擊的威脅，使用者需以目視比對雙方裝置上顯示數字的方式來防止，然而此種方法容易產生操作失誤，加上連接便利且省電可全天候開啟，更加深了被入侵的風險。

3. 藍牙 V 2.0 之前的安全協定-Legacy Pairing

3.1 協定流程

藍牙的安全機制包含金鑰管理、加密和鑑別三個部分。使用者在兩個藍牙裝置上輸入相同的 PIN 碼就能連結成功，為了減少 PIN 的外洩機會，所以兩個藍牙裝置會在首次連結的配對過程各自產生一個連結金鑰，此後的連結則改以連結金鑰進行鑑別與加密 [32]。

我們將本文所使用的名詞解釋整理列於表 1。

表 1 藍牙 V2.0 - Legacy Pairing 名詞解釋

BD_ADDR	藍牙裝置位址（如BD_ADDR_A，A的藍牙裝置位址）
RAND	亂數（IN_RAND_A當產生初始金鑰階段，A所產生亂數； AU_RAND_A，鑑別的階段，A所產生亂數）
PIN	個人識別碼（Personal Identification Number）
L	個人識別碼的長度
C_X	驗證值 （如C_A，由A產生的驗證值）
H()	不可逆推的雜湊函數

COF	密文偏移數（Ciphering Offset Number）
SRES	驗證值
ACO	鑑別密文偏移數
K_A、K_B	裝置金鑰（Unit key），（如K_A，由A產生裝置金鑰）
K_init	初始金鑰
K	鏈結金鑰
K_E	加密金鑰
⊕	互斥或（XOR）
g^{XY}	Diffie-Hellman產生的鏈結金鑰

(續表 1)

此研究主要是針對 Security Mode 3 進行研究。每個藍牙裝置皆有四個資訊用於維護連接層的安全：

- BD_ADDR：每一個藍牙裝置都有一個獨一無二的 48 位元藍牙裝置位址（Bluetooth Device Address），此位址是由 IEEE 所制定的。
- Link Key：用於身分鑑別的 128 位元連結金鑰。
- Encryption Key：8~128 位元的加密金鑰，用於對藍牙裝置間握手後傳輸的資料加密。
- Random Number（RAND）：由藍牙裝置自行產生的隨機亂數值。

我們將藍牙裝置的身分鑑別與加密流程彙整（見表 2）。兩個藍牙裝置首次連接時，會先經過配對（pairing）產生連結金鑰（步驟 0、1.a、1.b 與 1.c），完成配對後再進行後面的身分鑑別和資料傳輸加密（步驟 2.a、2.b 與 2.c），第二次以後的連結即可省略配對的過程，直接進行身分鑑別和資料傳輸加密（步驟 2.a、2.b 與 2.c）[11]。

表 2 藍牙 V2.0 - Legacy Pairing 裝置的身分鑑別與加密流程

0、裝置 A 啟始階段：	0、裝置 B 啟始階段：
產生單元金鑰 K_unit	產生單元金鑰 K_unit
1.裝置間首次連結的配對步驟	
a.產生初始金鑰 K_init	
b.使用初始金鑰 K_init 相互鑑別	
c. 使用初始金鑰 K_init 交換連結金鑰 K_link	
2.裝置間每次連結時的握手步驟	
a.使用連結金鑰 K_link 相互鑑別	
b. 使用連結金鑰 K_link 產生加密金鑰 K_E’	
c. 以加密金鑰 K_E’對傳輸資料加密	

資料來源：[32]

首先在步驟 0，藍牙裝置 A、B 將各自產生的 128bits 亂數 $RAND_A$，$RAND_B$ 與其裝置的位址帶入 E21 演算法產生出單元金鑰 K_unit （K_A 與 K_B）（見圖 5）。

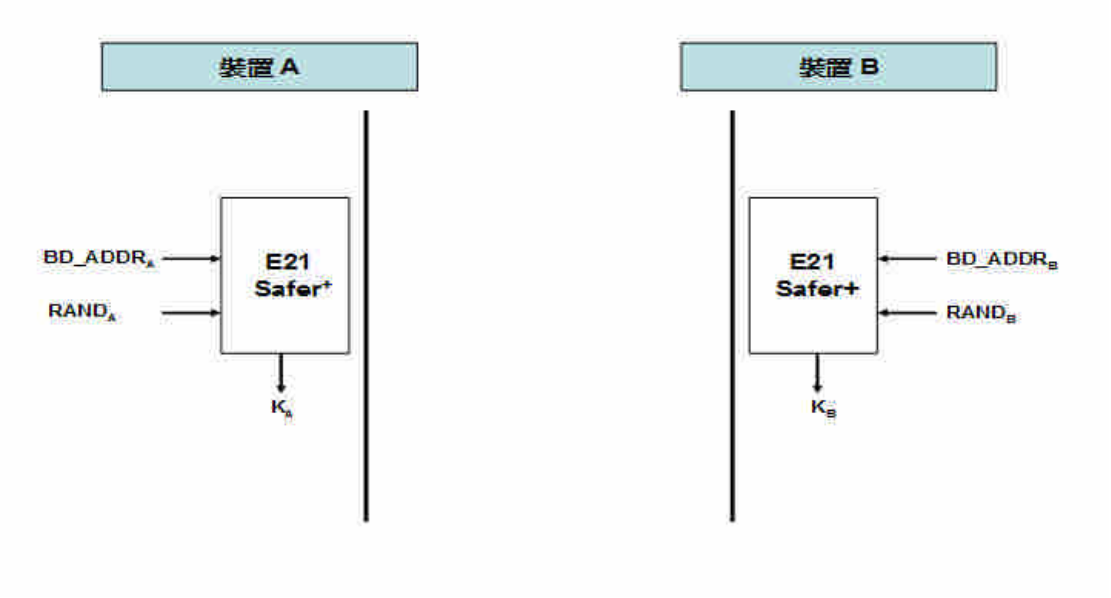


圖 5　步驟 0 產生單元金鑰 K_unit [32]

在步驟 1.a，藍牙裝置 A、B 以裝置 A 產生的亂數 IN_RAND_A、共享的 PIN、PIN 的長度 L 與裝置 B 的裝置位址 BD_ADDR_B 帶入 E22 演算法產生出初始金鑰 K_init（見圖 6）。

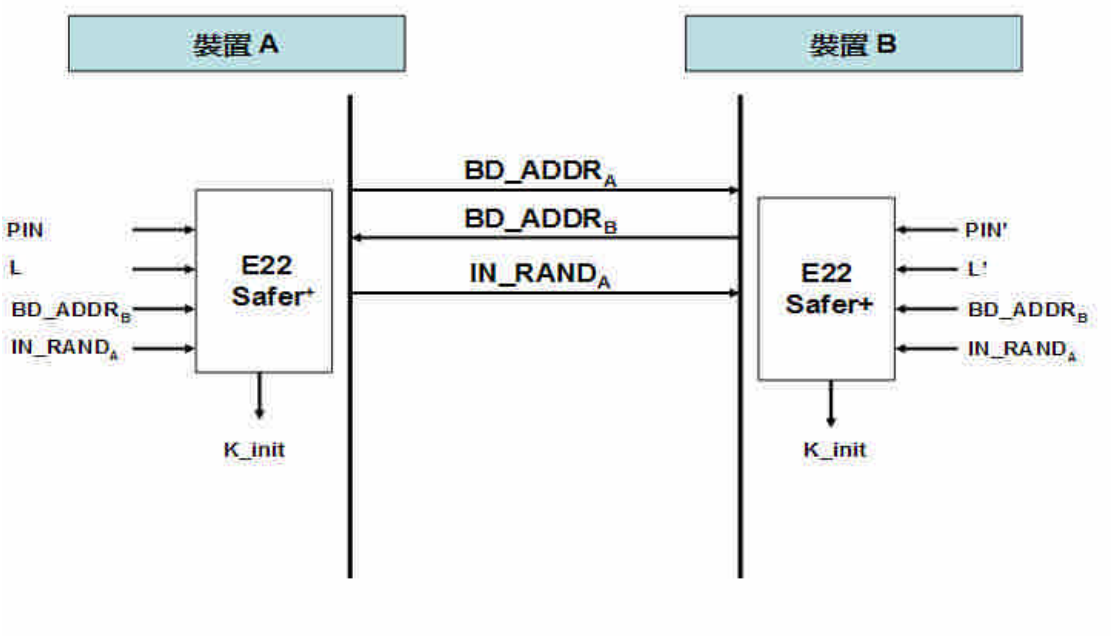


圖 6　步驟 1.a 產生初始金鑰 K_init [32]

在步驟 1.b 中，藍牙的身分鑑別是使用 E1 Safer$^+$演算法進行挑戰與回應。裝置 A 會發出一個 128 位元的隨機亂數 AU_RAND_A 挑戰值傳給裝置 B，B 則將收到的挑戰值，跟自己本身的藍牙位址 BD_ADDR_B 和連結金鑰 K_init 帶入 E1 Safer$^+$計算出 SRES'與 ACO'，再將 SRES'作為回應值傳給 A，供 A 鑑別其身分；反之可以經過裝置間角色互換的動作由裝置 B 當驗證者來識別 A 時會以上述同樣動作使 A 產生 SRES 值傳回給 B 供 B 鑑別其身分，達到相互鑑別（Mutual Authentication）（見圖 7）。

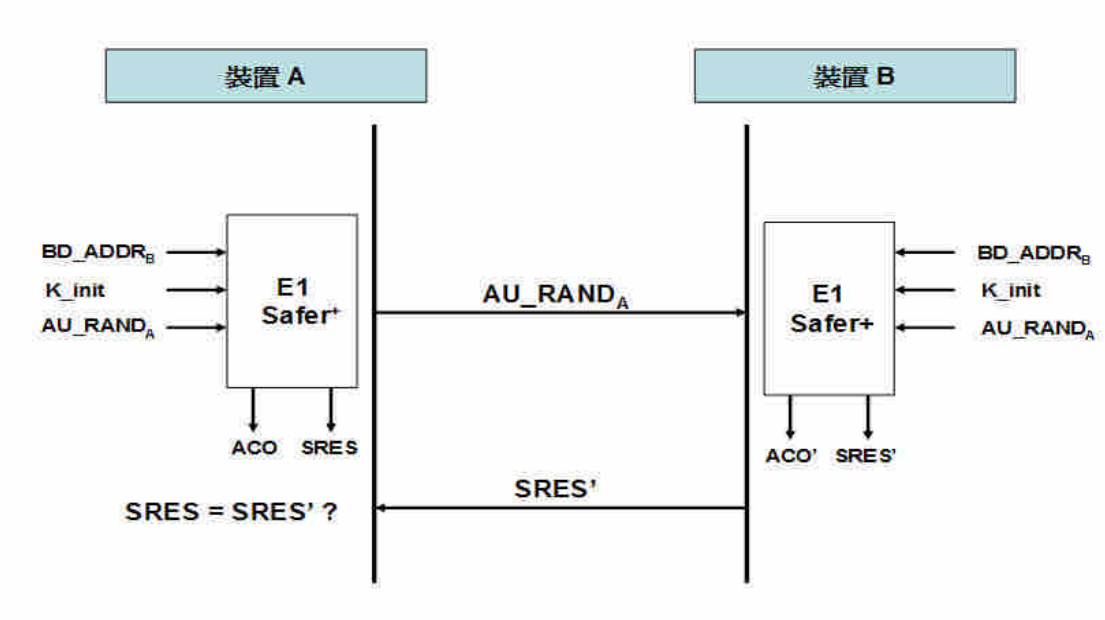


圖 7　步驟 1.b 使用初始金鑰 K_init 相互鑑別 [32]

當藍牙裝置記憶體有限的情況，進行步驟 1.c.1，就利用單元金鑰 K_unit（K_A）來作為連結金鑰 K_link。A 將 K_init 與 K_A 進行 XOR 運算產生 K 值傳給裝置 B，裝置 B 再利用 K_init 跟 K 值進行 XOR 運算取出單元金鑰 K_A，以達到連結金鑰的交換（見圖 8）。

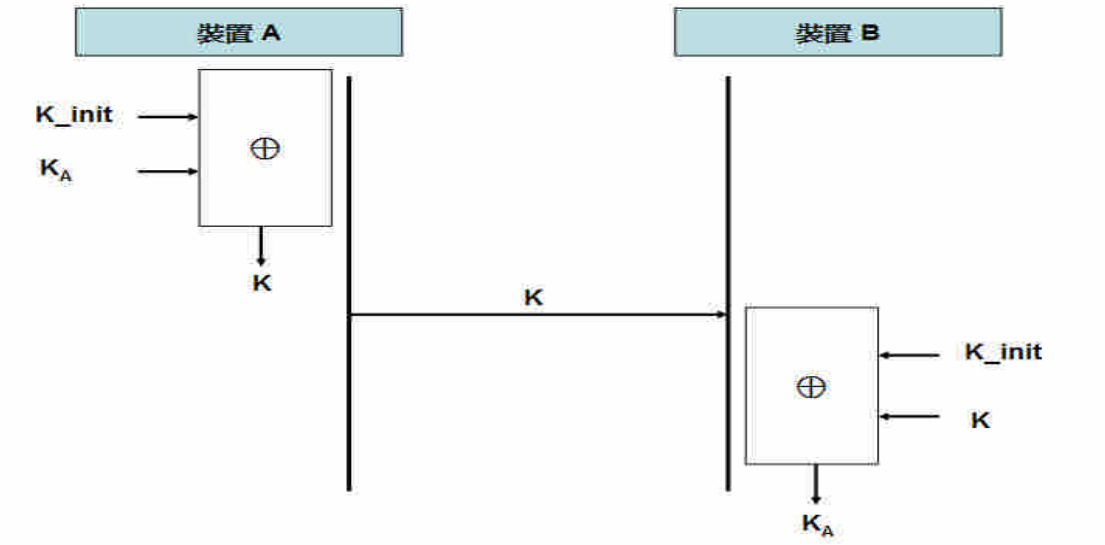


圖 8　步驟 1.c.1 記憶體有限時：連結金鑰 = 單元金鑰（K_A）[32]

記憶體足夠時則進行步驟 1.c.2，藍牙裝置 A 與 B 利用步驟 0 中各自產生的亂數以初始金鑰 K_init 作 XOR 運算保護（C_A 與 C_B），傳給對方；再各自以 K_init 取出對方產生的亂數值（$RAND_B$ 與 $RAND_A$），再以其與對方的 BD_ADDR 帶入 E21 計算出對方的單元金鑰（K_B 與 K_A），最後將雙方單元金鑰作 XOR 算出 K_{AB} 作為連結金鑰 K_link（見圖 9）。

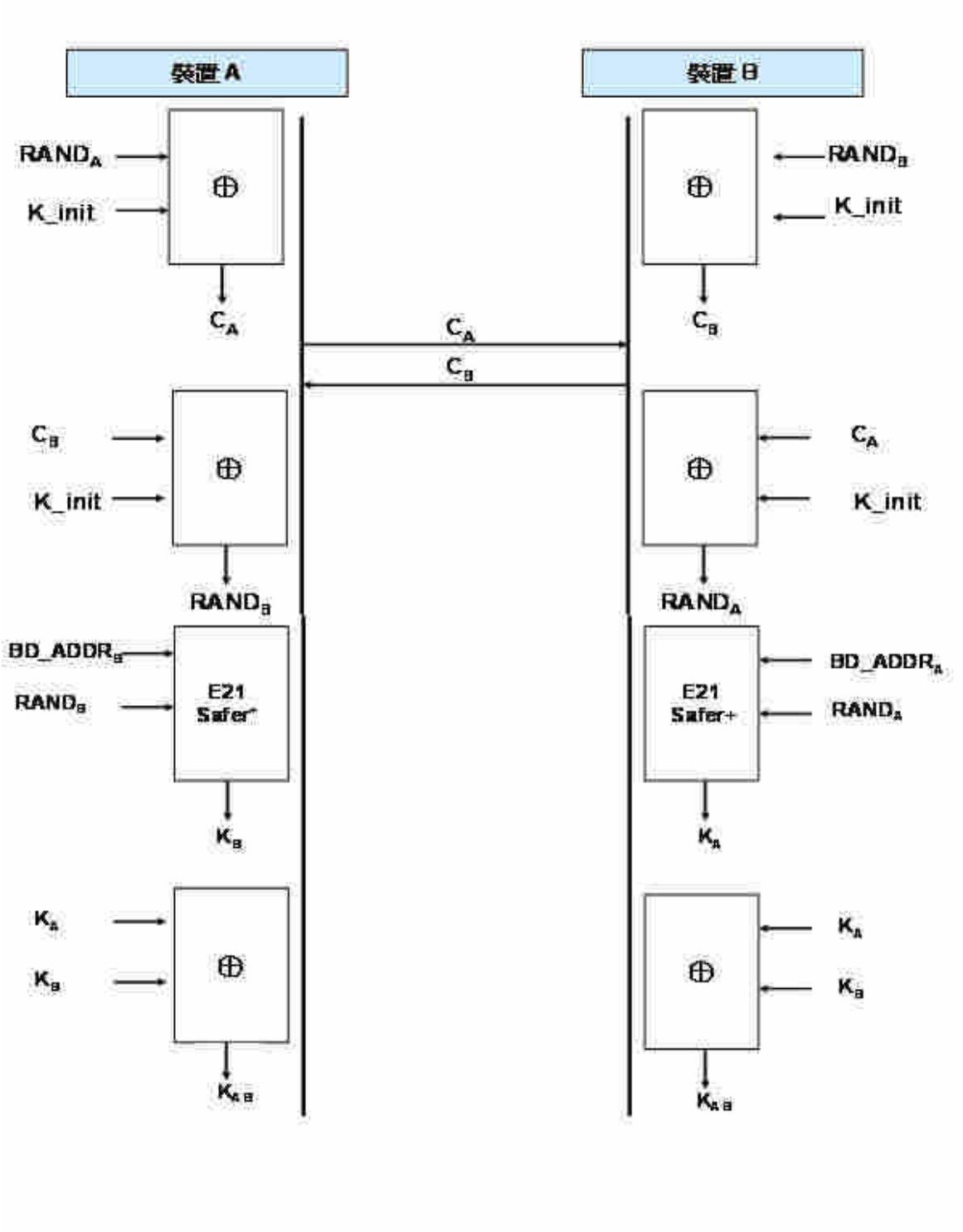


圖 9　步驟 1.c.2 在記憶體足夠時，連結金鑰 = K_{AB} [32]

以上為藍牙裝置首次連結時所需進行的配對過程，接下來是每次連結皆需進行的握手步驟，步驟 2.a 與藍牙裝置首次連結以 PIN 進行的身分鑑別的動作相似，差別只在於此以連結金鑰 K_link 進行身分鑑別（見圖 10）。

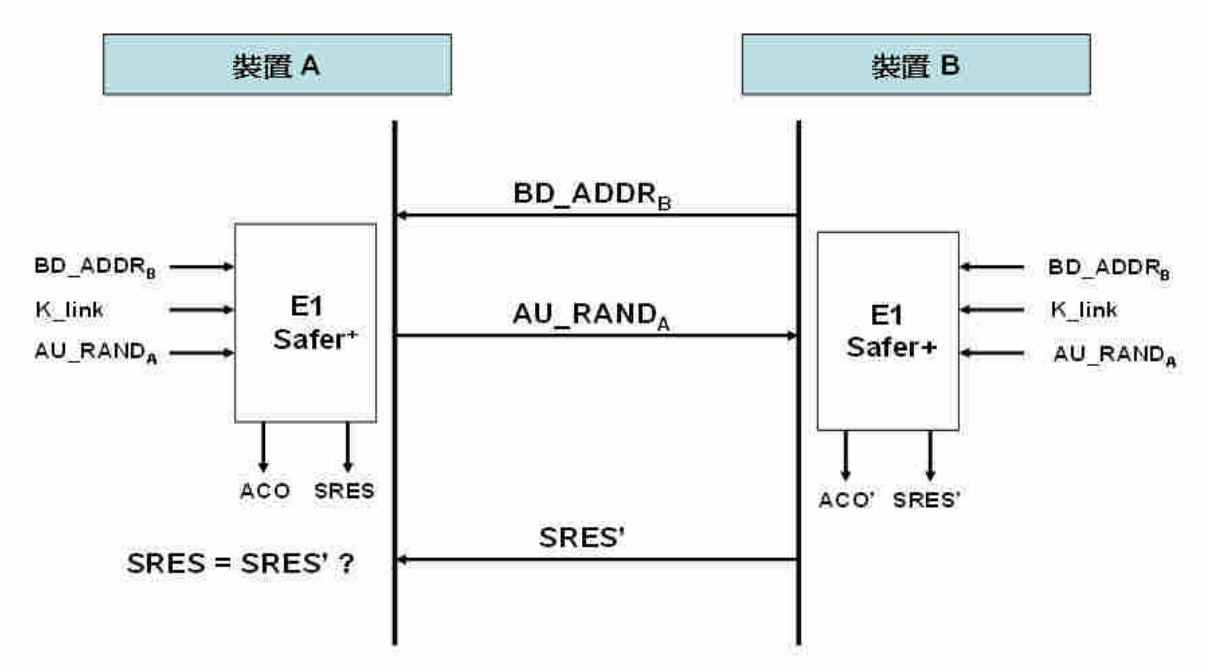


圖 10　步驟 2.a 使用連結金鑰 K_link 相互鑑別 [32]

步驟 2.b 中，藍牙裝置 A 先產生一個 128 位元隨機亂數 EN_RAND_A 並傳給 B，接下來各自以此亂數、K_link 與由上個步驟 ACO 推導出的 96 位元密文偏移數（Ciphering Offset Number，COF）帶入 E3 再經 RED 演算法產生加密金鑰 K_E'（見圖 11）。

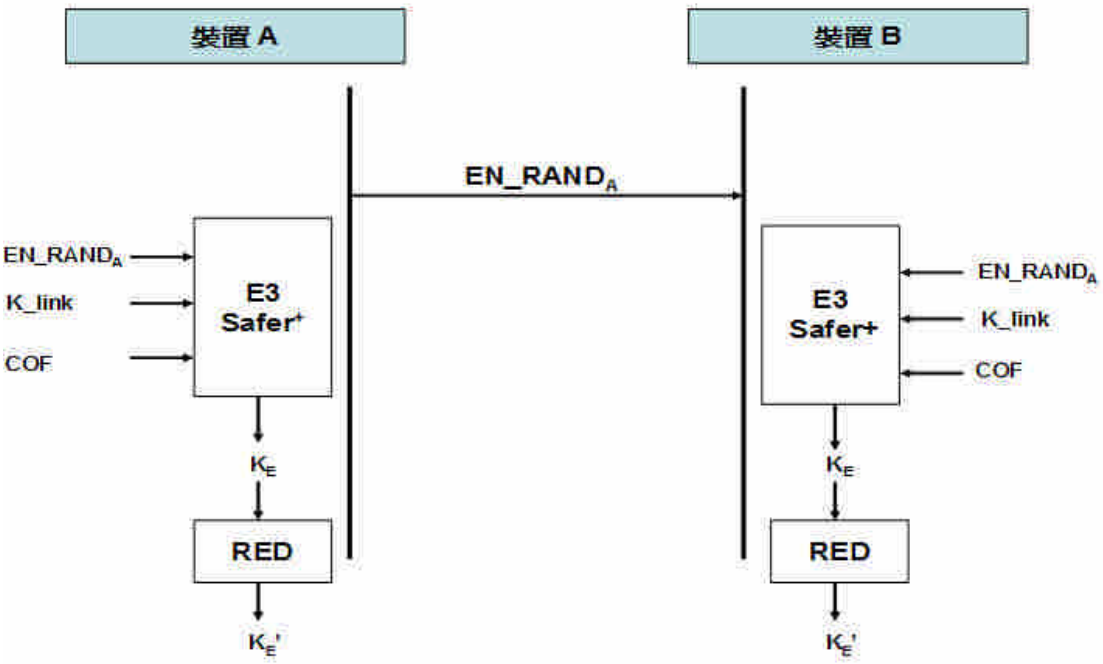


圖 11　步驟 2.b 產生加密金鑰 K_E' [32]

最後，藍牙裝置 A 與 B 將 K_E'、BD_ADDR_A 與 $Clock_A$（時間間格，從屬裝置的時間必須正確地與主裝置同步，以找出遺失和重送的封包）透過 E0 演算法計算出加密串流，將欲傳送的資料以 XOR 運算作加解密（見圖 12）。

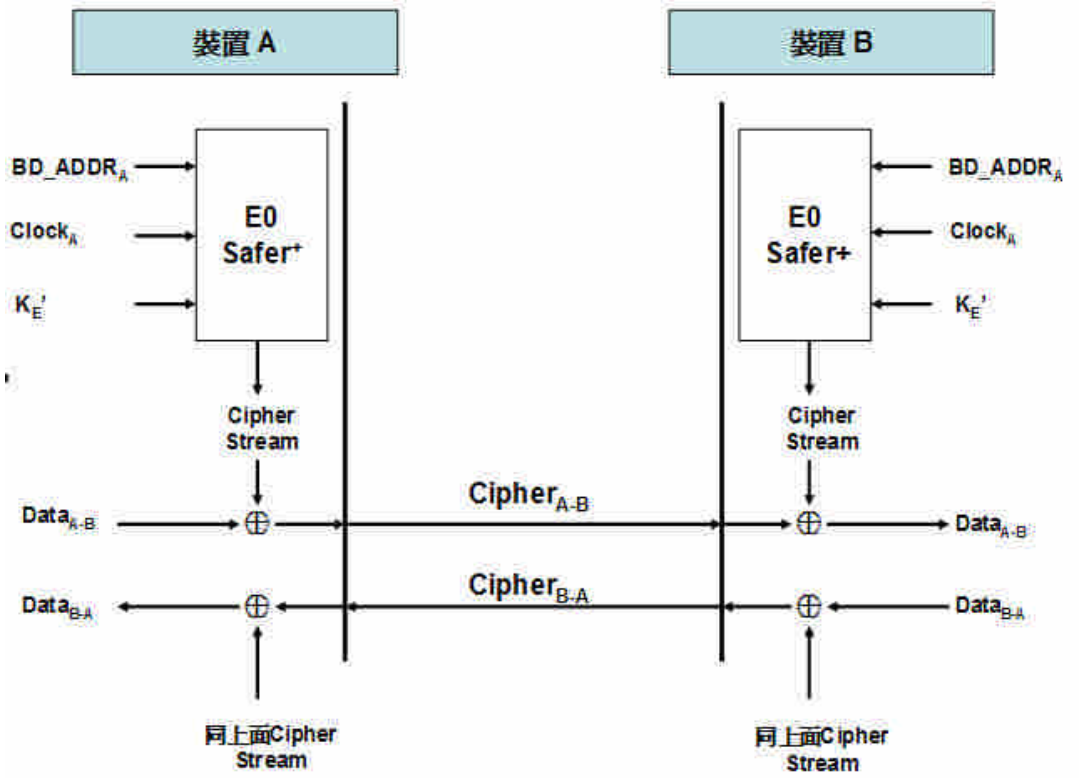


圖 12　步驟 2.c 對傳輸資料加密 [32]

3.2　問題

因為在兩個藍牙裝置中 PIN 碼為一個共享的秘密，但使用者多設定容易猜測的 PIN 碼，或未設定直接使用裝置的預設值 0000；加上在藍牙的身分鑑別和金鑰的建立過程中，許多資訊是以明文方式傳遞（見表 3），所以惡意的第三者因此可以假冒藍牙裝置通過鑑別，也可推導出通訊的加密金鑰 K_E'，進而監聽傳送的資料，流程如下：

表 3 藍牙 V2.0 - Legacy Pairing 的明文傳遞資訊

問題點	來源	目的地	訊息	備註
1.a	A	B	BD_ADDR_B 、IN_RAND_A	明文傳遞
1.b	A	B	AU_RAND_A、SRES’	明文傳遞
1.b	B	A	AU_RAND_B、SRES	明文傳遞
1.c.1	A	B	K	明文傳遞，由 K_unit 和 K_init 經由 XOR 運算得知
1.c.2	A	B	C_A、C_B	明文傳遞
2.a	A	B	BD_ADDR_B 、AU_RAND_A、SRES’	明文傳遞
2.a	B	A	BD_ADDR_A 、AU_RAND_B、SRES	明文傳遞
2.b	A	B	EN_RAND_A	明文傳遞

1、首先在步驟 1.a 中，攻擊者由明文傳遞的 BD_ADDR_B 和 IN_RAND_A，以及容易猜測的 PIN 碼或設為預設值 0000（L：為 PIN 碼的長度，因此得知 PIN 碼即能得知 L 的長度），即可推導出初始金鑰 K_init。
2、在步驟 1.b 中，攻擊者可由明文傳遞的 AU_RAND_A 值與上步驟 1.a 中的明文傳遞的 BD_ADDR_B 與推出的 K_init，經 E1 Safer$^+$運算，得知 SRES'和 ACO'，而假冒 B 通過 Device A 的鑑別。
3、在步驟 1.c.1 中，攻擊者由明文傳遞的 k 與步驟 1.a 推出的 K_init，即可計算連結金鑰 K_unit。
在步驟 1.c.2 中，攻擊者將明文傳遞的 C_B 與步驟 1.a 中推出的 K_init 作 XOR 運算以取得 $RAND_B$；再以 $RAND_B$ 與步驟 1.a 中明文傳的 BD_ADDR_B 帶入 E21 函數計算出 K_B。攻擊者再以明文傳的 C_A 與步驟 1.a 中推出的 K_init 作 XOR 運算以取得 $RAND_A$；再以 $RAND_A$ 與步驟 1.a 中明文傳的 BD_ADDR_A 帶入 E21 函數計算出 K_A，最後計算 $K_A \oplus K_B$ 推出連結金鑰 K_{AB}。
4、在步驟 2.a 中，攻擊者由明文傳遞的 BD_ADDR_B 和 AU_RAND_A，加上在步驟 1.c.1 或 1.c.2 中推出的 K_link（即 K_unit or K_{AB}）帶入 E1 Safer$^+$函數，計算出 SRES'和 ACO'，可假冒 B 通過 A 的身分鑑別。
5、在步驟 2.b 中，攻擊者由明文傳遞的 EN_RAND_A，與步驟 1.c.1 或 1.c.2 中得知的 K_link，再加上步驟 2.a 的 ACO'推出的 COF，帶入 E3 函數算出加密金鑰 $K_{E'}$。
6、在步驟 2.b 中，算出加密金鑰 K_E 後就能夠監聽傳送假訊息或惡意的竄改傳送的訊息。

藍牙裝置 PIN 碼可設為 1 到 16 碼，但由於人的記憶有限設定的 PIN 碼大多只有幾碼，在 Robert（2004）的研究指出有些裝置出廠時已經被設為特定值且無法再修改 [1]，因此惡意的第三者可以利用離線字典攻擊將所有可能的 PIN"一一代入測試，並藉由協定中傳遞的明文資訊推導出 K_init"，並計算出驗證值 SRES"再與配對過程中傳輸的 SRES'比對，以驗證猜測的 PIN"是否正確。找出正確的 PIN 後，接下來便可以假冒藍牙裝置通過鑑別，同時也可利用 K_init"推導出 K_link，進而推導出通訊的加密金鑰，進而監聽傳送的資料。根據 Shaked 與 Wool 學者（2005）的研究指出破解 4 碼的 PIN 使用 P4 的電腦僅需要 0.063 秒，而 7 碼的 PIN 值也只需要 76.127 秒 [39]。

3.3 文獻提出之解決方法

為了解決藍牙所產生的潛在安全與隱私問題，目前針對藍牙標準 V1.X~V2.0 相關文獻所提出的解決方案，可分為下列四大種類：

（1）PIN 碼加強

當使用者要進行初次藍牙裝置連結通訊時需先進行配對，此時雙方需輸入相同的 PIN 碼，但因使用者大多使用預設值 0000 或過於簡單的 PIN 碼，加上規定的 PIN 碼長度太短（4~8 個字元）且多固定不變，因此有心人士可利用被動竊聽攻擊與離線字典攻擊，進而猜出 PIN 碼；學者提出藉由將 PIN 加強 [26, 30, 46, 47]（例如：Encrypted Key Exchange，EKE 或是限制 PIN 碼長度為 16 碼。）來增加破解所需的時間，但因為目前科技進步快速，單純以 PIN 碼加長，仍然具有相當使用風險，使用者也不容易記憶長的 PIN 碼，而較難以被廣大的消費大眾所接受。

（2）關閉藍牙裝置的回應功能

藍牙裝置未使用時將回應功能關閉 [16, 47]，當其它藍牙裝置提出連線請求

時，便不會做出任何回應（或是將接送功率降低）；要啟用藍牙裝置時，再將回應功能開啟，如此能降低有心人士得知藍牙裝置的所在位置，以保護使用者不容易被追蹤。

（3）利用服務層提供安全性

以應用層來提供保護雙方連線的基礎（例如利用智慧卡提供的鑑別功能、IPSec、SSL、PPTP 保護連線資訊等 [13,16, 42-45]），然而雙方必需在相同的基礎之下才能通訊；如果標準不同，雙方必須降低安全性至相同標準才能連線，如此安全性將比鏈結層更低。

（4）橢圓曲線 Diffie-Hellman 金鑰交換

以熵度較高的橢圓曲線 Diffie-Hellman Exchange [47]來取代原先鏈結層中配對使用的 Safer^{+}演算法，以防止被動竊聽以及離線字典攻擊，增長被破解所需的時間。

3.4 我們提出的改善協定

Vaudenay（2005）的研究指出藍牙安全機制最弱的一環在兩個裝置首次連接的配對過程（Pairing） [46]，因此我們提出的新協定主要在改善配對的過程，以提高其安全性。

協定流程

在藍牙配對過程中，首先兩個藍牙裝置先互傳位址（見圖 13）。

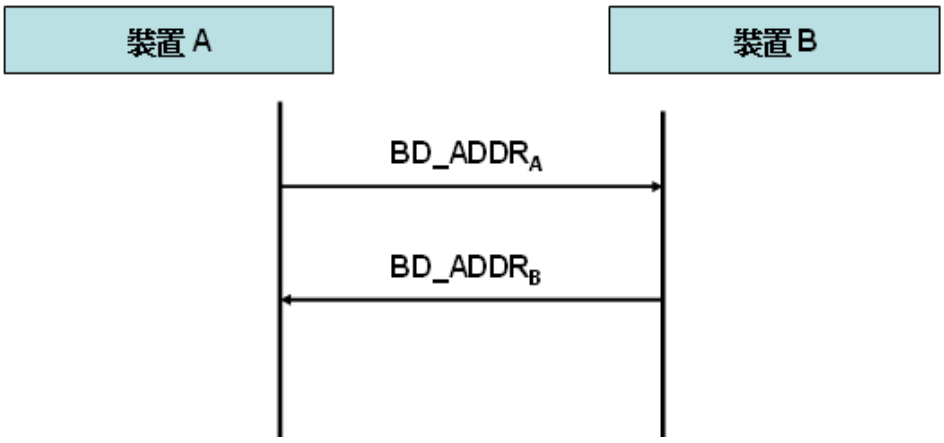


圖 13　步驟 1.a 藍牙裝置間交換彼此的裝置位址

接下來針對裝置記憶體有限的環境，裝置 A 產生亂數 $RAND_A$ 並與 PIN 的雜湊函數值 H（PIN）作 XOR 運算後傳給裝置 B，裝置 B 再以自己的 PIN 算出 H（PIN）與收到的值作 XOR 運算以取出 $RAND_A$，達到連結金鑰的交換（見圖 14）。

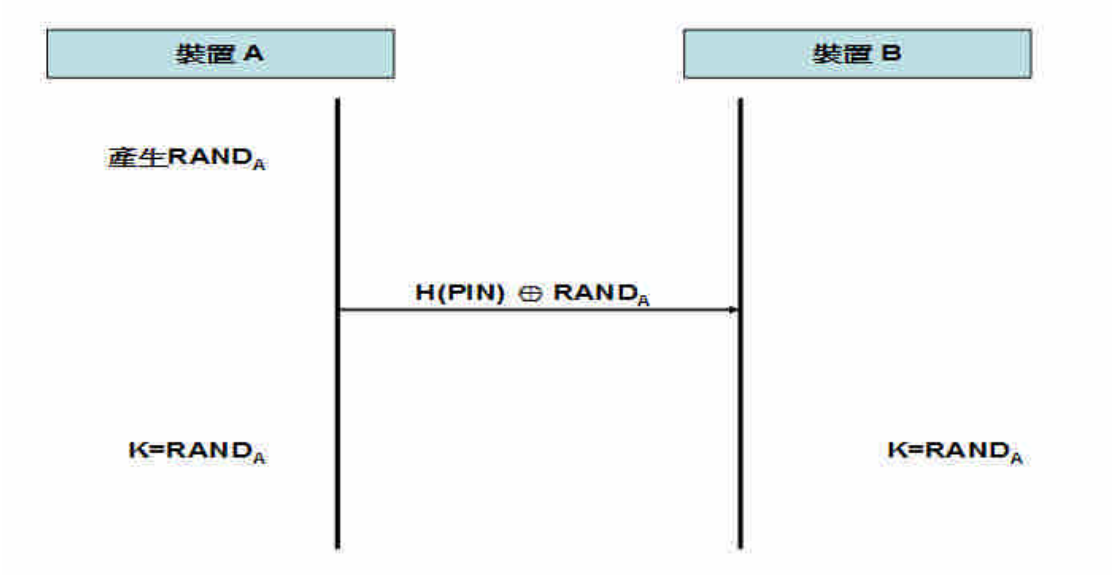


圖 14　步驟 1.b.1 記憶體有限時：連結金鑰 = $RAND_A$

若在記憶體足夠的環境下，則進行步驟 1.b.2，我們利用 Diffie-Hellman 金鑰交換的方式，裝置 A 先產生隨機亂數 $RAND_A$ 當作 X，透過運算產生對應的公開值 g^X 並與 h（PIN）做 XOR 運算後傳給裝置 B；裝置 B 也產生隨機亂數 $RAND_B$ 當作 Y，透過運算產生對應的公開值 g^Y 並與 h（PIN）做 XOR 運算後傳給裝置 A。裝置 B 收到訊息 $g^X \oplus$ h（PIN）後以 PIN 取出 g^X 後，與裝置 B 自己產生的隨機亂數 Y，然後計算出連結金鑰 $K_{AB}=(g^X)^Y$；而裝置 A 收到訊息 $g^Y \oplus$ h（PIN） 後以 PIN 取出 g^Y 後，與裝置 A 自己產生的隨機亂數 X 計算出連結金鑰 $K_{AB} = (g^Y)^X$ （見圖 15）。

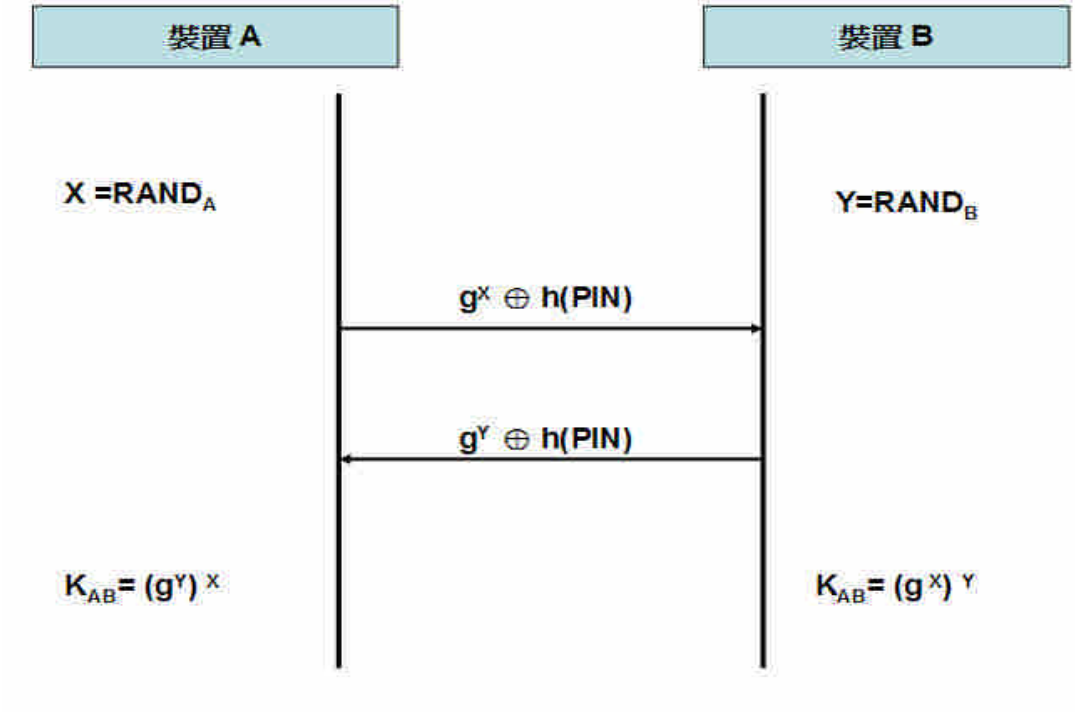


圖 15　步驟 1.b.2 記憶體足夠時：連結金鑰 = K_{AB}

接下來每次連結時的握手步驟與原有的藍牙機制相同。

比較分析

在原有的藍牙安全機制中僅有一個共享的秘密值 PIN。然而，使用者設定的 PIN 很容易猜測，加上配對過程中均以明文傳遞各項資訊，使惡意的第三者得以取得 SRES 作為驗證值，由此可進行離線字典攻擊，依序測試可能的 PIN，最後可找出正確的值。我們改善的部份主要是避免惡意的第三者取得驗證值，以提升藍牙的安全性。

在裝置記憶體有限的情況下，我們簡化了程序，省略單元金鑰 K_unit 與初始金鑰 K_init 的產生，提升了運作效率，並維持原有的安全性，裝置間仍以 PIN 作身分鑑別，並以亂數作傳輸保護。

在原有的藍牙機制中，因為有惡意的第三者能收集到明文資訊 SRES'作為驗證值利用字典或暴力攻擊法破解去依序代入測試找出正確的 PIN 值，由於這種方式可以離線進行，其使威脅增加。因此在裝置的記憶體足夠的情況下，我們利用 Diffie-Hellman 的金鑰交換方式，使得惡意的第三者無法利用離線攻擊的方式去猜測 PIN，每次的 PIN 猜測與驗證均需在線上進行，並且加入 H(PIN)以避免 Diffie-Hellman 可能有的中間人攻擊。

4. 藍牙 V 2.1 安全協定-Secure Simple Pairing

4.1 協定流程

Bluetooth SIG 於 2007 年 7 月 26 日提出 V2.1 新標準 [19]，在安全性方面提出新的配對方式 Secure Simple Pairing（圖 16） 以解決舊版 Pairing 現有的問題 （例如：離線字典攻擊、中間人攻擊），主要的改變是不需輸入 PIN 碼，由使用者進行視覺數字比對來進行鑑別，並可整合其它通訊技術如 NFC（Near Field Communication），也能與之前版本的藍牙裝置互相通訊。

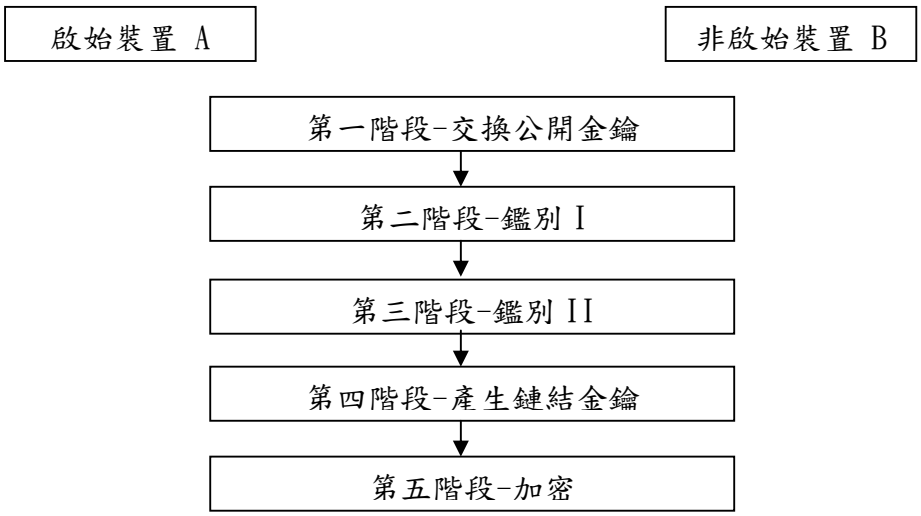


圖 16　Secure Simple Pairing [20]

第一階段交換公開金鑰：雙方裝置交換彼此的裝置位址與連線能力，以辨識對方與了解對方所支援的連線能力，並利用橢圖曲線Diffie-Hellman方式交換公開金鑰（圖17），計算出共享金鑰DH Key = FIPS-P192(g^X, g^Y)，FIPS-P192演算法的熵度比過去SAFER$^+$高，能有效防止離線字典攻擊。

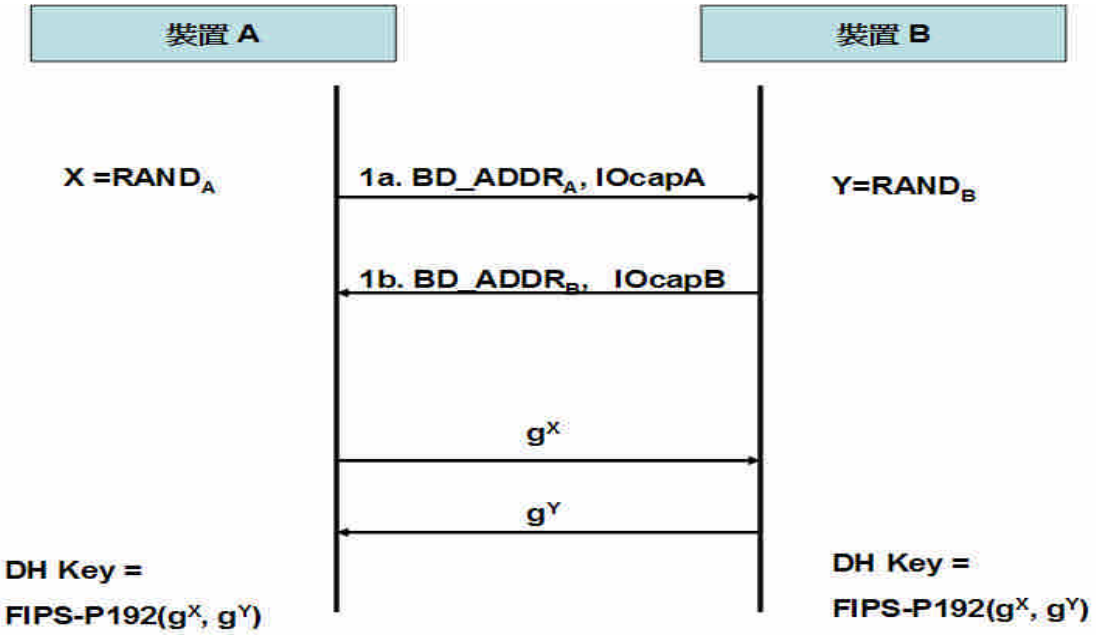


圖 17　交換公開金鑰 [20]

第二階段鑑別 I:驗證雙方於第一階段交換的公開金鑰(g^X, g^Y)與此階段交換的亂數(Na, Nb）皆傳送無誤。此階段依驗證方式的不同，可分為下列四種模式：

（1） Numeric Comparison 模式（圖 18）

適用於雙方裝置均具有六位數字的顯示能力，並能輸入是與否的情況，如:手機和 PC 連線。運作方式為雙方先各自產生亂數（裝置 A 產生 N_A ，裝置 B 產生 N_B）；接下來裝置 B 產生驗證值 Cb，並傳給裝置 A；雙方並交換彼此的亂數，裝置 A 自行計算出驗證值與收到的 Cb 比對，若不相同則拒絕連線，若相同則雙方裝置各計算出六位數字的視覺比對碼（Va, Vb），供使用者作自視比對，若 Va = Vb 則完成此階段的鑑別。

優點：

1. 在許多未具唯一命名的裝置時，使用者亦可確認裝置間正確鏈結。
2. 解決中間人攻擊的問題。
3. 惡意的第三者即使看見展示數字，也無法從解密獲利。
4. 適用於安全性需求高的環境。

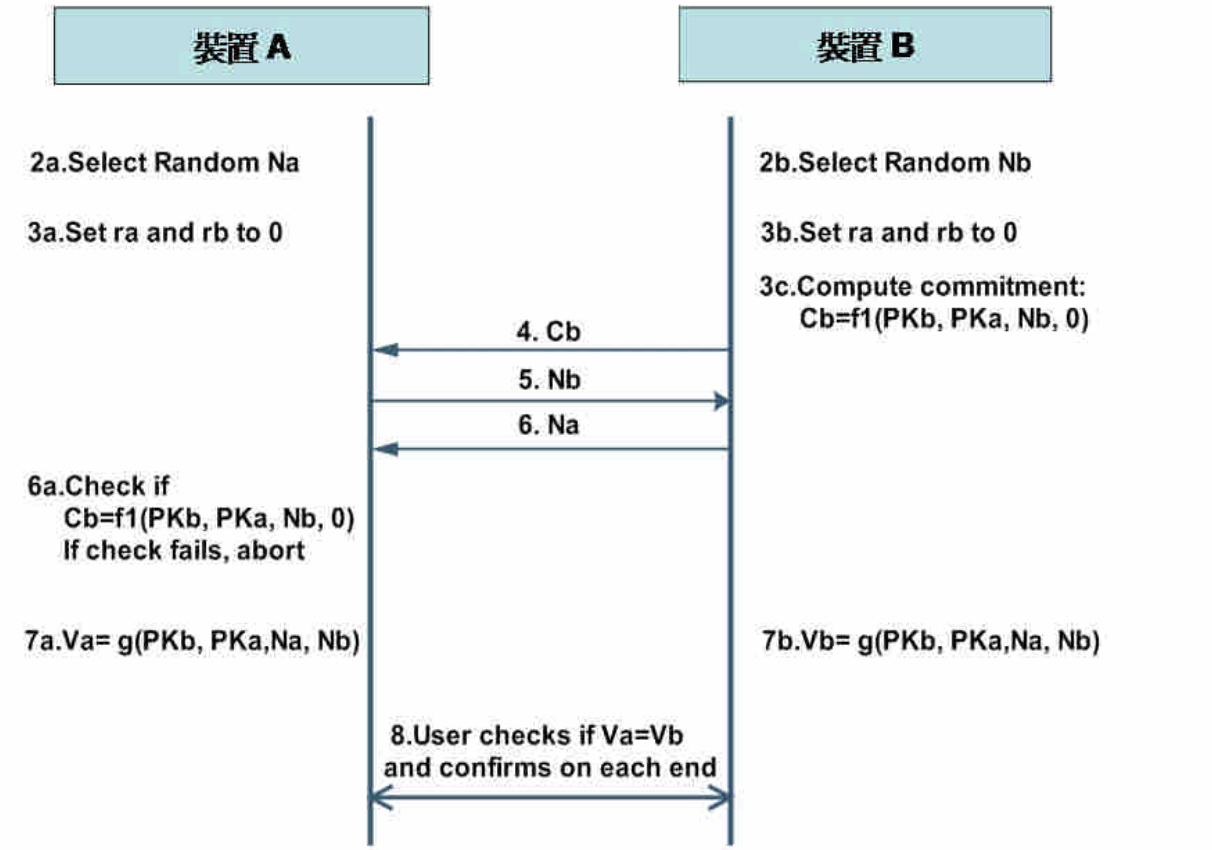


圖 18　鑑別 I -Numeric Comparison 模式 [20]

（2）Just Works 模式

此方法跟 Numeric Comparison 流程類似，不過至少有一方裝置沒有展示六碼數字的能力也沒有鍵盤輸入能力，如：行動電話跟耳機連線），可防止竊聽，但無法避免中間人攻擊，因此適用於對安全需求不高的環境。

（3）Out of Band 模式（圖 19）

為了提升連線的安全性，鑑別過程整合藍牙無線頻道之外不同特性的 OOB（Out of Band）頻道（例如：NFC），此頻道要能抵抗猜測、中間人攻擊等。運作流程為以 OOB 頻道傳送關鍵的安全資訊（如藍牙裝置位址、亂數、驗證值）後，雙方再進行驗證。

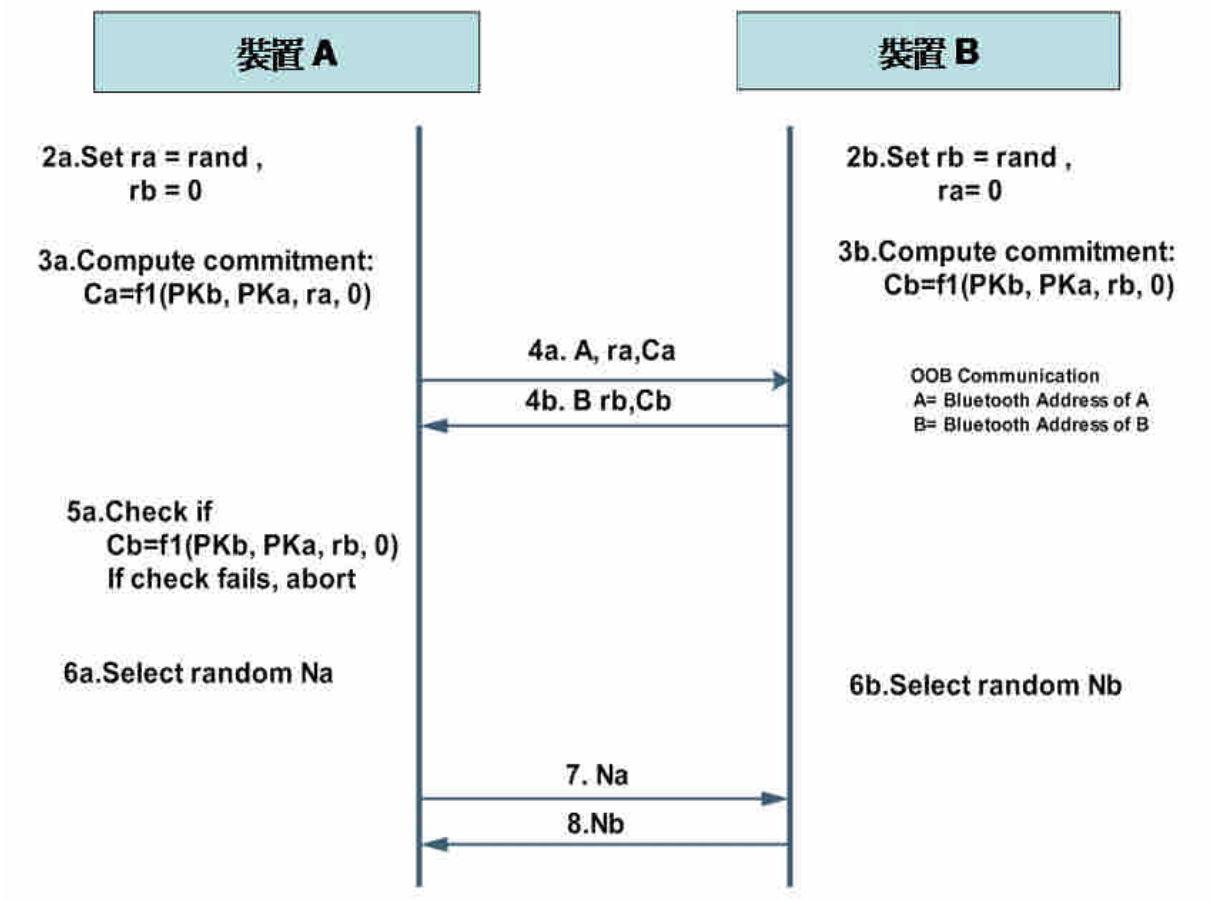


圖 19　鑑別 I - Out of Band 模式 [20]

（4）Passkey Entry 模式（圖 20）

適用於一方裝置具有輸入能力，但無顯示的能力（假設為裝置 A）；另一裝置則具有顯示能力（假設為裝置 B）（例如:藍牙鍵盤和 PC 連線），適用於安全需求為較低的環境。運作的流程為裝置 B 先隨機產生亂數 rb 並顯示於裝置上，供使用者看並輸入裝置 A（ra），此十進位之 6 位數轉成二進位的 20 位元，接下來各自分 20 次，每次雙方各取出一位元（rai，rbi），並與第一階段交換的公開金鑰（PKa，PKb）和自行產生的亂數（Nai，Nbi）計算驗證值（Cai，Cbi），並交換驗證值（Cai，Cbi）與亂數（Nai，Nbi），進行驗證。

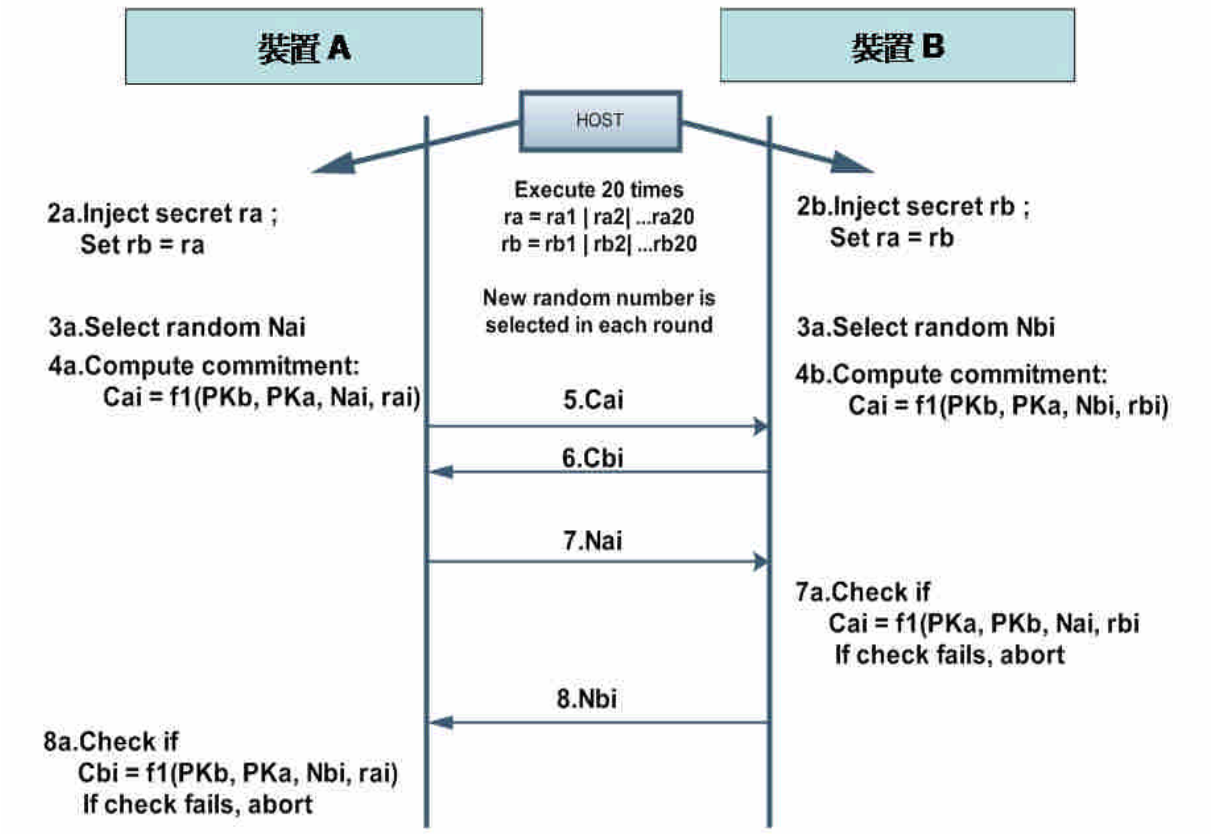


圖 20　鑑別 I - Passkey Entry 模式 [20]

第三階段鑑別 II：確認雙方裝置是否完整成功的交換資訊。（圖 21）

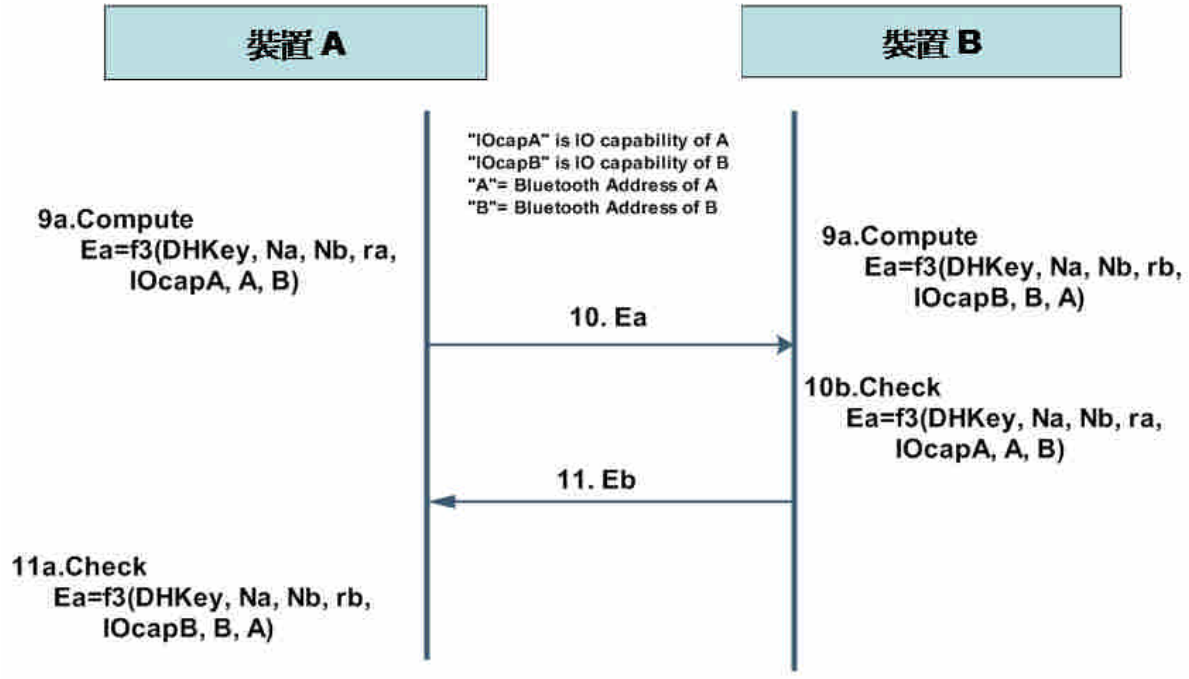


圖 21　鑑別 II　[20]

雙方裝置以前面產生或交換的資訊，各自產生確認值（Ea，Eb）並交換，以驗證雙方共享的資訊之正確性。

第四階段產生鏈結金鑰：雙方將前面三個階段中所得到的參數（DHkey 、亂數值、藍牙裝置位址）作為輸入，經由雜湊函數 f2，各自計算出鏈結金鑰 LK。（圖 22）

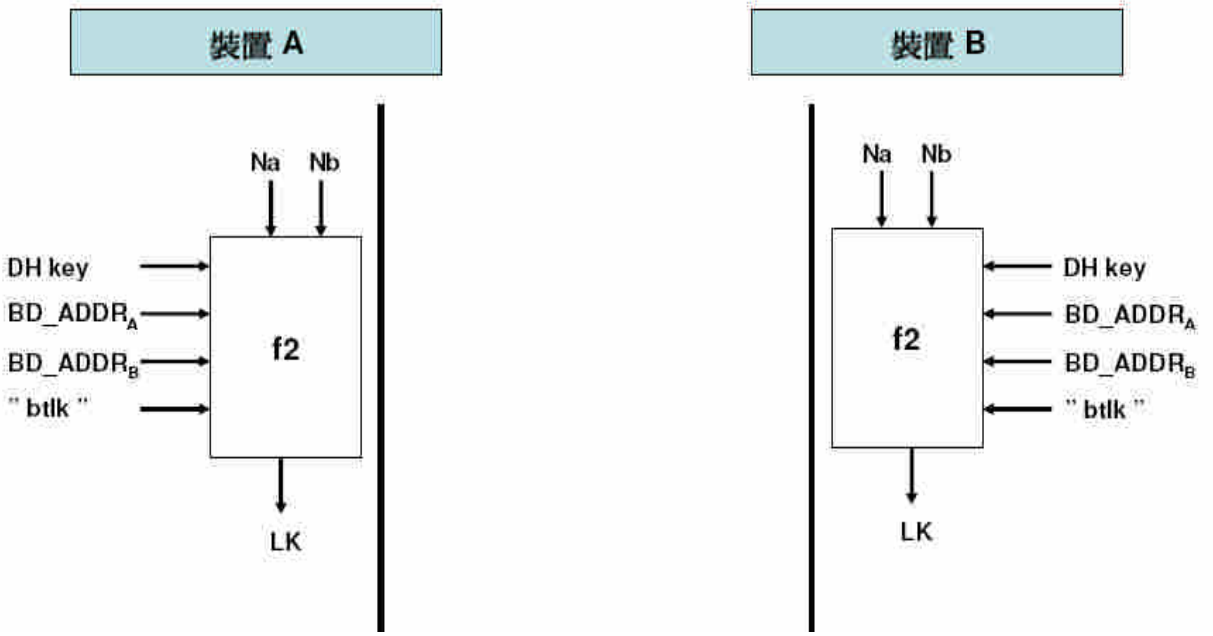


圖 22　產生鏈結金鑰 [20]

第五階段加密：加密的方式與過去舊標準 Pairing 的方式相同。此階段將會產生加密金鑰 K_E，是由長度 128-bits 的加密亂數、長度 96-bits 的密文偏移值（產生方式為上次鑑別方式所創造或是由雙方藍牙裝置位址聯繫在一起）與第四階段所產生的鏈結金鑰當作輸入參數，經由 SAFER$^+$的演算法 E3 產生加密金鑰。（見圖 23）

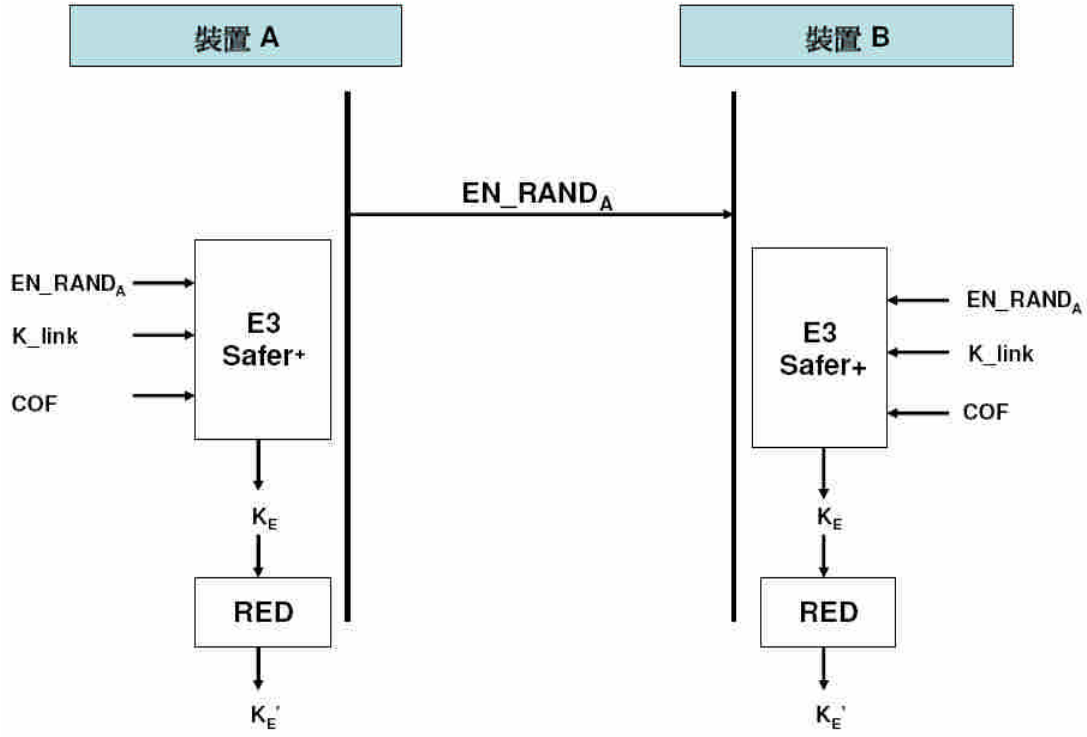


圖 23　產生加密金鑰 [20]

4.2 問題

- **中間人攻擊**

在 Secure Simple Pairing 第一階段中，使用橢圓 Diffie-Hellman 金鑰交換，雖然能有效的防止被動竊聽攻擊，但是 Diffie-Hellman 加密法沒有提供任何的身分驗證機制，可能遭受中間人攻擊。

- **使用者操作錯誤**

根據 Nokia 研究中心針 Secure Simple Pairing - Numeric Comparison 模式可用性分析測試 [45]，利用雙方裝置計算出六碼數字並顯示在雙方螢幕上，由使用者來比對螢幕上所呈現的數字是否相同，並利用按「Yes」鍵或「No」鍵，來達成鑑別的功能，雖然授測者大部分皆認為此方式操作容易，但實際結果呈現有近兩成的授測者，在雙方螢幕呈現不符合的數字，仍然按下「Yes」鍵。如此方式在其它應用利用視覺比對的方式，如網路釣魚、類似的帳號、軟體安裝未看清楚條文即按下一個步驟等。

- **誤導使用者降低連線安全度**

攻擊者利用瀑布法，阻止合法使用者存取服務 ，讓使用者認為鏈結金鑰無法使用，進而刪除鏈結金鑰，並重新進行 SSP 配對，攻擊者可竄改輸出入能力，使裝置間在低安全模式下連線 [31]。

4.3 文獻提出之解決方法

提供使用說明

針對使用者操作錯誤提供使用說明，讓使用者能更明確了解操作方式，當裝置螢幕所呈現數字碼不符合時，表示可能遭受攻擊者竊聽與竄改訊息，避免疏忽雙方裝置螢幕所呈現的驗證數字碼不一致，而直接按下「Yes」鍵通過驗證，或者因無法配對，進而降低所使用的安全模式，使用低安全模式的配對方式或毋需安全需求的模式 [29]。

4.4 我們提出的改善協定

我們所改善的藍牙安全機制為針對 2007 年提出的 Bluetooth V2.1 新標準之安全機制-Secure Simple Pairing 的 Numeric Comparison Protocol 進行深入研究，因為此 protocol 安全性較高、無需其它的輔助通訊技術，並可適用於一般具有顯示、輸入能力的付款裝置，如：手機、PDA、POS 終端機。我們提出輕便的改善機制，讓使用者能沿用原有熟悉的 PIN（Personal identification number）的輸入方式，來達到雙向鑑別與傳輸的機密性，並保護消費者的隱私，此外藉由精簡驗證步驟有效提升運作效率。

流程說明

我們在藍牙 Secure Simple Pairing 第一階段的交換公開金鑰中，增加以雙方共享的 PIN 之雜湊函數值作保護。1.首先雙方裝置先交換彼此的藍牙裝置位址、輸出入能力；2.裝置 A 先產生隨機亂數 $RAND_A$ 當作 X；3.透過運算產生對應的公開值 g^X，並與 h（PIN）做 XOR 運算後傳給裝置 B；4.裝置 B 則先產生隨機亂數 $RAND_B$ 當作 Y，透過運算產生對應的公開值 g^Y，並與 h（PIN）做 XOR 運算後連同 Cb 一起傳給裝置 A，Cb 為裝置 B 收到訊息 $g^X \oplus h(PIN)$，以使用者所輸入 PIN 取出的 g^X，再與 Y 計算出鏈結金鑰 DH key = $(g^X)^Y$，並以 DH key、雙方的裝置位址，經雜湊函數計算產生驗證值 Cb；裝置 A 收到訊息 $g^Y \oplus h$（PIN）後也以使用者輸入的 PIN 取出 g^Y 後，與裝置 A 自己產生的隨機亂數 X，計算出鏈結金鑰 DH key = $(g^Y)^X$，並自行計算出驗證值與收到的驗證值作比

對（圖 24）。我們所提出的協定目標為適用於 Numeric Comparison、Just Work 模式。

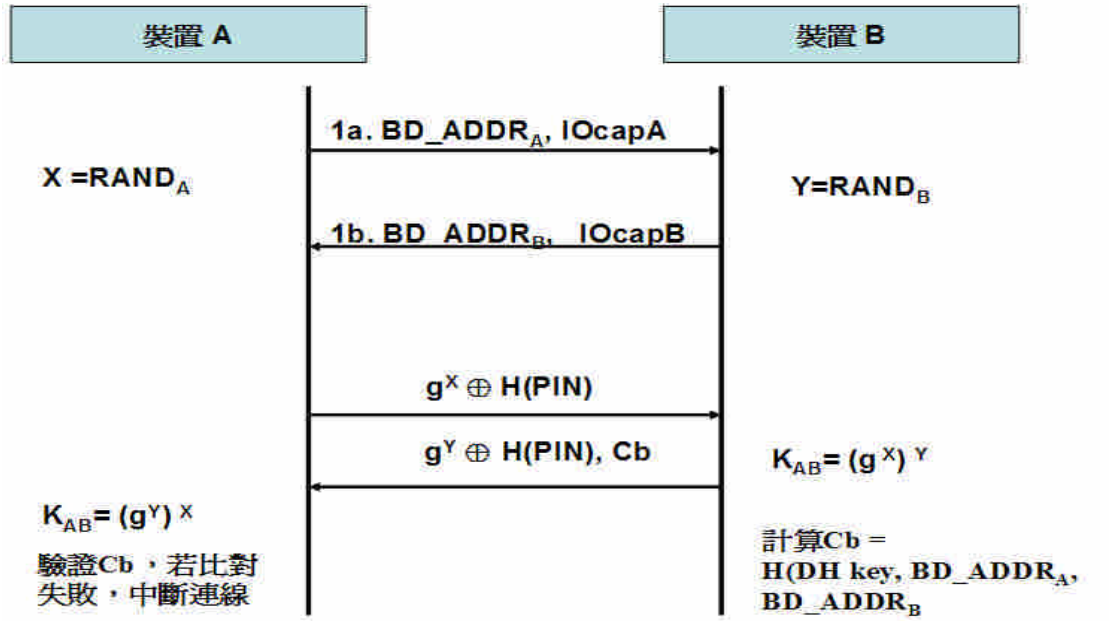


圖 24　我們提出的 Secure Simple Pairing 改善協定

接下來跳過 Secure Simple pairing 的第二、三階段，直接建立鏈結金鑰（LK）。（圖 25）

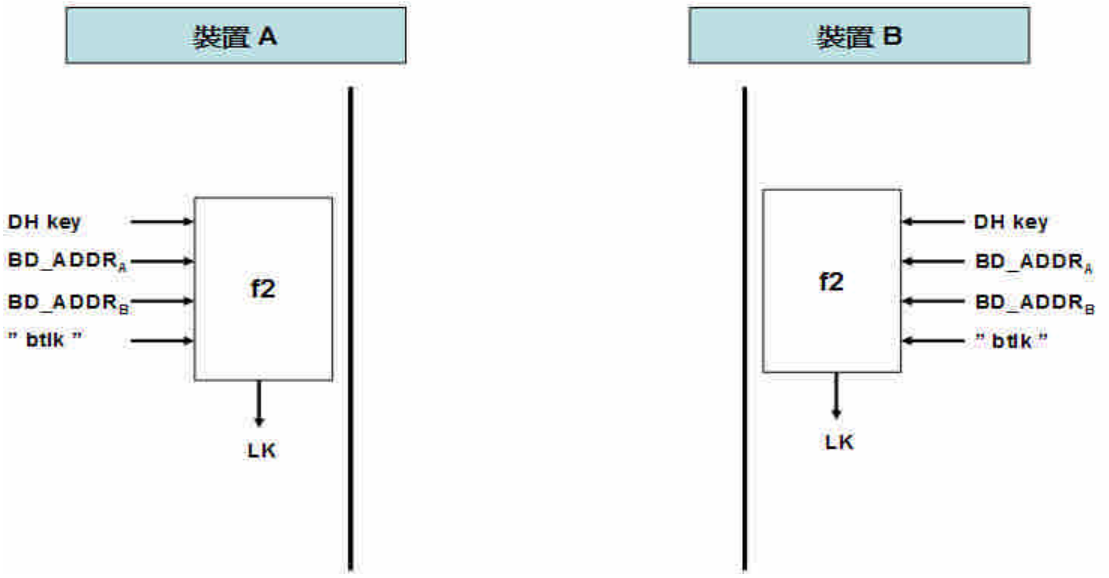


圖 25　我們提出的 Secure Simple Pairing 改善協定－鏈結金鑰產生

比較分析

藍牙安全機制最弱的一環在兩個裝置初次連接的配對過程（Pairing）[46]，在高安全需求的付款應用上，手機與商店 POS 多為初次連接，因此我們提出的新協定主要在改善配對的過程，以提高其安全性。

由於在現有的藍牙 V2.1 新標準安全機制 Secure Simple Pairing 中，Diffie-Hellman 金鑰交換沒有鑑別使用者身分的能力，以使用者目視比對的方式來避免 DH 金鑰交換可能遭受的中間人攻擊，然而這種方式可能因為使用者沒看清楚或不了解程序而誤按確認鍵，這種需要使用者比對而造成失誤的狀況也常出現在網路釣魚（類似的網址）、網路

拍賣截標信（類似的帳號）、軟體安裝（未看清楚條文即按下一步）等。

因此，為了提高配對的安全性與精簡流程，我們沿用使用者過去熟悉的 Pairing 中操作方式輸入共享秘密值 PIN 碼在高安全需求的付款環境，多為初次連接，可以在每次付款輸入不同的 PIN，使 PIN 的輸入不必擔心商家得知，也無需額外的保護，而並藉其保護公開金鑰（g^X,g^Y）的傳送，以避免中間人攻擊，同時也可省去第二、三階段重覆驗證所需時間，雙方裝置若未能輸入相同的 PIN，或未能正確交換參數，則無法通過驗證值 Cb 的確認，中斷連線。

5. 結論

近十年來，藍牙無線通訊技術發展迅速且持續進化，隨著科技成長快速與成本降低，使藍牙已廣泛普及於一般生活之中，藍牙具有效率高、基本安全、低成本、省電、操作簡單等優點，可傳送語音與數據資料，應用的領域除了行動電話與免持聽筒外，逐漸延伸到電玩、醫療、汽車、影音領域，未來更可能使用在金融付款領域。

現有藍牙 V2.0 之前的安全協定中，許多資訊是以明文傳遞，使惡意的第三者得以取得驗證值，由此可進行離線字典攻擊，找出正確的 PIN 值以假冒藍牙裝置通過鑑別，也可推導出通訊的加密金鑰，進而監聽傳送的資料。本研究改善的部份為：(1) 在記憶體資源有限環境下，維持原有的藍牙安全性並提升其配對的效率；(2) 在裝置記憶體足夠的情況，避免惡意的第三者取得驗證值來進行離線字典攻擊，以提升藍牙協定的安全性，保障資訊傳輸上的安全。

此外，Bluetooth SIG 在 2007 提出 V2.1 新安全協定-Secure Simple Pairing 雖然能夠解決上述問題，但藉由使用者目視比對數字碼以達成身分鑑別並避免中間人攻擊。然而，因為使用者的操作失誤可能產生安全的問題。因此我們也提出輕便改善機制，沿用使用者熟悉的鑑別方式-在雙方設備輸入相同的 PIN 以取代目視比對，避免了上述的問題，並有效地提升運作效率，讓藍牙技術可以安心地被應用於安全需求較高之應用上。

參考文獻

1. Lemos, R.，“安全缺口仍是藍牙的痛”，CNET 新聞專區，2004。存取日期 2007 年 10 月 2 日，取自：http://taiwan.cnet.com/news/comms/0,2000062978,20089087,00.htm
2. 余瑞琁，“全球 Bluetooth 晶片市場規模”，工研院 IEK-ITIS 計畫，民 94 年。
3. 李純、周開波與童兆豐譯，“無線通訊技術:探索藍牙”，五南，民 92 年。
4. 林俊宏、楊順興、李忠來、黃億翔與吳建偉編譯，“藍牙:無線連結技術”，全華，民 92 年。
5. 侯俊宇，“高整合/低成本/低耗電到位-藍牙擴大應用版圖”，新通訊元件雜誌，民 96 年。存取日期 97 年 3 月 20 日，取自：http://www.2cm.com.tw/coverstory_content.asp?sn=0711190006
6. 禹帆，“無線藍牙技術”，文魁資訊，民 90 年。
7. 陳劍、郭興明與劉曉東，“藍牙技術在醫療監護中的應用”，電子技術應用，民 91 年。存取日期 97 年 5 月 20 日，取自：http://www.chinaecnet.com/big5/xsj/xsj022421.asp
8. 粘添壽，“電腦網路與連結技術”，全華圖書，民 95 年。
9. 曾煜棋、潘煜鉉與林致宇編著，“無線區域及個人網路：隨意及感測器網路之技術與應用”，加樺國際，民 95 年。
10. 鄧榮惠，“藍牙+GPS-一美元單晶片方案呼之欲出”，民國 96 年。存取日期民 97 年 3 月 20 日，取自：http://www.eettaiwan.com/ART_8800450403_617723_NT_47b68ed0.HTM
11. “Bluetooth Core Specification v2.0 + EDR” , *Bluetooth SIG*, 2002, Retrieved Apr. 2007, from http://www.bluetooth.com/NR/rdonlyres/1F6469BA-6AE7-42B6-B5A1-65148B9DB238/840/Core_v210_EDR.zip
12. “Bluetooth SIG Member Directory,” *Bluetooth SIG*, Retrieved Feb. 5, 2008, from https://www.bluetooth.org/apps/directory/default.aspx.
13. “How can Bluetooth services and devices be effectively secured?,” *Computer Fraud & Security*, 2006.
14. “IEEE 802.15,” *The Wireless Personal Area Network Working Group*, from http://www.ieee802.org/15/
15. “ROLLPAY System Security Overview rev1,” *ROLLCOMM*, 2008, Retrieved Mar. 1, 2008, from http://www.rollcomm.com/downloads/ROLLPAY_System_Security_Overview_rev1.pdf
16. Bandyopadhyay, S., Majumdar, A., Ghosh, O., Chatterjee S., and Chattopadhyay, S., “A Proposal for Improvement in Service-Level Security Architecture of Bluetooth,” Department of Computer Science and Engineering, University of Calcutta, 2003.
17. Bluetooth SIG., “Bluetooth Protocol Architecture,” *Bluetooth SIG Whitepaper*, 1999, Retrieved Feb. 5, 2007, from http://www.bluetooth.com/NR/rdonlyres/7F6DEA50-05CC-4A8D-B87B-F5AA02AD78EF/0/Protocol_Architecture.pdf
18. Bluetooth SIG., “Bluetooth Security White Paper,” *Bluetooth SIG Whitepaper*, 2004, Retrieved Feb. 5, 2007, from http://www.bluetooth.com/Bluetooth/Technology/Building/Research/
19. Bluetooth SIG, “Bluetooth specifications 2.1+EDR,” *Bluetooth SIG Technical Specifications, 2007*, Retrieved Sep. 5, 2007, from

http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/Default.htm.
20. Bluetooth SIG, "Simple Pairing Whitepaper Version V10r00," *Bluetooth SIG Whitepaper*, 2006, Retrieved Feb. 5, 2007, from http://bluetooth.com/nr/rdonlyres/0a0b3f36-d15f-4470-85a6-f2ccfa26f70f/0/simplepairing_wp_v10r00.pdf.
21. Buennemeyer, T. K., Nelson, T. M., Gora, M. A., Marchany, R. C., and Tront, J.G., "Battery Polling and Trace Determination for Bluetooth Attack Detection in Mobile Devices," *The 2007 IEEE Workshop on Information Assurance*, 2007.
22. Candolin, C., "Security Issues for Wearable Computing and BluetoothTechnology," Retrieved Feb 5, 2007, from http://www.cs.hut.fi/Opinnot/Tik-86.174/btwearable.pdf
23. Chen, J. J., and Adams, C., "Short-range Wireless Technologies with Mobile Payments Systems," *ICEC '04 International Conference on Electronic Commerce*, ACM, 2004.
24. Foley, M., "We're exponential," *Signature*, Retrieved Mar. 1, 2008, from http://bluetooth.com/Bluetooth/Products/Signature/.
25. Haataja, K., "Bluetooth network vulnerability to Disclosure, Integrity and Denial of Service Attacks," *Department of CS University of Kuopio Finland*, 2005.
26. Hager, T., and Midkiff, F., "An Analysis of Bluetooth Security Vulnerabilities," IEEE, 2003.
27. Herfurt, M., "Bluesnarfing at CeBIT 2004 Detecting and Attacking bluetooth-enabled Cellphones at the Hannover Fairground," *Salzburg Research*, 2004. Retrieved Feb. 5, 2007, from http://www.trifinite.org/Downloads/BlueSnarf_CeBIT2004.pdf
28. Herfurt, M., "Bluetooone" , *Trifinite_Stuff*, Retrieved Feb. 5, 2007, from http://trifinite.org/trifinite_stuff_bluetooone.html
29. Hypponen, K., and Haataja, K., "Man-in-The-Middle Attack on Bluetooth secure simple pairing," *The 3rd IEEE/IFIP International Conference in Central Asia on Internet*, Tashkent Uzbekistan, IEEE, 2007.
30. Jakobsson, M., and Wetzel, S., "Security Weaknesses in Bluetooth," Topics in Cryptology , Vol. 2020, 2001, pp. 176-191.
31. Janssens, S., "Preliminary study: BLUETOOTH SECURIT," Jan. 2005.
32. Kitsos, P., Sklavos, N., Papadomanolakis, K., and Koufopavlou, O., "Hardware Implementation of Bluetooth Security," *The IEEE CS and IEEE Communications Society*, IEEE, 2003.
33. Kotadia, M., "Nokia admits multiple Bluetooth security holes," ZDNET, 2004, Retrieved Sep. 5, 2007, from http://news.zdnet.co.uk/communications/0,1000000085,39145886,00.htm.
34. Kui, M., and Xiuying, C., "Research of Bluetooth Security Manager," *The IEEE International Conference, Neural Networks & Signal Processing*, IEEE, 2003.
35. Kwan, M., "Pay Toll Booths with Bluetooth Phones," *Mobile Magazine*, 2007, Retrieved Sep. 5, 2007, from http://www.mobilemag.com/content/100/354/C13271/.
36. Labiod H., Afifi, H., and Santis, C. D., "Wi-Fi, Bluetooth, Zigbee and Wimax," Netherlands, *Springer*, 2007.
37. Laurie, A., and Laurie, B., "Bluetooth," *The Bunker*, 2004, Retrieved Feb. 5, 2007, from http://www.thebunker.net/resources/bluetooth.
38. Senese, B., McNutt, G., Bray, J., and Kammer, D., "Bluetooth Application Developer's Guide: The Short Range Interconnect Solution," *Syngress*, United States of America, 2002.
39. Shaked, Y.,and Wool, A., "Cracking the Bluetooth PIN," *The 3rd international conference on Mobile systems, applications, and services*, ACM, 2005.
40. Singelee, D., and Preneel, B., "Improved pairing protocol for Bluetooth," *AD-HOC*,

Mobile, and Wireless Networks, Vol.4104, 2006, pp. 252-265.
41. Smeets, B., Gehrmann, C., and Persson, J., "Bluetooth Security," *Congress*, United States of America, 2004.
42. Suri, P., and Rani, S., "Security Manager - Key to Restrict the Attacks in Bluetooth," *Journal of Computer Science*, 2007.
43. Taibi, F., and Othman, M., "A Proposed Bluetooth Service-level Security," *The International Conference on Information Technology and Multimedia at UNITEN*, 2001.
44. Tan, L., "Symantec warns users over Bluetooth security," *CNET News*, 2007, Retrieved Sep. 21, 2007, from http://www.news.com/Symantec-warns-users-over-Bluetooth-security/2100-1029_3-6209361.html.
45. Uzun, E., Karvonen, K., and Asokan, N., "002: Usability Analysis of Secure Pairing Methods," *Nokia Research Center Technical Reports*, 2007, Retrieved May 28, 2007, from http://research.nokia.com/tr/NRC-TR-2007-002.pdf.
46. Vaudenay, S., "On Bluetooth Repairing: Key Agreement based on Symmetric-Key Cryptography," *The First SKLOIS Conference on Information Security and Cryptology*, 2005.
47. Wong, F. L., Stajano, F., and Clulow, J., "Repairing the Bluetooth pairing protocol," *University of Cambridge Computer Laboratory*, 2005.
48. Wong, F. L., and Stajano, F., "Location Privacy in Bluetooth," *Security and Privacy in Ad-hoc and Sensor Networks*, 2005.
49. Zhang, Z., and Liu, P., "Application of Bluetooth Technology in Ambulatory Wireless Medical Monitoring," *The 4th International Conference on Microwave and Millimeter Wave Technology Proceedings*, IEEE, 2004.

明新科技大學　97 年度　研究計畫執行成果自評表

計　畫　類　別　：　□任務導向計畫 □整合型計畫 ■個人計畫
所 屬 院 (部) ：　□工學院　　■管理學院　□服務學院 □通識教育部
執　行　系　別：　　資管系
計 畫 主 持 人 ：　葉慈章　　職 稱：副教授
計　畫　名　稱　：藍牙無線通訊技術的安全機制
計　畫　編　號　：　MUST-97-資管-05
計畫執行時間：　　97 年 1 月 1 日 至 97 年 9 月 30 日

計畫執行成效

教學方面

1. 對於改進教學成果方面之具體成效：
   藉此研究計劃對藍牙安全及隱私作深入的了解，有助所教授課程"線上交易安全"的內容擴展
2. 對於提昇學生論文/專題研究能力之具體成效：
   藉此訓練培養學生專題研究與論文發表的能力
3. 其他方面之具體成效：完整蒐集相關文獻資料，有助於日後的深入探討

學術研究方面

1. 該計畫是否有衍生出其他計畫案　□是　　■否
   計畫名稱：
2. 該計畫是否有產生論文並發表■已發表　□預定投稿/審查中　□否
   發表期刊(研討會)名稱：明新學報 34 卷第 2 期
   發表期刊(研討會)日期：2008 年 8 月
3. 該計畫是否有要衍生產學合作案、專利、技術移轉　□是　　■否
   請說明衍生項目：

成果自評

計畫預期目標：將針對藍牙技術的安全性作深入的研究，首先整理藍牙的特性、需求、限制與問題；再仔細分析文獻中學者所提出的防護機制，接下來探討其安全上的問題，最後並提出我們的改善機制，以有效提升安全性，讓藍牙技術可以安心地被應用於安全需求性較高的應用上。

計畫執行結果：達成上述目標。

預期目標達成率：　95 %

其它具體成效：
1. 訓練學生在藍牙方面的知識與研究能力。
2. 將計劃成果發表成論文，刊登於研討會。
3. 藉此研究計劃對藍牙作廣泛了解，以便日後將會進行更深入的研究。