應用金鑰加密技術的車輛防盜系統

施閔懷　　李奕坊　　孫冠宏　　侯廷偉
財團法人車輛研究測試中心　成功大學工程科學所　和春技術學院　成功大學工程科學所
shih@artc.org.tw

摘要

目前車輛電子領域的技術發展一日千里，車輛上的各類零組件順應著這股潮流不斷地往電子化發展，因此造價較為昂貴的電子設備數量便逐漸攀升，也間接提高了車輛失竊的風險，市場上常見的防盜警報器或防盜鎖似乎已無法再滿足消費者所需。由於車輛失竊後絕大部分皆是遭到竊車集團解體並轉賣零件，因此本文提供一種車輛防盜機制以保護車內電子設備或組件，使貴重電子設備無法另外安裝至其他車輛上使用，藉由壓縮車輛電子零組件的轉售市場，以降低車體本身或車身組件之失竊風險。

本文旨在提供一種車用設備防盜的系統架構，包含車輛上設備的認證與其加密流程、認證識別碼的產生與變更流程，希冀以此架構能有效提高設備認證的安全性，確實達到車用設備防盜的最終目標。

關鍵詞: 車輛，零件識別技術，互信平台模組，金鑰管理

1. 簡介

國內近十年來汽車失竊案件平均每年約有四萬件發生，這數據反映出車輛防盜系統確有其市場需求。此外車輛上昂貴的電子設備日益增加，由於竊取車輛電子設備比整車竊案更加容易，不難推估往後的車輛失竊模式將會有所改變，據統計車輛電子設備總值佔整車成本在 2010 年後將由目前的 20%攀升至 50%，為因應高失竊率與失竊模式的改變，發展更適用且可靠的車用防竊系統便刻不容緩。

針對此類偷竊模式的改變，部分車廠會在較高階的車輛上使用電子晶片防盜系統(electronic immobilizer)以減少汽車被偷竊的機率，藉由特殊的電子識別程序，將防盜系統及電腦管理系統結合，落實車輛與其設備的專屬性，僅有合法的使用者才可正常操作。然而此類系統的相關細節訊息在車廠的保護下鮮少公開，因此本文中將提出一個完整的設計方案來作為可行的解決辦法，在如後的章節首先簡述本篇論文所使用到的技術背景；第 2 段提出一個完整的系統架構，並將在第 3 段做一小結。

1.1 零件識別技術

零件識別技術(component identification)是目前最主要的設備認證技術，其原理在於每個車上的零件都擁有一個專屬的識別 ID，由系統的認證中心判讀識別 ID 的正確性來認定零件是否存在，資料傳輸過程中更可以對認證 ID 加密[1]，使 ID 資料不至於外洩。部份電子晶片防盜系統即是利用此一技術，藉由中央處理器搜尋車身上的各項零件設備，判讀零件上的識別碼是否吻合，如果發現設備不存在或認證碼不正確的異常現象，則啟動警報器。

然上述架構有著如下缺點: 1.由於認證中心位在中央處理系統內，當中央處理系統被置換後，車上的電子設備依然可以正常運作。 2.當車輛某設備故障時，就有可能被中央處理系統判斷為系統異常而啟動警報，增加無謂的設定或安裝成本。 3.當竊賊目標為某項高單價的電子設備時，由於設備上並無認證單元，經由重新設定即可在他車上使用，無法有效遏止其銷贓市場。針對上述缺點本文在後面章節提出一個可行的改善架構以加強防盜系統的完整性。

1.2 硬體安全模組

硬體安全模組(hardware security module, HSM)是一個防竄改的硬體晶片環境，可以針對密鑰、密碼演算法或是其他高機密資料的處理作業，提供高安全性的實體與邏輯保護。此類硬體安全模組常應用在智慧卡(Smart Card/IC Card)[2]或互信平台模組(trusted platform module, TPM)[3]上。

而在車輛上為了確保設備識別碼具有高度保密性，在設備端與中央處理器間的傳輸過程不會受到外部改寫或資料竊取。最有效地解決方法就是在每個設備上加裝互信平台模組(TPM)，以提升識別碼的防護進而提高系統破解的難度。下圖 1 為一車用零件內嵌硬體安全模組的例子，硬體安全模組由微控制器和 TPM 晶片所組成。微控制器負責 I/O 通訊控制、電源開關控制、零件識別碼儲存以及 TPM 晶片的控制；TPM 晶片則負責將 I/O 通訊介面上的傳輸資料作加解密。

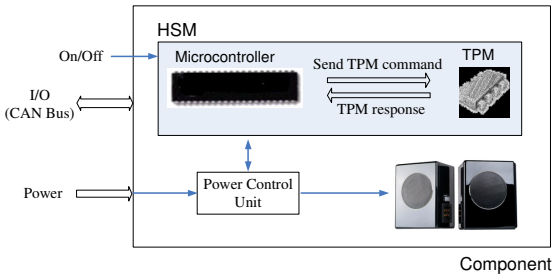

圖 1　內嵌 TPM 晶片之車用零件

1.3 互信平台模組

TPM 系統最早是由 Intel 所開發，內擁有不同的模組區塊，如圖 3 所示，其中最重要的部份在於其使用 RSA 公鑰演算法來對資料進行加密或解密，這種金鑰演算法能夠有效地達到資料的防護保密。

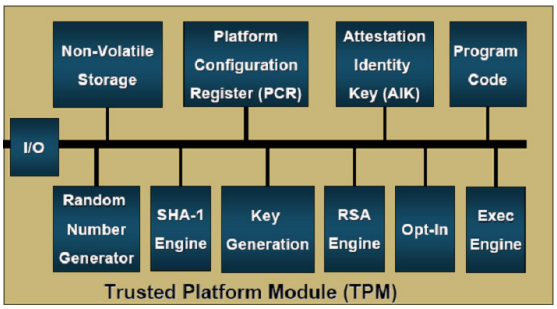

圖 2　TPM 區塊圖

本文以 TPM 應用在 Microsoft Outlook 上[4]為例來說明 TPM 晶片是如何運作。目前在電子郵件伺服器上，資料是完全明碼傳輸，可能受到駭客攔截，並非法利用。為了對電子郵件訊息加密，要先從可信賴、公正的第三方(trusted third party, TTP)得到數位憑證。TTP 像是 VeriSign, Inc.所提供的 VeriSign 伺服器數位憑證(VeriSign Server Certificate)，提供了資料傳輸時的資料具加密的安全機制，如圖 3，以下並詳述了電子郵件訊息加密過程的各個步驟(關於 RSA 公鑰演算法的運作原理，可參考相關書籍[5])。

STEP1: Outlook 得到"digital ID"(有 Digital ID 才可以對電子郵件訊息加密)後發出命令給 VeriSign Server Certificate。

STEP2: Verisign 使用 TPM 之加密服務提供(Crypto Service Provider, CSP)與 TPM 晶片溝通。

STEP3: TPM 晶片產生兩把鑰匙，一把為公鑰(public key)，一把為私鑰(private key)。

STEP4: TPM 晶片送出公鑰給 Verisign。

STEP5: Verisign 以公鑰將電子郵件訊息加密並傳回 Outlook。

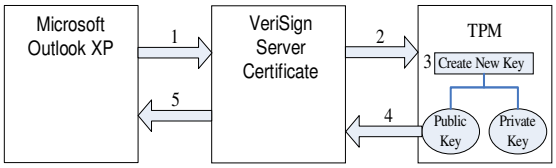

圖 3　TPM 對電子郵件訊息的加密

圖 4 說明 TPM 對電子郵件訊息的解密的流程，各個步驟的說明如下。

STEP1: Outlook 傳送電子郵件訊息之雜湊值(HASH value)給 TPM 晶片。

STEP2: TPM 晶片使用私鑰將雜湊值作訊息復原的簽署(sign)。

STEP3: TPM 晶片回傳已解密的電子郵件訊息到 Outlook。

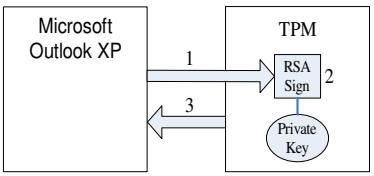

圖 4　TPM 對電子郵件訊息的解密

由於 TPM 初期是針對個人電腦及伺服器設計，因此其信號的溝通介面主要採用 LPC(Low Pin Count)，此種介面無法與微控制器溝通，為了改善此項缺點，部分 TPM 晶片[6]提供有雙線 SMBus 介面(two-wire system management bus)[7]，可以完成與嵌入式系統的溝通。SMbus 的規範是由 I^2C 簡化而來，係藉由兩條訊號所組成的一種匯流排，提供作為系統上較慢速的裝置及電源管理裝置間溝通之用，使系統可取得這些裝置的製造廠商、型號、一些控制資訊、錯誤訊息及狀態。

1.4 通訊介面

80 年代由 Bosch 首先發展的 CAN Bus (Controller Area Network)，為的就是支援目前汽車內不斷增加的電子裝置。在傳統的通訊環境中，控制系統與各感測器間大多是透過點對點的電纜連接以完成控制與資料交換，由於線路過長增加了成本也減低了訊號傳輸過程的穩定度。而 CAN Bus 則是透過簡單的串列介面完成對整個控制系統的連結，在信號傳輸上則使用差模訊號，使得系統傳輸的可靠度更為提升。其相關規範由 ISO(International Standards Organization) 及 SAE(Society of Automotive Engineers)所定義，能夠有效地支援分散式控制系統。綜合來說，CAN Bus 主要有以下數項優點: 1.經過標準化的通信協定。 2.通信的負擔由 CPU 轉移至智慧型節點，可分散系統負荷。 3.減少點對點需要的信號及簡化配線。 4.各設備間資源可共享，信號的運用更廣泛 5.降低設計複雜度且易於更新。

在本文所提供的金鑰系統中，將使用內建 CAN Bus 傳輸功能的微控制器，亦稱為「CAN-based Microcontroller」。其可以利用 CAN Bus、SMbus 等不同傳輸技術互相溝通，在電子裝置單元間可利用 CAN Bus 作為傳輸介面，而單元內部的微控制器與 TPM 晶片溝通途徑則可採用 SMbus。

2. 系統架構

本篇論文所提供之系統為車用設備的防盜，車用電子設備需先通過主系統的認證才可正常作動，此主系統一般係指車用電腦，其可連結一儲存了車輛所有電子設備認證碼的資料庫。當車輛上的電子設備欲啟動時，其內的控制單元會透過車身網路 CAN Bus 至主系統內取得設備的認證碼，經與電子設備原先內存的認證碼比對，如互相吻合即允許啟動該電子設備，如下圖 5 所示。

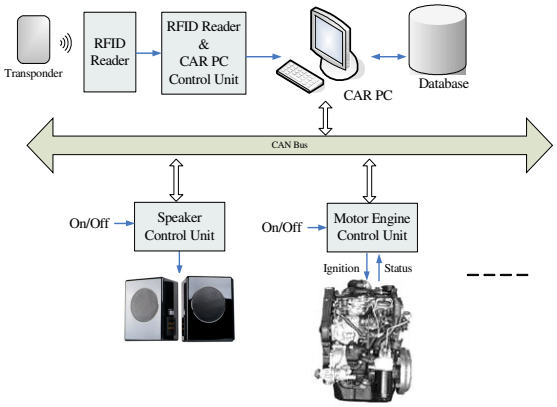

圖 5　車輛防盜系統架構

在上圖中 CAN Bus 上的認證碼傳輸都會透過金鑰管理來達到資料保密的功能，防止外部竊取或改寫。而車用電腦主系統的防盜則可搭配其他方式來完成來保護目的，如使用微控制器確認非接觸式卡片上之 ID 及輸入指紋或密碼等認證，成功後才被允許啟動車用電腦[8]。

2.1 認證與加密流程

當設備的微控制器偵測到啟動信號時，會要求 TPM 晶片產生相對應的公鑰及私鑰。微控制器以公鑰串接設備名稱後傳送予車用電腦，車用電腦依據設備名稱至資料庫搜尋出對應之識別碼，微控制器比較車用電腦傳回的識別碼與其內儲存之識別碼，認證通過才可啟動設備。其符號表示如表 1，細部流程如圖 6 所示。

表 1　認證流程符號表

Name1	可公開的零件代碼，儲存在 Device 與車用電腦的 TPM 上
ID1	零件識別碼
Pbk_Device1	由 Device 內 TPM 產生之公鑰
Pbk_Car	由車用電腦內 TPM 所產生之公鑰
Pvk_Car	由車用電腦內 TPM 所產生之私鑰
$E_{pbk\_device1}(\ )$	使用 Pbk_Device1 加密後的密文
$[\ ]_{sig\_car}$	使用 Pbk_Car 對訊息加密的數位簽章
Rand_Num	亂數

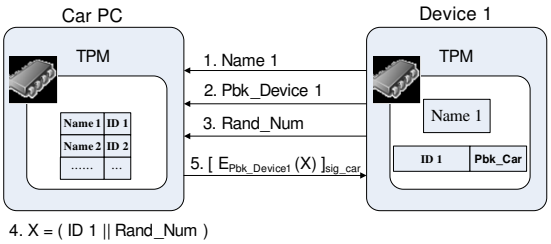

圖 6　認證與加密流程

設備啟動之認證流程：

STEP1: Device1 將名稱(Name1)傳送至車用電腦，車用電腦依其名稱查詢相對應的識別碼(ID1)，同時利用本身的 TPM 產生 Pbk_Car 和 Pvk_Car。

STEP2: 車用電腦得到 Pbk_Device1。

STEP3: 車用電腦得到 Rand_Num。

STEP4: 將 ID1 與 Rand_Num 串接起來，並命名為 X。將 X 利用 Pbk_Device1 加密成 $E_{pbk\_device1}(X)$，並利用 Pvk_Car 將其作數位簽章成 $[E_{pbk\_device1}(X)]_{sig\_car}$。

STEP5: 將 $[E_{pbk\_device1}(X)]_{sig\_car}$ 傳回 Device1。Device1 利用 Pbk_Car 驗證 $[E_{pbk\_device1}(X)]_{sig\_car}$，判斷是否為車用電腦所發出之訊息。最後，Device1 利用先前本身所產生的私鑰將其解密成(ID1||Rand_Num)，確認 Rand_Num 是否為 STEP3 所發出的 Rand_Num，並至多允許接收一次與 STEP3 所發出的相同 Rand_Num。若 Rand_Num 合法，才允許驗證 ID1 之正確性。

2.2 識別碼產生流程

對於識別碼的產生，本文亦制定一套標準流程，如圖 7 所示，以確保每個零件都有專屬的識別碼，避免不同車輛上的零件有識別碼重複的情況產生。

由車廠或可信的第三方來建立一金鑰發佈中心(key distribution center, KDC)，其內嚴格控管著多組主金鑰(master key)。將主金鑰與車輛的車牌號碼結合後可產生一組相對應的 Derived key，這些 Derived key 和各車輛存在著唯一識別的關係且儲存在車用電腦中。車用電腦可利用 Derived key 加入設備編號以產生所有設備之識別碼 Persol，當 Persol 加入其管理欄位元後即為完整的車輛設備識別碼，同時會儲存在車用電腦的資料庫內以供設備驗證時使用。關於金鑰產生的各個階段示意圖整理如圖 8 所示。

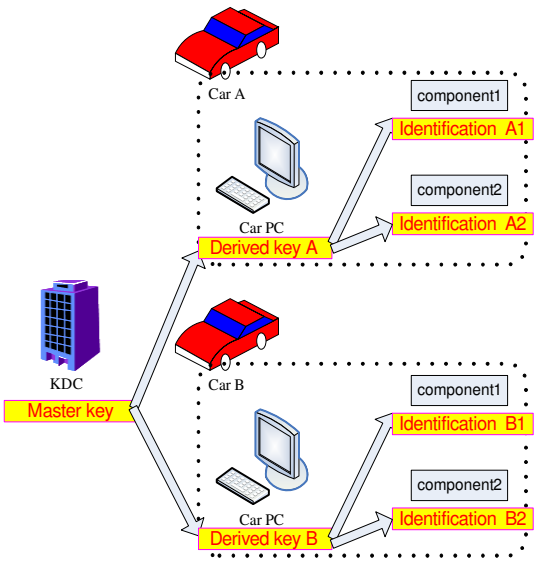

圖 7　金鑰產生流程

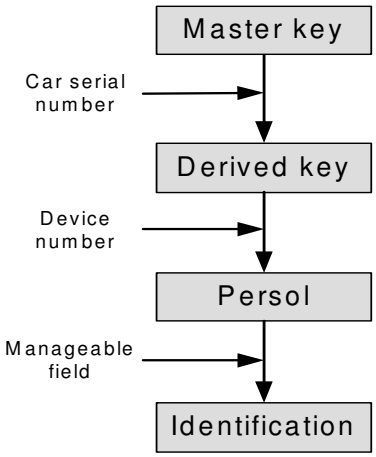

圖 8　金鑰產生之各階段示意圖

2.3 識別碼的改寫

當安裝新的車用電腦、電子設備抑或是舊的識別碼使用相當長的一段時間需要變更時，本系統提供一個可行的機制，即在識別碼前頭新增一個二位元的管理辨識欄位，相關定義的功能如表 2。管理欄位 01 及 10 的功能保留以作為系統擴充時使用。

表 2　管理欄位功能表

Manageable field	
00	Compare Identification
01	Reserved
10	Reserved
11	Write Identification

當系統正常作動時，管理欄位內的預設值為 00，即資料庫內的識別碼與微控制器內的識別碼前兩個位元都是 0。因此使用者開啟車上設備後，微控制器會自車用電腦讀取其專屬的設備辨識碼，並檢查管理欄位的值是否為 00，在符合的狀況下，微控制器便進一步進行識別碼的比對，並作出相對應的動作。

當車輛需要更新設備可以由管理介面來進行改寫，管理者從車用電腦管理介面，發出安裝訊號給車用電腦時，車用電腦會將已內存的 Derived key 和亂數產生一個 Persol，如圖 9 所示。並在 Persol 前頭的管理欄位寫入 00 且暫存起來，等待微控制器要求傳送識別碼回微控制器。

此時若按下新設備的按鈕，車用電腦會讀取其公鑰及設備名稱，配對先前新產生的識別碼並存入資料庫，接著將識別碼的管理欄位改寫為 11，隨後以公鑰加密且傳送回設備端的微控制器。

當微控制器判讀識別碼的管理欄位為 11 時，便將新 Persol 的管理欄位改寫為 00 並存入微控制器的儲存裝置當中，以完成識別碼的更新，同時允許設備啟動。

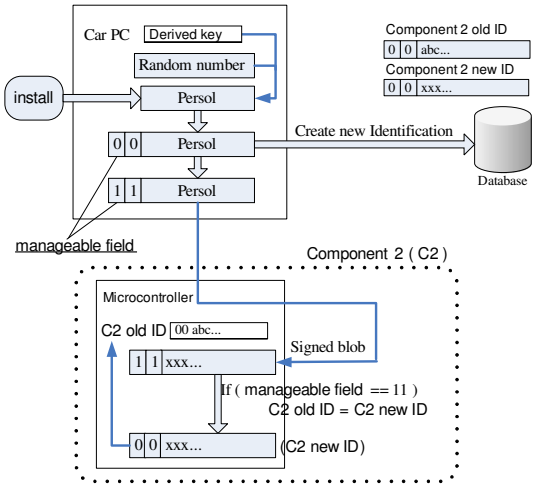

圖 9　識別碼的改寫流程

2.4 管理介面

在管理者的使用上，為簡化使用者的操作流程，本文設計一簡易的管理介面，其內包含初始化功能與新增設備功能，如圖 10。

當安裝新的車用電腦或是識別碼長期使用需要變更時，會將車上所有零件重新更換認證碼，因此可使用管理介面的初始化功能，由"開始安裝"至"結束安裝"過程中，依照車用電腦指示動作，若安裝成功，則會啟動元件，並將所有設備的新認證碼儲存至資料庫中。

新增設備功能則在車輛僅安裝單一零件時使

用，車用電腦會產生並給予單一零件新的認證碼，一次只能限制啟動一個預定新增的元件，若啟動其他元件則設定失敗需重新操作，當設定成功後，系統會將新設備的設備名稱及認證碼儲存至資料庫中。

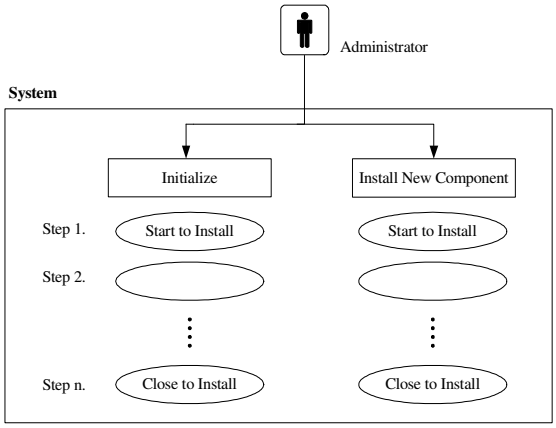

圖 10　管理者使用案例圖

3. 結論與未來展望

本研究設計了一種車用設備的防盜系統，其目的在於保護車上貴重的電子設備，使其被竊後無法進行銷贓。針對金鑰的部份亦制定一套完整的程序，包含設備的認證與金鑰加密流程、識別碼的產生與修改流程，應用零件識別技術以展現本電子晶片防盜系統的實用價值。

本系統將資訊領域的 TPM 技術應用至車輛防盜安全上，為傳統車輛防盜系統找到另一個可行的發展空間。未來除了持續進行硬體安全模組的系統研究以期能將此一概念商品化，亦希望透過類似的跨領域結合，以各領域的經驗來結合車輛系統的發展，為車輛領域的研究注入不一樣的新面貌。

4. 參考文獻

期刊論文:

[1] K.Höper, C.Paar, A.Weimerskirch, M.Wolf, "Cryptographic Component Identification: Enabler for Secure Vehicles," *IEEE Semiannual Vehicular Technology Conference (VTC)*, vol. 62, pp25-28, September 2005.

書籍:

[2] W. Rankl & W. Effing, *Smart Card Handbook*; January 2004.

[3] Trusted Computing Group, *Trusted Platform Module Main Specification*; June 2006.

[4] Sundeep Bajikar, *Trusted Platform Module (TPM) based Security on Notebook PCs - White Paper*, Mobile Platforms Group, Intel Corporation; 2002.

[5] Bruce Schneier, *Applied Cryptography*, John Wiley & Sons; 1996.

[6] Steven Kinney, *Trusted Platform Module Basics - Using TPM in Embedded Systems*; 2006.

[7] Smart Battery System Implementers Forum, *System Management Bus (SMBus) Specification*; 2000.

研討會論文:

[8] 張書源、侯廷偉、梁智能、孫冠宏,"RFID 智慧晶片卡應用於車輛整合系統之研究," *International Conference on Advanced Information Technologies (AIT)*, 2007.