Communications of the CCISA
Vol. 29 No. 2 May 2023

使用 BBS 簽章實現基地台身份驗證

孫沛靖[1*]、吳介騫[2]
[1]安華聯網科技股份有限公司、[2]國立高雄科技大學電腦與通訊工程所
[1]nate.sun@onwardsecurity.com、[2]jcwu@nkust.edu.tw

摘要

在行動通訊系統的演進當中，在安全性方面持續地得到增強。從 2G 環境中的單向身份驗證，到 3G 以及之後世代的雙向身份驗證，但還是有許多安全性問題沒有得到妥善解決，例如透過惡意基地台配合相應攻擊方式。為了減緩惡意基地台造成的安全性風險，本論文使用由 D. Boneh、X. Boyen 和 H. Shacham 所提出之 BBS 簽章實現基地台身份驗證方案，透過更改協定中基地台廣播的 SIB 內容，在其中附加 BBS 簽名使 UE 連接至基地台之前即可對基地台進行身份驗證，以此減緩惡意基地台所帶來的相關安全性風險。本文提出了兩種 BBS 簽章方案，並展示其實現方式及實驗結果。

關鍵詞：行動通訊系統、惡意基地台、數位簽章

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 29 No. 2 May 2023

Implementation of Base Station Identity Authentication using BBS Signatures

Pei-Jing Sun[1*], Jieh-Chian Wu[2]
[1] Onward Security Corporation, [2] National Kaohsiung University of Science and Technology, Kaohsing City,Taiwan R.O.C.
[1]nate.sun@onwardsecurity.com, [2]jcwu@nkust.edu.tw

Abstract

In the evolution of mobile communication systems, security is keeping enhancement. The security evolution involves the process of one-way authentication used in the second generation (2G) systems, and two-way authentication used in the third generation (3G) systems and beyond. However, there are still many security issues that have not been properly resolved, which might result from the attacks by rough base stations. To mitigate such attacks, this thesis proposes using the BBS signature, which is introduced by D. Boneh, X. Boyen and H. Shacham, in the base station identity authentication procedure. By changing the base station broadcast message SIB, in which the BBS signature is added, the User Equipment can perform authentication process before attaching to the base station, thereby mitigating the security issues resulted from rogue base stations. There are two BBS signature schemes proposed in this thesis and their implementation as well as experiment results are also demonstrated.

Keywords: Mobile Communication Systems、Rogue Base Station、Digital Signature

壹、前言

隨著行動通訊的演進，除了提供更多元的服務以及更好的通訊品質，在安全性方面也不斷的進行優化，但還是有許多問題是目前現行的第四代以及第五代行動通訊中並未妥善得到緩解的，其中包含了 IMSI 捕捉以及發送惡意災防訊息等，在接下來的小節中我們將會對行動通訊演進中各世代對安全性方面的改動進行探討，並且提出本論文所要解決的環境以及問題。

1.1 行動通訊各世代中存在的安全性問題

根據文獻[22,27]的研究指出在第二代行動通訊的 Global System for Mobile Communications (GSM) 系統中由於其單向身份驗證的特性，在 GSM 當中只有網路向用戶進行身份驗證，而用戶卻不對網路進行身份驗證，導致攻擊者可以透過架設惡意基地台 (Rogue Base Station) 實施中間人攻擊 (Man in the Middle，簡稱 MitM)，透過中間人攻擊可造成通話挾持，並且文獻[22]還指出了基於第二代行動通訊的所制定標準的協定弱點：當惡意基地台透過發送終端能力訊息 (Terminal Capability Messages) 聲明該惡意基地台不支援加密協定時，可以強制 UE 不將與惡意基地台相關的通訊進行加密，並且透過向 UE 發送 Identity Request 可取得用戶 UE 的明文國際移動用戶辨識碼 (International Mobile Subscriber Identity，簡稱 IMSI) 。

文獻[20]的研究則指出：在第三代行動通訊的 Universal Mobile Telecommunications System (UMTS) 中，提出的第三代合作夥伴計畫 (3rd Generation Partnership Project，簡稱 3GPP) 的身份驗證和密鑰協議 (3GPP Authentication and Key Agreement，簡稱 3GPP-AKA) 協定是用於解決 GSM 的安全性弱點，但是該協定容易受到惡意基地台攻擊的變體影響，例如 3GPP-AKA 的缺陷允許攻擊者將用戶流量從一個網路重新定向到另一個網路，當重新定向到惡意基地台上時，攻擊者可擷取用戶流量並且執行中間人攻擊。文獻[13]的研究也指明：由於信令 rrcConnectionRequest 當中包含明文國際移動用戶辨識碼 (IMSI)，因此當 UE 連接到惡意基地台後會造成國際移動用戶辨識碼的洩漏，並且在該研究中也展示：如何透過惡意基地台對用戶造成阻斷服務式 (Denial of Service，簡稱 DoS) 攻擊，文獻[17, 21]則展示了中間人攻擊實際是如何達成的。

文獻[7, 15, 16, 29]的研究則分別指出：在第四代行動通訊系統 (Long Term Evolution，簡稱 LTE) 環境中實際存在的各種安全性風險。以下引述自文獻[29]的內容摘要：「在 IMSI 捕捉器和第二代行動通訊中間人攻擊的幫助下，實現一個針對 LTE 手機實用且有效電話號碼捕捉器原型。當設備駐紮在我們的惡意基地台幾秒鐘，我們就擷取了 LTE 用戶的電話號碼」。文獻[16]則實際展示在 LTE 環境中，攻擊者是如何透過惡意基地台對用戶發送惡意災防訊息；在文獻[7]的研究中則證明了在 LTE 環境中可透過惡意基地台對用戶 IMSI 進行捕捉並且進行 DoS 攻擊。在第四代行動通訊 (LTE) 環境中雖然提出

了新的身份驗證和密鑰協議 (Evolved Packet System Authentication and Key Agreement，簡稱 EPS-AKA) 來保護用戶資料的安全，但是如文獻[7, 15, 16, 29]的研究所證明的有許多安全性風險是發生在 EPS-AKA 完成建立之前發生。

1.2 研究環境

本論文針對第四代行動通訊 (LTE) 環境進行研究，系統架構如圖 1 所示。其中，使用者裝置 (User Equipment，簡稱 UE) 與演進節點 B (evolved Node B，簡稱 eNB) 也就是第四代行動通訊基地台，透過空中介面 (Air Interface) 進行傳輸。

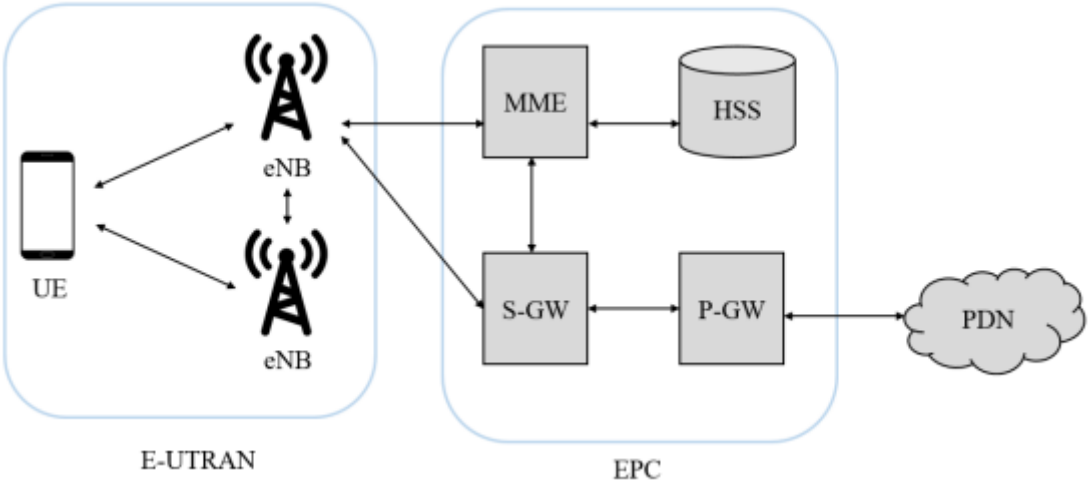

圖 1：第四代行動通訊系統架構

本論文中所指之惡意基地台為攻擊者自行架設之基地台，惡意基地台可能包含攻擊者架設之惡意核心網路，其場景如圖 2 所示，其中惡意基地台 (Rogue eNB) 以及惡意第四代行動通訊核心網路 (Rogue EPC) 為攻擊者自行架設，惡意基地台可能透過相較於合法基地台更高的傳輸功率誘使 UE 與其進行連接。

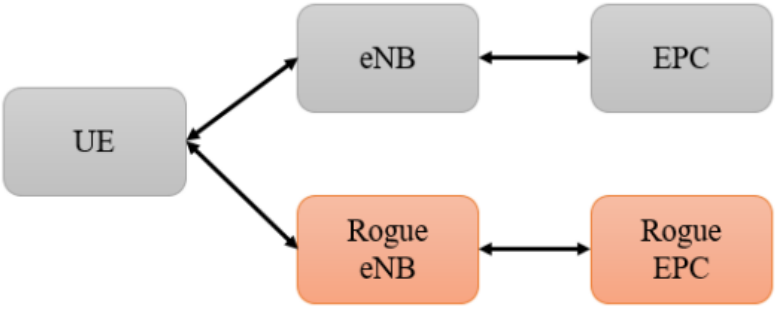

圖 2：第四代行動通訊惡意基地台攻擊場景

1.3 研究動機及目的

基於前兩節對行動通訊網路演進過程中存在的各種安全性風險探討，我們發現這些安全性風險要實際達成攻擊成效，必須透過惡意基地台配合後續攻擊手法才能實施，因此本論文計畫提出透過數位簽章之方式對基地台進行身份驗證，以此緩解惡意基地台的相關風險。

本論文首先將針對第四代行動通訊環境當中的各種攻擊手法進行研究，分析攻擊手法如何實行，再來探討惡意基地台辨識及防護之相關文獻，最後提出本論文如何對基地台進行身份驗證，也將透過架設模擬環境實現本論文所提出之基地台身份驗證方案。期望本論文之貢獻能夠減輕現行之第四代行動通訊，甚至是第五代行動通訊網路環境當中惡意基地台的相關風險。

貳、文獻探討

在本章節中將會對第四代行動通訊之相關安全性風險進行探討，探討實際達成手段以及安全性風險的觸發時間點，接著將會探討針對防範惡意基地台之相關文獻。

2.1 第四代行動通訊相關安全性風險文獻探討

在本小節中將會分別探討第四代行動通訊中的惡意攻擊手法，如國際移動用戶識別碼 (IMSI) 捕捉、阻斷服務式 (DoS) 攻擊、發送惡意災防訊息等等。

2.1.1 國際移動用戶識別碼 (IMSI) 捕捉

在 T. Fei 以及 W. Wang 的研究[7]中指明透過通用軟體無線電外圍設備 (Universal Software Radio Peripheral，簡稱 USRP) 架設惡意基地台，並將惡意基地台廣播之 System Information Block Type 5 (SIB5) 當中的 cellReselectionPriority 設為最高優先級 7，即可使得用戶 UE 因為小區選擇標準，連接上透過 USRP 架設的惡意基地台，當用戶 UE 於 EPS-AKA 中向惡意基地台發出 Attach Request 時，由於惡意基地台中並無記載用戶 UE 的臨時標識符 (SAE-Temporary Mobile Subscriber Identity，簡稱 S-TMSI)，因此會向用戶 UE 發出 Identity Request，用戶 UE 則將 IMSI 以明文方式包含在 Identity Response 當中傳送，如圖 3 所示。

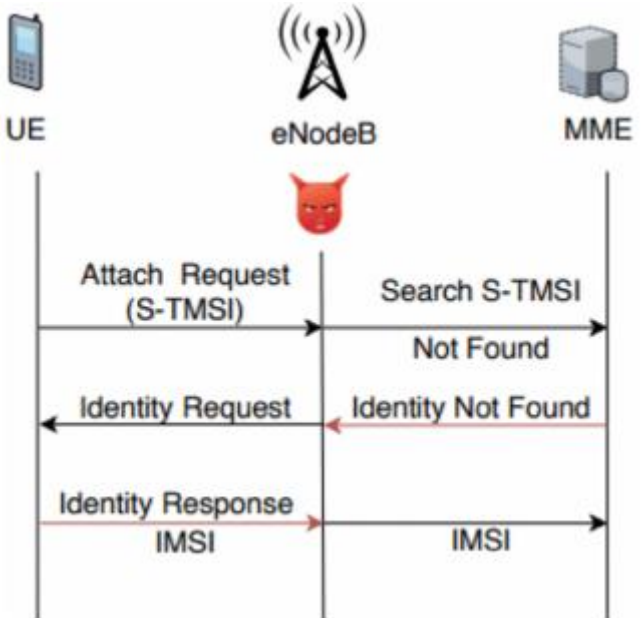

圖 3：IMSI 捕捉流程[7]

2.1.2 阻斷服務式 (DoS) 攻擊

在 T. Fei 以及 W. Wang 的研究[7]中也證明了當用戶 UE 連上惡意基地台後由於小區選擇標準的原因，當惡意基地台所廣播的 SIB 中下行頻率和合法基地台下行頻率設置相同時，由於 cellReselectionPriority 設為最高優先級 7，因此 UE 會駐留在惡意基地台中，只要惡意基地台存在，UE 將無法正常連接到合法網路中以此達成 DoS 的效果。

2.1.3 發送惡意災防訊息

在 2019 年的 HITB 安全會議 (Hack In The Box Security Conference) 上 W. Li [16]向大眾展示透過架設惡意基地台，在 LTE 的環境中發送惡意災防告警系統 (Public Warning System，簡稱 PWS) 訊息。其攻擊流程主要是透過惡意基地台廣播更改過之 SIB11 訊息，將 PWS 訊息透過細胞廣播服務 (Cell Broadcast Service，簡稱 CBS) 廣播至駐紮於惡意基地台的用戶 UE。

2.1.4 SIB 相關安全性風險分析

前三小節中的攻擊手法皆與 SIB 相關，在電信網路當中基地台會週期性廣播 Master Information Block (MIB) 和 SIB，MIB 當中包含的資訊主要是引導 UE 進行連接，例如 Broadcast Control CHannel (BCCH) 等等相關資訊，SIB 則是更為詳細的基地台資訊，如

小區重選設定值、PWS 訊息內容以及 Tracking Area Code (TAC) 等等資訊。在 M. Kim 等人的研究[15]中說明了各 SIB 可能面臨的各種安全性風險，如表 1 所示。

表 1：各 SIB 安全性風險

SIB1	可透過其中的 PLMN ID (Public Land Mobile Network) 和 TAC 追蹤 UE 在哪個國家哪個運營商的哪個基地台範圍內
SIB3	將所有參數與合法基地台設置相同且 cellReselectionPriority 設為 7 即可將 UE 導向至惡意基地台
SIB4	包含同頻 neighbor cell 和 black cell information，可使 UE 在不同惡意基地台中進行 Handover 或將合法基地台加入至黑名單中
SIB5	與 SIB3 相似，差異在於其包含兩個以上頻段和帶寬
SIB10/11	地震與海嘯預警系統 (Earthquake and Tsunami Warning System，簡稱 ETWS)，竄改及發佈惡意災防訊息內容

2.1.5 各安全性風險之觸發時間點

第四代行動通訊系統中惡意基地台連接流程及相關風險觸發時間點如圖 4 所示，首先 UE 透過同步序列 (Synchronization Sequence) 與基地台進行時間同步後，UE 解析基地台廣播之 MIB 以及 SIB 取得無線電資源的相關參數，文獻[16]中所提及附帶 PWS 訊息之 SIB10/11 也在此時進行解析，在解讀完 SIB 後 UE 將與基地台進行連線以及進行後續之 EPS-AKA，DoS 攻擊即是在 UE 連接上惡意基地台時達成的，[7]之 IMSI 捕捉流程則是在 EPS-AKA 中發生。

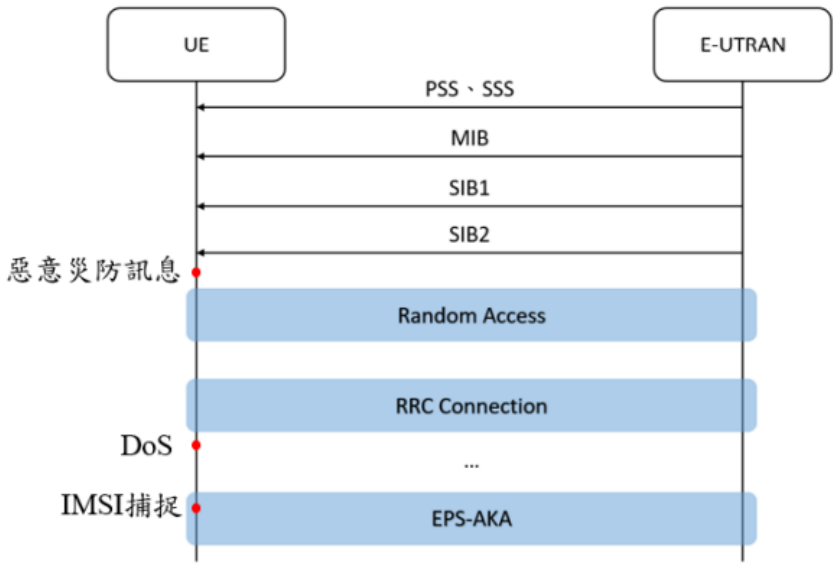

圖 4：惡意基地台連接流程及相關風險時間點

2.2 相關惡意基地台辨識及防護文獻探討

在本節將會針對惡意基地台辨識以及防護之相關文獻進行探討，並且本論文將這些相關防護文獻分為兩類：第一類為基於信號分析的相關文獻，第二類則是從身份驗證機制的角度進行辨識及防護。

2.2.1 基於信號分析的相關辨識及防護文獻

文獻[11]提出透過對平均接收同步信號強度 (Average Received Synchronization Signal Strength，簡稱 ARSSS) 進行分析以識別惡意基地台，該方案要求 UE 預先知道自己以及合法基地台的位置資訊，透過計算多路徑衰弱以及小尺寸衰弱等因素與實際接收之 ARSSS 進行比較，當 ARSSS 過大時則可能為惡意基地台發出之訊號。

而在文獻[2, 3]則是提出透過分析射頻指紋 (RF Fingerprinting) 的方案進行惡意基地台的辨識。

文獻[24]則是提出了透過測量報告 (Measurement Reports)，將接收到的訊號品質與已知的鄰近合法基地台訊號品質進行交叉比對以偵測是否為惡意基地台。

2.2.2 基於身份驗證機制的相關辨識及防護文獻

早在 2020 年 10 月份的 3GPP TR 33.809[28]中就已提出對系統訊息 (System Information，簡稱 SI) 進行數位簽章以此緩解惡意基地台所引發的相關風險，如圖 5 所示。

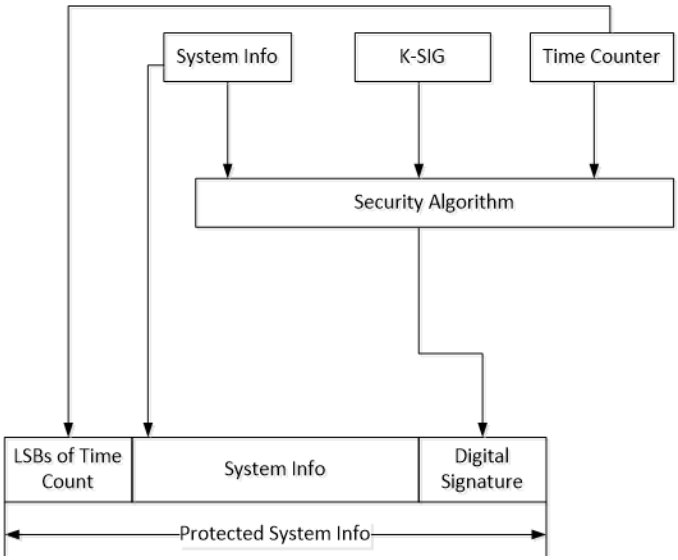

圖 5：使用數位簽章驗證系統訊息[28]

文獻[10]提出如圖 6 所示之架構對基地台進行身份驗證，並且基於其提出的架構比較三種數位簽章演算法 ECDSA[12]、BGLS[6]以及 SCRA-BGLS[30]。文獻[10]認為 SCRA-BGLS 為其方案之最優解，SCRA-BGLS 透過可預運算之特點相較其他兩種數位簽章演算法可使簽章生成延遲降低，該方案對 SIB1 的總額外負載為 181 Bytes，對 SIB2 額外負載為 39 Bytes，但該方案在 UE 端會有極長的驗證時間成本，其驗證平均時間成本為 119.19 ms。

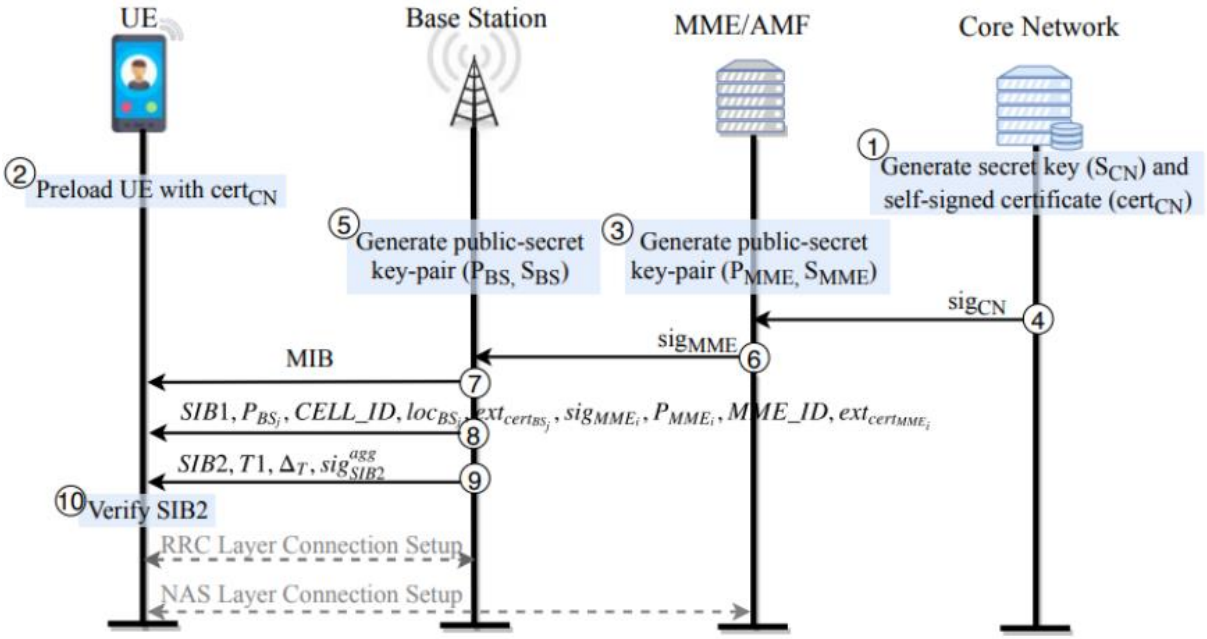

圖 6：文獻[10]所提出之基地台身分驗證方案

文獻[25]提出基於 schnorr 簽章[8]以及 HIBS[9]的基地台身份驗證方案，其方案首先由利用 HIBS 自 Core Private Key Generator (Core-PKG) 金鑰對中提取出其下級 Access and Mobility Management Function (AMF) 金鑰對，再自 AMF 金鑰對提取出下級之基地台 (Base Station，簡稱 BS) 金鑰對，取得以上三組金鑰對後再透過 schnorr 簽章可聚合多個簽名的特性，生成單一的聚合簽名 sig SIB1 後，將簽名合併於 SIB1 中傳送，根據文獻[25]所記載該方案運行於裝置 (Intel Core i5 2.4 GHz and 8 GB DDR4 RAM) 時上其簽名驗證時間成本為 0.52 ms，其方案對 SIB1 的額外負載為 144 Bytes。

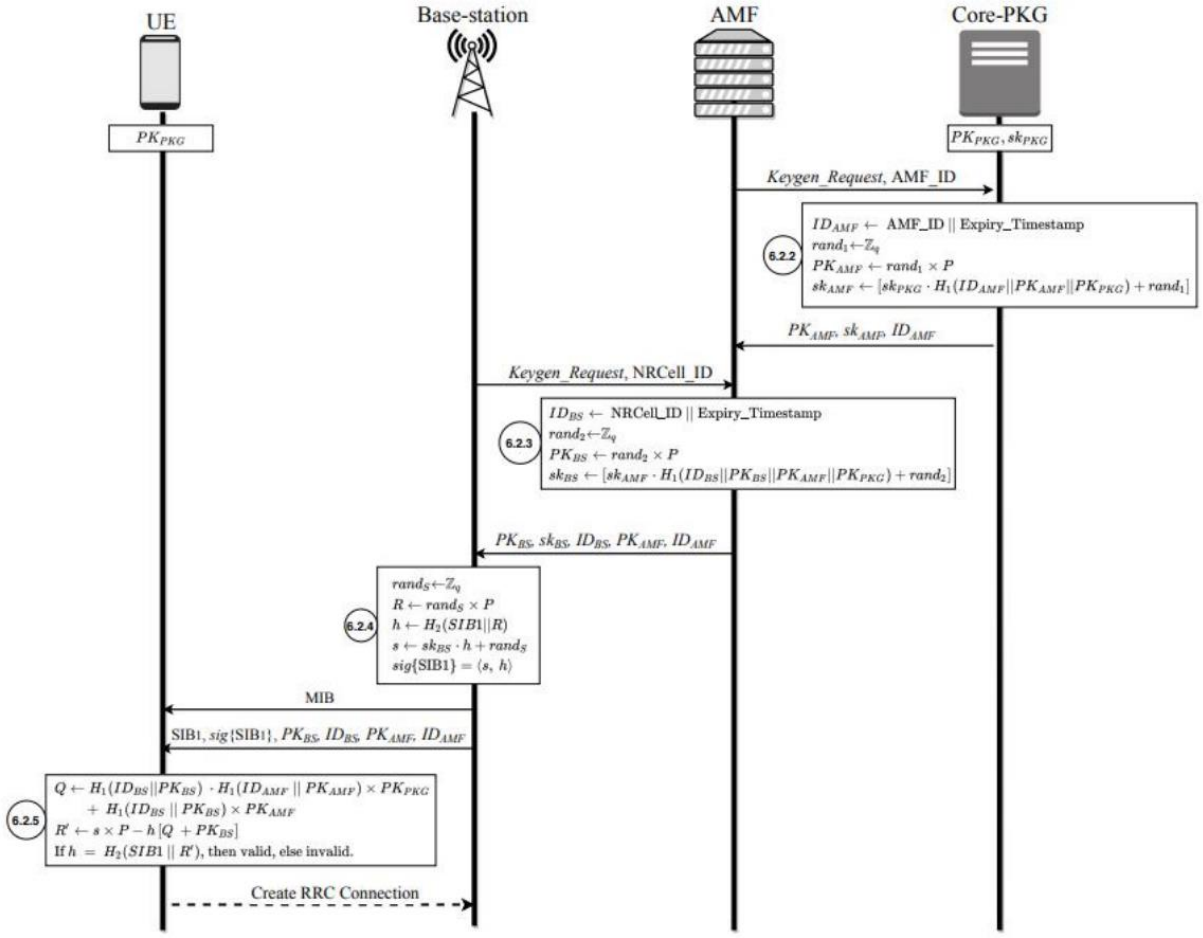

圖 7：文獻[25]所提出之基地台身分驗證方案

以上三種身分驗證機制中，前兩者[10, 28]是基於數位簽章對訊息本身進行驗證，後者[25]則是使用數位簽章對發送者身份本身進行驗證，後者相較於前者有較小的計算開銷，於本篇研究所提出的方案與文獻[25]類似，透過 BBS 簽章對發送者身份本身進行驗證以此緩解惡意基地台的風險。

在 A. B. Seyi, F. Jafaar 以及 R. Ruhl 的研究[26]中則是提出透過共享秘密認證模型完成基地台身份驗證。首先 UE 與基地台共同持有一組預先共享金鑰 (Pre-Shared Key，簡稱 PSK)，之後 UE 將隨機數 A 透過共享密鑰進行加密後發送至基地台，基地台將接收到的密文以共享密鑰解密取得隨機數 A 後，將隨機數 A 加上 UE 所指定的數值 B 後再進行加密，並將密文傳送至 UE，當 UE 接收到回傳的密文後進行解密，UE 比對解密後之數值是否為隨機數 A 加上指定數值 B，當比對結果為是，則代表基地台身份驗證成功。文獻[26]將此一流程置於 EPS-AKA 執行之前，以預防 UE 與惡意基地台進行 EPS-AKA 流程，避免 IMSI 之洩漏。

本論文認為文獻[26]之身份驗證方案由於必須與基地台進行通訊後才可確認基地台之合法性，因此用戶須先由原先所駐紮之基地台脫離並與要進行驗證之基地台建立連線，但是在建立連線後，即有可能受到惡意災防訊息以及 DoS 攻擊的風險。

參、方法

在本章節首先會對 UE 連接至基地台的基本流程以及協定中相關要素進行介紹以及探討，以此分析本論文之基地台身份驗證方案應該在 UE 連接流程中的哪個步驟進行，才能達成最佳的效益，接著將會對本論文所提出之基地台身份驗證方案所需使用到的數位簽章演算法 BBS 以及金鑰生成函式進行介紹。

3.1 UE 連接流程

UE 從開機的初始狀態到連接基地台的各個流程，如圖 8 所示，依序為時間同步 (解讀 PSS、SSS 訊息)、解讀 MIB 訊息、解讀 SIB1 訊息、解讀 SIB2 訊息。解讀完以上基地台廣播的訊息後，UE 將會與基地台進行通訊發起隨機接入 (Random Access) 以及 RRC Connection (Radio Resource Control，簡稱 RRC)，在完成以上步驟後才會進行 EPS-AKA 程序。基於圖 4 所示之各項風險觸發時間點，我們認為本論文所提出之身分驗證流程應置於解讀完 SIB2 後、進行 Random Access 之前完成，以此能夠更為全面的緩解惡意基地台帶來的風險。

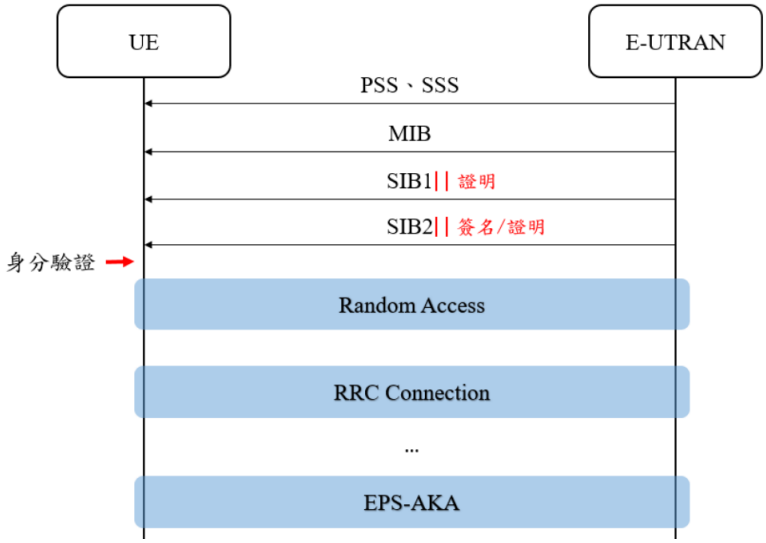

圖 8：本論文所提出之具身份驗證連接流程

3.2 數位簽章架構

本論文所提出身份驗證流程所使用之數位簽章為 BBS 簽章。BBS 簽章是由 T. Looker、V. Kalos[18]等人基於 D. Boneh、X. Boyen 和 H. Shacham 提出的學術著作[5]所實現的一種簽章演算法。BBS 簽章基於非對稱金鑰使私鑰持有者可對訊息進行簽名，公鑰持有者則透過公鑰對簽名進行驗證來確保訊息的真實性及完整性。本論文所使用之數位簽章方塊圖如圖 9 所示。

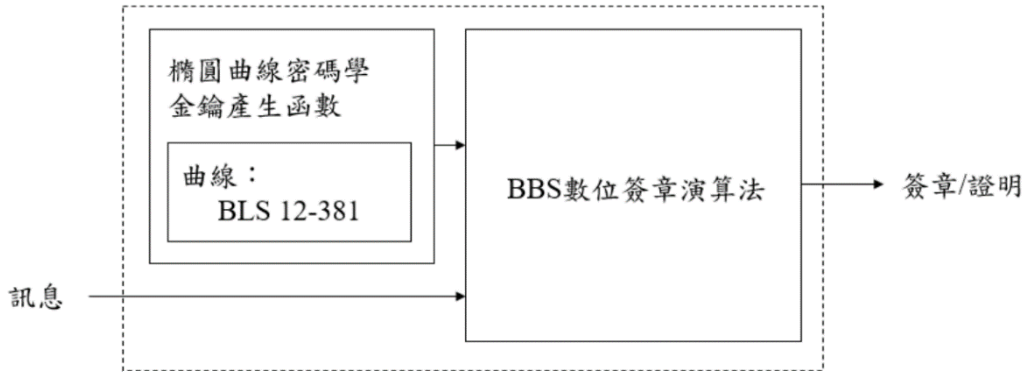

圖 9：本論文所使用之數位簽章方塊圖

在接下來的小節中將會依序說明：BBS 數位簽章程序、金鑰生成函數，其中金鑰生成函數包含：橢圓曲線密碼學 (Elliptic Curve Cryptography，簡稱 ECC) 的金鑰生成程序、以及金鑰生成時所選擇之曲線 BLS 12-381。

3.2.1 BBS 簽章

BBS 簽章中具有三個角色 1.簽名者 (私鑰持有者) 2.證明者 (公鑰持有者) 3.驗證者 (公鑰持有者)，如圖 10 所示。簽名者透過私鑰對訊息進行簽名後將訊息及簽名傳遞給證明者，證明者可以透過公鑰進行驗證，並可透過公鑰以及所要公開的部分原始資訊和簽名生成證明，在生成證明時也可額外添加資訊，將證明以及所要公開的訊息傳遞給驗證者，驗證者則可透過公鑰驗證接收到的訊息以及證明是否來自原始簽名當中，在此流程中驗證者不須獲得原始簽名。

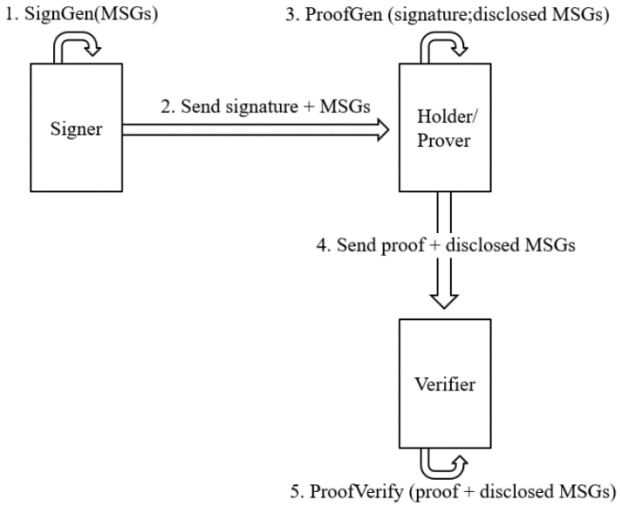

圖 10：BBS 簽章角色身份結構圖

3.2.2 金鑰產生函數

在使用 BBS 簽章之前我們必須先選擇所要使用的金鑰產生函數，在本論文中我們將採用橢圓曲線密碼學 (Elliptic Curve Cryptography，簡稱 ECC) 產生公私鑰對。最初將橢圓曲線應用於密碼學是由 Victor Miller 在 1985 年所提出[19]，橢圓曲線密碼學的相關演算法則是在 2004 年至 2005 年間開始廣泛被應用，橢圓曲線密碼學與同樣是非對稱加密演算法的 RSA [23]相比，能夠以較小的密鑰長度提供相同等級的安全性。

在 CRYPTO 2016 上由 T. Kim 以及 R. Barbulescu 提出的 exTNFS 算法 (Extended Tower Number Field Sieve) [14]，使解決離散對數問題的計算成本得以減輕，為了因應此一算法，S. Bowe 於 2017 年提出了曲線：BLS 12-381 (Boneh-Lynn-Shacham，簡稱 BLS) [4]，其中的 12 代表了曲線的嵌入度 (embedding degree)，由於該曲線具有無窮遠點，因此 381 則代表了該曲線在座標上最大可表示之位元數。

BLS 12-381 之曲線方程式為：$y^2 = x^3 + 4$

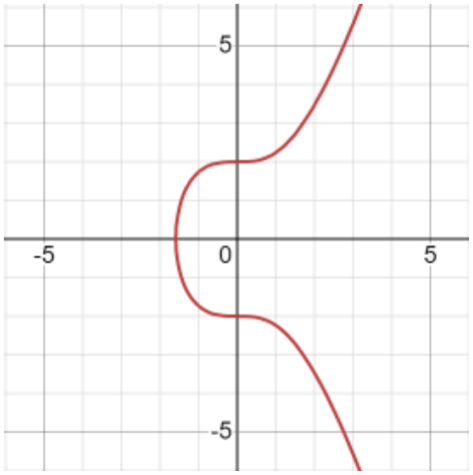

圖 11：BLS12-381 曲線

3.3 基於 BBS 簽章基地台身分驗證流程

本小節將會提出兩種基於 BBS 簽章之基地台身份驗證流程方案。方案一會由核心網路中的公鑰基礎建設 (Public Key Infrastructure，簡稱 PKI) 作為簽名者的角色，以私鑰對 MME/AMF 所提出之 TAC 進行簽名生成，MME/AMF 透過公鑰及基地台之 Cell ID 生成證明，UE 作為驗證者則透過公鑰來驗證證明，以此確認基地台以及 MME / AMF 的合法性。方案二則是由 PKI 作為簽名者對 TAC 及 Cell ID 生成簽名後，直接將簽名通過 MME / AMF 以及基地台傳遞至 UE 進行簽名驗證。

3.3.1 基地台身份驗證流程方案一

本方案首先由 PKI 生成公私鑰對，並且共享公鑰於 UE 以及 MME/AMF 當中，由 MME/AMF 對 PKI 發起簽名請求，請求中附帶 TAC，PKI 將 TAC 以及簽名之有效期 valid1 作為輸入生成簽名，並將簽名以及簽名之有效期 valid1 回傳至 MME/AMF，MME/AMF 將簽名及簽名之有效期儲存，當基地台對 MME/AMF 發起證明請求時，MME/AMF 將證明請求中所附帶之 Cell ID 以及證明之有效期 valid2 作為額外輸入生成證明，之後將〔1.簽名之有效期 2.證明之有效期 3.證明〕回傳至基地台，基地台收到證明及兩個有效期後，將這些資訊分為兩部分，第一部分為〔簽名之有效期||證明之有效期||證明之前半部〕；第二部分則為〔證明之後半部〕，並將第一部分附加於 SIB1 之後進行廣播，第二部分則附加於 SIB2 之後。

UE 在接收到 SIB1 及 SIB2 後透過公鑰對證明及有效期進行驗證，驗證通過則代表所連接之基地台及核心網路 MME/AMF 為合法網路。

方案之所以需將證明分為兩部分進行廣播是依據規範 3GPP TS 36.331[6]：「當 Downlink Control Information (DCI) 編碼格式為 1A 時 SIB 可容納最大長度為 2216 bits (277 Bytes)。」

本方案對於 SIB1 以及 SIB2 的額外負載 (overhead) 分別為 200 Bytes 以及 191 Bytes。

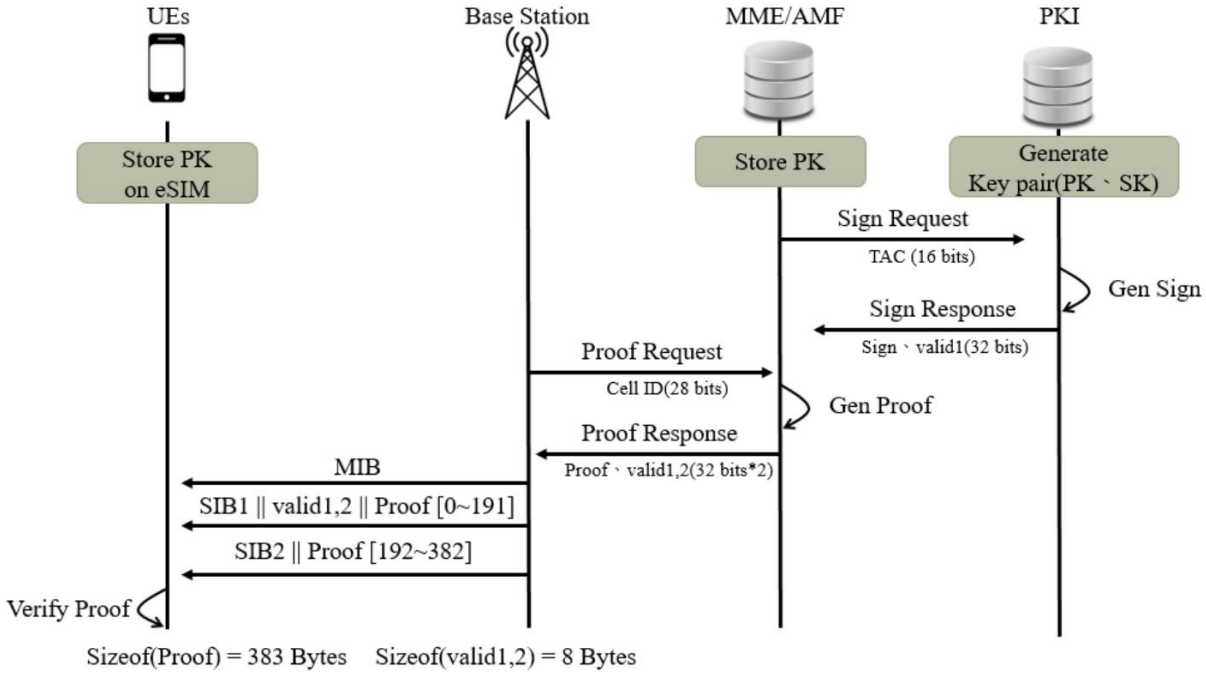

圖 12：身分驗證流程方案一

3.3.2 基地台身份驗證流程方案二

本論文提出之方案二，首先由 PKI 生成公私鑰對，並且共享公鑰於 UE 當中，當基地台對 MME/AMF 發起簽名請求並附帶 Cell ID 時，MME/AMF 會轉而再向 PKI 進行簽名請求並且附帶 Cell ID 以及 TAC，PKI 在收到請求後將 Cell ID、TAC 以及有效期作為輸入，透過私鑰進行簽名生成，並將簽名以及有效期回傳至 MME/AMF，MME/AMF 再將接收到的簽名及有效期回傳至基地台，基地台在收到簽名及有效期後將其合併於 SIB2 後進行廣播。

UE 在接收到 SIB2 以及附加資訊後，首先驗證有效期是否過期，若於有效期內則透過公鑰對簽名進行驗證，以此得知基地台以及核心網路 MME/AMF 的身份是否合法，本方案對於 SIB2 的額外負載 (overhead) 為 120 Bytes。

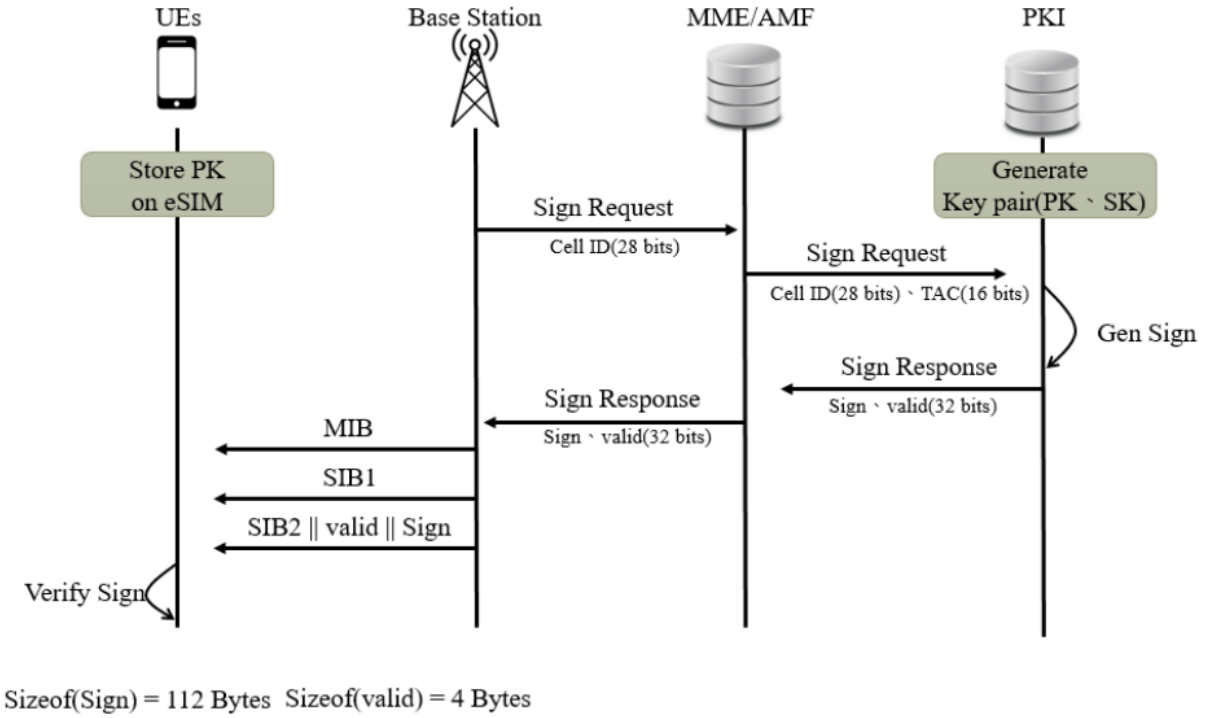

圖 13：身分驗證流程方案二

肆、數位簽章身分驗證實作

本論文之模擬環境系統架構如圖 14 所示，本實驗使用一台桌上型電腦掛載兩台虛擬機 (Virtual Machine，簡稱 VM)，透過 USB 3.1 連接兩台 USRP B210。VM1 用於模擬 UE，VM2 則模擬基地台及核心網路，VM1 與 VM2 經由 USRP B210 於空中介面 (Air Interface) 進行通訊。詳細設備規格清單如表 2 所示。

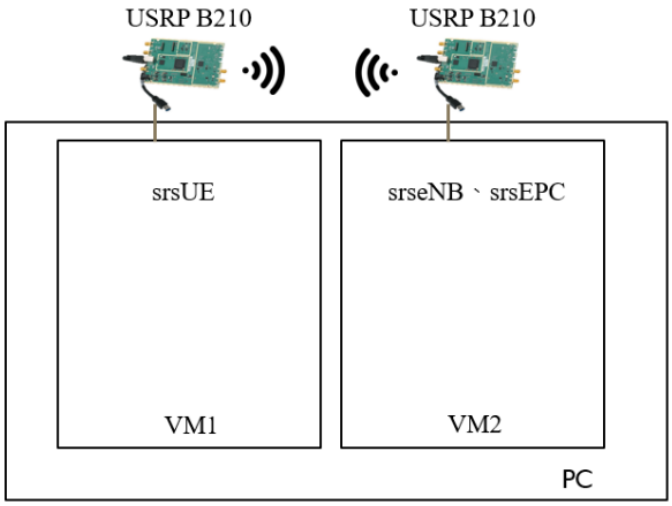

圖 14：模擬環境系統架構圖

表 2：設備規格表

設備名稱	詳細規格	
PC	作業系統	Win 10
	核心處理單元	CPU i7-9700 8core 3.00GHz
	記憶體	RAM 32GB (DDR4 16G * 2)
VM1	作業系統	Ubuntu 20.04
	核心處裡單元	CPU core * 4
	記憶體	RAM 8G
	連接埠	USB 3.1 port * 1
VM2	作業系統	Ubuntu 20.04
	核心處裡單元	CPU core * 4
	記憶體	RAM 8G
	連接埠	USB 3.1 port * 1

4.1 測試環境建置及修改

本論文使用 srsRAN 作為測試環境，並且更改 srseNB 原始碼來實現在 SIB1 以及 SIB2 當中額外附加 BBS 簽名。為了使 srsUE 在接收到 SIB 後能夠正確解讀，以及對簽名內容進行驗證，也需對 srsUE 之原始碼進行修改，對 srsRAN 之修改內容將於以下兩小節進行說明。

4.1.1 srsRAN 數位簽章發送實作

為了達成本論文所提出之基地台身份驗證流程，需使 srseNB 在發送 SIB 時額外附加 BBS 簽名，因此需修改 srseNB 之原始碼：1.sib.config 2.enb_cfg_parser.cc 3.si.cc 4.si.h。

sib.config 為基地台所要發送之所有 SI 訊息的設定檔，我們須將 BBS 簽名輸入至 sib.config 中，enb_cfg_parser.cc 則是負責讀取如 sib.config 等等設定檔之內容至 srseNB 的主要程式，si.cc 以及 si.h 主要作用為將 enb_cfg_parser.cc 讀取之 SI 相關訊息進行編碼成 bit String 之程式，編碼成 bit String 之後才能透過 USRP B210 進行發送，發送數位簽章之資料流 (Data Flow) 如圖 15 所示。

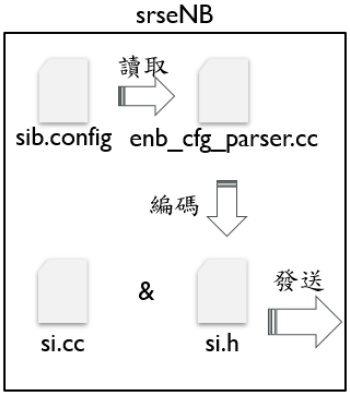

圖 15：發送數位簽章資料流

4.1.2 srsRAN 數位簽章驗證實作

上一小節修改完發送端之 srseNB 的相關設定及原始碼之後，接收端 srsUE 也需達成本論文之基地台身份驗證流程對修改後的 SIB2 進行正確解碼，以及驗證 SIB2 中包含的簽名及有效期，因此需更改檔案：1.rrc.cc 2.rrc.h 3.si.cc 4.si.h。

si.cc 以及 si.h 為對 SIB2 等等 SI 訊息進行解碼之程式，rrc.cc 以及 rrc.h 則是在解碼完 SI 訊息後進行無線電資源控制之程式，因此簽章驗證程式片段將置於 rrc.cc 當中執行，於 rrc.cc 透過驗證簽名確認 srseNB 之合法性後才會進行後續的 Random Access 等步驟，解碼及驗證數位簽章之資料流如圖 16 所示。

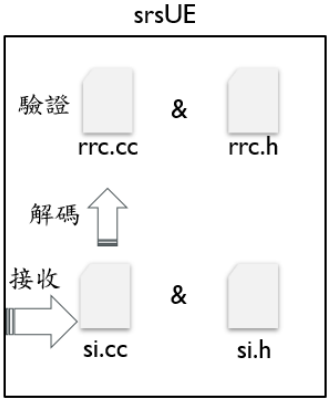

圖 16：驗證數位簽章資料流

4.2 完成 BBS 簽名實作

本篇研究之 BBS 簽名實作程式片段以 TypeScript 撰寫而成，並根據本論文所提出之兩種方案分別撰寫成兩個程式，其中方案一分為五個階段如圖 17 所示，方案二則分為三個階段如圖 18 所示，在接下來的小節中將依序說明：1.方案一之 BBS 程式執行過程及結果 2.方案二之 BBS 程式執行過程及結果。

方案一之五階段為：
- 階段 0. 生成金鑰對
- 階段 1. 生成簽名
- 階段 2. 驗證簽名
- 階段 3. 生成證明
- 階段 4. 驗證證明

方案二之三階段為：
- 階段 0. 生成金鑰對
- 階段 1. 生成簽名
- 階段 2. 驗證簽名

```
f459@ubuntu:~/node-bbs-signatures/sample/src$ ts-node proof.ts
stage0 Generate Keypair   : ts-node .ts 0
stage1 Generate Signature : ts-node .ts 1 "SK" "PK" "tac"
stage2 Verify Signature   : ts-node .ts 2 "PK" "tac" "valid1" "signature"
stage3 Generate Proof     : ts-node .ts 3 "PK" "tac" "valid1" "Cell_ID" "signature"
stage4 Verify Proof       : ts-node .ts 4 "PK" "tac" "valid1" "Cell_ID" "valid2" "proof"
```

圖 17：方案一之五階段程式碼敘述

```
f459@ubuntu:~/node-bbs-signatures/sample/src$ ts-node verify.ts
stage0 Generate Keypair   : ts-node .ts 0
stage1 Generate Signature : ts-node .ts 1 "SK" "PK" "tac" "eNB_ID"
stage2 Verify Signature   : ts-node .ts 2 "PK" "tac" "eNB_ID" "valid" "signature"
```

圖 18：方案二之三階段程式碼敘述

4.2.1 身份驗證流程方案一之 BBS 程式

本論文之身份驗證流程方案一當中，首先由 PKI 執行第零階段生成公私鑰對，並將其公鑰共享於 UE 以及 MME/AMF，生成公私鑰對結果如圖 19 所示，其中公私鑰對以 Base64 編碼表示，私鑰長度為 32 Bytes，公鑰長度為 112 Bytes。

```
f459@ubuntu:~/node-bbs-signatures/sample/src$ ts-node proof.ts 0

Secret key base64 = axMNRcrYiBjm8Fc1AjTFp31HpJzQPncM4OfVoqbAonA=

Public key base64 = iW9vvhKFLFpnn32Dkn8MBjY0QpVAjT5OIapHImRYzqyIamXOtVc/rdjtqVoX
WiuUFeI8pYIHeb0mu5Ay1BiEdAq8Ea+pdHlmAWOGXeMhVfY03SKReNiMrTK2/+uul3mv
```

圖 19：身份驗證流程一之第零階段-生成金鑰對

PKI 生成完公私鑰對後將使用公私鑰對以及 TAC = 7 生成簽名並傳遞給MME/AMF，生成簽名結果如圖 20 所示，其中橘框內為第零階段生成公私鑰對，紅框則為 TAC 數值，輸出簽名以無符號八位元陣列 (Uint8Array) 表示，其中每組數值為 0～255 以 8 bits

表示，總簽名長度為 112 Bytes，valid 設定為生成金鑰的當前 Unix 時間戳 (Unix timestamp) 加上 24 小時，valid0 表示有效期之高 16 bits，valid1 表示低 16 bits，此階段於 eNB 端執行。

Unix 時間戳為自 1970 年 01 月 01 日 00 時 00 分 00 秒起以秒為單位所統計之時間，1669183393 為 2022 年 11 月 23 日 14 時 03 分 13 秒。

```
f459@ubuntu:~/node-bbs-signatures/sample/src$ ts-node proof.ts 1 axMNRcrYiBjm8Fc
1AjTFp31HpJzQPncM4OfVoqbAonA= iW9vvhKFLFpnn32Dkn8MBjY0QpVAjT5OIapHImRYzqyIamXOtV
c/rdjtqVoXWiuUFeI8pYIHeb0mu5Ay1BiEdAq8Ea+pdHlmAWOGXeMhVfY03SKReNiMrTK2/+uul3mv 7

Secret key base64 = axMNRcrYiBjm8Fc1AjTFp31HpJzQPncM4OfVoqbAonA=
Public key base64 = iW9vvhKFLFpnn32Dkn8MBjY0QpVAjT5OIapHImRYzqyIamXOtVc/rdjtqVoX
WiuUFeI8pYIHeb0mu5Ay1BiEdAq8Ea+pdHlmAWOGXeMhVfY03SKReNiMrTK2/+uul3mv

Output signature = 180,112,144,196,239,116,197,195,215,28,60,197,129,44,225,164,
45,187,156,24,235,76,133,136,60,133,93,17,250,28,98,183,170,54,114,174,234,75,19
5,18,19,23,97,123,112,105,158,90,67,42,22,150,181,164,175,211,223,28,173,27,182,
119,93,244,46,127,248,18,105,68,136,112,29,82,20,12,52,107,208,203,55,227,250,74
,254,66,62,99,232,105,89,217,137,24,217,119,185,214,171,91,29,251,172,24,54,218,
62,77,237,76,202,194

valid0 = 0110001101111101
valid1 = 1011011110100001
valid = 1669183393
```

圖 20：身份驗證流程一之第一階段-生成簽名

MME/AMF 在接收到簽名後首先執行第二階段對簽名進行驗證，驗證結果如圖 21 所示，其中橘框部分為 TAC 數值以及簽名有效期，當驗證通過後於第三階段輸入 Cell ID =105217 生成證明如圖 22 所示，橘框部分依序為 TAC、簽名有效期、Cell ID，證明有效期設定為 1 分鐘，生成證明大小為 383 Bytes，與第二階段生成簽名同樣以無符號八位元陣列表示。

```
f459@ubuntu:~/node-bbs-signatures/sample/src$ ts-node proof.ts 2 iW9vvhKFLFpnn32
Dkn8MBjY0QpVAjT5OIapHImRYzqyIamXOtVc/rdjtqVoXWiuUFeI8pYIHeb0mu5Ay1BiEdAq8Ea+pdHl
mAWOGXeMhVfY03SKReNiMrTK2/+uul3mv 7 1669183393 180,112,144,196,239,116,197,195,2
15,28,60,197,129,44,225,164,45,187,156,24,235,76,133,136,60,133,93,17,250,28,98,
183,170,54,114,174,234,75,195,18,19,23,97,123,112,105,158,90,67,42,22,150,181,16
4,175,211,223,28,173,27,182,119,93,244,46,127,248,18,105,68,136,112,29,82,20,12,
52,107,208,203,55,227,250,74,254,66,62,99,232,105,89,217,137,24,217,119,185,214,
171,91,29,251,172,24,54,218,62,77,237,76,202,194

{"verified":true}
```

圖 21：身份驗證流程一之第二階段-驗證簽名

```
f459@ubuntu:~/node-bbs-signatures/sample/src$ ts-node proof.ts 3 iW9vvhKFLFpnn32Dkn8MBjY0QpVAj
T5OIapHImRYzqyIamXOtVc/rdjtqVoXWiuUFeI8pYIHeb0mu5Ay1BiEdAq8Ea+pdHlmAWOGXeMhVfY03SKReNiMrTK2/+u
ul3mv 7 1669183393 105217 180,112,144,196,239,116,197,195,215,28,60,197,129,44,225,164,45,187,
156,24,235,76,133,136,60,133,93,17,250,28,98,183,170,54,114,174,234,75,195,18,19,23,97,123,112
,105,158,90,67,42,22,150,181,164,175,211,223,28,173,27,182,119,93,244,46,127,248,18,105,68,136
,112,29,82,20,12,52,107,208,203,55,227,250,74,254,66,62,99,232,105,89,217,137,24,217,119,185,2
14,171,91,29,251,172,24,54,218,62,77,237,76,202,194

Output proof = 0,1,1,147,211,67,182,8,114,241,16,183,147,156,61,7,77,1,244,231,189,86,91,90,67
,68,132,84,161,168,8,4,175,182,14,247,51,186,88,218,246,53,96,9,188,47,241,192,8,103,204,174,2
36,146,66,71,9,137,200,249,81,169,54,23,176,174,5,216,199,253,5,232,253,108,77,253,161,146,150
,213,235,168,112,101,236,40,199,63,108,129,70,166,161,147,230,206,237,219,13,129,169,193,44,15
1,106,100,91,109,121,215,210,124,69,194,149,189,176,172,242,15,12,164,49,251,17,221,78,132,118
,245,62,206,194,49,83,50,3,4,135,125,55,183,120,120,248,65,86,0,0,0,116,136,69,51,155,24,226,1
65,218,144,162,159,100,46,197,14,170,120,74,4,177,172,136,160,188,17,182,250,243,249,77,248,11
3,160,36,154,83,2,109,217,171,155,107,37,72,117,172,13,26,0,0,0,2,44,151,141,157,180,89,107,21
0,134,100,47,178,199,38,17,173,22,226,125,24,153,154,125,208,100,156,185,112,95,19,198,165,103
,174,11,33,196,253,55,110,186,68,69,185,50,39,72,138,14,125,29,179,70,76,162,234,70,187,112,11
8,179,43,176,10,138,10,210,164,248,186,253,163,87,174,2,0,184,35,122,255,242,89,221,187,40,42,
255,159,233,136,234,231,235,172,251,99,100,13,90,38,164,240,212,212,199,60,32,246,157,176,134,
205,0,0,0,2,48,110,92,119,214,197,14,35,126,176,31,194,163,228,233,161,72,65,252,51,20,103,235
,156,184,37,96,16,148,52,206,241,98,71,88,102,125,4,22,219,34,155,77,160,11,254,184,233,79,128
,195,241,105,39,222,68,28,41,134,224,130,112,48,47

valid0 = 0110001101111100
valid1 = 0110100011100100
valid = 1669097700
```

圖 22：身份驗證流程一之第三階段-生成證明

當 UE 在接收到 SIB1、2 後將其中所包含 TAC = 7、Cell ID = 105217、有效期以及證明，透過公鑰進行驗證以確保所連接之基地台以及核心網路為合法的，驗證過程如圖 23 所示，橘框部分依序為 TAC、簽名有效期、Cell ID、證明有效期。

```
f459@ubuntu:~/node-bbs-signatures/sample/src$ ts-node proof.ts 4 iW9vvhKFLFpnn32Dkn8MBjY0QpVAj
T5OIapHImRYzqyIamXOtVc/rdjtqVoXWiuUFeI8pYIHeb0mu5Ay1BiEdAq8Ea+pdHlmAWOGXeMhVfY03SKReNiMrTK2/+u
ul3mv 7 1669183393 105217 1669097700 0,1,1,147,211,67,182,8,114,241,16,183,147,156,61,7,77,1,2
44,231,189,86,91,90,67,68,132,84,161,168,8,4,175,182,14,247,51,186,88,218,246,53,96,9,188,47,2
41,192,8,103,204,174,236,146,66,71,9,137,200,249,81,169,54,23,176,174,5,216,199,253,5,232,253,
108,77,253,161,146,150,213,235,168,112,101,236,40,199,63,108,129,70,166,161,147,230,206,237,21
9,13,129,169,193,44,151,106,100,91,109,121,215,210,124,69,194,149,189,176,172,242,15,12,164,49
,251,17,221,78,132,118,245,62,206,194,49,83,50,3,4,135,125,55,183,120,120,248,65,86,0,0,0,116,
136,69,51,155,24,226,165,218,144,162,159,100,46,197,14,170,120,74,4,177,172,136,160,188,17,182
,250,243,249,77,248,113,160,36,154,83,2,109,217,171,155,107,37,72,117,172,13,26,0,0,0,2,44,151
,141,157,180,89,107,210,134,100,47,178,199,38,17,173,22,226,125,24,153,154,125,208,100,156,185
,112,95,19,198,165,103,174,11,33,196,253,55,110,186,68,69,185,50,39,72,138,14,125,29,179,70,76
,162,234,70,187,112,118,179,43,176,10,138,10,210,164,248,186,253,163,87,174,2,0,184,35,122,255
,242,89,221,187,40,42,255,159,233,136,234,231,235,172,251,99,100,13,90,38,164,240,212,212,199,
60,32,246,157,176,134,205,0,0,0,2,48,110,92,119,214,197,14,35,126,176,31,194,163,228,233,161,7
2,65,252,51,20,103,235,156,184,37,96,16,148,52,206,241,98,71,88,102,125,4,22,219,34,155,77,160
,11,254,184,233,79,128,195,241,105,39,222,68,28,41,134,224,130,112,48,47
{"verified":true}
```

圖 23：身份驗證流程一之第四階段-驗證證明

4.2.2 身份驗證流程方案二之 BBS 程式

本論文所提出的基地台身份驗證方案二中，首先由 PKI 執行公私鑰對產生，產生結果如圖 24 所示，其中公私鑰對以 Base64 編碼表示，私鑰長度為 32 Bytes，公鑰長度為 112 Bytes。

```
f459@ubuntu:~/node-bbs-signatures/sample/src$ ts-node verify.ts 0

Secret key base64 = bOpvYiaHVzepdIsPo7idkNoQF1jjli4YkRfduPD3Cvo=

Public key base64 = lCseIRyAyT7Xa7ExD2tZJcywygCVy4TLdpniEvXEf37xalL8WRAmHuxhTAQv
N9amAnSjnNyIW9iNDS3qLwmpKdKo59KGOkpuAz6zL5M3W+m3P9ukKOVncXq7IjR1gK8A
```

圖 24：身份驗證流程二之第零階段-生成公私鑰對

在生成完公私鑰對後，使用公私鑰對及 TAC 和 Cell ID 生成簽名，簽名生成結果如圖 25 所示，橘框部分為公私鑰對，紅框部分為 TAC＝7 以及 Cell ID＝105217， 生成簽名長度為 112 Bytes，有效期則為生成簽名當下時間加上 10 分鐘。

```
f459@ubuntu:~/node-bbs-signatures/sample/src$ ts-node verify.ts 1 bOpvYiaHVzepdI
sPo7idkNoQF1jjli4YkRfduPD3Cvo= lCseIRyAyT7Xa7ExD2tZJcywygCVy4TLdpniEvXEf37xalL8W
RAmHuxhTAQvN9amAnSjnNyIW9iNDS3qLwmpKdKo59KGOkpuAz6zL5M3W+m3P9ukKOVncXq7IjR1gK8A
7 105217

Secret key base64 = bOpvYiaHVzepdIsPo7idkNoQF1jjli4YkRfduPD3Cvo=
Public key base64 = lCseIRyAyT7Xa7ExD2tZJcywygCVy4TLdpniEvXEf37xalL8WRAmHuxhTAQv
N9amAnSjnNyIW9iNDS3qLwmpKdKo59KGOkpuAz6zL5M3W+m3P9ukKOVncXq7IjR1gK8A

Output signature = 177,37,94,45,226,34,221,126,93,110,210,189,88,54,215,82,26,19
8,83,82,241,104,30,194,109,69,173,80,236,173,207,58,67,27,125,174,21,33,9,1,111,
84,46,161,229,233,169,237,12,178,114,157,150,192,205,223,63,83,137,183,239,48,18
0,148,100,233,20,93,204,145,202,52,126,185,38,220,168,12,51,85,28,179,48,174,228
,166,2,41,42,214,202,177,83,225,249,80,111,175,1,172,51,236,108,91,239,94,166,14
,174,162,111,210

valid0 = 0110001101111100
valid1 = 0111101000000011
valid = 1669102083
```

圖 25：身份驗證流程二之第一階段-生成簽名

BBS 簽名驗證執行結果如下圖 26 所示，其中紅框部分依序為 TAC、Cell ID、 簽名有效期 valid，當驗證通過後輸出結果顯示為 verified : true 則代表身份驗證通過，此階段於 UE 端執行。

```
f459@ubuntu:~/node-bbs-signatures/sample/src$ ts-node verify.ts 2 lCseIRyAyT7Xa7
ExD2tZJcywygCVy4TLdpniEvXEf37xalL8WRAmHuxhTAQvN9amAnSjnNyIW9iNDS3qLwmpKdKo59KGOk
puAz6zL5M3W+m3P9ukKOVncXq7IjR1gK8A 7 105217 1669102083 177,37,94,45,226,34,221,1
26,93,110,210,189,88,54,215,82,26,198,83,82,241,104,30,194,109,69,173,80,236,173
,207,58,67,27,125,174,21,33,9,1,111,84,46,161,229,233,169,237,12,178,114,157,150
,192,205,223,63,83,137,183,239,48,180,148,100,233,20,93,204,145,202,52,126,185,3
8,220,168,12,51,85,28,179,48,174,228,166,2,41,42,214,202,177,83,225,249,80,111,1
75,1,172,51,236,108,91,239,94,166,14,174,162,111,210

{"verified":true}
```

圖 26：身份驗證流程二之第二階段-驗證簽名

本論文所使用之 BBS 簽章程式在各階段執行一千次之時間成本平均值如表 3 所 示。

表 3：各階段時間成本平均值

階段	時間成本 (單位 ms)
生成金鑰對	0.694
生成簽名	2.911
驗證簽名	5.672
生成證明	7.964
驗證證明	5.48

伍、結論

在本章節中將會對本論文所提出之基地台身分驗證流程經由模擬環境實現後之結果進行說明，並且與已知相關文獻進行比較，最後將對本論文所提出之基地台驗證流程進行弱點分析。

5.1 實驗結果

我們分別以 wireshark 對兩種方案中 UE 端接收之 MAC Layer 訊息進行分析，身份驗證流程方案一之結果如圖 27 所示，SIB1 總長度為 251 Bytes，SIB2 總長度則為 259 Bytes。

No.	Time	Sou	Des	Protocol	Length	Info
1	0.000000			LTE RR…	37	MasterInformationBlock (SFN=80)
2	0.395018			LTE RR…	251	SystemInformationBlockType1
3	0.639011			LTE RR…	259	SystemInformation [SIB2]
4	0.760554			LTE RR…	37	MasterInformationBlock (SFN=99)
5	0.815042			LTE RR…	251	SystemInformationBlockType1
6	0.958947			LTE RR…	259	SystemInformation [SIB2]
7	25.340330			LTE RR…	37	MasterInformationBlock (SFN=201)
8	25.535324			LTE RR…	251	SystemInformationBlockType1
9	25.599267			LTE RR…	259	SystemInformation [SIB2]
10	25.720569			LTE RR…	37	MasterInformationBlock (SFN=211)
11	25.775272			LTE RR…	251	SystemInformationBlockType1
12	25.919246			LTE RR…	259	SystemInformation [SIB2]
13	30.281211			LTE RR…	37	MasterInformationBlock (SFN=69)
14	30.555371			LTE RR…	251	SystemInformationBlockType1

圖 27：以 wireshark 觀察方案一之 MAC Layer

下圖 28 為方案一之 SIB1 內容，紅框部分為簽名有效期 4 Bytes，綠框則為證明有效期 4 Bytes，藍框為證明 0 至 191 Bytes 之內容，傳遞之有效期及證明數值與圖 22 相符。

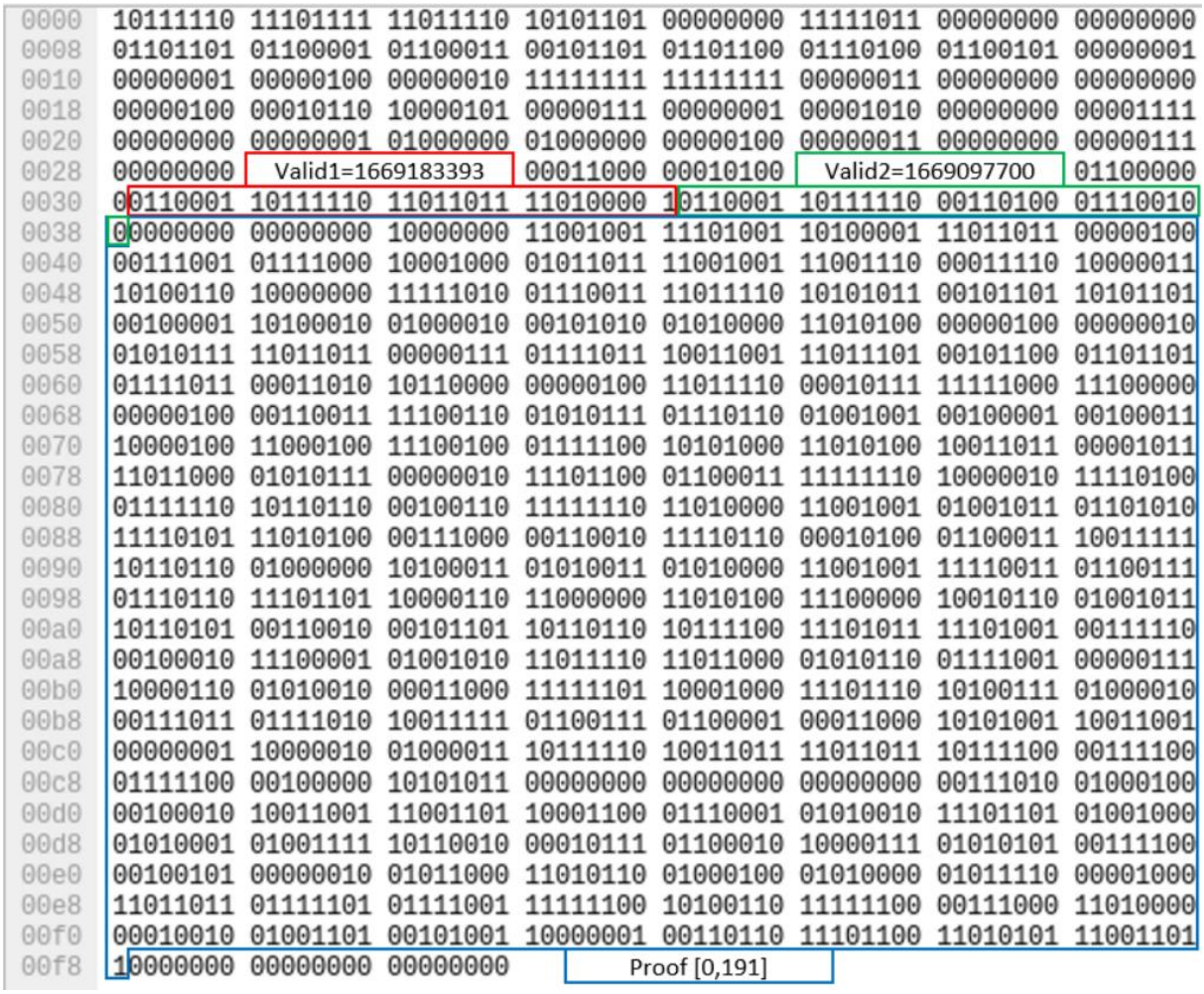

圖 28：以 wireshark 觀察方案一之 SIB1 內容

下圖 29 為身份驗證方案一中 SIB2 解析之內容，藍框部分為證明後半段 192 至 382 Bytes 之內容。

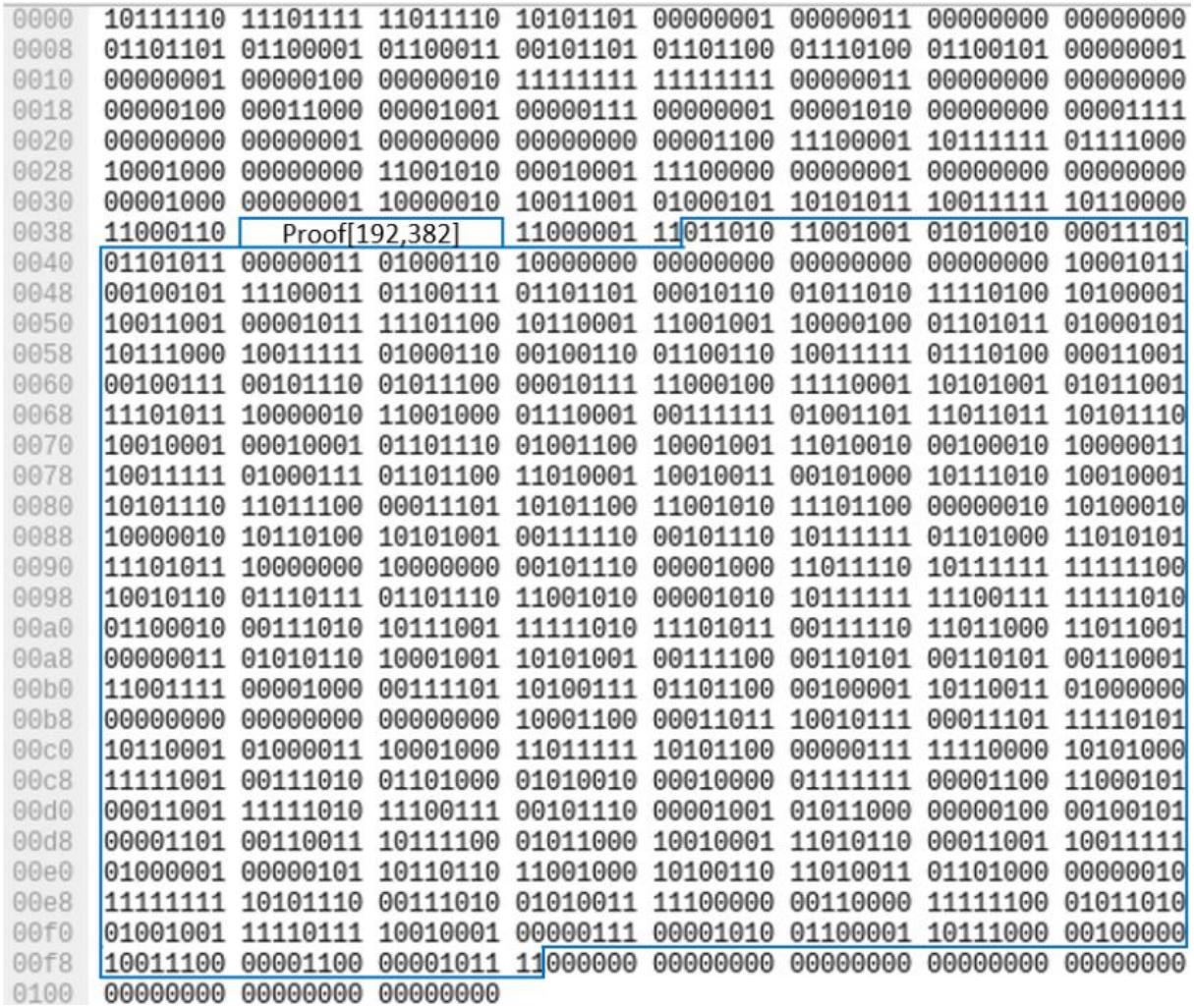

圖 29：以 wireshark 觀察方案一之 SIB2 內容

方案二以 wireshark 分析之結果如圖 30 以及圖 31 所示，圖 30 中顯示 SIB2 總長度為 179 Bytes，圖 31 中，紅框部分為 valid 8 Bytes，藍框部分為 BBS 簽名之 112 Bytes，傳遞的有效期以及簽名與圖 25 簽名生成結果相同，除紅框及藍框外其餘皆為原始資訊。

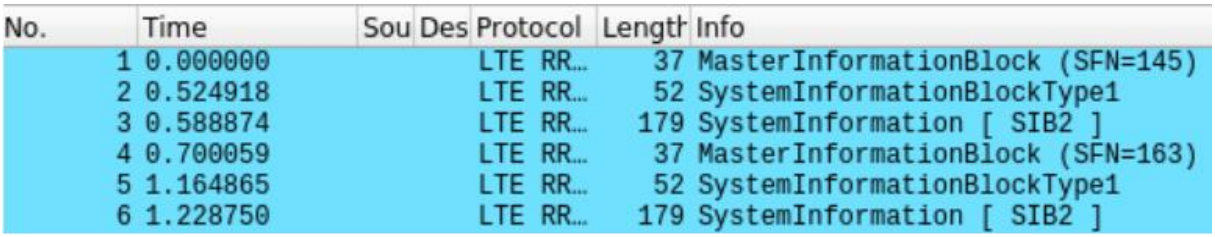

圖 30：以 wireshark 觀察方案二之 MAC Layer

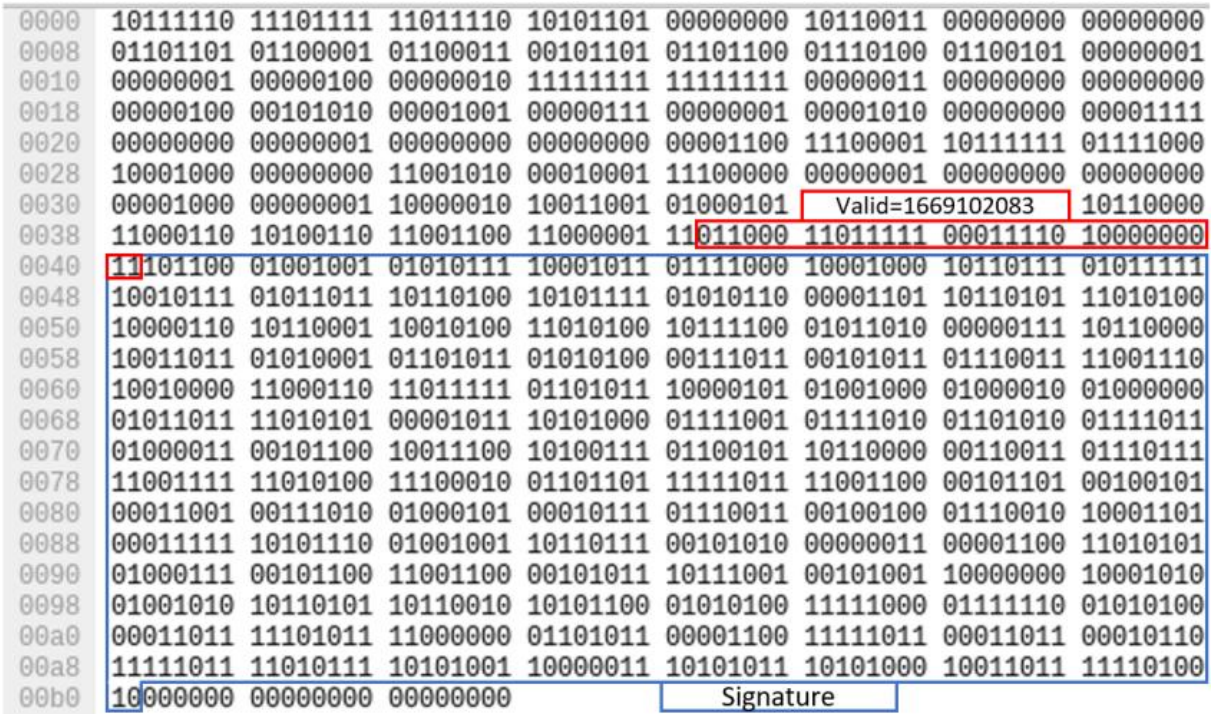

圖 31：以 wireshark 觀察方案二之 SIB2 內容

5.2 成效比較

在本小節中以本論文所提出之方案與相關文獻[10, 25]進行成效比較，首先針對 SIB 之額為負載進行比較如表 4 所示，總額外負載為本論文所提出之方案二總額外負載 116 Bytes 為最優，即使方案一對單一 SIB 之額外負載為最高之 201 Bytes，但單一 SIB 依舊於 10ms 內發送完畢，因此額外負載並不會造成顯著的時間成本。

表 4：SIB 額外負載

	文獻[10]	文獻[25]	方案一	方案二
SIB1 額外負載	181 Bytes	144 Bytes	200 Bytes	N/A
SIB2 額外負載	39 Bytes	N/A	201 Bytes	116 Bytes
總額外負載	220 Bytes	144 Bytes	401 Bytes	116 Bytes

對 UE 端之額外時間成本進行比較如表 5 所示，本論文所提出之方案皆約為 5.5 ms 與文獻[10]相比有極大的改進，於 UE 連接流程中 UE 需等待接收完整之 SIB 訊息，因此需依照廣播流程之安排等待 SIB2 之訊息，SIB2 之廣播週期最短為 80 ms，因此即使在最短廣播週期設定下，UE 下依舊可能需等待 80ms 才能接收到完整的 SIB 訊息，因此我們認為本論文提出之方案對 UE 端之額外時間成本 5.5 ms 對 UE 端使用者而言並不會造成影響。

本論文所提出之方案時間成本為於 CPU i7-9700 4 core 3.00 GHz 8G RAM 運行一千

次之平均值，相關文獻[10, 25]之時間成本為原文所記載之數據，額外時間成本依設備計算能力及演算法而定。

表 5：UE 端額外時間成本

文獻[1.]	文獻[25]	方案一	方案二
119.19 ms	0.52 ms	5.67 ms	5.48 ms

本論文所提出之方案於核心網路中生成簽章時相較文獻[16, 17]有明顯的時間成本如表 6 所示。

表 6：UE 端額外時間成本

文獻[10]	文獻[25]	方案一	方案二
0.06 ms	0.02 ms	2.911 ms	7.964 ms

5.3 弱點分析

我們假設攻擊者僅能取得空中介面 (Air Interface) 中所廣播的訊息，並且符合以下所列條件。

- 能夠竊聽或竄改 MIB、SIB
- 能夠冒充合法基地台
- 無法經由實體連接途徑取得用戶 SIM 卡或基地台及核心網路中的敏感資訊 (如加密所使用之私鑰)

可能遭受的攻擊流程如圖 32 所示，首先攻擊者於 Air Interface 中取得合法基地台廣播之簽章內容，並且架設一惡意基地台，當此一惡意基地台之 Cell ID 以及 TAC 與合法基地台相同時，攻擊者將取得之簽章內容置於 SIB 當中傳送，此時當 UE 接收到來自惡意基地台之 SIB 內容後，由於 Cell ID 以及 TAC 與簽章所驗證之數值相同，因此惡意基地台之數位簽章將會通過驗證，UE 則會依據小區選擇標準決定與合法基地台或惡意基地台何者進行連接。

上述所提出之攻擊手法攻擊者需於簽章有效期內完成惡意基地台的架設，當簽章有效期過期後則須重新取得新的簽章內容。本論文所提出之身份驗證流程方案一由於其分散於各 MME 當中生成證明，而非方案二統一由單一 PKI 生成簽名，因此流程一當中各別設施需負擔計算負荷相較流程二能夠顯著的減少，基於此一因素我們認為方案一相較方案二，較能透過增加計算成本以降低有效期之時長，縮短攻擊者可利用之攻擊窗口。

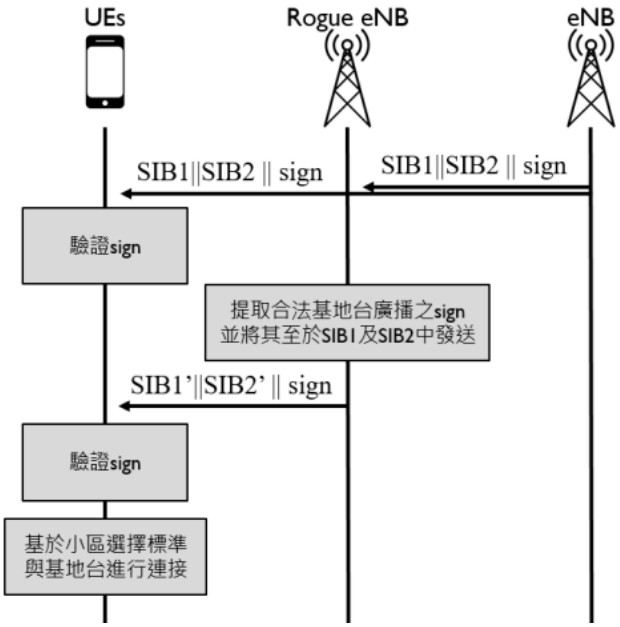

圖 32：本身分驗證方案可能面臨之攻擊手法

5.4 未來工作

依據我們對於文獻的研究，我們認為在第五代行動通訊當中依舊可能存在惡意基地台的風險，因此我們認為本論文所提出之身份驗證流程也可適用於第五代行動通訊當中，並且根據規範 3GPP TS 38.331[1]，第五代行動通訊網路中 SIB 的可乘載最大大小為 2976 bits (372 Bytes)，因此可能有效果更好的身份驗證演算法可應用在基地台身份驗證這個問題上。

根據規範 3GPP TS 38.331[1]，在第五代行動通訊當中與第四代行動通訊 SI 廣播流程不同，其 UE 在與基地台進行接取時並不一定需要 SIB2 之訊息，因此根據需求 UE 及基地台可能只依據 MIB 以及 SIB1 即可完成連線的建立，此一更動可能使本論文所提出之基地台身分驗證流程方案一無法實現，由於僅使用單一 SIB1 時將無法完整傳送方案一之證明內容。在第五代行動通訊中不論是 Non-Standalone 或者 Standalone 其 SI 廣播流程皆屬上述所提及之流程。

於本論文之實驗中簽名以及證明的生成及配發均為人工進行，在未來工作中可以嘗試自動對每個獨立的 SI 生成簽名並透過加入 System Frame Number (SFN) 來防止於弱點分析中所提出的重送簽名此一攻擊手法。

參考文獻

[1] *5G;NR;Radio Resource Control (RRC);Protocol specification Release 17*, TS 38.331 V17.2.0, 3GPP, Oct. 2022.

[2] A. Ali and G. Fischer, "The Phase Noise and Clock Synchronous Carrier Frequency Offset based RF Fingerprinting for the Fake Base Station Detection," in *2019 IEEE 20th Wireless and Microwave Technology Conference (WAMICON)*, 8-9 April 2019 2019, pp. 1-6.

[3] A. Ali and G. Fischer, "Enabling Fake Base Station Detection through Sample-based Higher Order Noise Statistics," in *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, 1-3 July 2019 2019, pp. 695-700.

[4] S. Bowe, "BLS12-381: New zk-SNARK Elliptic Curve Construction," ed, 2017.

[5] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," Berlin, Heidelberg, 2004: *Springer Berlin Heidelberg, in Advances in Cryptology – CRYPTO 2004*, pp. 41-55.

[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," *presented at the Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques*, Berlin, Heidelberg, 2003.

[7] T. Fei and W. Wang, "LTE Is Vulnerable: Implementing Identity Spoofing and Denial-of-Service Attacks in LTE Networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 9-13 Dec. 2019 2019, pp. 1-6.

[8] D. Galindo and F. D. Garcia, "A Schnorr-Like Lightweight Identity-Based Signature Scheme," in *Progress in Cryptology – AFRICACRYPT 2009*, Berlin, Heidelberg, B. Preneel, Ed., 2009: Springer Berlin Heidelberg, pp. 135-148.

[9] C. Gentry and A. Silverberg, "Hierarchical ID-Based Cryptography," in *Advances in Cryptology — ASIACRYPT 2002*, Berlin, Heidelberg, Y. Zheng, Ed., 2002: Springer Berlin Heidelberg, pp. 548-566.

[10] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, "Insecure connection bootstrapping in cellular networks: the root of all evil," presented at the *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, Miami, Florida, 2019.

[11] K. W. Huang and H. M. Wang, "Identifying the Fake Base Station: A Location Based Approach," *IEEE Communications Letters*, vol. 22, no. 8, pp. 1604-1607, 2018.

[12] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)" *International journal of information security*, vol. 1, pp. 36-63, 2001.

[13] M. Khan, A. Ahmed, and A. R. Cheema, "Vulnerabilities of UMTS Access Domain Security Architecture," in *2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*,

6-8 Aug. 2008, pp. 350-355.

[14] T. Kim and R. Barbulescu, "Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case," Berlin, Heidelberg, 2016: Springer Berlin Heidelberg, in *Advances in Cryptology – CRYPTO 2016*.

[15] M. Kim, J. Park, D. Moon, J. Jang, Y. Kim, and J. Lee, "Long-Term Evolution Vulnerability Focusing on System Information Block Messages," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, 21-23 Oct.2020, pp. 837-842.

[16] W. Li, "Hacking Public Warning System in LTE Mobile Network," presented at the *Hack In The Box Security Conference, Amsterdam*, 2019.

[17] H. Li, S. Guo, K. Zheng, Z. Chen, Z. Zhang, and X. Du, "Security Analysis and Defense Strategy on Access Domain in 3G," in *2009 First International Conference on Information Science and Engineering*, 26-28 Dec. 2009, pp. 1851-1854.

[18] T. Looker, V. Kalos, A. Whitehead, and M. Lodder, "The BBS Signature Scheme," 6 October 2022.

[19] V. S. Miller, "Use of Elliptic Curves in Cryptography," Berlin, Heidelberg, 1986: Springer Berlin Heidelberg, in *Advances in Cryptology — CRYPTO '85 Proceedings*, pp. 417-426.

[20] Z. Muxiang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Transactions on Wireless Communications*, vol. 4, no. 2, pp. 734-742, 2005.

[21] U. Meyer and S. Wetzel, "A man-in-the-middle attack on UMTS," presented at the *Proceedings of the 3rd ACM workshop on Wireless security*, Philadelphia, PA, USA, 2004.

[22] M. Pannu, R. Bird, B. Gill, and K. Patel, "Investigating vulnerabilities in GSM security," in *2015 International Conference and Workshop on Computing and Communication (IEMCON)*, 15-17 Oct. 2015 2015, pp. 1-7.

[23] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[24] S. Steig, A. Aarnes, T. V. Do, and H. T. Nguyen, "A Network Based IMSI Catcher Detection," in *2016 6th International Conference on IT Convergence and Security (ICITCS)*, 26-26 Sept. 2016 2016, pp. 1-6.

[25] A. Singla, R. Behnia, S. R. Hussain, A. Yavuz, and E. Bertino, "Look Before You Leap: Secure Connection Bootstrapping for 5G Networks to Defend Against Fake Base-Stations," presented at the *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, Virtual Event, Hong Kong, 2021.

[26] A. B. Seyi, F. Jafaar, and R. Ruhl, "Securing the Authentication Process of LTE Base Stations," in *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 12-13 June 2020, pp. 1-6.

[27] M. Toorani and A. Beheshti, "Solutions to the GSM Security Weaknesses," in *2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies*, 16-19 Sept. 2008, pp. 576-581.

[28] *Technical Specification Group Services and System spects Study on 5G Security Enhancement against False Base Stations (FBS) (Release 17)*, TR33.809 R17 V0.11.0, 3GPP, Oct. 2020.

[29] C. Yu, S. Chen, and Z. Cai, "LTE Phone Number Catcher: A Practical Attack against Mobile Privacy," *Security and Communication Networks*, vol. 2019, 2019, Art no. 7425235.

A. A. Yavuz, A. Mudgerikar, A. Singla, I. Papapanagiotou, and E. Bertino, "Real-Time Digital Signatures for Time-Critical Networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2627–2639.

[作者簡介] Biography

孫沛靖為國立高雄科技大學電腦與通訊工程碩士，現任職於安華聯網科技股份有限公司，其研究領域為：行動通訊系統、IoT 安全、及資訊安全。

吳介騫為美國南加州大學電機工程博士，現為國立高雄科技大學電腦與通訊工程系副教授，其研究領域為：行動通訊系統、光纖網路、及資訊安全。