一個新的使用多項式池技術之車載網路匿名認證系統

A New Anonymous Authentication Scheme in Vehicular Networks by Using Polynomial Pool-based Technology

王智弘
Chih-Hung Wang
國立嘉義大學 資訊工程研究所
wangch@mail.ncyu.edu.tw

李泊縉
Po-Chin Lee
國立嘉義大學 資訊工程研究所
s0970397@mail.ncyu.edu.tw

***摘要*—在車載網路(Vehicular Ad-hod Networks,VANETs)中，安全及隱私是兩項重要的研究議題。本研究將針對認證使用者的合法性以及達到隱私性作為主要研究方向。本論文提出使用基於多項式池(Polynomial Pool-Based)的技術加入假名(Pseudonym)的概念並結合兩者達到以匿名認證合法使用者，同時建立安全通訊的金鑰。我們提出的匿名認證協定不但可以保護使用者的隱私，在認證協定中我們使用對稱式密碼學系統比非對稱式密碼學系統來的有效率，並適合用在高速移動下進行安全通訊的車載網路中。**

***關鍵詞*—車載網路、隱私性、認證協定、多項式金鑰池**

***Abstract*—In vehicular networks (VANETs), security and privacy are two important issues. This study will not only address the legality of the user authentication but also achieve privacy. We propose a pseudonym and polynomial pool-based authentication protocol to authenticate legitimate user in anonymity and furthermore, to establish a secure communication key. The proposed anonymous authentication protocol can preserve user privacy, and improve efficiency by using symmetric cryptosystem instead of asymmetric cryptosystem, which is particularly suitable for secure communications in the system with high-speed movement.**

***Keywords*—Vehicular Networks, Privacy, Authentication Protocol, Polynomial Pool**

一、 緒論

隨著無線網路技術的進步，車載網路(Vehicular Ad-hod Networks,VANETs)也成為近幾年越來越紅的研究領域，車載網路是基於移動式隨意網路(Mobile Ad-hoc Network)架構所衍生出來的，由於是應用在汽車上，所以車載網路可以視為是 Computers on wheel 或是 Computer Networks on wheel[1][5]。美國的聯邦通訊委員會(Federal Communications Commission, FCC)分配 75MHz 的頻寬給車用系統使用，這項技術被稱為專用短距離通信(Dedicated Short Range Communication, DSRC)；其他各國車載網路研究組織包括歐洲的 C2CCC(Car to Car Communication Consortium)及 SeVeCom(Secure Vehicular Communication)；日本的 Internet ITS；德國的 Now(Network on Wheels)；以及台灣的 ITS Taiwan 等眾多組織爭相投入車載網路的研究。

車載網路的應用相當廣泛，其中包括了:

1. 協同駕駛 (Cooperative Driving)：行車期間如有緊急車輛通過(如救護車)，可協助相互告知其位置，以便駕駛閃避緊急車輛。
2. 碰撞避免 (Collision Avoidance)：當前方發生交通事故時可以提早改道或遠離事故車道，避免誤撞造成二次車禍事故。
3. 交通路況資訊傳送 (Traffic Information)：收集附近交通路況相關資訊，讓駕駛人可以提早駛離交通擁擠的地區。
4. 車輛診斷 (Vehicle Diagnostics)：車輛行駛期間如發生故障問題可以將車輛資訊送至維修中心做初步故障的診斷以利駕駛人做行車判斷。
5. 電子收費系統 (Electronic Toll System)：包含 ETC 系統、商店餐廳 GPS 定位或是其他消費行為。
6. 娛樂相關 (Entertainment)：包含網路電視、網路電話、車上上網等等。

從以上敘述看，車載網路應用層面相當廣泛，不過大致上可以分類成以下兩大類[5]：

1. 行車安全相關應用
2. 行車娛樂及其他相關應用

在車載網路中，安全議題受到不少研究學者重視，在 2005 年 Raya 跟 Hubaux[5]針對車載網路安全議題提出探討。Raya 跟 Hubaux 對車載網路的應用進行分類，並討論攻擊者的行為以及相關的安全需求，而其中有關隱私性及認證方面的議題吸引了不少學者相繼探討。在 2007 年，Calandriello 等人[2]在車載網路的隱私性及認證上提出使用假名認證的方法，Calandriello 等人的研究主要針對車載網路中的行車安全訊息傳輸做探討，配合使用假名憑證及私鑰來簽署安全訊息，訊息驗證者藉由假名憑證及公鑰來認證其訊息的合法性。而 Xi 等人[7]在 2007 年則提出使用對稱式金鑰池(Symmetric Random Key Set)的方法來增加車載網路中的隱私並提出隱私保護的認證協定。在 Xi 等人提出的方法中，同時使用了公開金鑰系統及對稱式加密系統來達成認證。

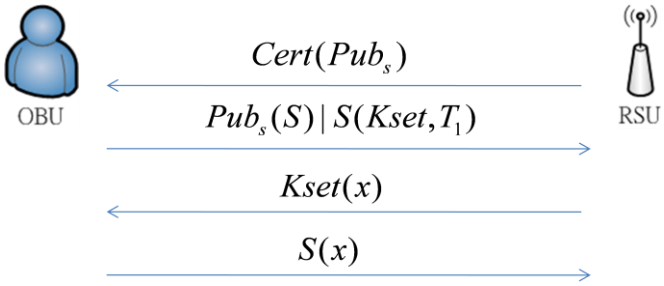
在本論文中，我們考慮使用對稱式加密系統來達到認證並保護隱私，我們提出使用基於多項式池(Polynomial Pool-Based)的方法並加入使用假名的概念來達到認證合法使用者並且保護使用者的隱私。在原本多項式池之金鑰分配的方法中，金鑰建立過程必須透過彼此交換每個使用者的真實身份來計算成對溝通金鑰。然而，在車載網路的環境中為了保護隱私，匿名與假名是最常被使用的方法。我們參考 Calandriello 等人的研究與 Xi 等人的方法，結合了對稱式加密系統與假名的概念來達成合法使用者的認證並達到保護使用者身份的隱私。我們提出的方法除了可以提供使用者匿名認證以確保使用者身份的隱私外，運用對稱式加解密系統會比非對稱式加解密系統的效率更好且更適合用在需要高速移動下進行安全通訊的車載網路中。

本論文架構如下：第二章回顧 Xi 等人提出的方法；第三章則是介紹研究背景包含網路架構、安全需求以及基於多項式池之金鑰分配的方法；第四章則是介紹我們提出基於多項式池之認證協定的方法。第五章討論方法的安全分析及使用限制等分析;最後第六章則是對整個方法作簡短的結論。

二、 相關研究

Xi 等人[7]在 2007 年提出了使用對稱式隨機金鑰池的方法應用於車載網路。這個概念目前也常使用在無線感測網路(Wireless Sensor Networks)金鑰分佈機制的研究上[3][6]。每輛車子預先從金鑰分佈中心得到 m 把對稱式金鑰並保存在車子的機上盒(On Board Unit, OBU)，這 m 把金鑰我們稱之為金鑰環(Key Ring)，而使用對稱式隨機金池有下列幾項優點：

1. 對稱式金鑰加密及解密所需要的時間比非對稱式密碼技術少。
2. 由於對稱式隨機金鑰池內每一把金鑰會隨機分配給多個使用者，所以無法從單一把金鑰來辨識該使用者的真實身份，對於隱私性



圖一 Xi 等人提出的隱私保護認證協定

則能獲得提昇。

認證協定方面，Xi 等人提出一個簡易的隱私保護認證協定如圖一。*Cert* 表示憑證；Pub_s 表示是路側單元(Road Side Unit, RSU)的公鑰；*Kset* 表示被挑選出的數把對稱式金鑰；*T* 表示時間訊息。認證協定詳細敘述如下：

步驟 1　首先路側單元不斷廣播自身憑證及公鑰。

步驟 2　當車輛收到廣播後，OBU 使用路側單元的公鑰加密一個隨機亂數 *s*，使用此隨機亂數 *s* 加密 OBU 隨機從金鑰環中選出的 *k* 把金鑰傳送給路側單元。

步驟 3　路側單元收到後解開內容並確認 *k* 把金鑰的合法性，再以這 *k* 把金鑰加密一個隨機亂數 *x* 傳送給 OBU。

步驟 4　最後 OBU 再以當初選的 *s* 加密 *x* 傳送給路側單元，完成整個協定過程即完成認證。

三、　研究背景

3.1　網路架構

車載網路的架構如圖二所示，其中分為有線通訊與無線通訊兩個部分。在有線通訊中，由授權認證中心、金鑰分佈中心、車輛註冊中心以及路側單元所組成，透過網際網路來傳輸資訊。在無線通訊方面，則是由車輛上所安裝的 OBU 透過無線網路來達到車輛跟車輛之間或是車輛與路側單元的通訊。

3.2　安全需求

一個安全的車載網路系統應具備下列安全需求：

1. 機密性與完整性

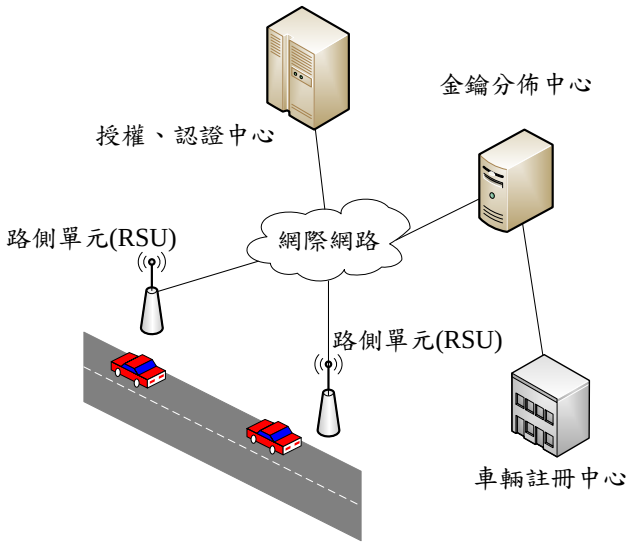
在通訊過程中，車輛跟車輛之間或是車輛與路側單元之間的通訊應避免被竊聽，資訊的傳送應保有機密性。並且資訊傳輸應保有完整性，避免傳輸過程中遭到攻擊者惡意修改通訊內容。

2. 認證

在車載網路中，車輛或是路側單元必須經過認證與授權成為合法的使用者，在通訊之前要先相互認證彼此是否為合法使用者才能進行通訊。

3. 隱私性

隱私需求在車載網路中是一項頗為重要的議題。一般而言，路側單元並不需要隱藏自己的身份。然而，對使用者而言，隱私卻是重要的需求。車輛在通訊時希望能保護自己的身份不被其他車輛或路側單元知道，防止本身被惡意追蹤其行車路線。



圖二 車載網路架構

3.3 基於多項式池之金鑰分配

基於多項式池之金鑰預先分配機制是由 Liu 與 Ning[4]於 2003 年所提出，主要結合了「基於多項式之金鑰預先分配」與「金鑰池」的想法，目的是利用基於多項式之金鑰分配機制與金鑰池隨機金鑰分配機制結合成多項式池之金鑰分配機制在無線感測網路的節點間建立成對金鑰。而利用基於多項式池之金鑰分配的概念，在多重的多項式下增加了攻擊者破解的困難性。同時具有隨機金鑰分配機制的特性，在不需花費太多儲存空間的情況下，只需令任意兩個感測節點之間能建立直接連結的機率達到一個理想值，則可使得整個網路連通。

基於多項式之金鑰分配方法中，一個具有級數(Degree) t 的雙變數多項式(Bivariate Polynomial)如下:

$$f(x,y)=\sum_{i=0}^{t}\sum_{j=0}^{t}a_{i,j}x^{i}y^{j} \qquad (1)$$

並且有 $f(x,y)=f(y,x)$ 的特性。而 t 可根據使用者的安全需求來做調整。

使用多項式之金鑰分配建立成對通訊金鑰的方法時，每一個使用者一開始會被分配到一個多項式子金鑰(Polynomial Share)，例如使用者 i 會得到 $f(i,y)$，使用者 j 會得到 $f(j,y)$。若是使用者 i 想跟使用者 j 通訊時，步驟如下：

1. 使用者 i 會將使用者 j 的真實身份代入自己的 $f(i,y)$ 中 y 的變數，則得到 $f(i,j)$。
2. 使用者 j 會將使用者 i 的真實身份代入自己的 $f(j,y)$ 中 y 的變數，則得到 $f(j,i)$。
3. $f(i,j)=f(j,i)$ 即為使用者 i 與 j 的成對通訊金鑰。

而多項式池(Polynomial Pool)即是產生許多單一多項式聚集起來，換句話說，多項式池中會保存許多單一多項式。

多項式之金鑰分配的安全性會依據其多項式的級數 t 的大小，攻擊者必須收集超過 t+1 個多項式子金鑰，攻擊者透過共謀收集其他多項式子金鑰，當收集的多項式子金鑰不超過 t+1 個數量即無法還原該多項式，同時也無法輕易取得其他使用相同一個多項式使用者的成對通訊金鑰。

四、 基於多項式池之認證協定

在本章節中，我們將仔細描述基於多項式池的認證協定。以車載網路的環境來說，在原本的多項式之金鑰分配方法中，使用者跟路側單元必須代入彼此的真實身份來計算成對金鑰。但是，使用者希望使用匿名或是假名來讓路側單元認證其合法性並建立成對金鑰。而在路側單元的部份則與使用者不同，一般而言，路側單元並沒有隱私需求，所以不需要使用匿名或假名，使用者可直接將路側單元的真實身份代入多項式子金鑰的函數中計算成對金鑰。所以我們同時結合兩者的想法，使用者在被認證時使用假名讓路側單元代入多項式子金鑰的函數中計算成對金鑰，而路側單元則直接使用真名讓使用者代入多項式子金鑰的函數中計算成對金鑰。根據系統設定的不同我們提出兩種方法如下：

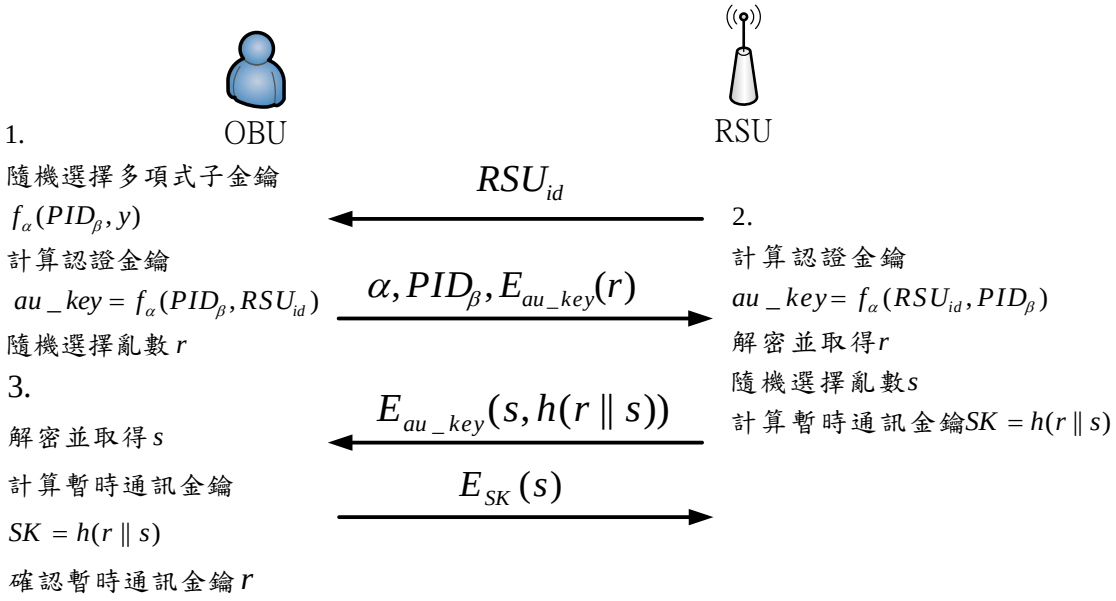
4.1 方法一

1. 系統設定

表一 縮寫與符號表

RSU_i	編號 i 路側單元真實身份
PID_i	編號 i 的假名
$f_n(x,y)$	編號 n 的多項式
$f_n(RSU_i,y)$	多項式編號 n 且代入路側單元真實身份的多項式子金鑰
$f_n(PID_i,y)$	多項式編號 n 且代入假名的多項式子金鑰

在金鑰分佈中心(KDC)產生 n 個級數 t 的多項式，每個多項式會各別擁有不重複的編號(ID



圖三　方法一認證協定與金鑰建立

Number)，例如： $f_1(x,y), f_2(x,y),..., f_n(x,y)$ 。

而路側單元與 OBU 的分配設定如下：

RSU_i ：金鑰分佈中心會分配多項式池中所有已經代入 RSU_i 的多項式子金鑰 $f_{1\sim n}(RSU_i, y)$ 給 RSU_i ，這裡 RSU_i 為該路側單元的真實身分。

OBU：一開始使用真實身份向車輛註冊中心註冊。而金鑰分佈中心會隨機分配 k 個已經代入假名的多項式子金鑰給該使用者並存於 OBU 中，其中假名與多項式的編號並無關連性。例如： $f_1(PID_1, y), f_3(PID_{10}, y),..., f_{55}(PID_{17}, y)$ 等共 k 個已經代入假名的多項式子金鑰。然後授權認證中心將會把該使用者分配到的 k 個帶有假名的多項式子金鑰及其假名與真實身份記錄在資料庫中，如表二。

2.　認證協定與金鑰建立

方法一的認證協定與金鑰建立如圖三所示。使用者跟路側單元進行通訊時，彼此接收對方

表二 方法一中記錄於資料庫的資料表

使用者真實身份：OBU_ID	
PID_1	$f_1(PID_1, y)$
PID_{10}	$f_3(PID_{10}, y)$
⋮	
PID_{55}	$f_{17}(PID_{55}, y)$
PID_{67}	$f_{113}(PID_{67}, y)$

的身份代入自己擁有的多項式子金鑰來計算成對金鑰，使用者提供假名身份給路側單元，路側單元則提供真實身份給使用者。在此，我們可以將計算出來的成對金鑰當成***認證金鑰*** (Authentication Key)。當使用者與路側單元皆為合法的成員並從金鑰分佈中心合法取得各自的多項式子金鑰，可藉由此認證金鑰透過相互認證的機制來建立此次通訊的暫時通訊金鑰。認證協定與金鑰建立的詳細步驟如下：

步驟 1 首先路側單元會不斷廣播自己的真實身份，當車輛行進到路側單元的通訊範

圍會接收到該路側單元的真實身份。當車輛收到該訊息後，OBU 會隨機從自身擁有的多項式子金鑰隨機挑選一個來使用。例如：挑選到 $f_\alpha(PID_\beta, y)$ 這個帶有假名多項式子金鑰。然後計算出與該路側單元共有的認證金鑰 $au\_key = f_\alpha(PID_\beta, RSU_{id})$。完成後再選擇一個隨機亂數 r，並且使用剛計算的認證金鑰 au_key 加密，然後傳送此次使用的多項式編號、假名及加密過的 r 給該路側單元。

步驟 2 該路側單元收到後，先確認使用哪個多項式編號，接著將假名代入本身相同多項式編號的多項式子金鑰中計算認證金鑰 $au\_key = f_\alpha(RSU_{id}, PID_\beta)$，然後使用 au_key 解出 r。完成後再選擇一個隨機亂數 s，並計算此次通訊要使用的暫時通訊金鑰 $SK = h(r \| s)$。最後將 s 及 SK 加密後傳送給該車輛。

步驟 3 車輛收到後由 OBU 解出 s 及 SK，再計算 $SK = h(r \| s)$ 是否等於接收到的 $h(r \| s)$。如果正確無誤，最後使用 SK 加密 s 回送給路側單元完成相互認證的步驟，而接下來就使用暫時通訊金鑰 SK 來加密與該路側單元的通訊內容。

4.2 方法二

方法二的作法則是參考 Traynor 等人[6]與 Chen 等人[3]的金鑰分配方法，將其改良應用於車載網路，同時也讓使用者達到隱私需求。

1. 系統設定

在金鑰分佈中心(KDC)產生 n 個級數 t 的多項式，每個多項式會各別擁有不重複的編號例如：$f_1(x, y), f_2(x, y), ..., f_n(x, y)$。

在方法二中，路側單元與 OBU 的分配設定如下：

RSU_i：金鑰分佈中心會隨機分配多項式池中 m 個已經代入 RSU_i 的多項式子金鑰，例如 $f_1(RSU_i, y), f_{17}(RSU_i, y), ..., f_{55}(RSU_i, y)$ 等共 m 個給 RSU_i，這裡 RSU_i 為該路側單元的真實身份。

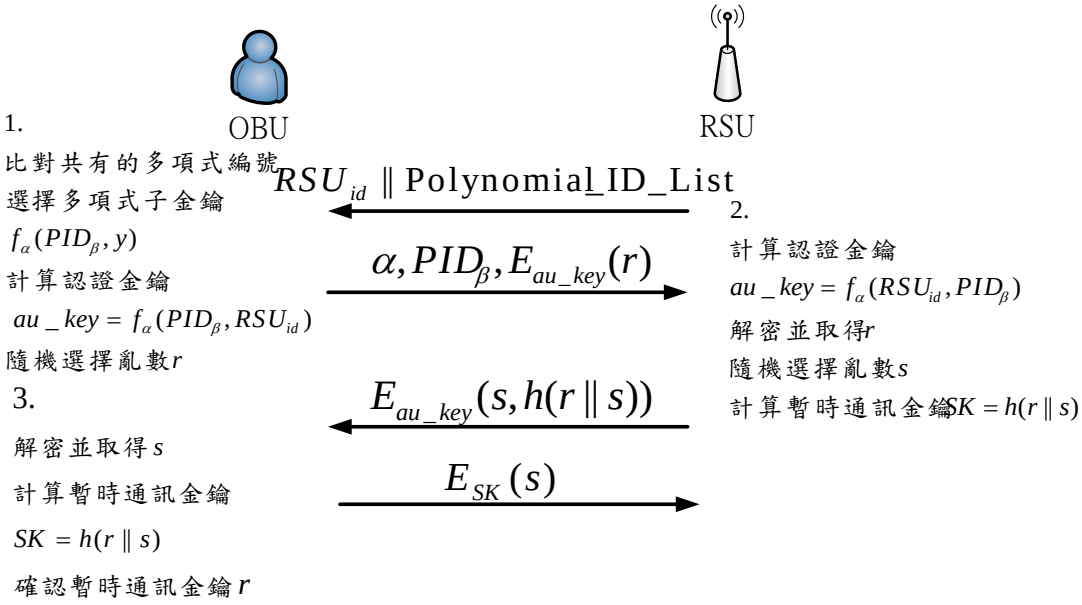
OBU：一開始使用真實身份向車輛註冊中心註冊。而金鑰分佈中心會隨機分配 k 個已經代入假名的多項式子金鑰給該使用者並存於 OBU 中，而且在同一個多項式中會被分配到兩個以上的多項式子金鑰，例如：$f_1(PID_1, y), f_1(PID_{13}, y), f_3(PID_{10}, y), f_3(PID_{51}, y)$ 等共 k 個已經代入假名的多項式子金鑰且同一多項式中會被分配到兩個以上的多項式子金鑰。然後授權認證中心將會把該使用者分配到的 k 個帶有假名的多項式子金鑰及其假名與真實身份記錄在資料庫中，如表三：

表三 方法二中記錄於資料庫的資料表

使用者真實身份：OBU_ID	
PID_1, PID_{13}	$f_1(PID_1, y), f_1(PID_{13}, y)$,
PID_{10}, PID_{51}	$f_3(PID_{10}, y), f_3(PID_{51}, y)$
⋮	
PID_{55}, PID_{15}	$f_{17}(PID_{55}, y), f_{17}(PID_{15}, y)$
PID_{67}, PID_{99}	$f_{73}(PID_{67}, y), f_{73}(PID_{99}, y)$

2. 認證協定與金鑰建立

方法二的認證協定與金鑰建立如圖四所示。不同於方法一的認證協定，在方法二中，路側單元與使用者的 OBU 必須擁有共的多項式才能建立通訊。而方法二的作法，當每次車輛來到同一個路側單元時，通常只有會分享到一個或少數個多項式，假設只分享一個多項式時，每次行經同一路側單元需要兩個以上的假名來替換才能達到保護隱私，這就是為什麼方法二在同一多項式中需要分配兩個以上的多項式子金鑰。方法二的認證協定與金鑰建立的詳細步驟



圖四 方法二認證協定與金鑰建立

如下：

步驟 1 首先路側單元會不斷廣播自己的真實身份以及自己擁有的多項式編號列表(Polynomial ID List)，當車輛行進到路側單元的通訊範圍會接收到該路側單元的真實身份及多項式編號列表。當車輛收到該訊息後，OBU 便會比對本身與路側單元共有的多項式編號，因為 OBU 本身在同一個多項式中會擁有兩個以上的多項式子金鑰，所以可隨機挑選屬於該編號中的多項式子金鑰來使用。例如：挑選到 $f_\alpha(PID_\beta, y)$ 這個帶有假名多項式子金鑰。即可計算出與該路側單元共有的認證金鑰 $au\_key = f_\alpha(PID_\beta, RSU_{id})$。再選擇一個隨機亂數 r，並且使用認證金鑰 au_key 加密，然後傳送共有的多項式編號、假名及加密過的 r 給該路側單元。

步驟 2 該路側單元收到後，確認使用哪個多項式編號，並計算認證金鑰 $au\_key = f_\alpha(RSU_{id}, PID_\beta)$，然後使用 au_key 解出 r。之後選擇一個隨機亂數 s，並計算此次通訊要使用的暫時通訊金鑰 $SK = h(r \| s)$。最後將 s 及 SK 加密後傳送給該車輛。

步驟 3 之後由 OBU 解出 s 及 SK，再計算 $SK = h(r \| s)$ 是否等於接收到的 $h(r \| s)$。如果正確無誤，最後使用 SK 加密 s 回送給路側單元完成相互認證的步驟，而接下來就使用暫時通訊金鑰 SK 加密與路側單元的通訊內容。

五、 分析

5.1 安全分析

在我們提出的方法中，多項式之金鑰分佈的安全性會依據其多項式的級數 t 的大小，當攻擊者企圖取得認證金鑰時，攻擊者必須收集超過 t+1 個多項式子金鑰來還原多項式。因為當多項式被攻擊者還原後，即可任意代入使用者的假名與路側單元的真實身份計算使用該條多項式的任意一對認證金鑰。

當級數 t 設定越大時，攻擊者還原一條多項式所需的共謀人數勢必要越多，原因在於本身擁有的多項式子金鑰只能計算自己與他人的認證金鑰，無法計算他人之間的認證金鑰。而且多項式池中更有著為數不少的多項式，而且每個使用者的多項式子金鑰是金鑰分佈中心隨機分配的，如此會增加攻擊者還原多項式的困難度。在多項式無法被攻擊者還原的情況下，認證時使用的認證金鑰就不會被攻擊者輕易得到，同時也無法取得用認證金鑰加密的通訊內容，因此能達到通訊的機密性。

在我們的方法中，使用者與路側單元傳送訊息認證時，所使用的資訊皆為公開資訊，透過交換公開資訊來計算認證金鑰，我們假設認證金鑰沒有被第三方取得的情況下，路側單元與使用者之間的相互認證以及暫時通訊金鑰等秘密訊息的交換皆受認證金鑰保護。同時，為了降低認證金鑰被攻擊者攻破的風險，在完成相互認證後，立即使用暫時通訊金鑰來加密傳輸訊息，降低使用認證金鑰加密傳輸資料的次數。

5.2 匿名性與不可追蹤性

在方法一中，每一個使用者會拿到 k 個已經代入假名的多項式子金鑰，例如：$f_3(PID_{10}, y)$，這表示 PID_{10} 這個假名用在多項式編號為 3 的多項式中，而 $f_3(PID_{10}, y)$ 這個多項式子金鑰只有一個使用者擁有，金鑰分佈中心不會重複分配同一個已經代入假名的多項式子金鑰給兩個以上的使用者。然而，我們的匿名性則是基於一個假名並不專屬於某個特定的使用者，也就是說 PID_{10} 可能會有多個使用者同時擁有，必須配合多項式編號才能決定多項式子金鑰分配給哪個使用者。例如：使用者 i 拿到 $f_3(PID_{10}, y)$，而使用者 j 拿到 $f_{12}(PID_{10}, y)$，雖然 i 跟 j 同時各擁有叫做 PID_{10} 的假名，但是因為多項式編號不同，所以 i 跟 j 並不為同一個人，路側單元則無法從單一假名辨別某個特定的使用者。優點是可以避免被路側單元進行追蹤。例如：使用者 i 將依序行經 RSU1 與 RSU2 這兩個路側單元，使用者 i 在 RSU1 這個路側單元通訊時使用名為 PID_{10} 的假名，當他離開 RSU1 並進入 RSU2 進行通訊時，他使用名為 PID_3 的假名，假設使用者 j 剛好同時進入 RSU2 進行通訊並使用名為 PID_{10} 的假名。此時，RSU1 與 RSU2 則無法連結同一個名為 PID_{10} 的假名到同一個使用者身上，因為名為 PID_{10} 的假名會有許多使用者同時擁有。另一方面，當使用者 i 下一次行經 RSU1 進行通訊時，使用者 i 將重新選擇一個多項式子金鑰來與 RSU1 進行通訊，也就是說使用者 i 每次跟路側單元進行通訊時都會使用不同的假名與多項式子金鑰，以便於達到匿名的效果。

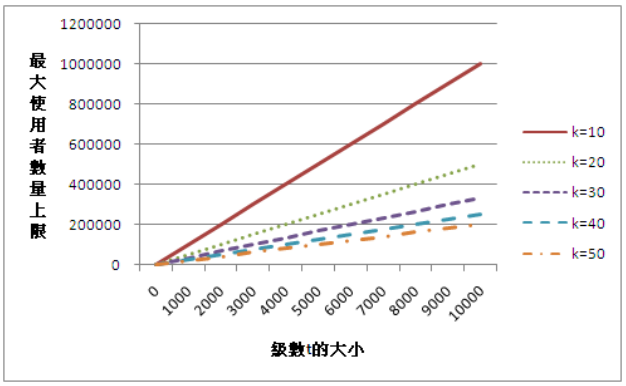
在方法二中，每一個使用者會被分配 k 個已經代入假名的多項式子金鑰，而且在同一個多項式中會被分配兩個以上的多項式子金鑰。因為在路側單元與車輛通訊時，必須比對出共同分享的多項式編號以表示擁有相同的多項式來計算認證金鑰。然而當車輛每次行經相同的路側單元時，通常只會與路側單元分享到某一個固定的多項式。所以在方法二中，我們提出使用者在同一多項式中被分配兩個以上的多項式子金鑰，如此，使用者在行經相同一個路側單元時，便能交換使用同一多項式中的多項式子金鑰來達到匿名的效果。

5.3 最大使用者數量上限

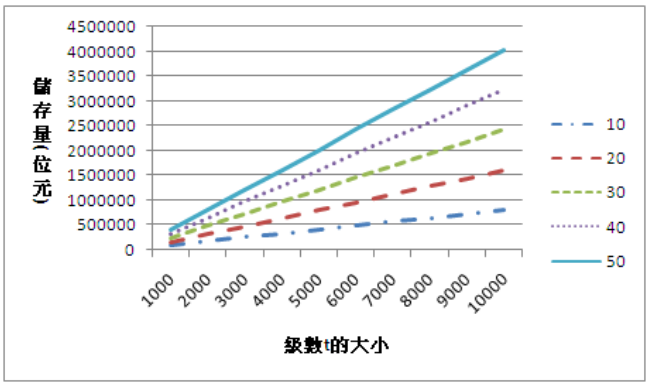
根據 Liu 與 Ning[4]的研究中提到，使用多項式池的方法會有最大使用者數量上限的限制，使用者數量上限依據多項式池中多項式的數量 n、使用者被分配多項式子金鑰數量 k 與級數 t 的大小可根據下列公式(2)計算：

$$\frac{(t+1)\times n}{k} \tag{2}$$

圖五繪出級數 t 與多項式子金鑰數量 k 在不同情況下最大使用者數量上限的變化。從圖五來看，多項式池中多項式的數量設定在 1000，當使用者被分配到 10 個多項式子金鑰且級數 t 大小為 10000 時，最大的使用者數量上限大約



圖五 最大使用者數量上限



圖六 儲存負載量

是 100 萬。而使用者被分配到 50 個多項式子金鑰且級數 t 大小為 10000 時，最大的使用者數量上限大約是 20 萬。在車載網路中，我們可依據預估的使用者數量來調整級數 t 的大小。

5.4 儲存負載量

雖然車載網路在系統資源上並沒有受到限制，但在儲存負載量方面 Liu 與 Ning[4]也提出下列公式來計算使用者的多項式子金鑰儲存負載量：

$$k \times (t+1) \log q \qquad (3)$$

在公式(3)中，k 表示使用者被分配多項式子金鑰數量，t 表示多項式的級數，q 表示一個質數，也可看做是金鑰長度。在密碼學系統中，q 的長度建議在 64 個位元(bit)以上。如為 RC5，我們則是設定為 256 個位元。

圖六繪出使用者擁有的多項式子金鑰數量與級數在不同情況下儲存負載量的變化。假設使用者被分配到 50 個多項式子金鑰且級數 t 大小為 10000 時，使用者的儲存負載量大約需要 4025327 個位元(bit)，相當於 492KBytes。比較圖五與圖六可看出，依據使用者數量來調整級數 t 的大小在車載系統的資源上對於儲存負載量不會造成太大的負擔。

5.5 比較

本小節中我們將針對我們的方法與 Xi 等人[7]的方法做比較。我們的研究採用多項式池之技術為基礎，而 Xi 等人提出的研究則是以對稱式金鑰池為基礎。根據表四，我們提出的方法一、方法二與 Xi 等人的方法皆達到匿名性與相互認證，因此皆可匿名認證使用者並保護使用者的隱私。

然而 Xi 等人的方法在認證協定中使用到非對稱式加解密系統，包含憑證與非對稱式金鑰。Xi 等人的方法總共使用到 3 次對稱式加解密以及 2 次非對稱式加解密。在我們提出的匿名認證協定中，我們只使用到對稱式加解密系統。其中，方法一與方法二皆只使用了 3 次對稱式加解密，所以我們的方法在計算效能上會比 Xi 等人的方法來的有效率一些，對於在高速移動中通訊的車輛，我們的方法更符合即時(Real Time)的需求。

在我們的兩種方法中，方法一與方法二主要差異是在系統初始的配置不同。方法一的配置上，路側單元被分配了多項式池中他所屬的全部多項式子金鑰。在使用者與路側單元通訊時，能確保使用者跟路側單元一定能通訊。方法二的配置上，路側單元與使用者皆被分配了多項式池中一部分的多項式子金鑰，雙方必須擁有相同共享的多項式才能進行溝通，使用者有機率無法直接與路側單元通訊，必須視多項式子金鑰的分配情況進行調整以提高擁有相同

共享多項式的機率。而方法二在路側單元的儲存負載量方面會比方法一來的少，因為方法一的路側單元儲存負載量取決於多項式池中多項式的數量。當多項式池中多項式的數量提昇時，路側單元的儲存負載量也隨之提昇。而方法二的路側單元儲存量則是固定在某個數量，不會因為多項式池中多項式數量增加而使路側單元的儲存量隨之增加。簡言之，方法一的優點是沒有驗證失敗的風險，缺點是必須在每個 RSU 皆儲存所有的多項式。而方法二的缺點在於可能會出現車輛與 RSU 之間沒有共同金鑰，造成建立通訊金鑰失敗，但優點是可以減少 RSU 內大量的儲存空間。

表四 我們的方法與 Xi 等人的方法比較表

	方法一	方法二	Xi 等人[7]
匿名性	有	有	有
相互認證	有	有	有
密碼學系統	只使用對稱式	只使用對稱式	非對稱式與對稱式同時使用
對稱式加解密次數	3 次	3 次	3 次
非對稱式加解密次數	0 次	0 次	2 次

六、 結論

在本研究中，我們提出了使用多項式池的方法加入假名的概念並結合兩者達到以匿名方式認證合法使用者同時建立安全通訊的金鑰。在認證協定中，我們依據不同的系統配置提出兩種認證協定的方法，並分析我們的方法達到認證合法使用者且同時具備匿名性，也分析我們的方法中匿名認證協定的安全、最大的使用者數量上限、及儲存負載量，最後再與其他論文比較。在我們提出的方法中，使用對稱式金鑰系統以降低加解密的時間，並且做到認證使用者並保護使用者的隱私。從分析中我們可以看出我們的方法除了達到匿名外，再與 Xi 等人的研究相較之下，在計算效能方面比他們來的有效率，更適合在快速移動中且要求即時的車載系統中使用。在未來的工作上，我們將考慮減少金鑰分佈中心的計算複雜度，例如使用多個金鑰分佈中心共同進行多項式池之分配，減少單一金鑰分佈中心可能造成計算複雜度太高的情況。

七、 參考文獻

[1] Now:Network on wheels, http://www.network-on-wheels.de/

[2] G. Calandriello, P. Papadimitratos, J-P. Hubaux and A. Lioy, ”Efficient and Robust Pseudonymous Authentication in VANET,” ACM international workshop on Vehicular ad hoc networks(VANET’07), pp.19-28, 2007.

[3] H. Chen, A. Perrig and D. Song, “Random Key Predistribution Scheme for Sensor Networks,” Proc. IEEE Symp. Security and Privacy (S&P’ 03), pp.197-213, 2003.

[4] D. Liu and P. Neng, “Establishing pairwise keys in distributed sensor networks,” The 10th ACM Conference on Computer and Communications Security (CCS), pp.52-61, 2003.

[5] M. Raya and J-P. Hubaux, ”The Security of Vehicular Ad Hoc Networks,” The 3rd ACM workshop on Security of ad hoc and sensor networks(SASN), pp.11-21, 2005.

[6] P. Traynor, R. Kumar, H. Choi, G. Cao, S. Zhu, and T-L. Porta, “Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks,” IEEE Transactions On Mobile Computing, VOL. 6, NO. 6, pp.663-677, 2007.

[7] Y. Xi, K. Sha, W. Shi, L. Schwiebert and T. Zhang, “Enforcing privacy using symmetric random key-set in vehicular networks,” International Symposium on Autonomous Decentralized Systems(ISADS '07), pp. 344-351, 2007.