世新大學管理學院

資 訊 管 理 學 系

碩士學位論文

第三代行動通訊認證機制之研究

A Study on 3G Mobile Authentication Mechanism

指導教授：廖鴻圖 博士

郭明煌 博士

研 究 生：周碧欣 撰

中 華 民 國 九 十 五 年 六 月

致謝

短短的兩年研究所生涯，隨著論文的完成也即將進入尾聲，回想這一段難忘的歷練過程，心中的感受實在是難以言喻；在此過程中，不僅讓我學會了獨立的思考與研究，更慶幸能夠獲得許多人的幫助與鼓勵。

非常謝謝我的指導教授廖鴻圖老師和郭明煌老師，兩年的師生情誼與感謝實在是難以在此以短短的幾個字來表達，廖老師您不只是學生敬愛的好老師，更是生活上的好朋友！謝謝您的付出、謝謝您的教誨，謝謝您的鼓勵！同時，也要感謝口試委員吳瑞堯老師、鄭伯炤老師與吳美玉老師所給予的寶貴建議，使得我的論文更盡完善。

當然，我要感謝我敬愛的爸爸和媽媽，無論在何時何地總是全力的支持著我，讓我永遠能積極進取的面對一切挑戰。特別要謝謝我的婆婆和我的先生在細心的幫我照顧我的乖女兒，使我能夠安心且順利的完成論文。

此外，我要對同學們說聲謝謝，因為有你們的陪伴，才會讓我的研究所生活多彩多姿，也讓我擁有許多美好的回憶。淑君、醇瑞、金龍、孟勳、宇丞...，謝謝你們兩年來的幫助與扶持，很高興有你們這樣的同學，帶領著我一同學習與成長。

最後，謹以本篇論文獻給所有曾經幫助過我的家人、老師、同事，以及所有朋友和同學們，希望能將這份喜悅與榮耀分享給大家。

摘要

資訊科技 (Information Technology, IT) 的演進即將改變的不只商業行為，還包括了人們的生活方式。行動化 (Mobile) 、無線化 (Wireless) 與個人化 (Personal) 將促使行動通訊在未來展現前所未有的重要性。隨著第三代行動通訊 (Third Generation Telecommunoication, 3G) 網路的積極佈建與各項應用服務的陸續推出，3G已被視為未來的明星產業之一。為了提供資訊在無線傳輸過程中的安全性，在本論文中提出兩個應用於全球行動電信系統 (Universal Mobile Telecommunication System, UMTS) 的新認證機制。

本論文提出的第一個機制是改良 Zhang 及 Fang 所提出的 AP-AKA (Adaptive Protocol for Mobile Authentication and Key Agreement)的高安全性之 3G 認證機制。AP-AKA 的安全傳輸處理只考慮到行動基地台(Mobile Station, MS) 和 HLR/HN (Home Location Register/Home Network)之間安全，而無考慮到 MS 和 VLR/SN (Visit Location Register/Serving Network) 及 VLR/SN 和 HLR/HN 之間的安全，本論文提出的改良機制除了補強 AP-AKA 的不足，還提供預防竊聽攻擊、中間人攻擊、反射攻擊、假冒攻擊及平行會議攻擊等。

此外，本論文提出的第二個機制是有效跨網域之間的 3G認證機制，本論文的方法將橢圓曲線簽密法應用於電信網路的憑證申請程序，同時採用適當的憑證分發管理，減少VLR/SGSN 與HLR/AuC之間在MS憑證申請程序中的訊息交換。一般而言，當MS在VLR/SN向HLR/AuC申請憑證時，若HLR/AuC確認無誤，則會把憑證分發給MS。本論文的機制會把HLR/AuC發的憑證傳給MS目前拜訪的VLR/SGSN。此種方式讓MS再需要認證時，不必向HLR/AuC請求，直接向擁有該憑證VLR/SGSN請求即可。

本論文提出的機制不但可應用於目前的電信網路，亦可使用於All IP Network對行動服務提供者，或是像公車、計程車、移動咖啡館及小攤販等行動消費者中所需要的行動認證，本論文的研究亦可提供相同的助益。

關鍵詞：第三代行動通訊、全球行動電信系統、資訊安全、橢圓曲線密碼學、
認證。

ABSTRACT

The recent progress of the information technology (IT) not only changes the business behavior, but also changes our life style. The unprecedented importance of the advances in mobile communication will be prompt by mobility, wirelessness and individuality. Third Generation Telecommunication is one of future star's industries as constructively in deploying 3G network and many kinds of mobile services. Communication is typically over wireless links and it becomes critical to ensure secure message exchange. Thus, in this thesis, we propose two authentication protocols for UMTS (Universal Mobile Telecommunication System).

The first mechanism is an improvement over Zhang and Fang's protocol, called the adaptive protocol for mobile authentication key agreement (AP-AKA). That protocol only considers the security between MS (Mobile Station) and VLR/SN (Visit Location Register / Serving Network). We proposed a protocol to improve the drawback of the AP-AKA. Our protocol can prevent the eavesdrop attack, the impersonation attack, the reflection attack and the parallel session attack among MS, SN and HN.

The second mechanism is a cost effective roaming in mobile network that based on the Elliptic Curve Cryptography. It is capable of solving the critical problem of key management and distribution. This mechanism also provides non-reputation of part of the transmitted data. HLR have certificates of MS and VLR. The characteristic of this scheme is that the new VLR can obtain the certificates of MS from the previously visited VLR. MS does not need to go back to HLR authentication every time. Thus, this mechanism can reduce the bandwidth consumption between VLR and HLR.

Our authentication protocols not only conform to the specification of UMTS,

but also improve the security of the published authentication protocol of UMTS. The research of this thesis can offer the benefit to the authentication of the consumers and the mobile service providers like buses, taxis, moving cafes and street vendors, etc.

Keywords：3G Telecommunication, Universal Mobile Telecommunication System (UMTS), Information Security, Elliptic Curve Cryptography (ECC), Authentication.

目錄

圖目錄

表目錄

第1章　緒論

1.1. 研究背景與動機

資訊科技 (Information Technology, IT) 的演進即將改變的不只商業行為，還包括了人們的生活方式。行動化 (Mobile) 、無線化 (Wireless) 與個人化 (Personal) 將促使行動通訊在未來展現前所未有的重要性。隨著第三代行動通訊 (Third Generation Telecommunication, 3G) 網路的積極佈建與各項應用服務的陸續推出，3G 已被視為未來的明星產業之一。

在行動通信網路中，行動基地台與固定網路之間的所有通信都是透過無線介面來傳輸的。由於無線介面是開放的，因此在通信過程中非常容易受到侵犯 -- 任何人只要有適當的連線到該設備就可以對其進行攻擊。一般來說，行動通訊網路存在的不安全因素主要有無線介面的不安全、網路端的不安全，以及行動端的不安全等。為了提供更穩定的通訊服務，行動通訊網路的安全問題越來越受到人們的注目。

1.2. 研究目的

為了提供資訊在無線傳輸過程中的安全性，本論文將提出兩個應用於全球行動電信系統 (Universal Mobile Telecommunication System, UMTS) 的新認證機制。

本論文提出的第一個機制是改良AP-AKA (Adaptive Protocol for Mobile Authentication and Key Agreement)[30]的高安全性之 3G認證機制。AP-AKA的安全傳輸處理只考慮到行動基地台MS (Mobile Station, MS) 和HLR/HN (Home Location Register/Home Network)之間安全，而無考慮到MS和VLR/SN (Visit Location Register/Serving Network) 及 VLR/SN 和 HLR/HN 之間的安全

[15][28]，本論文提出的改良機制除了補強AP-AKA的不足，還提供預防竊聽攻擊、中間人攻擊、反射攻擊、假冒攻擊及平行會議攻擊等。

本論文提出的第二個機制是有效跨網域之間的 3G認證，為了降低VLR和HLR之間的消耗頻寬，及減少跨網路之間的資訊流[16][29]，本論文的方法是將橢圓曲線簽密法應用於電信網路的憑證申請程序，同時採用適當的憑證分發管理，減少VLR/SGSN 與HLR/AuC之間在MS憑證申請程序中的訊息交換。一般而言，當MS在VLR/SGSN向HLR/AuC申請憑證時，若HLR/AuC確認無誤，則會把憑證分發給MS。本論文的機制將會把HLR/AuC發的憑證傳給MS目前拜訪的VLR/SGSN。此種方式讓MS再需要認證時，不必向HLR/AuC請求，直接向擁有該憑證的VLR/SGSN請求即可，無論在同一個Serving Network 或者是不同的Serving Network的認證不必每次都回至HLR認證。

本論文提出的機制不但可應用於目前的電信網路，而且對未來的All IP網路，來支援一些多媒體的服務時，可藉由本研究機制及多媒體通訊服務的整合。對行動服務提供者，或是像公車、計程車、移動咖啡館及小攤販等行動消費者中所需要的行動認證，本論文的研究亦可提供相同的助益。

1.3. 研究範圍

本研究將探討寬頻分碼多工存取 (Wideband Code Division Multiple Access, W-CDMA) 的核心網路 (Core Network, CN) 的安全，核心網路CN可以分為電路交換域 (Circuit Switch Domain, CS) 及封包交換域 (Packet Switch Domain, PS)，CS域的設備主要是用戶提供電路交換資料的服務，PS域的設備則是提供封包資料的服務。CS域有關的元件包括：行動交換中心(Mobile Services Switching Center, MSC)、閘道MSC (Gateway MSC, GMSC)、客籍位置暫存器(Visitor Location Register, VLR)。PS域有關的元件為：閘道GPRS支援節點 (Gateway GPRS Support Node, GGSN)、服務GPRS支援節點 (Serving

GPRS Support Node, SGSN)。至於本籍位置暫存器 (Home Location Register, HLR)、認證中心 (Authentication Center, AuC) 則是屬於CS和PS域共用的元件。W-CDMA的CN是定義在 3GPP TS 23.002[5]。目前共有三個不同的版本存在，分別為：

1. R99-3GPP TS 23.002 V3.4.0,2000-12
2. R4-3GPP TS 23.002 V4.2.0 2001-4
3. R5-3GPP TS 23.002 V4.2.0 2001-4

本論文是以R99 版的網路及通訊協定為基礎。基本上R4 和R5 版網路的基本架構還是建構在R99 版的網路上，唯一的差別是增加一些新的元件和功能，例如R5 版的網路支援All-IP的網路架構。

圖 1-1為 3GPP的安全架構[5]，安全性功能的定義如下:

1. Network Access Security(I)：網路存取安全提供使用者和 3G 網路之間的安全存取，保護使用者的資料，可防止無線存取的相關攻擊。
2. Provider Domain Security(II)：網路提供者安全主要能夠安全地交換信號資訊，並且防止有線網路的攻擊。
3. User Domain Security(III)：提供使用者和行動基地台之間的安全存取，使用者和 USIM 的認證，USIM 卡和終端的認證。
4. Application Security(IV)：應用領域安全主要提供使用者及供應者之間可安全的交換訊息，包括資料的完整性的檢查。
5. Visibility and Configurability of Security (V)：使用者端可識別所要使用的網路服務端是否安全，以及使用者端的服務是否安全。

本論文的主要研究範圍是針對網路存取安全 (Network Access Security) 部份。

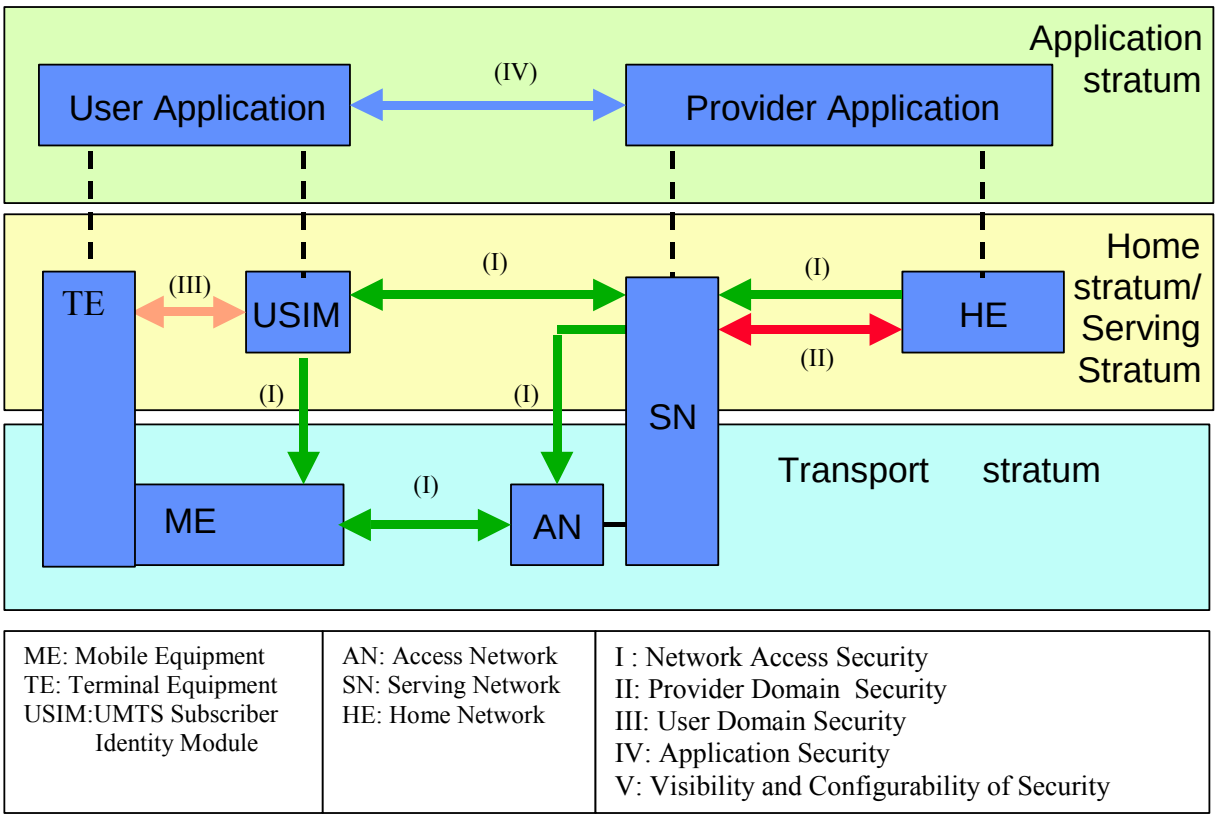

圖 1-1. 3GPP安全架構[6]

1.4. 研究架構

本篇論文架構如后所示，第一章為緒論，第二章與第三章分別介紹相關的背景知識 (如Universal Mobile Telecommunication System, UMTS)、相關行動認證機制及本論文中所使用到的一些理論與技術等。第四章說明高安全性之 3G認證機制，第五章提出有效跨網域之間的 3G認證機制，並與目前的UMTS機制[6]及黃明祥和鍾松剛的機制[40]做比較分析。最後第六章提出本研究之結論，並說明未來發展的方向。

第2章　文獻探討

2.1. 第三代行動通訊系統

第三代行動通訊 (Third Generation Telecommunication, 3G) 是目前被看好的行動通訊技術，也被視為未來 10 年的技術主流。國際電信組織 (International Telecommunication Union, ITU) 已於 1985 年宣佈將IMT-2000 技術規格列為 3G的標準[32]，由於IMT-2000 只定義基本傳輸速率的要求而未指定空中介面的規格，因此ITU的各成員體分別向ITU提出各自的技術規範來達到IMT-2000 的要求。目前符合IMT-2000 對 3G系統要求技術計有：歐洲電信標準化機構(European Telecommunications Standards Institute, ETSI) 所主導的 UMTS FDD/TDD[37]、中國所主導的TD-SCDMA[37]及部份北美和歐洲電信業者所主推的EDGE[37]。在這些技術中，UMTS FDD 及cdma2000 較受系統業者青睞，並由 3GPP (The Third Generation Partnership Project) 及 3GPP2 (The Third Generation Partnership Project 2) 來分別制定及管理這兩種技術規格 (3GPP負責UMTS FDD，而 3GPP2 負責cdma2000) [10][37]。

2.2. 全球行動電信系統簡介

全球行動電信系統(Universal Mobile Telecommunications System, UMTS）[10][23][36]是由國際電信組織 (International Telecommunication Union, ITU)於 1996 年提出，屬於 3G Mobile Cellular Communication System的一個標準。由於UMTS使用W-CDMA 空中介面技術的第三代行動通訊系統的標準，所以通常也將UMTS稱為W-CDMA系統。UMTS採用了第二代行動通訊系統類似的架構，包括用戶端設備 (User Equipment, UE)、UMTS陸地無線近接網路 (UMTS Terrestrial Radio Access Network, UTRAN)及核心網路(Core Network,

CN)。其中UTRAN處理所有與無線傳輸有關的功能，而CN則是負責語音和數據的處理並實現和外部網路的介接。從邏輯上CN又可以為電路交換域(Circuit Switch Domain, CS) 和封包交換域(Packet Switch Domain, PS)。**圖 2-1** 顯示 3G R99 架構圖：

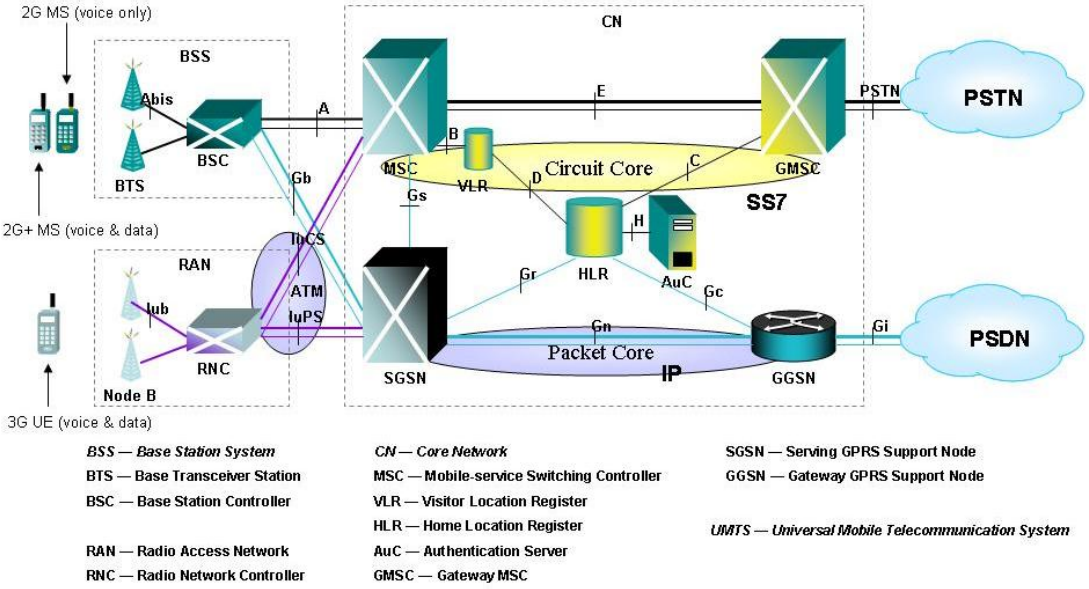

圖 2-1. 3G R99 架構圖[26]

2.2.1. 核心網路

在無線通訊的網路中，所有的使用者都會有一個專屬的本籍位置暫存器(Home Location Register, HLR)，負責記載該使用者基本的資料。而在每個 MSC 所負責的網域範圍內會有一個客籍位置暫存器(Visited Location Register, VLR)，用來記錄目前有哪些屬於其他網域的使用者漫遊到這個 MSC/VLR 所負責的網域範圍。透過這樣的基本概念，一個無線行動通訊的網路世界即已成型，當我們漫遊到其他網域時，該網域會透過我們所提供的國際移動用戶識別碼(International Mobile Subscriber Identity, IMSI)，得知我們所屬的 HLR 所在位置，進而向該 HLR 取得使用者通訊的基本資料，所以說 HLR 如同使

用者的家，而每個 VLR 就是其他網域範圍的管理人，VLR 會記錄了目前有哪些使用者到了其所管轄的範圍中，並且向其 HLR 進行登記的動作，以便於在有資料要送給該使用者時，可以透過 HLR 查詢得知目前使用者所在的外部網域位置 VLR，再來把連線要求繞送到該 VLR 網域位置，完成整個連線過程。

以下將對WCDMA/UMTS核心網路主要的設備部分進行介紹，而WCDMA/UMTS 網路基本架構如下**圖 2-2**所示。WCDMA/UMTS網路基本的架構包含無線接取網路(Radio Access Network, RAN) 與核心網路。RAN又包含了GSM與GPRS的基地台子系統(Base Station Subsystem, BSS)與UMTS 陸地無線電接取網路(UMTS Terrestrial Radio Access Network, UTRAN)。RAN主要是負責處理與Radio有關的工作。而核心網路部分，主要負責交換與繞送使用者通話或是資料的連線到外部網路。

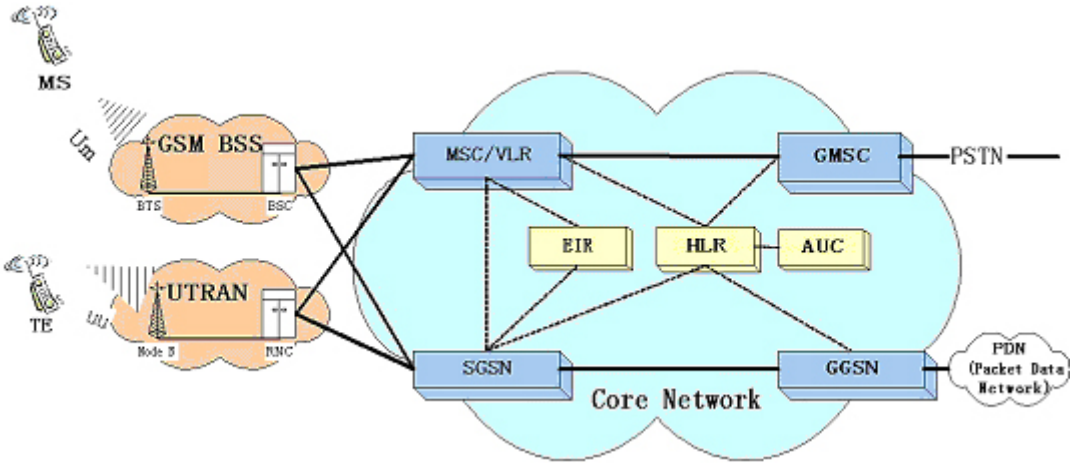

圖 2-2. 核心網路[36]

SGSN

服務 GPRS 支援節點(Serving GPRS Support Node, SGSN)主要的工作就是把使用者無線部分的資料轉送到 GPRS 網路中，以及負責把外部網路送給 GGSN 的資料，再由 GGSN 交給 SGSN 轉到無線網路介面傳送給使用者。例如原本 GPRS 使用 Gb 介面的 Frame Relay，或是 3GPP R99 核心網路中透過 ATM 來傳送原本無線介面的資料到 SGSN，SGSN 都必須要把這些資料依不同格式轉換到 GPRS 的網路上。

如下**圖 2-3**所示，SGSN如同MSC一樣，都可以連接許多的RAN，當使用者使用GPRS服務時，如果使用者因為移動而發生Handover。這時新的SGSN會去跟舊的SGSN要這位使用者的IMSI，以便去向使用者的HLR索取該使用者的資料。如果舊的SGSN並沒有那位使用者的IMSI資料，則新的SGSN才會跟使用者的行動設備索取IMSI。要如此大費周章傳送IMSI的原因，就是因為透過無線資源傳遞IMSI號碼是不安全的。

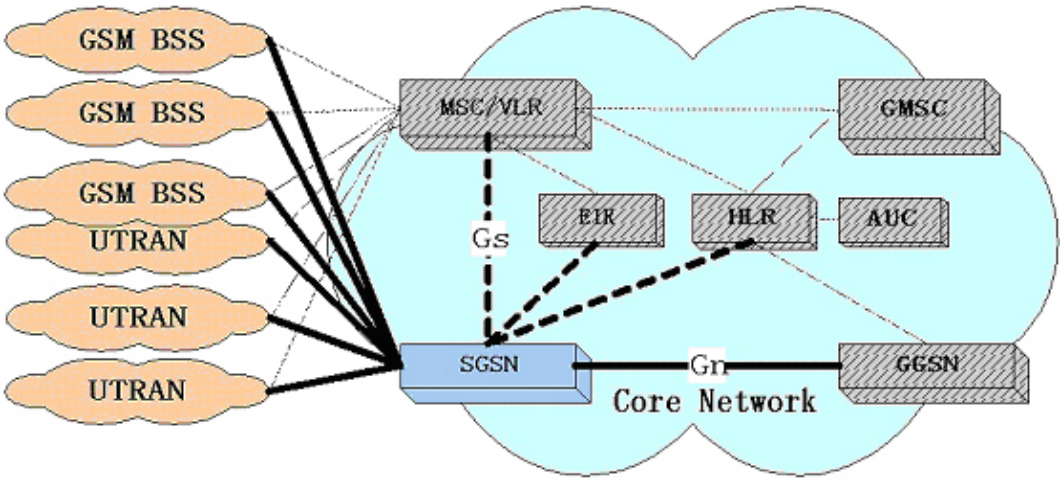

圖 2-3. SGSN (GPRS服務節點)[36]

當使用者使用 GPRS 服務傳遞資料且因為移動而產生 Handover，則原本傳送封包資料的行為將持續。不過那些封包會被傳到舊的 SGSN，並且被丟棄。採用此方法的原因是當使用者完成了 Handover 之後，重送的封包會送到新的 SGSN 再透過 Radio Network 轉送給使用者，對於使用者在使用 GPRS

服務來說是不會有影響的。

GGSN

如下**圖 2-4**所示，閘道GPRS支援節點(Gateway GPRS Support Node, GGSN)對網路而言，它就如同是系統業者的閘道器Gateway。而且現在IPv4的網路位址數目並不足以讓每個手機都擁有一個IP位址，所以說GGSN必須採用NAT (Network Address Translation) 來處理手機的IP位址分配。手機的IP位址可以分為靜態配置 (固定使用者的IP位址存放在HLR)或是動態配給(由GGSN來負責配發，通常都會透過業者位於GGSN的DHCP伺服器)。

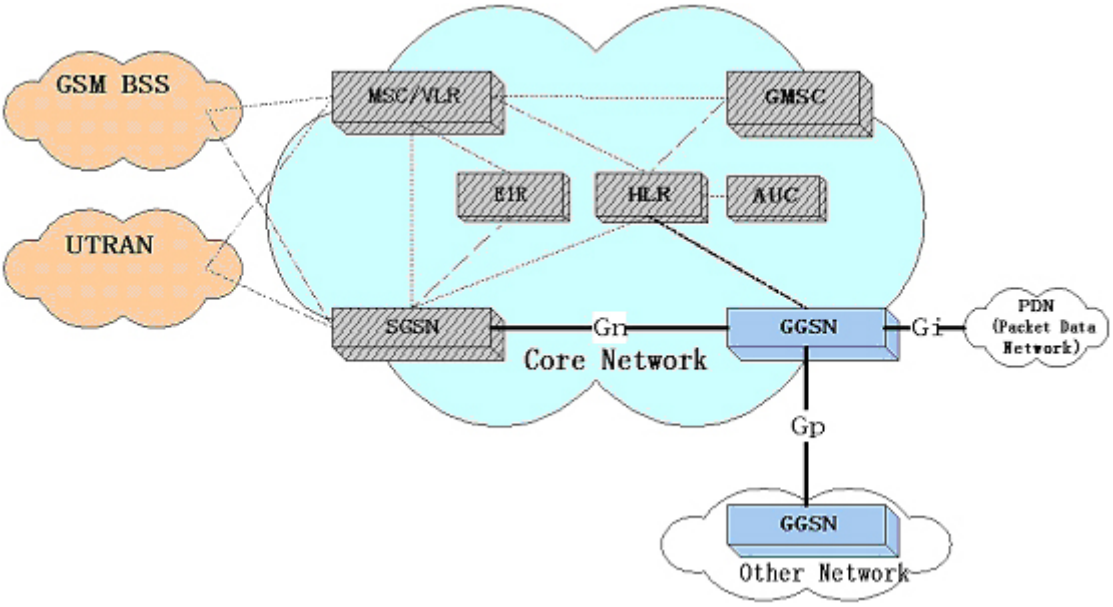

圖 2-4. GGSN(GPRS閘道節點)[36]

GGSN 除了負責把在系統業者內部網路的封包轉送到外部網路，也要負責把外部網路的封包轉送到系統業者的內部網路。由於這兩端可能使用不同的線路，因此 GGSN 還必須擁有資料切割與分封轉換的能力。

HLR

本籍位置暫存器(Home Location Register, HLR)是行動通訊網路上用來儲存使用者資料的設備，且每一個使用者都會歸屬於一個 HLR。HLR 紀錄的資

料可分為兩種，一類為永久性的資料，例如國際移動用戶識別碼(International Mobile Subscriber Identify, IMSI)與國際移動設備識別碼(International Mobile Station Equipment Identify, IMEI)。另一類為暫時性需要即時更新的資料，例如行動用戶目前所在的 MSC/VLR 位置。當使用者移動位置時，HLR 就必須要作資料的同步更新，以隨時掌握使用者目前的位置。

VLR

客籍位置暫存器(Visitor Location Register, VLR)是一個行動通訊網路會有多個行動交換中心(Mobile Switching Center, MSC)，而每個 MSC 都會有一個 VLR。VLR 都會存放目前所有在該 MSC 管理區域內的所有手機資料，而一個 VLR 也可以同時被多個 MSC 所使用。每當使用者進入一個新的 LA (Location Area)時，就要向新區域 MSC 所擁有的 VLR 註冊，並且更新 HLR 中的目前位置資訊，以便於在有使用者的電話接入時，可以透過 HLR 找出使用者目前所在的 MSC 位置，再把電話連線轉到目前使用者所在的 MSC，以進行後續的動作。

VLR 需負責提供行動設備漫遊號碼(Mobile Station Roaming Number, MSRN）給其他的 MSC 處理行動設備通話，並提供行動設備臨時使用號碼（Temporary Mobile Station Number, TMSI）、最新註冊位置區(LA)及從 HLR 複製過來的用戶資料。因此在空中傳遞用戶識別碼時，就可以用 TMSI 來代替 IMSI。因為 TMSI 是臨時配發的，且會隨著使用者移到不同區域時而有所不同，因此用 TMSI 代替 IMSI 可以避免被竊取的危險。

AuC

認證中心（Authentication Center, AuC） 是 W-CDMA 核心網路 CS 和 PS 域共有的實體，它主要是負責通訊的安全和加密。AuC 將加密的數據通過 HLR 傳送至 VLR、MSC 及 SGSN，以確保通訊的安全和合法。每個 AuC 只

會和相對應的 HLR 連接，並透過該 HLR 和外部通訊。通常 AuC 和 HLR 會結合在一起形成單一的網路實體(HLR/AuC)。

2.2.2. 行動管理

在過去使用傳統電話的環境中，所有的線路都是預先裝設好的，以目前使用的 PSTN 來說，家家戶戶幾乎都會裝設有 PSTN 的電話機，在臺北的用戶如果要跨區撥電話到臺北以外的地區，就必須要加上對方的地區碼，以供電信局的局端設備辨認。在這樣的通訊網路環境中，撥電話的一方很清楚的知道目前所要通話的對象所在的位置。正因為如此，這類固定線路的通話設備，可以輕易的透過指定的電話號碼把各地的用戶連接起來。但是在無線通訊的網絡中，使用無線通訊設備的使用者，隨時都可能在各地漫遊移動，因此如何掌握使用者現在所在的位置與辨認使用者的身分，便成為了在無線通訊領域中一個極為重要的關鍵點。

以下將介紹在 WCDMA/UMTS 無線通訊的領域中，系統是如何辨認使用者身分，並且是透過怎樣的機制讓在無線通訊網絡中的使用者可以順利的與另一端使用者進行通話。要瞭解這些流程，首先介紹系統是如何辨認與定址使用者與他的行動設備。由於牽涉到一些系統用來識別使用者身分以及目前所在位置的識別碼，以下將介紹在行動管理機制中，所會用到的識別碼:

IMSI

國際移動用戶識別碼 (International Mobile Subscriber Identify, IMSI) 號碼是唯一的。當向手機系統業者申請服務時，在業者所給的 SIM 卡(Universal Subscriber Identity Module, USIM) 中就會包含 IMSI 號碼。系統業者可以透過唯一的 IMEI 號碼與唯一的 IMSI 號碼，來確定目前使用者所使用的手機與所使用的 SIM 卡是否是有效的。

當使用者漫遊到其他業者的網路時，目前使用者所在的網域可以透過要

求使用者的 IMSI 號碼，來辨認出使用者所屬的 HLR。因為 IMSI 是唯一的，所以 HLR 可以透過搜尋 IMSI 號碼，來傳回使用者的基本資料與其他相關資訊。

IMSI 主要由以下幾個部分所組成:

1. MCC + MNC + MSIN
2. MCC (Mobile Country Code) 行動電話國碼，共 3 個 10 進位數字。如中國的 MCC 為 460、德國的 MCC 為 262 而台灣的 MCC 為 466。
3. MNC (Mobile Network Code) 行動電話網路碼，共 2-3 個 10 進位數字。用來識別使用者所歸屬的無線通訊網路。例如:中華電信(Chunghwa)為 92 、台灣大哥大(TWN GSM 1800)為 97、遠傳電信(Far Eas Tone) 為 01、泛亞電信(TransAsia) 為 99 及信電訊(KGT-ON LINE)為 88 。
4. MSN(Mobile Subscriber Number)移動用戶識別碼，最多不超過 10 個 10 進位數字。用來識別無線通訊網錄中的使用者。

TMSI

國際移動用戶暫時識別碼 (Temporary Mobile Subscriber Identity, TMSI) 的組成結構由系統業者自行訂定，不過總長度不超過 32 bites。如同 IMSI 號碼在全世界是唯一的，TMSI 號碼在所屬的 MSC/VLR 業務範圍內必須是唯一的。為了避免 IMSI 被盜錄，目前在空中傳送用戶識別碼時用，大家都採用 TMSI 來代替 IMSI，不過 TMSI 只在目前位置的 MSC/VLR 區域內有效，而且只會記憶在使用者手機的 SIM 卡與目前的 VLR 上，並不會傳回 HLR。

如同 TMSI，P-TMSI 是屬於 SGSN 所管轄的範圍，並且紀錄在 SGSN 當中。當我們離開目前的 SGSN 所負責的網路範圍進入下一個新的 SGSN 網路

範圍時，P-TMSI 就會由新的 SGSN 來重新指定，並且只限在目前新的 SGSN 通訊範圍內有效。

IMEI

國際移動設備識別碼 (International Mobile Station Equipment Identify, IMEI) 號碼是唯一的，用來識別移動設備的號碼。IMEI 主要是由設備製造商所配給的，並且被行動電話系統業者儲存在 EIR。可以用來監控被竊取的手機，例如被竊的手機就算換了 SIM 卡，可是 IMEI 號碼仍然不變，系統業者可以辨認被竊的手機是透過哪一個 SIM 卡所撥出的，進而找出目前是誰在使用被偷竊的手機，或是透過 IMEI 號碼拒絕對特定的手機提供服務。

IMEI 主要由 TAC、FAC、SNR 及 SP 所組成，以下針對各個部份逐一介紹。

1. 型號批准碼 (Type Approval Code, TAC)，共 6 個 10 進位數字，由歐洲型號批准中心分配。例如 Nokia、Ericsson 與 Motorola 被分配到不同的批准碼，同一家公司所生產的不同型手機也會有不同的型號批准碼，所以如果同型的手機卻有不同的型號批准碼，很可能是仿冒品。
2. 最後裝配碼(Final Assembly Code, FAC)，共 6 個 10 進位數字，表示手機最後的生產工廠或是安裝完成的地點，由各廠商負責編碼。
3. 序號碼(Serial Number, SNR)，共 6 個 10 進位數字。由各手機製造商負責分配編碼，具有唯一性。例如同一個廠牌的同一型號的手機，每一隻手機的 SNR 號碼不可能重複。
4. 備用碼 (Spare, SP)，共 1 個 10 進位數字，通常為 0。

LAI

位置區識別碼 (Location Area Identity, LAI) 用於使用者手機的位置更

新。一個基地台的廣播頻道 (Broadcast Channel, BCH) 會不斷的廣播該基地台所屬的 LAI。每一個 Location Area 都會擁有一個唯一個 LAI，當使用者從原本的 LAI 跨越到另一個 LAI 時，就會對 VLR 發出位置更新 (Location Update) 的要求。

LAI 主要由 MCC、MNC、LA code 所組成，以下針對各個部份逐一介紹。

1. 行動電話國碼(Mobile Country Code, MCC)，共 3 個 10 進位數字。與 IMSI 中的 MNC 相同，其餘資料可參閱 IMSI 中的 MCC 介紹。
2. 行動電話網路碼(Mobile Network Code, MNC) ，共 2-3 個 bytes。與 IMSI 中的 MNC 相同，用來識別使用者所歸屬的無線通訊網路。其餘資料可參閱 IMSI 中的 MNC 介紹。
3. 位置區號碼 (Location Area Code, LA Code)，用來定義無線通訊網路中不同的位置區。

如下**圖 2-5**所示，通常一個LA (Location Area) 所指的是一個MSC/VLR底下所有Cells包含的範圍。而RA (Routing Area) 所指的是一個SGSN所包含的範圍，一個LA底下可以包含數個RA，也就是說MSC/VLR所包含的Cells範圍中，可以包含有一個以上的SGSN。URA (UTRAN Registration Area) 所指的範圍就是每個UTRAN所包含的區域，這裡面也會含有數個由RNC所控制的Cell。

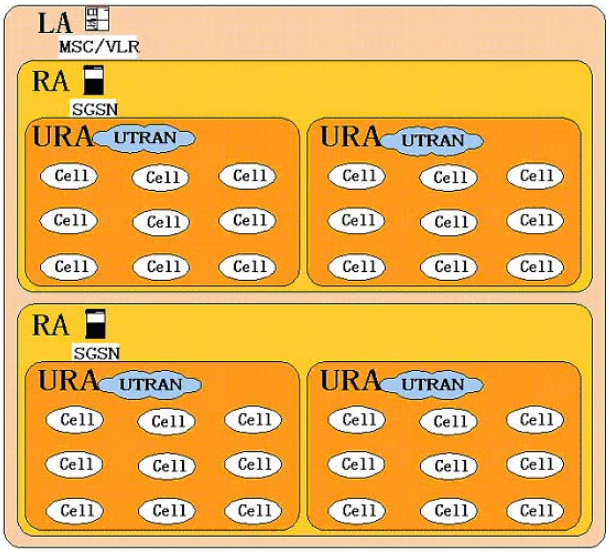

圖 2-5. LA 一個MSC/VLR底下所有Cells包含的範圍[36]

2.3. 相關行動認證機制

2.3.1. 現今 GSM 的認證機制

第一代行動通訊系統在手機發話時會將個人資料，包括電話號碼、序號等，經由無線電波傳送至基地台進行手機用戶身分鑑別。此種身分鑑別程式很容易讓惡意人士從空中攔截用戶資料並進行盜拷，造成合法使用者遭受一號多機的盜打損失。

針對第一代行動通訊系統的上述鑑別缺失，第二代行動通訊GSM系統[2][11][33][38]則改變了上述鑑別方式，在資料經由無線電波的傳輸途中，並不會直接將電話號碼等個人資料，而是先核對用戶與呼叫用戶身份，再將資料加密成亂碼後再傳送，並經過MS 與HLR雙向的鑑別程式，有效降低遭受盜拷與盜打的可能性。由上可知GSM的鑑別程式可以提供以下幾個特點：鑑別性、機密性與匿名性等特點。

1. 鑑別性(Authentication)：GSM Network operator（通常為在HLR中的AuC）透過RAND碼與MS端SIM卡中的用戶個人鑑識密碼Ki以A3 演

算法[33]進行認證動作，以驗證MS是否為合法使用者，進而達到不容易被盜拷號碼的目的。

2. 機密性(Confidentiality)：透過RAND碼與Ki利用A8 演算法[33]產生加密用的Kc，收送雙方借由frame number與Kc利用A5 演算法來進行訊息的加解密，進以達到訊息不容易被竊聽得知內容的目的。
3. 匿名性(Anonymity)：利用傳遞TMSI取代IMSI，以避免因為手機IMSI的資訊被擷取而造成使用者相關資訊被竊取。

GSM 利用 SIM 卡來達到以上的安全機制，同時俱有著高可攜性與高個人化的特性，同時只要 GSM 主機系統所支援的漫遊區域，使用者即可在不洩漏 SIM 資料的情況下享用通訊服務。

2.3.2. 現行的 UMTS

UMTS系統[10][11][32][38]是由GSM核心網路架構發展而來，以下說明UMTS的安全設計：

1. 學術界對於GSM未公開加密演算法批評甚多，而且A5/1 與A5/2 演算法後來更被Marc Briceno、Ian Goldberg和David Wagner用逆向工程法破解[12]；因此UMTS在安全設計上藉由公開加密演算法來接受考驗與測試，以提昇安全性。
2. GSM的身分驗證並未納進標準中，所以業者可以自行設計。有許多業者使用COMP-128 已被證實該演算法會遭受攻擊[11][12] (雖然GSM Association隨即提出取代的演算法[4])。為了避開類似的問題再度發生，UMTS將一些公開、安全的演算法納進標準中，如MILENAGE[4][8]與KASUMI[7]等。
3. GSM 的金鑰長度 64bits，初始設計前 10bits 並未使用，真實金鑰僅54bits，雖然後來已改成使用 64 bits，而且要再增加金鑰長度是很困

難，因為演算法與協定需要修改、甚至重新設計，硬體也因此可能需要升級。為了避免重倒覆轍，UMTS 的金鑰長度採 128 bits 來因應現在的安全問題。

4. GSM沒有明確的設計用來抵禦來自網路端的主動式攻擊，GSM原本的考量是因為主動式攻擊需要一個假基地台，成本太高，故認為不太可能有如此的攻擊行為。隨著網路設備與服務越來越普及、成本越來越低及可獲得性越來越高，目前是有可能透過假基地台取得使用者資訊，雖然之後GSM有提出因應對策[11]。在未雨綢繆下，UMTS在設計上利用AUTN(i)來對網路端進行認證。
5. GSM 的 Circuit-Switched Service 僅在 MS 與 BS 之間進行加密保護，而 UMTS 在設計上則除了在 MS 與 BS 之間進行加密保護外，更拓展到整個網路，包括網路設備與網路設備之間。

UMTS 認證機制

UMTS認證身份可採用以對稱式加密系統為基礎之方式，MS及HLR共用一把秘密金鑰K，該把金鑰只對使用者USIM和HLR認證中心AuC有效。此外使用者端USIM維護追蹤計數器SQN，HLR也維護追蹤計數器SQN，以便網路的鑑別，每一個使用者都有自己一個獨立的序號SQN，使用此種鑑別的方式是為了和GSM系統的相容，以便GSM漫遊到UMTS系統。其使用者認證步驟如圖 2-6及 **圖 2-7**所示，詳細步驟如下：

1. MS 首次登錄系統時，VLR 要求 MS 註冊，MS 將 IMSI 及所要求的服務形式，電路交換域 CS 或封包交換域 PS 連線服務，傳給 VLR。
2. VLR 將 IMSI 傳給 HLR 請求認證向量(Authentication Vector, AV)。
3. HLR 產生 n 組有順序的認證向量 AV，回傳給 VLR。每組認證向量 AV 包含了隨機亂數(Random, RAND)、預期的結果(Expect Output,

XRES)、用戶鑑識密碼(Cipher Key, CK)、完整金鑰(Integrity Key, IK)及 AUTN。

4. HLR 將剛產生的 n 組認證向量 AV 傳送給 VLR。
5. VLR 將儲存 n 組認證向量 AV。
6. 從 n 組認證向量 AV 中挑選一組認證向量 AV。
7. 將對應的亂數 RAND(i)及 AUTN(i)傳送給 MS。
8. MS 先驗證 AUTN(i)是否正確，若正確，則根據亂數 RAND(i)算出結果 RES(i)。
9. 將結果 RES(i)回傳給 VLR。
10. VLR 比對收到的結果 RES(i)與既有的預期結果 XRES(i)，若相同則 accept 否則 reject。認證成功後，同意 MS 利用本身的對稱式金鑰 K 及亂數 RAND(i)透過 f3、f4 演算法，計算出用戶鑑識密碼(Cipher Key, CK)、完整金鑰(Integrity Key, IK)，完成金鑰協議程序，以備往後用來加密功能及完整性功能使用。

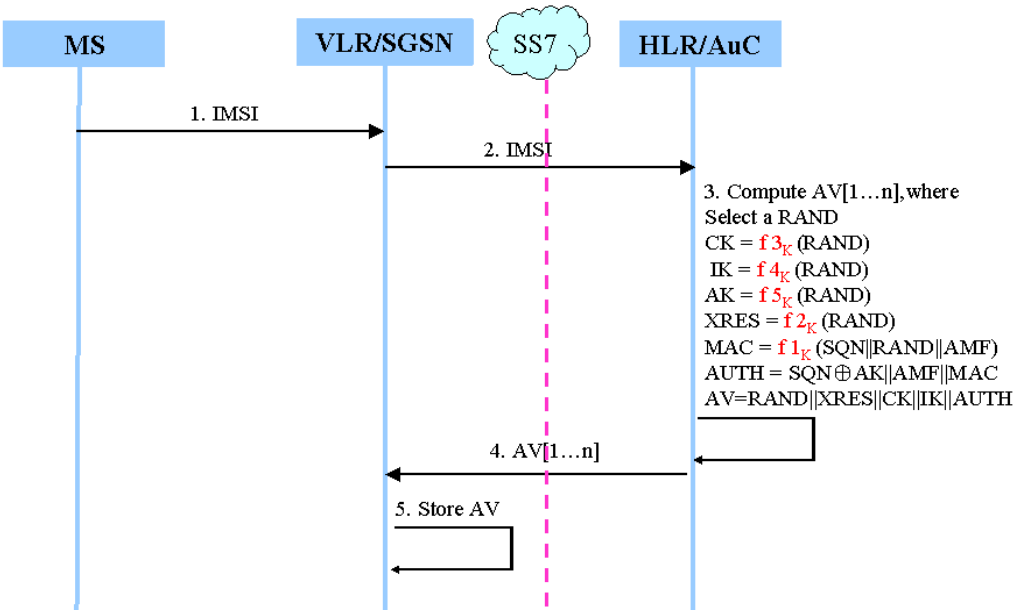

圖 2-6. UMTS認證機制-分發認證向量

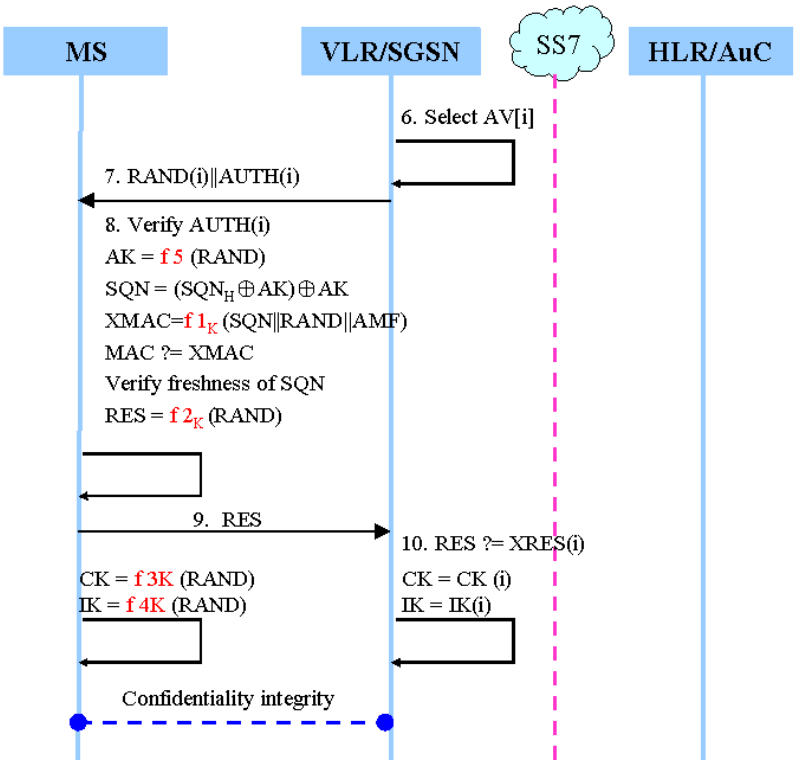

圖 2-7. UMTS認證機制-認證與金鑰協定

UMTS 國際漫遊

UMTS 漫遊時都必需回到家網路(Home Network) 的HLR認證，漫遊時的步驟如圖 2-8 所示。

1. VLR 會送給基地台 LAI 位置區域識別碼。
2. 手機端檢查位置是在家網路或是漫遊到別的網路。
3. 手機端再將暫時性號碼 TMSI 送給 VLR。
4. 若漫遊時新的 VLR 必須回到家網路的 HLR 作認證請求，從 TMSI 中可知國碼及手機端的 IMSI。
5. 當 VLR 欲對漫遊於其管轄範圍之內行動台執行認證時，透過 VLR/SGSN 向所屬的 HLR 的 AuC 請求憑證。AuC 資料庫存有行動使用者之識別碼及與對應之認證向量，HLR 將 AV 傳送給 VLR。
6. 從 n 組 AV 中挑選一組 AV。將 RAND(i)及 AUTN(i)傳給行動使用者

MS。

7. MS 先驗證 AUTN(i)是否正確，若正確，則根據 RAND(i)算出 RES(i)。將 RES(i)回傳給 VLR/SGSN。

8. 比對收到的 RES(i)與既有的 XRES(i)，相同則 accept 否則 reject。

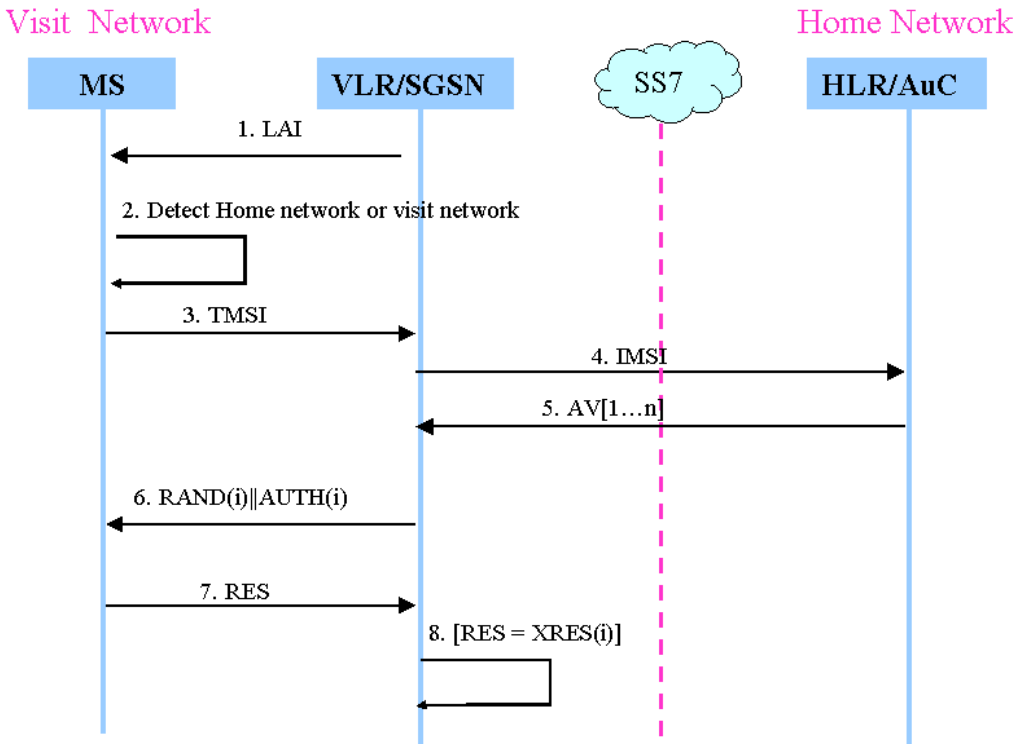

圖 2-8. UMTS國際漫遊

UMTS 安全性分析

UMTS的認證向量從HLR傳送給需要認證一個移動的用戶VLR時，還是用明文傳送，如此將使得用戶的IMSI仍然暴露在所拜訪的網路環境中。如果一個主動攻擊者偽造成合法的基地台，它可要求用戶向其傳送IMSI，在沒有驗證網路端的身份的功能下，輕而易舉地得到用戶的IMSI。雖然VLR和HLR之間的傳遞訊息時基於SS7 網路，但對未來All IP network時，安全性還是不足。

2.3.3. AP-AKA 機制[30]

機制介紹

AP-AKA (Adaptive Protocol for Mobile Authentication and Key Agreement)為Zhang 和Fang學者所提出[30]，包含MS和家網路之間的一個對稱金鑰K及三個演算法F、G、H；其中F 及H用來驗證訊息，使用G計算出金鑰。AP-AKA並不像 3GPP AKA 需要維護每一次簽署者的動態資訊，只針對新的使用者拜訪到VLR時才會請求認證。AP-AKA的步驟如下**圖 2-9**，它的執行是可以彈性選的。

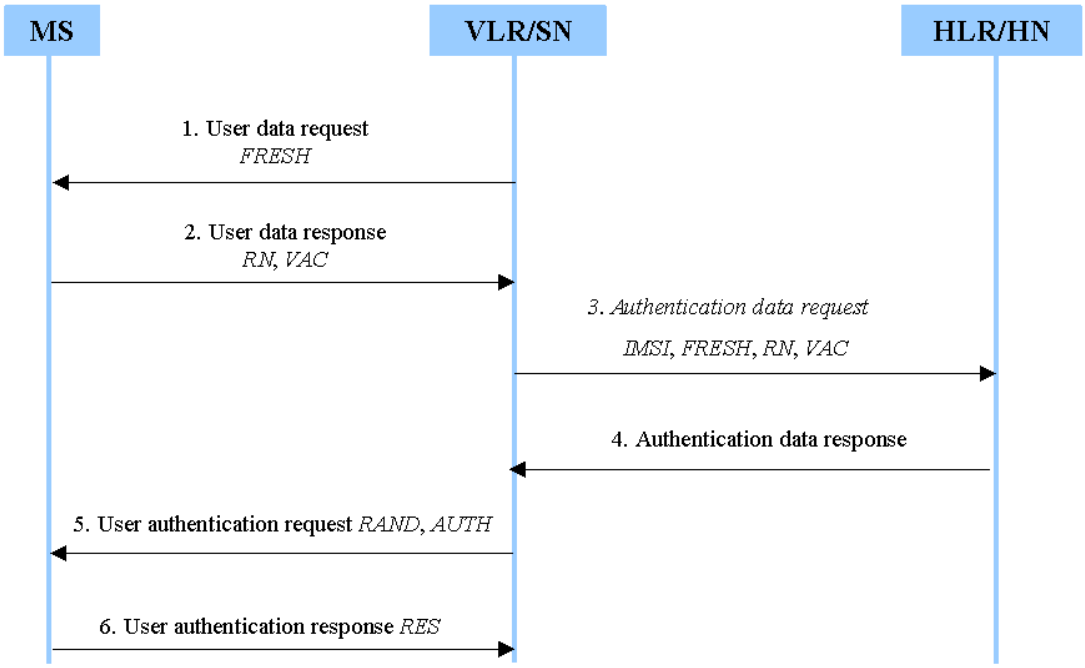

圖 2-9. Zhang 及Fang學者提出的 3GPP認認機制

1. SN→MS：當 VLR 是一個新的 VLR 時會要求行動使用者認證。
2. MS→SN：行動基地台回應一個亂數 RN 及認證碼 VAC 給 VLR。
3. SN→HN：接著 SN 會將國際行動用戶識別碼(International Mobile

Equipment Identity, IMSI)、FRESH 代表第一次拜訪到新的 SN、亂數 RN 及認證碼 VAC 送給家網路。

4. HN→SN：HN 從認證請求資料中取出秘密金鑰 K 及驗證認證碼的正確性。若失敗則 reject 國際行動用戶識別碼 IMSI、FRESH 代表第一次拜訪到新的 SN、亂數 RN、認證碼 VAC 及斷掉連線。若成功會送出認證向量給 VLR/SN。
5. SN→MS：VLR/SN 會從認證向量中取出 RAND 及 AUTH 送給 MS。
6. MS→SN：MS 先驗證 AUTN 是否正確，若正確，則根據 RAND 算出 RES。將 RES 回傳給 VLR/SN。

當行動使用者 MS 漫遊到他網路 VLR/SN 時，可依照 VLR/SN 是否存有其行動使用者之認證向量而分為兩種不同的執行方式。

漫遊到無認證向量的他網機制

當漫遊到沒有認證向量的他網VLR/SN而且驗證認證碼失敗時，執行步驟如**圖 2-10**所示。

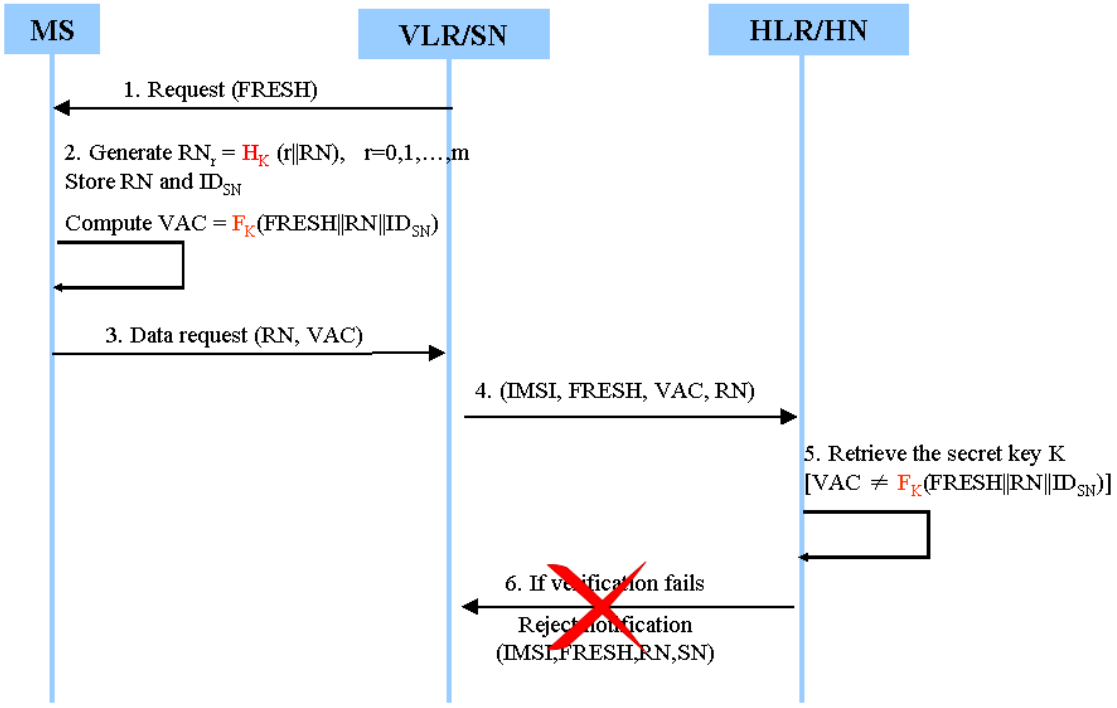

圖 2-10. 在無認證向量他網中漫遊失敗

1. SN→MS：當 VLR 是一個新的 VLR 時會要求行動使用者認證。
2. MS：行動使用者端選擇一個亂數 RN，每一個亂數只會使用一次，行動使用者端會依照網路的序號維護一列的亂數。
3. MS→SN：MS 將亂數 RN 及認證碼 VAC 回應給 SN 的 VLR。
4. SN→HN：接著 SN 會將國際行動用戶識別碼 IMSI (International Mobile Equipment Identity)、FRESH 代表第一次拜訪到新的 SN、亂數 RN 及認證碼 VAC 送給家網路。
5. HN→SN：HN 從認證請求資料中取出秘密金鑰 K 及驗證認證碼的正確性。

6. HN：若失敗則 reject 國際行動用戶識別碼 IMSI、FRESH 代表第一次拜訪到新的 SN、亂數 RN、認證碼 VAC 及斷掉連線。

當漫遊到無認證向量的他網VLR/SN而且驗證認證碼成功時，執行步驟如**圖 2-11**所示。

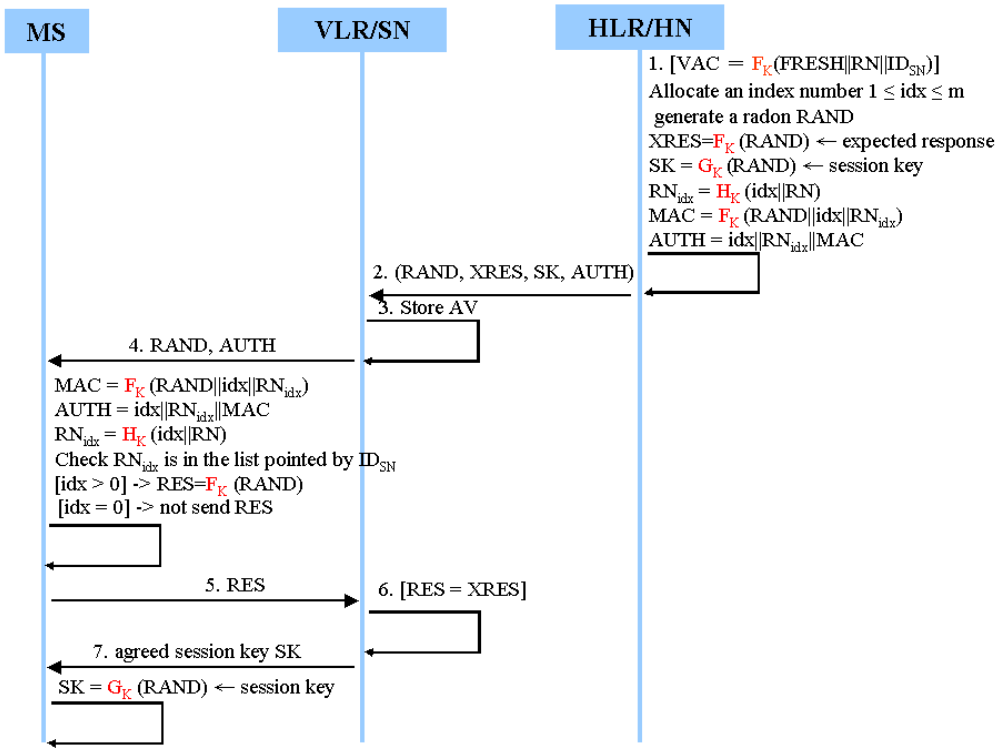

圖 2-11. 成功漫遊到無認證向量的他網

1. HN：若成功Home Network，分配認證向量的索引及產生亂數RAND，計算預期的回應XRES，會議金鑰SK及兩個認證碼(RN_{idx}、MAC)組合Authentication Token(AUTH)。
2. HN→SN：HN 會送出認證向量(亂數 RAND, XRES, SK, AUTH)給VLR。
3. SN：SN 儲存認證向量 AV。
4. SN→MS：VLR 會從認證向量中取出 RAND 及 AUTH 送給 MS。
5. MS→SN：MS 先驗證 AUTN 是否正確，若正確，則根據 RAND 算出 RES。將 RES 回傳給 VLR。

6. SN：VLR 會檢查 RES 及 XRES 是否相等，若失敗則 VLR 結束連線。

7. SN：成功則同意 MS 使用 G 計算出會議金鑰 SK。

漫遊到有認證向量的他網機制

當漫遊到有使用者的認證向量的他網VLR/SN時，執行步驟如**圖 2-12**所示。

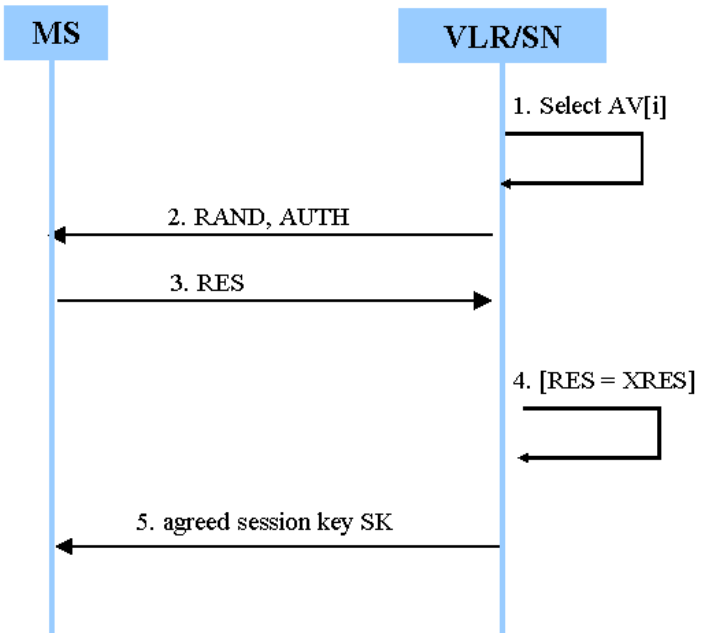

圖 2-12. 漫遊到已經有認證向量的他網

1. SN：SN 的 VLR 會從認證向量中取出 RAND 及 AUTH。

2. SN→MS：SN 的 VLR 會將 RAND 及 AUTH 送給 MS。

3. MS→SN：MS 先檢驗 AUTN 是否正確，若正確，則根據 RAND 算出 RES，將 RES 回傳給 VLR。

4. SN：VLR/SN 會檢查 RES 及 XRES 是否相等，若失敗 VLR 結束連線。

5. SN→MS：若成功則可用 SK 會議金鑰來加密。

在無認證向量的家網路中執行

在無使用者的認證向量的家網路中執行失敗的步驟如**圖 2-13**所示。

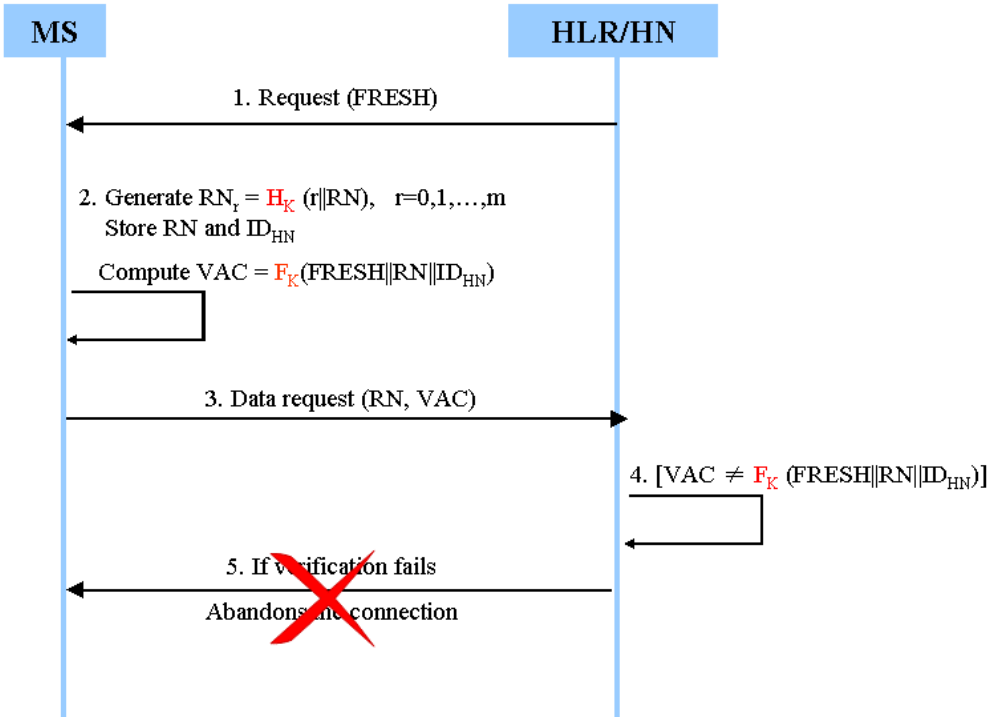

圖 2-13. 在無認證向量的家網路中執行失敗

1. HN→MS：HLR 會送出使用者請求資料。
2. MS：MS 計算出亂數RN，並且將及亂數RN及家網路的編號ID_{HM}存放在行動使用者端。
3. MS→HN：MS 會將認證碼 VAC 及 RN 回應給 HLR/HN。
4. HN：HN的HLR 檢查VAC 是否與F_K(FRESH||RN||ID_{HLR})相等。
5. HN：若失敗則中止連線。

在無使用者的認證向量的家網路中成功執行的步驟如**圖 2-14**所示。

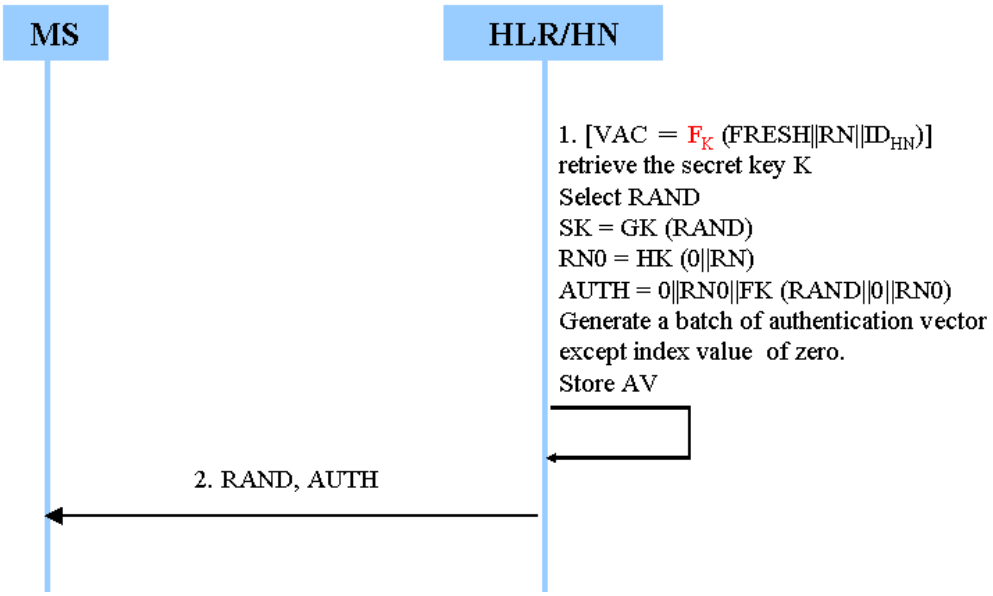

圖 2-14. 在無認證向量的家網路中成功執行

1. HN：HN的HLR 檢查到VAC = F_K(FRESH||RN||ID_{HLR})相等，則將計算出會議金鑰SK、亂數RAND、產生另一個認證向量為以後使用，每一個向量都有不同的index必須大於 0
2. HN→MS：HLR 會從認證向量中取出 RAND 及 AUTH 送給 MS。

在已經有認證向量的家網路中執行

在已經有使用者的認證向量的家網路中執行如**圖 2-15**所示，可直接使用資料庫裏的認證(RAND, AUTH)傳送到MS。

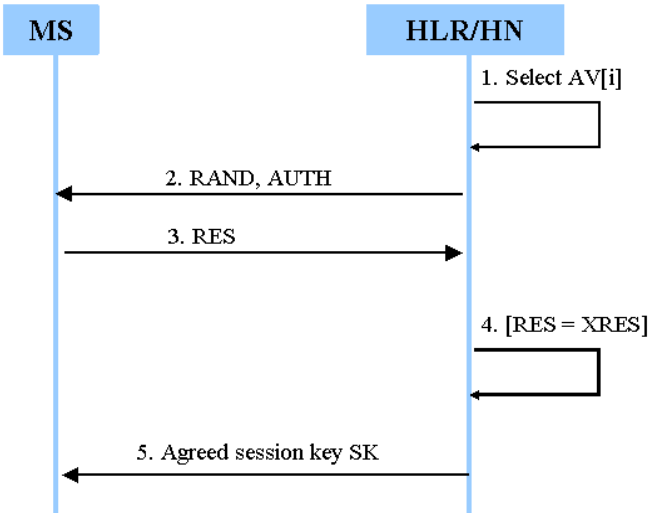

圖 2-15. 在已經有認證向量的家網路中執行

1. HN：HN 的 HLR 會從認證向量中取出 RAND 及 AUTH。
2. HN→MS：HN 的 HLR 會將 RAND 及 AUTH 送給 MS。
3. MS→HN：MS 先檢驗 AUTN 是否正確，若正確，則根據 RAND 算出 RES，將 RES 回傳給 HLR。
4. HN：HLR/HN 會檢查 RES 及 XRES 是否相等，若失敗 HLR 結束連線。
5. HN→MS：若成功則可用 SK 會議金鑰來加密。

AP-AKA 的安全性分析

AP-AKA 機制使用對稱加密系統，整個過程只需要一把秘密金匙，金鑰是永遠不變的，只要入侵者有心就可盜取或推算出金鑰。

行動用戶維護RN及ID_{SN}的安全

此機制中的行動使用者端所選擇的亂數RN及Serving network 的編號必須要存放在行動使用者端，為預防攻擊者對資料的攻擊，行動使用者端要維護RN與ID_{SN}的資料量及資料的安全。

假冒攻擊Impersonation Attack

VLR 傳送 IMSI、FRESH 及 RN 給 HLR 時完全未經保護地暴露在空中，攻擊者取得 IMSI 後假冒合法的 VLR 或 HLR。

反射攻擊Reflection Attack

攻擊者取得 IMSI、FRESH 及 RN 後，可以假冒 HLR 反向傳給 VLR。

竊聽攻擊Eavesdrop Attack

送出認證向量(RAND 亂數、XRES、SK、AUTH)給 VLR 時並沒有做保護，攻擊者可用竊聽攻擊法持續觀察並記錄通訊雙方之前認證過程中的通訊內容。

平行會議攻擊法Parallel Session Attack

是重送攻擊的一種，攻擊者使用 VLR 送給 MS 的資訊，反向傳給 VLR 使得可以成功假冒假使用者 MS。

中間人攻擊Man-in-the Middle Attack

攻擊者在 MS 及 VLR 之間或 VLR 及 HLR 之間取得通訊雙方的資料，假冒為合法使用者。

2.3.4. 黃明祥和鍾松剛學者的機制[40]

機制介紹

在黃明祥和鍾松剛學者提出UMTS認證機制[40]中，假設HN在認證系統中應該是部份被信任 (Partial Trusted)，為了避免HN會為了利益將其用戶的認證金鑰 (Authentication Key) 洩露給他人，導致合法用戶的權益受到侵害，因此提出一個新的防護機制，機制內容如**圖 2-16**及**圖 2-17**所示。

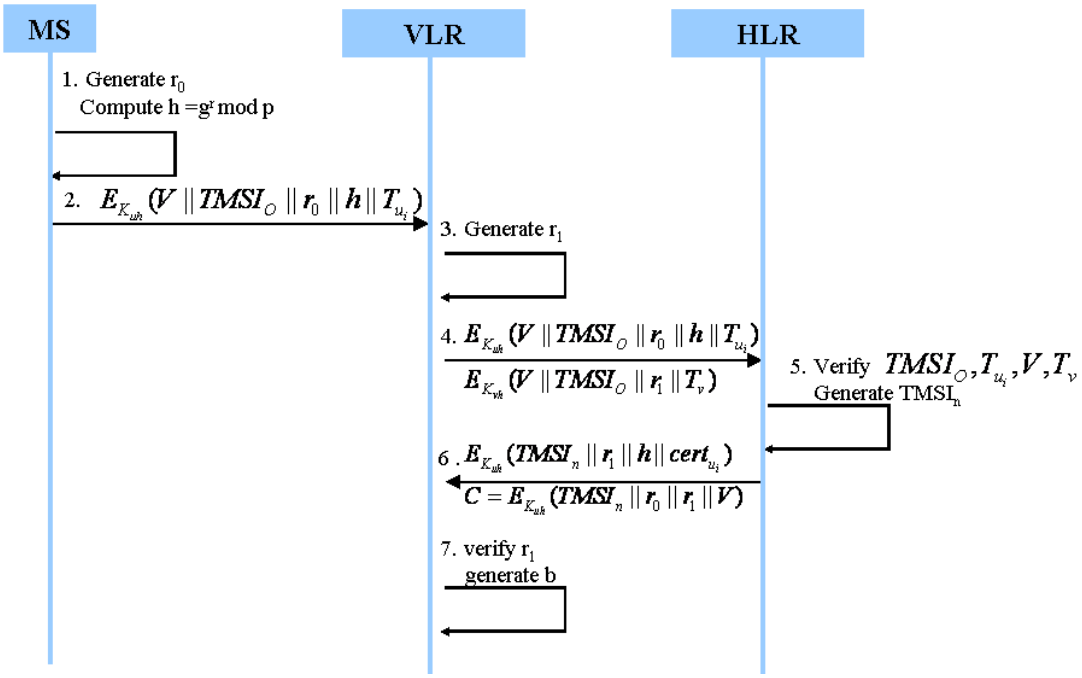

圖 2-16. 黃明祥和鍾松剛學者的UMTS機制-分發認證向量

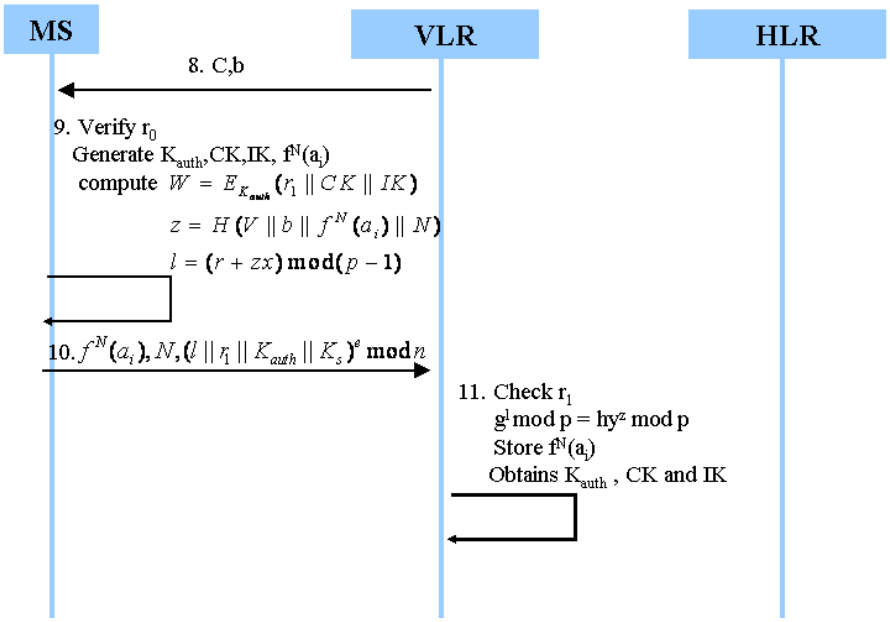

圖 2-17. 黃明祥和鍾松剛學者的UMTS機制-認證與金鑰協定

1. MS：MS 選擇一亂數 r_0，0 ≤ r ≤ p-1，計算 $h=g^r \bmod p$ 。
2. MS→VLR：使用 MS 及 VLR 的共用秘密金鑰(share secret key)K_{uh} 將(V、$TMSI_0$、r_0、h、時戳 T_{ui})加密後向 VLR 請求。
3. VLR：VLR 收到請求資料後，選擇了另一個亂收 r_1。
4. VLR→HLR：VLR 使用 VLR 及 HLR 的共用秘密金鑰(share secret key) K_{vh} 將 V、$TMSI_0$、r_1、時戳 T_v 加密後，送 $E_{K_{uh}}(V \| TMSI_O \| r_0 \| h \| T_{u_i})$ 及 $E_{K_{vh}}(V \| TMSI_O \| r_1 \| T_v)$ 至 HLR。
5. HLR：HLR 驗證 $TMSI_0$ 後,從資料連中取出 MS 的憑證及產生新的 $TMSI_n$。
6. HLR→VLR：HLR使用K_{uh}將訊息加密後送 $E_{K_{uh}}(TMSI_n \| r_1 \| h \| cert_{u_i})$ 及 $C = E_{K_{uh}}(TMSI_n \| r_0 \| r_1 \| V)$ 至VLR。
7. VLR：VLR 收到訊息後確認 r_1 是否一樣，若一樣代表憑證可信賴及簽署者的正確性，VLR 再選擇一個亂數 b。
8. VLR→MS：VLR 再將 C 及 b 送給 MS。

9. MS：MS收到VLR的訊息後檢查r_0的值，MS使用RSA產生一把金鑰K_{auth}，秘密金鑰CK及完整金鑰IK。為了減少金鑰的長度，使用hash-chaining技術先計算$f^N(a_i)$，使用金鑰K_{auth} 將r_1、CK及IK加密後產生W，之後計算z及l。

10. MS → VLR：MS 將訊息 $f^N(a_i), N, (l \| r_1 \| K_{auth} \| K_s)^e \bmod n$ 送給VLR。

11. VLR：VLR驗證都正確時，VLR可獲得K_{auth}、CK、IK。

安全性分析

黃明祥和鍾松剛學者提出的 UMTS 認證機制可防止以下的攻擊：

假冒攻擊 Impersonating Attack

MS及VLR之間的資訊傳送，使用了金鑰K_{uh}來加密。同時在VLR及HLR之間是使用了K_{vh}加密訊息，所以在MS、VLR及HLR之間的資訊流是屬於安全，可以防止了假冒攻擊。

重送攻擊 Replaying Attack

使用了時戳的方式，所以可防止重送攻擊。

第3章　相關理論與技術介紹

3.1.　對稱式加/解密

透過加密演算法將明文做各種不同的取代與置換，而加密演算法的輸入就是祕密鑰匙(Secret Key)，所謂的鑰匙是與明文無關的數值，利用鑰匙加明文加密，同樣的可以利用這個鑰匙將密文解密。

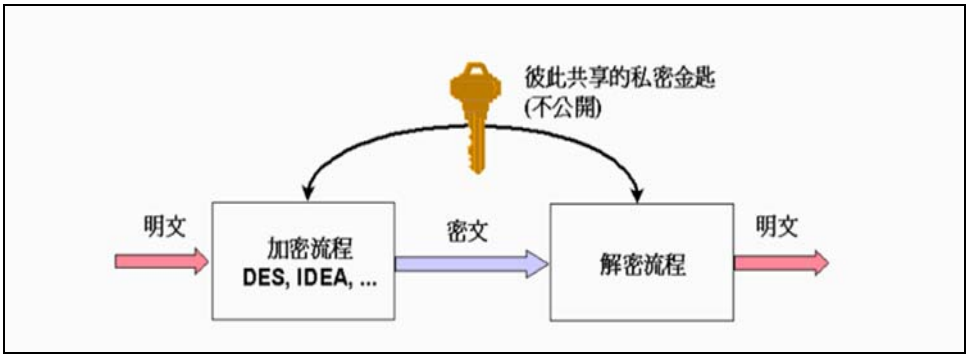

圖 3-1. 對稱式金鑰密碼系統

在對稱式加密系統中[26][44]，加密和解密都是使用同一把鑰匙(Secret Key)，所以訊息傳送雙方都必須擁有同一把鑰匙，故在此加密系統中，如何有效的傳送鑰匙到對方手中，而不會被駭客攔截或是竊取，就是一個很重要的課題。

3.2.　非對稱式加/解密

在非對稱式加密系統中[26][44]，每個人都可以產生一對金鑰，稱為公開金鑰(Public Key)和私密金鑰(Private Key)，各自保管好自己的私密金鑰，而在非對稱式的加密系統下，所有參與者都可以取得每個人的公開金鑰，而私密金鑰為個人所擁有，故不在網路上傳輸，而一個訊息用同一個人的公鑰加密，就必須用私鑰解開，反之用私鑰加密就必須用公鑰解開。

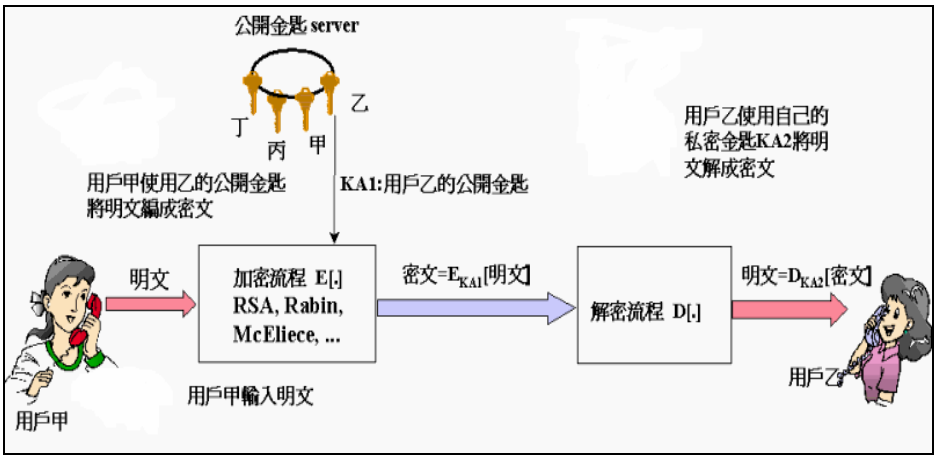

圖 3-2. 非對稱式金鑰密碼系統圖

如**圖 3-2**所示用戶甲和用戶乙，分別產生了一對金鑰(甲的公鑰、甲的私鑰、乙的公鑰、乙的私鑰)

甲使用「乙的公鑰」(乙的公鑰所有人都可以得到)，將要傳送的訊息加密後傳送給乙。在此狀況下，唯有「乙的私鑰」才可以解開，而「乙的私鑰」只要乙自己擁有，所以這封訊息只有乙可以解開，故可以達到私密性。

甲使用「甲的私鑰」將要傳送的訊息加密，然後透過網路傳送到乙，乙只要取得「甲的公鑰」即可解開訊息，如果解得開就表示這封訊息一定是甲傳送的訊息，因為只有甲擁有私鑰，如果不是就表示這封訊息可能遭到竄改，不一定是甲發出的，所以，用自己的私鑰將訊息加密，可以達到認證的效果。

甲使用「甲的私鑰」將要傳送的訊息加密，在將加密過後的密文用「乙的公鑰」加密，這樣此訊息就包含認證和加密兩項功能。乙得到訊息後，先用自己的私鑰解開密文，再使用「甲的公鑰」解一次密文，就得到最終的明文，此訊息就包括了認證和加密兩項功能。

3.3. 橢圓曲線密碼學

3.3.1. 橢圓曲線定義

在實數系上橢圓曲線[34][35][39]可定義成所有滿足方程式 $\varepsilon: y^2=x^3+ax+b$ 的點(x, y)所構成的集合。其中若方程式 $\varepsilon: y^2=x^3+ax+b$ 沒有重複的因式或 $4a^3+27b^2\neq 0$，則此方程式可成為群 (Group)。為了將橢圓曲線實作在密碼系統上，必須將橢圓曲線定義在有限體Z_p與GF(2^n)上。有限體Zp橢圓曲線方程式 $\varepsilon: y^2 \pmod p = x^3+ax+b \pmod p$，其中 $4a^3+27b^2\neq 0$；有限體GF(2^n)橢圓曲線方程式為 $\varepsilon: y^2+xy=x^3+ax^2+b$，其中$b\neq 0$，本論文將以$Z_p$為主要介紹對象。

3.3.2. 橢圓曲線加法運算

假設$P=(x_P, y_P)$和$Q=(x_Q, y_Q)$為Z_p之橢圓曲線上的點，其中$x_P\neq x_Q$且$-P\neq Q$，並視點$-P=(x_P, -y_P)$為點P的負點，則$R=P+Q=(x_R, y_R)$的負點為P與Q之連線相交於橢圓曲線上唯一的交點$-R=(x_R, -y_R)$，其結果如下：

$$\overline{PQ} = \lambda = \frac{(y_Q - y_P)}{(x_Q - x_P)}$$

方程式$x_R=\lambda 2-x_P-x_Q \pmod p$，且$y_R=\lambda(x_P-x_R)-y_P \pmod p$

假設點 Q=－P，P+Q 將為橢圓曲線上的直線，無法與橢圓曲線交會點-R，所以 P+Q=P+(－P)=O，此點稱為無限遠點O（point at Infinity），為橢圓曲線上一特殊點。

3.3.3. 橢圓曲線的乘法運算

假設$P=(x_P, y_P)$為Z_p之橢圓曲線上的點，若$y_P\neq 0$，橢圓曲線的乘法運算可以將 2P視為$R=P+P=(x_R, y_R)$，則R的負點為點P之正切線將與橢圓曲線的交點

－R=(x_R, $-y_R$)，則 $\overline{PQ} = \lambda = \frac{(3x_P^{\,2} + a)}{2y_P}$ ，方程式$x_R = \lambda^2 - 2x_P$，且$y_R = -\lambda(x_P - x_R) - y_P$。

假設$y_P=0$，則點P之正切線將無法與橢圓曲線交會點－R，所以 2P=P+P=O，而 3P=2P+P+P= P，其餘依此類推。

3.3.4. 橢圓曲線密碼系統

採用橢圓曲線來對通訊資訊加解密，首先必須選擇大質數p（$p > 2^{160}$），與兩個整數元素a、b$\in Z_p$（a、b滿足 $4a^3 + 27b^2 \pmod p \neq 0$）。並選定橢圓曲線方程式 ε ：$y^2 = x^3 + ax + b \pmod p$，挑選橢圓曲線上一點G，令此點的秩（order）為質數n（$n > 2^{160}$且$n > 4\sqrt{p}$），同時n・G＝O。接著，通訊成員A隨機選擇亂數$d_A \in Z^*_n$做為其私密金鑰，並計算對應之公開金鑰$e_A = d_A \cdot G$。同樣地，通訊成員B隨機選擇亂數$d_B \in Z^*_n$做為其私密金鑰，並計算對應之公開金鑰$e_B = d_B \cdot G$。

假設通訊成員A欲將明文M加密後傳送給通訊成員B，首先需將明文M轉換成橢圓曲線上一點P_m，其轉換方式可以參考[34]。假設通訊成員A隨機選擇一正整數K，並且產生密文C ={K・G, Pm＋K・e_B}。待通訊成員 B 收到密文C後，透過下列計算解密$P_m + K \cdot e_B - (K \cdot G) \cdot d_B = P_m + K \cdot e_B - K \cdot e_B =$ Pm計算解密，如此通訊成員B可以將Pm轉換回明文M。

橢圓曲線密碼系統其安全性取決於解離散對數問題的困難度，也就是給定 K 與 G 的話要求 Q=K・G 是相當簡單的，而給定 K・G 與 G 要求 K 則是相當困難的一件事。另外，ECC 可以採用較短金鑰長度的模運算，得到與 RSA 採用較長金鑰的模運算相同等級的安全度。

3.4. 簽密法

透過不安全的網路上傳送重要資料時，為確保文件私密性（Privacy），達成送訊者的不可否認性（Non-repudiation）與攻擊者與收訊者的不可偽造性（Unforgeability），建立一個安全可靠的機制來傳送資料。傳統做法是結合數位信封（Digital Envelope）與數位簽章（Digital Signature）的技術來達成。以公開金鑰技術為例，通訊雙方各自擁有私密金鑰（Private Key）與公開金鑰（Public Key）的金鑰對。送訊者利用本身持有的私密金鑰與數位簽章技術來對欲傳送之文件或訊息做簽署的動作，以產生數位簽章。因為此把私密金鑰由送訊者自行私密持有保管，其他人無從得知，故藉此可以達到送訊者之不可否認性。送訊者利用收訊者的公開金鑰對此數位簽章與訊息加密，再傳送給收訊者。因為只有持有收訊者私密金鑰者方可以解密，故藉此可以達成訊息的私密性。收訊者收到密文後，利用自己的私密金鑰做解密的動作，便可藉由數位簽章來鑑別收到文件是由何人簽署。

公開金鑰技術的計算與通訊成本較高，為改善此一問題，近期有一些簽密法的概念[19][34][39][41]陸續被提出，本論文中將以橢圓曲線為基礎制定了一套應用於 3G認證機制的簽密法。藉此達成私密性與不可否認性的特點。以下為以橢圓曲線為基礎的明文驗證簽密法機制中四個階段之介紹。

3.4.1. 系統初始化階段

1. 選擇大質數p（$p > 2^{160}$），與兩個整數元素a、$b \in Z_p$（a、b滿足 $4a^3+27b^2 \pmod p \neq 0$）。
2. 選定橢圓曲線方程式 $\varepsilon : y^2 = x^3 + ax + b \pmod p$，挑選橢圓曲線上一點$G$，令此點的秩（order）為質數n（$n > 2^{160}$且$n > 4\sqrt{p}$），同時$n \cdot G = O$。
3. 公佈系統參數：q、ε、G、n、h()（單向雜湊函數）、E（對稱式加密

函數）及 D（對稱式解密函數）。

4. 通訊成員可利用此公佈的系統參數，來產生金鑰對，例如：成員*A*隨機選擇亂數$d_A \in Z^*_n$做為其私密金鑰，並計算對應之公開金鑰$e_A=d_A \cdot G$，再以此公鑰向公正第三者申請憑證。

3.4.2. 送訊者產生簽密文階段

1. 對欲傳送檔或訊息加密之方法，首先利用收訊者B之憑證驗證公鑰e_B之正確性，並隨機選取一亂數$r \in Z^*_n$，計算橢圓曲線上之點$R=r \cdot G=(x_R, y_R)$，接著以收訊者*B*之公鑰e_B計算橢圓曲線上之點$K_{AB}=r \cdot e_B=(x_K, y_K)$，並以$x_K$做為對稱式加密之金鑰對明文m加密，產生密文$C = E_{x_K}(M)$。

2. 對欲傳送的檔或訊息簽章之方法，首先利用明文M、x_R與送訊者*A*之私鑰d_A計算出$H=h(M||x_R)$，並產生簽章$s=d_A-H \cdot r \pmod n$。

3. 將簽密文（C、R、s）傳送給收訊者 *B*。

3.4.3. 收訊者解密與驗證簽密文階段

1. 收訊者收到簽密文（C、R、s）後，可對密文C進行解密，首先利用送訊者A之憑證驗證公鑰e_A之正確性。接著以私鑰d_B計算橢圓曲線上之點$K_{AB}=d_B \cdot R=(x_K, y_K)$，則可以用$x_K$做為對稱式加密之金鑰對密文C解密，得到明文$M = D_{x_K}(C)$。

2. 對收到的s進行驗證的階段，首先利用收到的$R=(x_R, y_R)$與解密得到的明文M，計算出$H=h(M||x_R)$，並利用送訊者公鑰e_A計算橢圓曲線上的點$e_{AB}=s \cdot G+H \cdot R$。若$e_{AB}=e_A$，則表示收訊者B所收到的明文M確實由送訊者A所傳送。

3.5. 單向雜湊函數

單向雜湊函數[44]又可稱為單向雜湊函數，對任意長度的明文m，經由赫序函數h可產生固定長度的雜湊函數，通常用符號h(m)來表示之。其在密碼學中扮演相當重要的角色，通常運用在明文鑑別(Authentication)或數位簽章(Digital Signature)方面。數位簽章的法定效力，將相等於一般的“手簽名”。使用數位簽章更需要單向雜湊函數的配合，才可防止各種可能的攻擊。目前較廣為運用的單向雜湊函數有二種：MD5[24]是目前普遍雜湊函數，而SHA-1[13]是由美國政府 1993 年公佈的。

簡而言之，單向雜湊函數具有下列特性：

1. 單向性（One-way）：對任意長度的明文 M，經過 h()計算後，可以很容易計算出固定長度的雜湊值 h(M)。相反的，藉由所給定的 h(M)逆推出明文 M，此在計算上是不可行的。
2. 抗碰撞性（Collision-free）：對任意一對不同的明文M_1與M_2，產生相同的雜湊值，即$h(M_1)=h(M_2)$，此在計算上不可行的。

第4章　高安全性之 3G 認證機制

Zhang及Fang學者提出的認證機制AP-AKA 只考慮到行動基地台MS 和HLR/HN之間安全，並無考慮到MS 和VLR/SN之間安全及VLR/SN和HLR/HN之間的安全，使用對稱加密系統，整個過程只需要一把秘密金匙，這種方法應用在行動通信認證協定時只要入侵者有心就可盜取或推算出金鑰[42]。

所以本論文使用非對稱式金鑰的方式來補足 Zhang 及 Fang 的機制不足，藉以預防竊聽攻擊、中間人攻擊、反射攻擊、假冒攻擊及平行會議攻擊等。

4.1. 機制介紹

針對本機制所使用到之相關符號如**表 4-1**所示：

表 4-1 高安全性之 3G認證機制符號表

符號	說明
HLR	Home Location Register
VLR	Visitor Location Register
MS	Mobile Station
SN	Serving Network
HN	Home Network
F,H	驗證訊息的演算法
G	計算金鑰的演算法
K	對稱式的金鑰存放在 USIM 及 HLR
K_{MU}	Public Key between MS and HN
K_{VU}	Public Key between SN and HN

4.1.1. 到無認證向量他網中漫遊失敗機制的改善

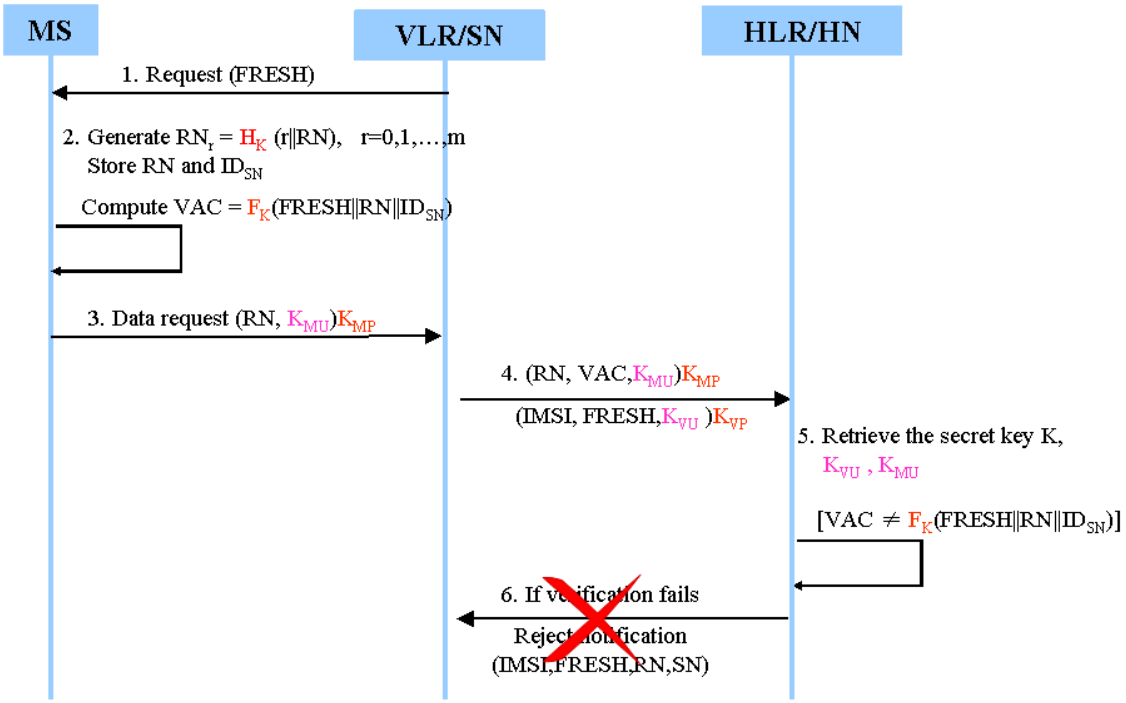

圖 4-1. 在無認證向量他網中漫遊失敗機制的改善

1. SN→MS：當 VLR 發現有新的使用者時，會送出使用者資料請求。
2. MS→SN：行動基地台回應一個亂數RN、行動用戶的公開金鑰K_{MU}及認證碼VAC給VLR。使用行動用戶的私密金鑰K_{MP}將訊息加密之後到客籍註冊資料庫VLR，作為身份認證資料。
3. SN→HN：接到訊息之後VLR會用私鑰K_{VP}將國際行動用戶識別碼IMSI (International Mobile Equipment Identity)、FRESH代表第一次拜訪VLR、亂數RN、公鑰K_{VU}(SN和HN之間公鑰)加密後送給HN。
4. HN：HN從認證請求資料中取出MS及SN之間的公鑰K_{MU}、SN及HN之間的公鑰K_VU、秘密金鑰K。
5. HN： 驗證認證碼 VAC 的正確性。
6. HN→SN：若失敗則reject國際行動用戶識別碼IMSI (International Mobile Equipment Identity)、FRESH代表第一次拜訪到新的SN、亂數

RN、認證碼VAC及斷掉連線。

4.1.2. 成功漫遊到無認證向量他網機制的改善

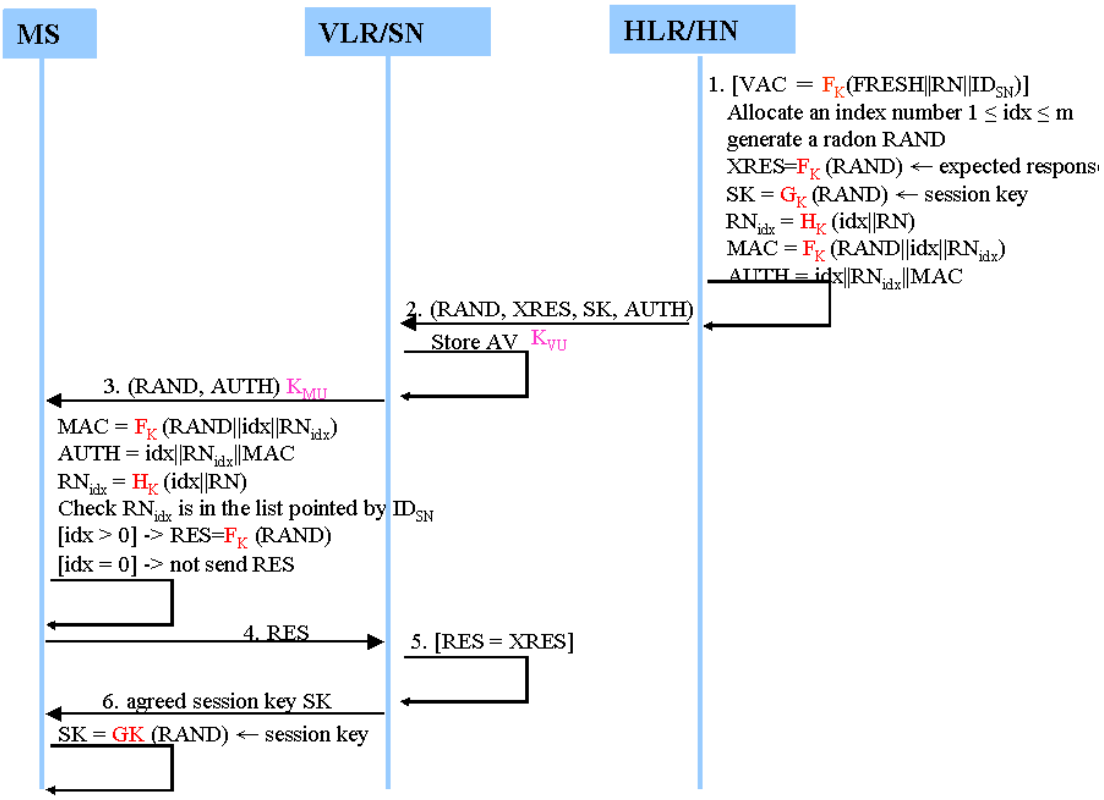

圖 4-2. 成功漫遊到無認證向量他網機制的改善

1. HN：若成功Home network，分配認證向量的索引及產生亂數RAND，計算預期的回應XRES，會議金鑰SK及兩個認證碼(RN_{idx},MAC)組合Authentication Token(AUTH)。
2. HN→SN：使用公鑰K_{VU}將認證向量(RAND亂數、XRES、SK、AUTH)加密後傳送給VLR。
3. SN→MS：VLR會從認證向量中取出RAND及AUTH，再用公鑰K_{MU}將RAND及AUTHK加密後送給MS。
4. MS→SN：MS 先檢驗 AUTN 是否正確，若正確，則根據 RAND 算出 RES。將 RES 回傳給 VLR。
5. SN：VLR 會檢查 RES 及 XRES 是否相等，若失敗則 VLR 結束連

線。

6. SN：成功則可用 SK 會議金鑰來加密。

4.2. 相關分析

4.2.1. 安全性分析

以下就本篇論文所提的機制在防止竊聽攻擊、假冒攻擊、反射攻擊及平行會議攻擊等方面逐一討論。

竊聽攻擊

行動用戶利用私密金鑰K_{MP}將訊息加密後再傳給VLR，VLR接到訊息之後利用私鑰K_{VP}將IMSI、FRESH(代表第一次拜訪VLR)、亂數RN及公鑰K_{VU}(SN和HN之間公鑰) 加密後送給HN。在此機制下，惡意者將無法從中竊聽到想關的訊息。

假冒攻擊

基於公開金鑰加密的安全，要從(RN, VAC, K_{MU}) K_{MP} 及 (IMSI, FRESH, K_{VU}) K_{VP}訊息中取得相關資料來假冒為合法的使用者是非常困難。

反射攻擊

為了防止假冒HN的反射攻擊，在傳送訊息(RAND, XRES, SK, AUTH)之前使用公鑰K_{VU}先加密。

平行會議攻擊

本論文的機制採用非對稱金鑰的方式加密，所以可以防止了平行會議攻擊。

4.2.2. 功能分析

以下係本研究機制與Zhang及Fang學者的機制功能分析整理。下列**表 4-2**分析中可看得出本研究的認證協定補強了Zhang及Fang學者的機制；VLR 和 HLR之間的相互認證、MS 和 VLR之間的相互認證、預防了竊聽攻擊、防止中間人攻擊、預防反射攻擊及平行會議攻擊。

表 4-2 高安全性之 3G認證機制功能分析表(本研究整理)

功能	Zhang 及 Fang 的機制[30]	本機制
MS 及 HLR 相互認證	V	V
使用者資料流的機密	V	V
資料的完整性	V	V
VLR 及 HLR 之間的相互認證	X	V
MS 及 VLR 之間的相互認證	X	V
預防竊聽攻擊	X	V
中間人攻擊	X	V
反射攻擊	X	V
平行的會議攻擊	X	V
符號說明：V-達成，X-未達成		

4.2.3. 時間複雜度分析

以下本研究機制與Zhang及Fang學者的機制的效能分析，相關的比較結果整理於**表 4-3**。

表 4-3.高安全性之的 3G認證機制時間複雜度分析表(本研究整理)

機制 項目	Zhang 及 Fang 的機制[30]	本機制
在無認證向量他網中漫遊失敗	$T_H + 2T_{SYN}$	$T_H + 2T_{SYN} + 4T_{ASY}$
成功漫遊到無認證向量的他網	$9T_{SYN}$	$9T_{SYN} + 4T_{ASY}$
漫遊到已經有認證向量的他網	$4T_{SYN}$	$4T_{SYN}$
在無認證向量家網中執行失敗	$T_H + 2T_{SYN}$	$T_H + 2T_{SYN}$
在無認證向量的家網路中成功執行	$9T_{SYN}$	$9T_{SYN}$
在已經有認證向量的家網路中執行	$4T_{SYN}$	$4T_{SYN}$
備註	T_{SYN}：執行一次對稱式金鑰加解密所需時間 T_{ASY}：執行一次非對稱式金鑰加解密所需時間 T_H：執行一次單向赫序函數所需時間	

上列**表 4-3**分析中可看得出本研究機制在無認證向量他網中漫遊失敗階段及成功漫遊到無認證向量的他網階段，可發現本研究所提機制之運算成本皆高於Zhang 及 Fang 的機制[25]。此部分主要是因為Zhang 及 Fang 的機制並無考慮到MS和VLR/SN之間的安全及VLR/SN和HLR/HN之間的安全。因此在不相等的安全條件下，本研究提供的安全度高於Zhang 及 Fang 的機制，所以本研究認為此增加的運算成本是值得的。

4.3. 小結

本機制補強了 Zhang 及 Fang 學者提出的認證機制 AP-AKA 的不足，可預防了防竊聽攻擊、中間人攻擊、假冒攻擊及平行會議攻擊等。

第5章　有效跨網域之間的 3G 認證機制

5.1. 機制介紹

為了改善在行動通訊網路中移動用戶與網路端之間的金鑰管理，橢圓曲線密碼系統(ECC)近年來已被廣泛地制訂於國際標準如 ISO 11770-3[18]、ANSI X9.62[9]、IEEE P1363[17]、FIPS 186-2[22]等，與傳統RSA及DSA的相關技術在相同安全程度相比，橢圓曲線公開金鑰密碼系統的優點是所需系統參數與金鑰長度較少，且計算速度也較快。目前以模數為 1024 位元RSA與DSA之安全程度為基準，橢圓曲線密碼技術在質數場只需 160 位元便可達到相同安全性。這使得ECC非常適合在行動裝置的有限資源環境下使用。

本研究提出一個以橢圓曲線為基礎第三代行動通訊認證機制，符號如**表 5-1**所示，各階段說明描述於后。

表 5-1 有效跨網域之間的 3G認證機制符號表

符號	說明
HLR	Home Location Register
VLR	Visitor Location Register
MS	Mobile Station
l	Prime
E_l（a,b）	$y^2 \equiv (x^3 + ax + b) \bmod l$ ， and $(4a^3 + 27b^2) \bmod l \neq 0$ 。
G	限定點$G(x_G, y_G)$＝ ，其秩 （Order）為在E 上的一大質數。
Z_l	The finite fields of Z_l ,include the numbers from 0 to l – 1
S_{VLR}	Secret Key of VLR
P_{VLR}	Public Key of VLR
S_{HLR}	Secret Key of HLR

5.1.1. 系統初始化階段

系統初始化階段如**圖 5-1**所示，詳細步驟如下：

1. Let l be a prime or a power of two（$l > 2^{160}$），
   real number a,b $\in Z_l$ and
   $4a^3 + 27b^2 \pmod{l} \neq 0$

2. Define ECC $\varepsilon : y^2 = x^3 + ax + b \pmod{l}$
   Select G=(X_G,Y_G) where $n > 2^{160}$ and $n > 4\sqrt{l}$)
   $n \cdot G = O$

3. Select a secret key S_{HLR}={1,2,...,l-1}
   Public key $P_{HLR} = S_{HLR} \cdot G$

圖 5-1. 系統初始化階段

1. HLR產生系統的橢圓曲線公開參數，先選擇一個大質數 l（$l > 2^{160}$），與兩個整數元素 a、b ∈ Z_l（Z_l 表示小於l 的正整數所成之集合），a 和b 必需滿足 $4a^3 + 27b^2 \pmod{l} \neq 0$。
2. 訂定一橢圓曲線方程式ε：$y^2 = x^3 + ax + b \pmod{l}$ 挑選橢圓曲線上一點為基準點G=(X_G,Y_G)，令此點的秩（order）為質數n（滿足$n > 2^{160}$且$n > 4\sqrt{l}$），同時n · G= O ，其中 O 代表橢圓曲線上之無線遠點

(Point at infinity)，“·”則代表橢圓曲線上的點乘法運算簡稱ECPM (Elliptic Curve Point Multiplication)。

3. HLR選擇一個亂數S_{HLR} {1，2，…，l-1}做為其私鑰，並且計算出公鑰$P_{HLR}=S_{HLR}\cdot G$。

5.1.2. 註冊階段

註冊階段如圖 5-2及圖 5-3所示，詳細步驟如下：

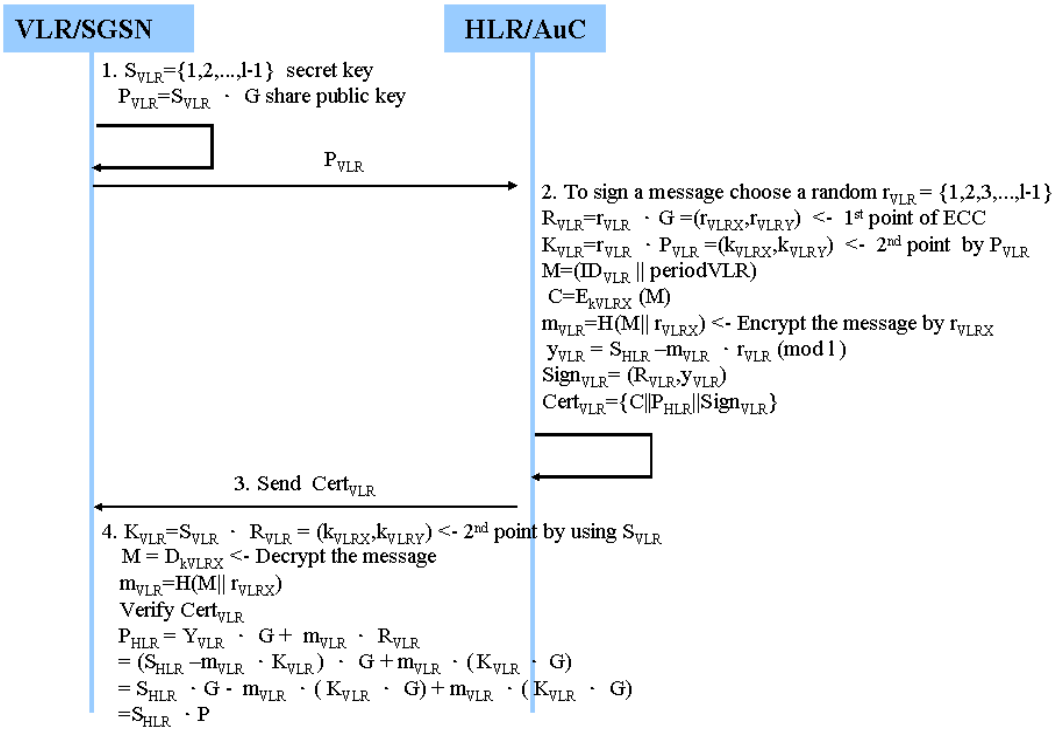

圖 5-2. VLR 註冊階段

1. VLR→HLR：並由參與成員 VLR 自行產生私鑰與公鑰對，向 HLR 申請憑證。

2. HLR：針對每次通訊HLR選取一亂數r_{VLR}為簽章所用，計算橢圓曲線上之點$R_{VLR}=r_{VLR}\cdot G=(r_{VLRX},r_{VLRY})$，利用VLR的公開金鑰$P_{VLR}$計算橢圓曲線上的第二點$K_{VLR}=r_{VLR}\cdot P_{VLR}=(k_{VLRX},k_{VLRY})$，使用$k_{VLRX}$加密訊息M(包含了VLR的ID 及有效期限)，HLR採用其私鑰

S_{HLR}在橢圓曲線上的第一點R_{VLR}對憑證作簽章$Y_{VLR} = S_{HLR} - m_{VLR} \cdot r_{VLR} \pmod{l}$，及產生憑證$Cert_{VLR}$。

3. HLR→VLR：HLR 頒發 VLR 的憑證 (密文 C、HLR 的公開金鑰及簽章)。

4. VLR：以VLR的私鑰計算橢圓曲線上之點$K_{VLR}=S_{VLR} \cdot R_{VLR} = (k_{VLRX}, k_{VLRY})$，利用$k_{VLRX}$將密文C解密得到明文M，用單向雜湊函數計算$m_{VLR}=H(M \| r_{VLRX})$，再驗證$P_{HLR} = Y_{VLR} \cdot G + m_{VLR} \cdot R_{VLR}$是否成立就可以確定簽章是否有效。任何人想偽造HLR的簽章，就涉及到求解橢圓曲線上的離散對數的問題。

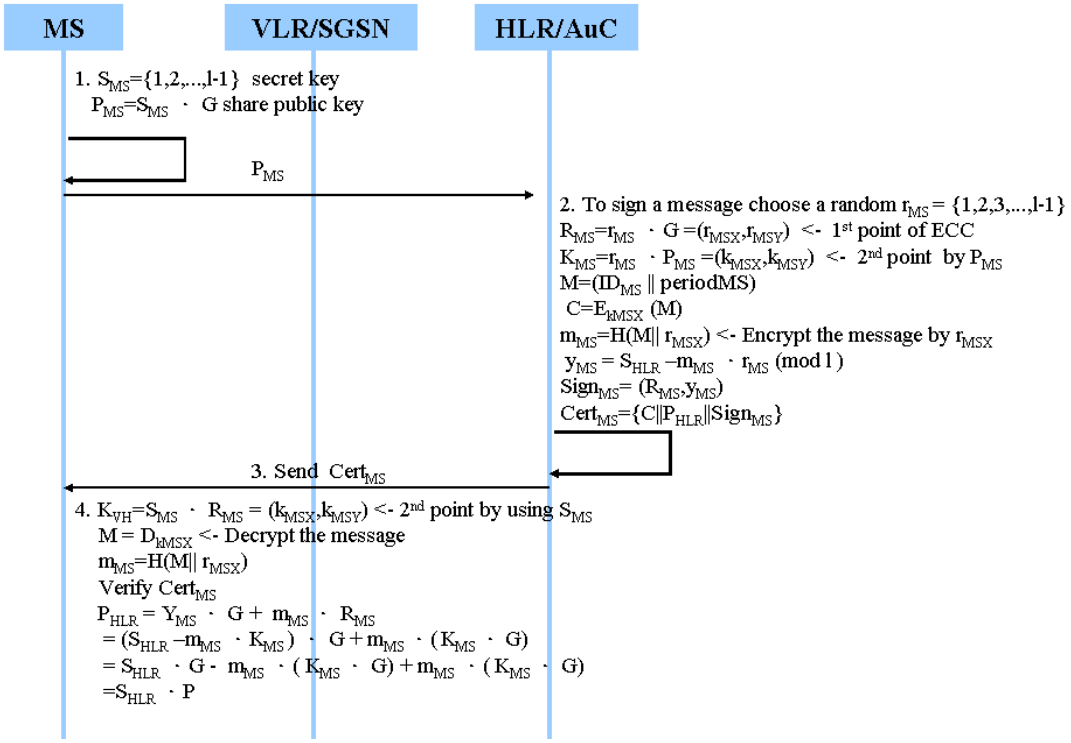

圖 5-3. MS註冊階段

1. MS→HLR：並由參與成員 MS 自行產生私鑰與公鑰對，向 HLR 申請憑證。

2. HLR：針對每次通訊HLR選取一亂數r_{MS}為簽章所用，計算橢圓曲線

上之點$R_{MS}=r_{MS}$ ‧G =(r_{MSX},r_{MSY})，利用使用者的公開金鑰P_{MS}計算橢圓曲線上的第二點$K_{MS}=r_{MS}$ ‧$P_{MS}=(k_{MSX},k_{MSY})$ ，使用k_{MSX}加密訊息M(包含了MS的ID 及有效期限)，HLR產生簽章及憑證:採用其私鑰S_{HLR}在橢圓曲線上的第一點R_{MS}對憑證作簽章$Y_{MS} = S_{HLR} - m_{MS}$ ‧r_{MS} (mod l) 及產生憑證$Cert_{MS}$。

3. HLR→MS：HLR 頒發 MS 的憑證 (密文 C, HLR 的公開金鑰及簽章)。
4. MS：以MS的私鑰計算橢圓曲線上之點$K_{VH}=S_{MS}$ ‧ $R_{MS} = (k_{MSX}, k_{MSY})$，利用$k_{MSX}$將密文C解密得到明文M，用單向雜湊函數計算$m_{MS}=H(M|| r_{MSX})$，及驗證$P_{HLR} = Y_{MS}$ ‧ $G + m_{MS}$ ‧R_{MS}是否成立就可以確定簽章是否有效。任何人想偽造HLR的簽章，就涉及到求解橢圓曲線上的離散對數的問題。

5.1.3. MS 及 VLR 之間的認證及金鑰交換階段

MS及VLR之間的認證及金鑰交換階段如**圖 5-4**所示，詳細步驟如下：

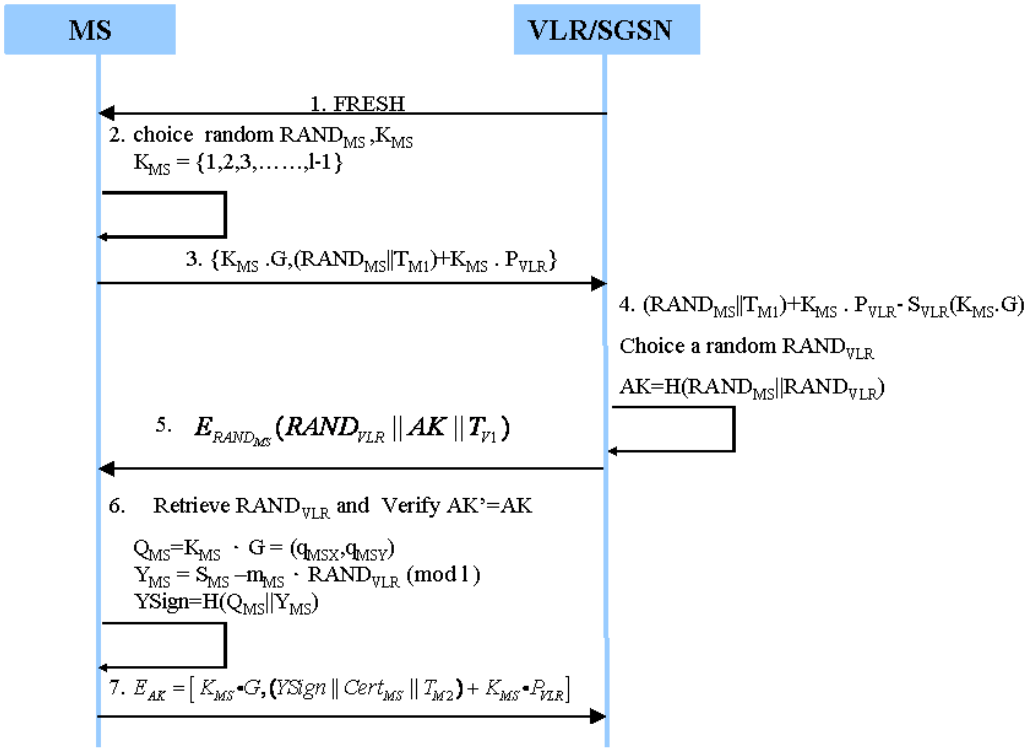

圖 5-4. MS 及VLR之間的認證及金鑰交換階段

1. VLR→MS：當行動使用者漫遊到新的 VLR 時，會送出使用者資料請求。
2. MS：行動基地台回應一個亂數$RAND_{MS}$(金鑰產的亂數) 及時戳T_{M1}(timestamp)。也選了一個亂數 K_{MS}(要用來做簽章用)並且計算了Q_{MS}。
3. MS→VLR：採用 ECC 橢圓曲線的方式加密之後送給 VLR。
4. VLR：VLR也會選出一個亂數$RAND_{VLR}$，會議金鑰AK是由兩個隨機數$RAND_{MS}$和$RAND_{VLR}$計算出來的。
5. VLR→MS：VLR 將會議金鑰AK用MS所選擇的隨機數$RAND_{MS}$加

密後傳送給MS，只有VLR 和MS知道$RAND_{MS}$，在傳送過程中很難被竊聽。

6. MS：在對VLR的身分進行驗證的時候，只要驗證AK'是否等於AK就可以判別VLR的身分是否合法，因為只有VLR才擁有其私鑰而解密出MS的訊息，合法得到正確的$RAND_{MS}$，計算出正確的會議密鑰AK。

7. MS→VLR：利用 AK 將行動使用者 MS 的憑證送給 VLR 做驗證。

5.1.4. 頒發行動使用者在同一個 Serving Network 的憑證階段

頒發行動使用者在同一個Serving Network 的憑證階段如圖 5-5所示，詳細步驟如下：

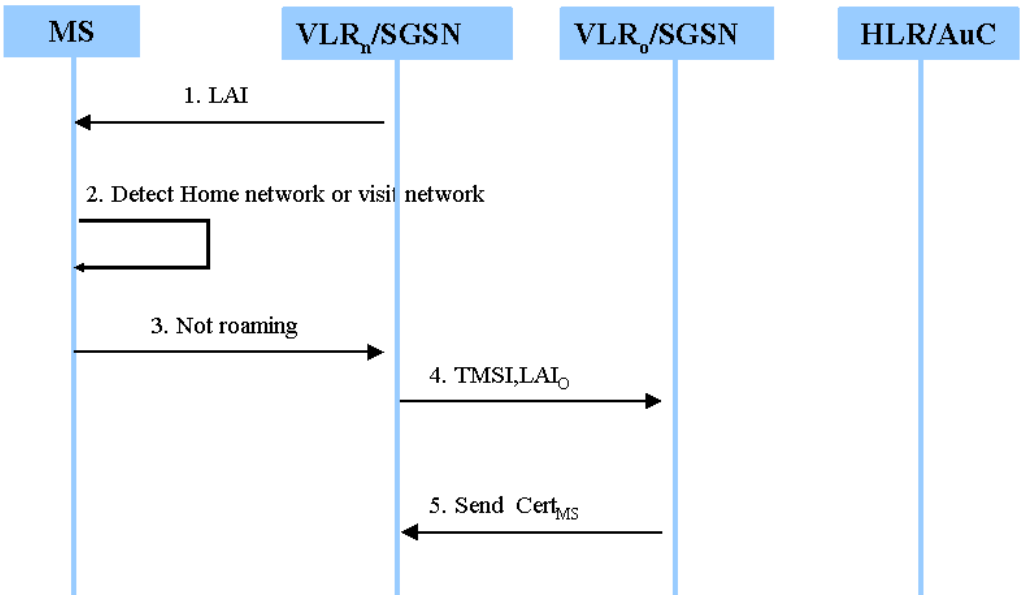

圖 5-5. 頒發行動使用者在同一個Serving Network的憑證階段

1. VLR 會送給基地台 LAI 位置區域識別碼給行動使用者。

2. 手機端檢查位置是在 HN 或是漫遊到別的網路。

3. 若沒有漫遊時，要求新的 VLR 向已拜訪過的 VLR 提出使用者認證憑證的請求。

4. 新的 VLR 會將使用者的 TMSI 及舊的 LAI 向已拜訪過的 VLR 請求使用者的認證憑證。

5. 新舊 VLR 之間的認證及金鑰交換的方法，會依照 MS 及 VLR 之間的方法產生會議金鑰，再將行動使用者的憑證傳送給新的 VLR。

5.1.5. 頒發行動使用者在漫遊時的憑證階段

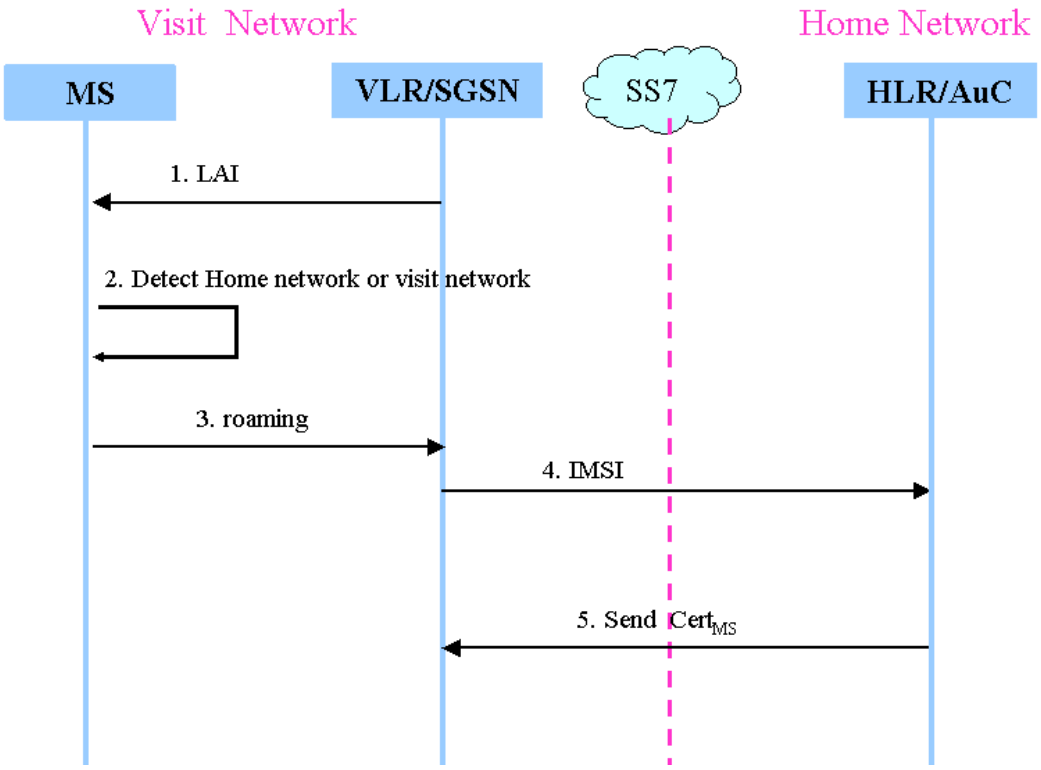

圖 5-6. 頒發行動使用者在漫遊時的憑證階段

1. VLR 會送給基地台 LAI 位置區域識別碼給行動使用者。

2. 手機端檢查位置是在 HN 或是漫遊到別的網路。

3. 若漫遊時，VLR 會將使用者的 IMSI 送給 HLR。

4. 向 HLR 提出使用者的憑證請求

5. HLR會找出使用者的憑證。

5.2. 相關分析

5.2.1. 安全性分析

本篇論文所提的機制可防止竊聽攻擊、中間人攻擊、重送攻擊、內部攻擊、主動攻擊及偽造簽章，同時也具備了不可否認性。

竊聽攻擊

在身份認證過程中，MS所採用了是橢圓曲線加密演算法來加密訊息，任何人想進行竊聽攻擊都面臨著求解橢圓曲線上的離散對數問題。傳輸過程中的會議金鑰AK是使用兩個隨機數$RAND_{MS}$和$RAND_{VLR}$計算出來。而隨機亂數$RAND_{MS}$和$RAND_{VLR}$只有VLR和MS知道，故整個過程都有效地防止竊聽攻擊。

中間人攻擊

MS對VLR的身分進行驗證的時候，只要驗證AK'是否等於AK就可以判別VLR的身分是否合法，因為只有VLR才擁有其私鑰而解密出MS的訊息，合法得到正確的$RAND_{MS}$，計算出正確的會議密鑰AK。MS對VLR做身份驗證來避免了中間人攻擊。

重送攻擊

每次認證過程所傳送的訊息同時，採用了時戳技術，有效防止重送攻擊。

內部攻擊

在認證過程中 MS 始終沒有暴露自己的真實身分，保證了用戶的匿名性，攻擊者無法發起內部攻擊。

主動攻擊

MS 對 VLR 及 HLR 的身分認証，所以可防止主動攻擊。

偽造簽章

MS的簽章是單向簽章，其安全性比較高，再加上只有VLR才知道其私密金鑰S_{VLR}，簽章只能由VLR驗證。其他任何人必須要先知道$RAND_{VLR}$後才能偽造簽章，但是要知道$RAND_{VLR}$是屬於橢圓曲線離散對數問題，很難竊聽得到。如果先知道$RAND_{VLR}$再來計算$Q_{MS}=K_{MS}\cdot G$，則由於Q'點和Q點矛盾無法使方程式$P_{MS}= Q_{MS}\cdot RAND_{VLR} + Y_{sign}\cdot G$成立。如果VLR 想要偽造簽章，由於其不知道Q點和亂數K_{MS}，它要由$K_{MS}\cdot G$計算Q_{MS}也是橢圓曲線離散對數問題，無法偽造簽章。

不可否認性

傳送憑證時使用簽章，所以具備有不可否認性。

5.2.2. 功能分析

以下係本研究機制與UMTS機制、黃明祥及鍾松剛學者的機制的功能分析整理。下列**表 5-2**分析中可看得出本研究的認證協定不但符合目前UMTS需求規格[3][6]；MS 及 HLR相互認證、使用者資料流的機密、在同一個 Serving network 的認證不必到HLR作認證及降低VLR和HLR之間的消耗頻寬。也可改善了UMTS在認證過程中安全上之不足；可預防了竊聽攻擊、中間人攻擊、重送攻擊、內部攻擊、主動攻擊和偽造簽章。VLR 和 HLR之間的相互認證及不可否認性，同時減少跨網路之間的資訊流及每一次的認證不必向HLR/AuC請求認證。

表 5-2. 有效跨網域之間的 3G 認證機制功能分析表(本研究整理)

功能	UMTS-AKA[6]	黃明祥、鍾松剛學者的機制[40]	本機制
MS 及 HLR 相互認證	V	V	V
使用者資料流的機密	V	V	V
資料的完整性	V	V	V
在同一個 Serving network 的認證不必到 HLR 作認證	V	V	V
降低 VLR 及 HLR 之間的消耗頻寬	V	V	V
預防竊聽攻擊	X	V	V
防止中間人攻擊	X	V	V
防止重送攻擊	X	V	V
防止內部攻擊	X	V	V
防止主動攻擊	X	V	V
防止偽造簽章	X	X	V
不可否認性	X	X	V
VLR 及 HLR 之間的相互認證	X	V	V
跨越網路之間的資訊流	6	6	2
call setup HLR 的次數	每次跨網域	每次跨網域	首次跨網域
符號說明：V-達成，X-未達成			

5.2.3. 時間複雜度分析

以下本研究機制與UMTS機制、黃明祥及鍾松剛學者的機制的效能分析整理。下列**表 5-3**分析中可看得出本研究機制在頒發行動使用者在同一個網路的憑證階段及漫遊階段所需要運算時間大幅減少。

表 5-3. 有效跨網域之間的 3G 認證機制時間複雜度分析表(本研究整理)

機制 / 項目	UMTS-AKA[6]	黃明祥、鍾松剛學者的機制[40]	本機制
註冊階段	-	-	$1T_{SGNECC} + 2T_H$
認證及金鑰頒發階段	$3T_{XOR}+10T_{SYN}$	$5T_{RSA}+3T_E+1T_H$	$1T_{SGNECC} + 3T_{ASYECC} + 2T_{ASY} + 1T_H$
頒發行動使用者在同一個網路的憑證階段	$3T_{XOR}+10T_{SYN}$	$5T_{RSA}+3T_E+1T_H$	$1T_{SGNECC}$
漫遊階段	$3T_{XOR}+10T_{SYN}$	$5T_{RSA}+3T_E+1T_H$	$1T_{SGNECC}$
備註	T_{XOR}：執行一次XOR所需時間 T_{SYN}：執行一次對稱式金鑰加解密所需時間 T_{RSA}：執行一次RSA所需時間 T_{ASYECC}：執行一次橢圓曲線乘法運算所需時間 T_{SGNECC}：執行一次橢圓曲線簽密所需時間 T_{ASY}：執行一次非對稱式金鑰加解密所需時間 T_H：執行一次單向雜湊函數所需時間 T_E：執行一次模數指數運算所需時間		

5.3. 小結

本機制除了低計算量與傳輸量，以及提供訊息傳遞時的資料安全與身份鑑別的雙重功能外，也降低VLR及HLR之間的頻寬消耗量。本機制方便在同一個網域時MS不需到HLR認證，只要向前所拜訪的VLR請求使用者的認證憑證即可。此種方式大量減少VLR 與HLR之間的訊息量。也方便使用者跨網路時，不需要重覆回到家網路的HLR請求認證。

第6章　結論與未來研究方向

資訊科技 (Information Technology, IT) 的演進即將改變的不只商業行為，還包括了人們的生活方式。行動化 (Mobile) 、無線化 (Wireless) 與個人化 (Personal) 將促使行動通訊在未來展現前所未有的重要性。隨著第三代行動通訊 (Third Generation Telecommunication, 3G) 網路的積極佈建與各項應用服務的陸續推出，3G 已被視為未來的明星產業之一。

3G 開展了一個行動通訊的新世界，它將過去許多固定式的服務變成了行動式，在這樣的架構下，我們可以想像許多新的服務，例如網路電話 (Voice over IP, VoIP) 、多媒體視訊會議 (Video Conference) ，或是手機上的網路連線遊戲都有機會普及到使用者的生活中。因此我們可以說，3G 讓人們的生活更便利、品質更好、也更豐富，而不僅僅是提供了高速的資料傳輸而已。

未來，消費者能選購的 3G 產品將會非常多樣化。單純的 3G 手機（例如專門供使用者上網瀏覽或收發電子郵件的大螢幕手機）、聲控或網路遙控的無線通訊設備和一些整合性質的產品（例如車或各類家電結合的 3G 設備），都會紛紛出爐，未來的無線寬頻生活將是個充滿想像的世界，行動通訊多元化。

在行動通信網路中，行動基地台與固定網路之間的所有通信都是透過無線介面來傳輸的。由於無線介面是開放的，因此在通信過程中非常容易受到侵犯 -- 任何人只要有適當的連線到該設備就可以對其進行攻擊。一般來說，行動通訊網路存在的不安全因素主要有無線介面的不安全、網路端的不安全，以及行動端的不安全等。為了提供更穩定的通訊服務，行動通訊網路的安全問題越來越受到人們的注目。

為了提供資訊在無線傳輸過程中的安全性，本論文提出兩個應用於全球行動電信系統 (Universal Mobile Telecommunication System, UMTS) 的新認證

機制。

本論文提出的第一個機制是改良 Zhang 及 Fang 所提出的 AP-AKA (Adaptive protocol for Mobile Authentication and Key Agreement)的高安全性之 3G 認證機制。AP-AKA 的安全傳輸處理只考慮到行動基地台(Mobile Station, MS) 和 VLR/SN (Visit Location Register/Serving Network) 之間安全，而無考慮到 VLR/SN 及 HLR/HN (Home Location Register/Home Network) 之間的安全，所以本論文使用非對稱式金鑰的方式來補足 AP-AKA 的機制不足，藉以預防竊聽攻擊、中間人攻擊、反射攻擊、假冒攻擊及平行會議攻擊等。

本論文提出的第二個機制是有效跨網域之間的 3G 認證機制，本論文的方法將橢圓曲線簽密法應用於電信網路的憑證申請程序，同時採用適當的憑證分發管理，減少 VLR/SGSN 與 HLR/AuC 之間在 MS 憑證申請程序中的訊息交換。一般而言，當 MS 在 VLR/SN 向 HLR/AuC 申請憑證時，HLR/AuC 確認無誤後會把憑證分發給 MS，每次的認證都必須回到 HLR/AuC。本論文的機制將會把 HLR/AuC 頒發的憑證傳給 MS 目前拜訪的 VLR/SGSN。此種方式讓 MS 再需要認證時，不必向 HLR/AuC 請求，直接向擁有該憑證 VLR/SGSN 請求即可，無論在同一個 Serving Network 或者是不同的 Serving Network 的認證不必每次都回至 HLR 認證，降低 VLR 和 HLR 之間的消耗頻寬，及減少跨網路之間的資訊流。同時也可達到 MS 和 HLR 之間的相互認證、VLR 和 HLR 之間的相互認證、MS 和 VLR 之間的相互認證及使用者資料流的機密，也可改善了 UMTS 在認證過程中安全上之不足；預防竊聽攻擊、防止重送攻擊及不可否認性。

未來的電信網整合成一個 All IP 網路時，將會提供固定網路、無線網路及行動網路上所有服務，包括語音、多媒體、資料等各類服務。此種革命性的整合型 All-IP 網路不但可以降低建置成本、營運管理成本，使得跨網路的應用成為可能。欲達到整合型網路的理想國度，其中關鍵的問題之一即是安全問題。

本論文提出的機制不但可應用於目前的電信網路，改善了UMTS在認證過程中安全上之不足。對未來的All IP 網路支援一些多媒體的服務時，亦可藉由本研究機制及多媒體通訊服務的整合。對行動服務提供者，或是像公車、計程車、移動咖啡館、小攤販等行動消費者中所需要的行動認證，本論文的研究亦可提供相同的助益。

目前 3GPP 的蜂巢系統擁有的是當前最廣泛的覆蓋率、最普及的用戶群，以及完善的認證（Authentication）、授權（Authorization）和計費（Accounting）AAA 機制。但在地下室或極封閉的室內環境中，仍存在著許多死角，而這些領域正是 WLAN 定位的涵蓋範圍，WLAN 則具有建置容易、建置成本低、採用免費頻段，以及頻寬足以滿足室內多媒體應用需求的優勢，兩者整合的利基是存在的。如果將 WLAN 與 3G 整合起來，將會是一種更方便且吸引人的網路存取方式。當使用者高速移動時可使用 3G 的行動網路，當使用者慢速移動到某一特定地點時則可使用 WLAN。

在整合的形式上，可以分為寬鬆性的結合（loose coupling）與緊密性的結合（tight coupling）。寬鬆性結合的原則是保有兩大網路的既有屬性，讓 WLAN 仍專注提供 Internet/Intranet 接取，而 3GPP 的服務內容也不變；由於只針對 AAA 機制做整合，避免了不同網路間資料流量的混合流通，是較容易達成的方式。

若採用緊密性結合的架構，則是將WLAN視為與 3GPP互補的一項接取技術，並讓WLAN網路與 3GPP系統的核心網相連[43]，進而能充分利用該網路既有的行動、安全與服務品質等機制。

關於WLAN與 3GPP系統的整合，3GPP發表的 3GPP TR22.934（Feasibility Study on 3GPP System to Wireless Local Area Network Interworking）[1]文件中即已提出從簡單互連到完全無縫互連的系統間操作的六種情景（Scenario）模式：

1.公共計費和客戶服務

這是最簡單的互通方式。在這種方式下，僅對客戶關係上是統一的，用戶收到行動電信公司包含行動和 WLAN 服務的統一帳單，但兩個系統的安全機制可完全獨立。

2.基於 3GPP 系統的接取和計費

3GPP 系統和 WLAN 在安全上採用相同的機制，其中認證、授權和計帳由 3GPP 系統來提供，採用的是 SIM-based 的認證。不過，對 WLAN 用戶來說，服務內容上並沒有什麼不同。

3.將 3GPP PS 服務延伸到 WLAN

可從 WLAN 接取到 3GPP 系統封包交換式（PS）的服務，包括 IMS、定位服務（LBS）、即時訊息（IM）及 Presence Based Services。筆記型電腦的雙模網卡可透過 3GPP 或 WLAN 來接收 MMS。不過，在兩系統間的服務連續性支援仍未被要求建立。

4.服務連續性

基於 3GPP 系統的 PS 服務在兩系統間轉換時，仍然能保有服務的連續性。不過，用戶可能會察覺其中轉換過程的變化，這是因為兩系統的特性不同，在此階段仍未做到最佳化的溝通，而且某些服務在此架構下並無法提供。

5.無縫的服務

基於 3GPP 系統的 PS 服務能達成兩系統轉換上的無縫連結。無縫服務的連續性是指：在兩種無線接取技術之間，盡可能降低資料丟失和切換的延遲時間，在服務品質（QoS）上的差異性也要盡量縮小。舉例來說，在此情況下當用戶離開 WLAN 的涵蓋範圍時，仍能繼續多媒體及 VoIP 的應用，而且不會察覺有異。

6.對 3GPP 系統電路交換（CS）服務的接取

透過 WLAN 也能接取到 3GPP 電路交換核心網路。可以由以下技術方式實現：透過 WLAN 介面接取到 3GPP 電路交換核心網路中，在不同接取技術之間進行無縫和用戶透明的交換，以連接承載電路交換的服務。

WLAN傳輸所使用的頻率是未給予專用執照（Unlicenced）的，較容易受到干擾，加上在安全性的風險上，要比行動通訊要來得高，這也是個人無線網路必須要考慮的因素。然而現今整合WLAN 與 3G 仍然有一些認證、安全方面及服務品質的問題存在[14][20][21][25][27][31]，例如：認證協定的效率問題、使用者的匿名性問題及帳單的否認性問題。目前 3GPP和WLAN中使用EAP-SIM、EAP-AKA個人密碼為基礎的認證方式，提供使用者認證及收費機制。當HLR和WLAN距離遙遠時，會產生來回傳遞延遲(round-trip delay)。此外，收費機制必須具備有不可否認性，來確保使用者漫遊到不同系統之間的安全，如：3G家網路、3G的他網路及WLAN，EAP-AKA機制對保護使用者的私密性仍然有加強的空間。未來可針對整合WLAN與 3G/UMTS時使用之認證協定的安全服務品質與效率問題探討。

在未來釋出資訊後，上述的分析可能得作因應的修正。而隨著時代進步，新技術與新的服務種類的出現，也有可能危及 UMTS 的安全，屆時還須結合更快速安全的演算法，尋求安全的機制，建置於標準內。

參考文獻

英文部份（以字母順序排序）：

[1] 3GPP TR 22.934, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6). V6.2.0. 2003-09

[2] 3GPP TR 33.801, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access Security (Release 7). V0.2.0. 2005-07

[3] 3GPP TR 33.900, 3rd Generation Partnership Project; Technical Specification Group SA WG3; A Guide to 3rd Generation Security (Version 1.2.0). V1.2.0. 2000-01

[4] 3GPP TR 33.909, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Report on the Design and Evaluation of the MILENAGE Algorithm Set. V.4.0.1. 2001-06

[5] 3GPP TS 23.002, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Architecture. V3.4.0. 2000-12

[6] 3GPP TS 33.102, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 6). V6.3.0. 2004-12

[7] 3GPP TS 35.202, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2; Kasumi algorithm specification.

[8] 3GPP TS 35.206, 3rd Generation Partnership Project; Technical Specification

Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions f1, f1*, f2, f3, f4, f5 and f5* .Document 2: Algorithm Specification

[9] ANSI X9.62, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 1999.

[10] Bannister Jeffrey, Mather Paul and Coope Sebastian, "Convergence Technologies for 3G Networks IP, UMTS, EGPRS and ATM", *Wiley Inter Science*, March 2004.

[11] Boman Krister, Horn Guenther, Howard Peter and Niemi Valtteri, "UMTS security", *Electronics & Communication Engineering Journal*, Vol. 14, No. 5, pp. 191-204, October 2002.

[12] Briceno Marc, Goldberg Ian, and Wagner David, "A Pedagogical Implementation of the GSM A5/1 and A5/2-voice Privacy Cryption Algorithms", http://cryptome.org/gsm-a512.htm (originally on www.scard.org), 1998.

[13] .Federal Information Processing Standards Publication (FIPS PUB) 180-1, "Secure Hash Standard", April 1995.

[14] Grecas Constantinos F., Maniatis Sotirios I. and Venieris Iakovos S., "Introduction of the Asymmetric Cryptography in GSM, GPRS, UMTS, and Its Public Key Infrastructure Integration," *Mobile Networks and Applications*, Vol. 8, No. 2, pp. 145-150, 2003.

[15] Harn Lei, and Hsin Wen-Jung, "On the security of wireless network access with enhancements", *Proceedings of the 2003 ACM Workshop on Wireless Security*, pp. 88-95, 2003.

[16] Huang Chung-Ming, and Li Jian-Wei, "Authentication and Key Agreement Protocol for UMTS with Low Bandwidth Consumption", *IEEE Proceedings of*

the 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers), pp. 392-397, March 2005

[17] IEEE P1363, "Standard Specifications for Public-Key Cryptography", Ballot draft, 1999.

[18] ISO/IEC 11770-3, "Information Technology-Security Techniques-Key Management-Part 3: Mechanisms Using Asymmetric Techniques", 1999.

[19] Johnson Don, Menezes Alfred and Vanston Scotte, "The Ellipic Curve Digital Signature Algorithm (ECDSA)", *International Journal of Information Security*, Vol. 1, No.1, Springer-Verlag, pp. 36-63, 2001.

[20] Kambourakis Georgios , Rouskas Angelos, Kormentzas George and Gritzalis Stefanos,"Advanced SSL/TLS-based authentication for secure WLAN-3G interworking", *Communications, IEE Proceedings*, Vol. 151, pp. 501-506, 2004.

[21] Lin Phone, Lin Yi-Bing, Feng Vincent, Lai Yen-Cheng, "GPRS-based WLAN authentication and auto-configuration", *Journal of Computer and Communications*, Vol. 27, Issue: 8, pp. 739-742, 2004.

[22] National Institute of Standards and Technology, "Digital Signuatre Standard", *FIPS Publication 186-2*, February 2000.

[23] NMS communication 3G Tutorial www.nmscommunications.com/3Gtutorial

[24] Rivest Ronald, "The MD5 Message Digest Algorithm", *RFC 1321*, 1992.

[25] Shi Minghui, Shen Xuemin, and Mark Jon W., "IEEE802.11 Roaming and Authentication in Wireless LAN/Cellular Mobile Networks", *IEEE Wireless Communications*, Vol, 11, Issue: 4, pp. 66-75, 2004.

[26] Stallings William, "Cryptography and Network Security: Principles and Practice, 3rd Edition", *Prentice Hall Media type*, August 2002.

[27] Tseng Yuh-Min, Yang Chou-Chen and Su Jiann-Haur, "An Efficient

Authentication Protocol for Integrating WLAN and Cellular Networks," *Advanced Communication Technology, The 6th International Conference on*, pp. 416-420, 2004.

[28] Wong Duncan S., "Security Analysis of Two Anonymous Authentication Protocols for Distributed Wireless Networks", *IEEE Proceedings of the 3rd International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05)*, pp. 284-288, March 2005.

[29] Zhang Fangguo, Mu Yi, and Susilo Willy, "Reducing Security Overhead for Mobile Networks", *IEEE Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers)*, pp. 398-403, March 2005.

[30] Zhang Muxiang, and Fang Yuguang, "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol", *IEEE Transaction on Wireless Communication*, Vol. 4, No. 2, pp. 734-742, March 2005.

[31] Zhao Yao, Lin Chuang, Yin Hao, "Security Authentication of 3G-WLAN Interworking", *IEEE proceeding of the 20th International Conference on Advanced Information Networking and Applications* , Vol. 2 (AINA'06), pp. 429-436, 2006.

中文部份（以筆劃排序）

[32] 立川敬、張志文、陳名吉，『W-CDMA 行動通訊系統』，全華科技圖書股份有限公司，民國 92 年 11 月。

[33] 林一平，『行動電話及數據網路管理』，維科圖書有限公司，第九章，民國 88 年 8 月。

[34] 林文儀，『橢圓曲線版的 ElGamal 數位簽署及其變形』，東海大學應用數學研究所碩士學位論文，民國 92 年。

[35] 林祝興、黃國榮，『植基於橢圓曲線密碼學之具有身分驗證金鑰交換協定研究』，東海大學資訊科學與工程研究所碩士學位元論文，民國 92 年 6 月。

[36] 周宏霖，『WCDMA/UMTS 第三代無線通訊系統-核心網路架構介紹』，工研院電通所無線通訊技術組。http://www.lee-1.com/hlchou

[37] 張英彬，『第三代行動通訊系統 W-CDMA For UTMS』，儒林圖書公司，民國 94 年 4 月。

[38] 陳聖詠，『傳輸網路與行動通訊』，全華科技圖書股份有限公司，民國 93 年 5 月。

[39] 黃仁俊、賴峙樺，『以橢圓曲線為基礎之簽密法的研究』淡江大學資訊工程學系-碩士論文，民國 92 年 6 月。

[40] 黃明祥、鍾松剛，『全球移動式網路之安全性研究』朝陽科技大學網路與通訊研究所-碩士論文，民國 94 年 5 月。

[41] 黃景張，『資訊安全—電子商務之基礎』，華泰文化事業股份有限公司，第四章，民國 90 年 6 月。

[42] 塗世雄、李世傑，『第三代行動通訊金鑰更新認證協定之研究』，中原大學電機工程學系-碩士論文，民國 92 年 1 月。

[43] 楊朝成、楊雅雯，『無線網路與 3G/UMTS 整合環境之認證協定研究』，朝陽科技大學網路與通訊所-碩士論文，民國 94 年 5 月。

[44] 賴溪松、韓亮、張真誠，『近代密碼學及其應用』，旗標出版股份有限公司，民國 93 年。