全球行動網路服務之匿名性認證機制

楊仁和　　溫柏旻
開南大學多媒體與行動商務學系
{ jenhoyang, m10108007}@mail.knu.edu.tw

摘要

本論文研究在全球行動網路下之漫遊服務的匿名性認證，因為先前學者所提出的相關匿名認證機制仍存在安全性的弱點，因此本文將提出全新的全球行動網路服務之匿名性認證機制。在我們的方法中，主基地台於認證時不需維護認證相關的資料表格，可降低設備負擔及搜尋成本。此外我們也利用互斥或及單向雜湊函數運算來降低計算量，因此本文所提出的方法將比先前相關研究更加安全以及有效率。

關鍵字：全球行動網路、行動漫遊服務、匿名性、交互認證。

Abstract

In this paper, we propose an anonymous authentication mechanism for roaming services in global mobility networks. Because the related works still have some security problems, we propose a new anonymity authentication mechanism for roaming services in global mobility networks. The proposed mechanism does not need to maintain a verification table, and thus the authentication time and the storage loads can be greatly reduced. In addition, we use exclusive-or operations and one-way hash functions to reduce the computation cost of the mobile device. According to the above reasons, the proposed authentication mechanism is securer and more efficient than the related works.

Keyword: Global mobility networks, mobile roaming service, anonymity, mutual authentication.

1. 前言

在 1997 年 Suzuki and Nakada [1]學者提出適用在全球通訊的分散式安全管理，在全球行動網路下提供行動用戶進行漫遊服務的認證機制，使行動用戶漫遊在外部基地台就能夠存取主基地台提供之服務，並與基地台間進行交互認證，以防止惡意攻擊。於 2003 年，Hwang and Chang [2]學者接著提出具匿名性的認證機制。隨著行動裝置的進步與行動網路服務的發展，企業也逐漸由電子商務轉型為行動商務，行動用戶能隨時隨地的存取各種資訊服務，為通訊界中快速增長的市場。然而行動裝置與行動服務提供者之間的認證有別於傳統的有線網路，是透過開放式的無線訊號，只要行動用戶在基地台電波的涵蓋範圍之下就能夠接聽到傳輸的資訊，該特性也使得行動裝置面臨資訊安全相關的潛在威脅。行動網路安全始終是一個重要的問題，由於無線電波的本質，只要在無線電波的廣播範圍內，任何人都能夠將已發送出去的資訊封包攔截[3]，因此使用無線通訊技術進行資料傳輸時，比有線網路更容易有被竊聽或未經授權的存取行為[4]。

近年來，已有許多的學者提出利用全球行動網路的認證機制來提供行動用戶漫遊相關服務[5]，且對於行動用戶的身分進行認證是非常重要的，以防止非法使用者存取資源。另外行動用戶越來越看重個人的隱私，達到匿名性認證將會是認證機制的重點之一[6, 7]。

在 2011 年，Mun 等學者[8]指出雖然已有學者強化 Wu 等學者[6]架構之弱點，不過仍有如未達成匿名性、合法用戶密碼洩漏、完備前向機密性不完全等弱點存在，於是 Mun 等學者提出強化的匿名認證機制，在交談金鑰的協議過程中使用許多單次隨

機亂數達到匿名性認證，並於協議金鑰部分使用橢圓曲線加密法(ECDH)[9]，使金鑰破解難度建立在解離散對數的問題上。但是我們發現 Mun 等學者架構仍有弱點存在，如行動用戶與外部基地台間使用的交談金鑰可能被竊取的威脅，因此我們在本文中的第二章節回顧 Mun 等學者之認證機制，並展現出其機制之弱點，接著於第三章提出我們的方法，並修正這些弱點，我們使用低運算成本的單向雜湊函數以及互斥或運算保護重要資訊，且主基地台不需要儲存行動用戶認證的相關資訊，能夠降低硬體負擔，減少搜尋成本。最後於第四章則提出安全性分析。

2. Mun 等學者之增強全球行動網路漫遊服務之安全匿名認證機制

本節將介紹 Mun 等學者[8]提出之增強全球行動網路漫遊服務之安全匿名認證機制。有三個參與者：行動用戶、外部基地台以及主基地台，且分為註冊、認證與協議交談金鑰及更新交談金鑰三個階段，其所使用的符號如表 1 所示：

表 1、Mun 等學者的方法之符號說明

符號	敘述
MU	行動用戶
FA	外部基地台
HA	主基地台
PW_x	角色 x 的密碼
ID_x	角色 x 的身分識別碼
$h(.)$	單向雜湊函數
N_x	角色 x 所產生的單次使用隨機亂數 N
$\|\|$	字串連接運算
$\oplus$	互斥或運算
f_k	用秘密金鑰 k 做訊息鑑別碼函數運算
K_{XY}	於角色 x 與 y 之間所使用的交談金鑰
E	橢圓曲線方程式
P	橢圓曲線方程式上的一點
$*$	橢圓曲線的乘法運算

註冊階段

步驟一、 行動用戶產生的單次隨機亂數 N_{MU} 後，與身分識別碼一同傳送給主基地台。

步驟二、 主基地台收到行動用戶的資訊後，產生單次隨機亂數 N_{HA} 並計算行動用戶密碼 $PW_{MU} = h(N_{MU} \| N_{HA})$以及 $r_{MU} = h(ID_{MU} \| PW_{MU}) \oplus ID_{HA}$。

步驟三、 主基地台將註冊完成資訊$\{ID_{HA}, N_{HA}, PW_{MU}, h(.), r_{MU}\}$ 回傳給行動用戶儲存。

認證與協議交談金鑰階段

步驟一、 行動用戶將完成註冊的$\{ID_{HA}, N_{HA}, r_{MU}\}$傳送給外部基地台，當外部基地台收到$\{ID_{HA}, N_{HA}, r_{MU}\}$後會將其儲存，作為之後交互認證使用，並產生隨機亂數 N_{FA}，將$\{ID_{FA}, N_{FA}, N_{HA}, r_{MU}\}$一起傳送給主基地台。

步驟二、 主基地台驗證行動用戶之身分，計算 $r'_{MU} = h(ID_{MU} \| PW_{MU}) \oplus ID_{HA}$ 並與收到的 r_{MU} 比較，假若行動用戶認證失敗，則拒絕提供服務給非法用戶。若比較結果相等，則認證成功且行動用戶為合法用戶。接著，主基地台計算 $P_{HA} = h(PW_{MU} \| N_{FA})$ 及 $S_{HA} = h(ID_{FA} \| N_{FA}) \oplus r_{MU} \oplus P_{HA}$ 後將$\{S_{HA}, P_{HA}\}$回傳給外部基地台。

步驟三、 外部基地台收到$\{S_{HA}, P_{HA}\}$，計算 $S'_{HA} = h(ID_{FA} \| N_{FA}) \oplus r_{MU} \oplus P_{HA}$ 並與收到的 S_{HA} 比較，以確認主基地台是否合法。如果比較結果不同，則認證流程終止。當結果相同，外部基地台計算 $S_{FA} = h(S_{HA} \| N_{FA} \| N_{HA})$後選擇隨機亂數$a$，使用 Elliptic Curve Diffie-Hellman (ECDH) [9]計算出在橢圓曲線方程式 E 上的一點 $a*P$，$a*P$ 可表示為 aP，後將$\{S_{FA}, aP, P_{FA}=(S_{HA} \| ID_{FA} \| N_{FA})\}$傳送給行動用戶。

步驟四、 行動用戶計算 $S'_{HA} = h(ID_{FA} \| N_{FA}) \oplus r_{MU} \oplus P_{HA}$，且與收到的 S_{HA} 比較。接著計算 $S'_{FA} = h(S_{HA} \| N_{FA} \| N_{HA})$，並與收到的 S_{FA}

比較是否相等，如比較結果皆相等，則行動用戶可以認證主基地台與外部基地台為合法的，否則流程終止。之後，行動用戶選擇隨機亂數 b 計算出橢圓曲線方程式 E 上的一點 $b*P$，$b*P$ 可表示為 bP 且 $aP*bP$ 可表示為 abP，行動用戶使用 aP 與 bP 計算出交談金鑰 $K_{MF} = h(abP)$，與 $S_{MF} = f_{KMF}(N_{FA} \| bP)$後，將$\{bP, S_{MF}\}$傳送給外部基地台。

步驟五、 外部基地台收到$\{bP, S_{MF}\}$後，使用 aP 與 bP 計算 $K_{MF} = h(abP)$，再計算 $S'_{MF} = f_{KMF}(N_{FA} \| bP)$，並與收到的 S_{MF} 比較，如果不相同那麼該 K_{MF} 於行動用戶與外部基地台間並不合法，則流程結束。若比較結果相等，則外部基地台可以認證行動用戶為合法的。

交談金鑰更新階段

步驟一、 行動用戶選擇新的隨機亂數 b_i，計算出 b_iP (i = 1, 2, …, n)將$\{b_iP\}$傳送給外部基地台。

步驟二、 外部基地台收到$\{b_iP\}$，選擇新的隨機亂數 a 並計算 a_iP (i = 1, 2, …, n)，產生新的 $K_{MFi} = h(a_ib_iP)$，計算 $S_{MFi} = f_{KMFi}(a_ib_iP \| a_{i-1}b_{i-1}P)$將$\{a_iP, S_{MFi}\}$傳送給行動用戶。

步驟三、 行動用戶收到$\{a_iP, S_{MFi}\}$，使用 a_iP 計算出新的 $K_{MFi} = h(a_ib_iP)$，再計算出 $S'_{MFi} = f_{KMFi}(a_ib_iP \| a_{i-1}b_{i-1}P)$，並與收到的 S_{MFi} 比較。若結果相等，則行動用戶使用新的 $K_{MFi} = h(a_ib_iP)$。若結果不同，則不使用此把 $K_{MFi} = h(a_ib_iP)$，並通知外部基地台與主基地台此結果。

根據以上步驟，我們在此提出 Mun 等學者機制[8]的弱點，他們的方法在認證與協議交談金鑰階段可能存在著非法用戶冒用合法行動用戶存取服務的可能性，說明如下。

離線資訊破解

於此節將呈現 Mun 等學者架構交談金鑰洩漏之弱點。首先，攻擊者於與行動用戶相同之外部基地台註冊完成後，可以在認證與協議交談金鑰階段之步驟一至四中，取得其他合法行動用戶的$\{ID_{HA}, N_{HA}, r_{MU}\}$、$\{ID_{FA}, N_{FA}\}$、$\{S_{HA}, P_{HA}\}$、$\{aP\}$和$\{bP\}$。攻擊者透過這些資訊可以計算出 $K_{MF} = h(abP)$，並計算出行動用戶回合交談金鑰 $S_{MF} = f_{KMF}(N_{FA} \| bP)$。為了解決上述弱點，我們將在下一章節提出我們的方法。

3. 我們的架構

本文所提出的方法分為行動用戶註冊與交互驗證兩個階段。三個主要參與者：行動用戶、外部基地台及主基地台。本方法所使用的符號如表 2。

表 2、我們的架構之符號說明

符號	敘述
MU	(Mobile User)行動用戶
FA	(Foreign Agent)外部基地台
HA	(Home Agent)主基地台
ID_a	角色 a 的身分識別碼
PWa	角色 a 的密碼
$h(.)$	單向雜湊函數
A_a	驗證角色 a 的資訊
N_x	角色 a 的大隨機亂數
$\oplus$	XOR 運算
$\|$	字串連結運算
X_a	角色 a 的私密金鑰
T	時間戳記
$A \stackrel{?}{=} B$	比較 A、B 是否相等

行動用戶註冊階段

在這個階段中，行動用戶 MU 透過安全通道向主基地台 HA 註冊，以取得身分認證相關資訊，詳細說明如下：

步驟一、 行動用戶將自身的身分識別碼 ID_{MU} 以及密碼 PW_{MU} 傳送給主基地台。

步驟二、 主基地台產生隨機亂數 N_{HA}，計算 $SID = h(ID_{MU} \| N_{HA})$ 及 $r_{MU} = h(SID \| X_{HA}) \oplus PW_{MU}$，將$\{SID, r_{MU}\}$透過安全通道(Secure channel)傳送回去給行動用戶。

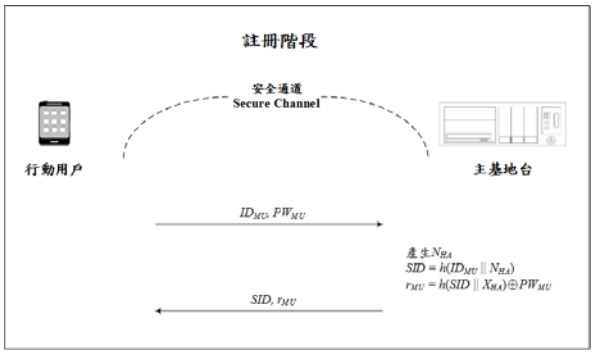

圖 1、行動用戶註冊階段

交互認證階段

此階段中，行動用戶已於外部基地台(FA)服務範圍內漫遊，外部基地台將行動用戶認證資訊轉送至主基地台並透過主基地台的協助來認證行動用戶身分，同時行動用戶也可以透過主基地台來認證外部基地台，步驟詳細說明如其下。

步驟一、 行動用戶輸入密碼 PW_{MU}，計算 $h(SID \| X_{HA}) = r_{MU} \oplus PW_{MU}$，產生亂數 N_{MU} 和時間戳記 T，計算 $A_{MU} = h(h(SID \| X_{HA}) \| T) \oplus N_{MU}$ 與 $C_{MU} = h(SID \| N_{MU}) \oplus ID_{MU}$，並將$\{SID, A_{MU}, C_{MU}, T\}$傳送給外部基地台。

步驟二、 外部基地台收到$\{SID, A_{MU}, C_{MU}, T\}$，將$\{SID, A_{MU}, C_{MU}, T, ID_{FA}\}$轉送至主基地台。

步驟三、 主基地台收到$\{SID, A_{MU}, C_{MU}, T, ID_{FA}\}$後為驗證用戶身分，計算 $N_{MU} = A_{MU} \oplus h(h(SID \| X_{HA}) \| T)$、$ID_{MU} = C_{MU} \oplus h(SID \| N_{MU})$與 $SID' = h(ID_{MU} \| N_{HA})$。比較 SID' 是否與 SID 相等。如果相等則 SID 為真，且與 ID_{MU} 為同一組，A_{MU} 與 C_{MU} 於傳送過程中沒有被竄改，行動用戶是合法用戶。

步驟四、 主基地台計算出 $A_{HA} = h(SID \| X_{HA}) \oplus h(ID_{FA} \| ID_{MU})$與 $C_{HA} = h(h(ID_{FA} \| SID) \| ID_{FA})$以及交談金鑰 $SK = h(ID_{FA} \| SID \| N_{MU})$和 $C_{SK} = h(SK \| h(ID_{FA} \| ID_{MU}))$之後將$\{A_{MU}, C_{HA}, C_{SK}\}$傳送給外部基地台。

步驟五、 外部基地台收到$\{A_{MU}, C_{HA}, C_{SK}\}$後，將$\{A_{MU}, C_{HA}, C_{SK}\}$回傳行動用戶。

步驟六、 行動用戶收到$\{A_{MU}, C_{HA}, C_{SK}\}$後計算 $h(ID_{FA} \| ID_{MU}) = A_{HA} \oplus h(SID \| X_{HA})$，接著計算 $C'_{HA} = h(h(ID_{FA} \| SID) \| ID_{FA})$，並比較 C'_{HA} 與 C_{HA} 是否相等，若相等則主基地台是有效的，且外部基地台也可以被認證。

步驟七、 接著計算 $SK = h(ID_{FA} \| SID \| N_{MU})$以及 $C'_{SK} = h(SK \| h(ID_{FA} \| ID_{MU}))$，之後核對 C'_{SK} 與 C_{SK} 是否相等，若相等則完成交互認證，並產生出行動用戶與主基地台之間加解密的回合金鑰 SK。

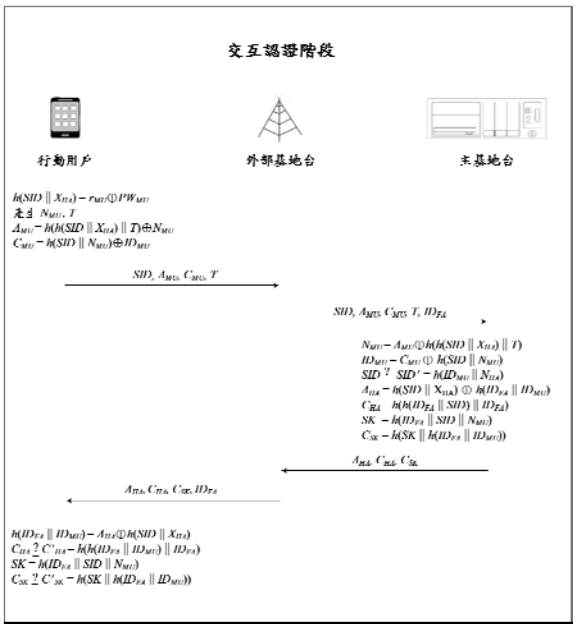

圖 2、交互認證階段

根據上述步驟，主基地台不需要將 SID、行動用戶身分識別碼或是其他相關資訊另外儲存在資料庫中。

4. 討論與分析

在此節中，我們對本文所提出的方法做安全性的分析，以下我們提出幾種攻擊方法來分析安全性

以及與 Mun 等學者的架構作計算成本之比較。安全性分析如下。

外部攻擊(Outsider attack)

假設有一攻擊者想要計算主基地台之秘密金鑰 X_{HA}，攻擊者可以從行動用戶傳送給外部基地台的$\{SID, A_{MU}, C_{MU}, T\}$中，擷取 SID, A_{MU} 做分析。假設一，若攻擊者想計算 $SID = h(ID_{MU} \| N_{HA})$，那麼攻擊者需要 ID_{MU} 及 N_{HA}，但於認證過程中並不會傳送 N_{HA}，因此攻擊者無法計算出 SID。假設二，若攻擊者想分析 $A_{MU} = h(h(SID \| X_{HA}) \| T) \oplus N_{MU}$，首先得知道 N_{MU} 才能夠和取得的 A_{MU} 一起運算得到 $h(h(SID \| X_{HA}) \| T)$，再經過分析得到 X_{HA}，但認證過程中並不會明文傳送 N_{MU}，因此攻擊者無法取得，即使攻擊者取得 N_{MU}，X_{HA} 也有單向雜湊函數所保護，因此攻擊者無法計算出主基地台的私密金鑰 X_{HA}。根據上述的推斷可以顯示出我們的方法能夠抵檔攻擊者發出的外部攻擊。

內部攻擊(Insider attack)

假設有 N 個惡意的行動用戶企圖逃避主基地台認證，並試圖計算主基地台之秘密金鑰 X_{HA}，當攻擊者取得 $A_{MU} = h(h(SID \| X_{HA}) \| T) \oplus N_{MU}$，但是 X_{HA} 使用了單向雜湊函數保護，因此即使利用 SID、T 及 N_{MU} 想要計算出來是不可能的。因此根據上述分析，我們的方法可以防止內部攻擊。

偽裝攻擊(Impersonation attack)

假設有一攻擊者想要偽裝成合法的行動用戶，並擷取行動用戶與外部基地台以及外部基地台與主基地台之間傳送的$\{SID, A_{MU}, C_{MU}, T, ID_{FA}\}$，來偽裝成是一個合法行動用戶嘗試騙取主基地台的認證，但是 A_{MU} 內包含有時間戳記，一但時戳過期即無法通過認證且 SID、A_{MU} 和 C_{MU} 皆有單向雜湊函數所保護，攻擊者無法竄改其內容或計算出更多的訊息，也因此攻擊者是無法偽裝成合法用戶的。根據上述之原因，可以證明我們的方法能夠防止攻擊者的偽裝攻擊。

重送攻擊(Replay attack)

假設有一攻擊者想要透過攔截合法使用者交互認證階段傳輸的資訊，並且透過將資訊重送來達到騙取服務或者破解相關資訊的目的。以上述流程來看，若攻擊者竊取 $A_{MU} = h(h(SID \| X_{HA}) \| T) \oplus N_{MU}$ 與 $C_{MU} = h(SID \| N_{MU}) \oplus ID_{MU}$，$X_{HA}$ 皆有單向雜湊函數保護且僅有主基地台知道，N_{MU} 並未公開傳輸且僅有行動用戶知道、主基地台可解出，且若直接將$\{A_{MU}, C_{MU}\}$重新傳送給外部基地台，將會因時戳過期而被捨棄，而修改 A_{MU} 則會使與 SID 無法相互認證，讓我們判定為攻擊者所傳送。根據上述的推斷可以顯示出我們的方法能夠抵檔攻擊者發出的重送攻擊。

驗證表竊取攻擊(Stolen-Verifier attack)

現今行動用戶的認證的主體主要是行動裝置本身或是 SIM 卡，在這種情況下當手機遺失被撿取，合法用戶即有被冒用的風險，我們假設有一合法使用者不小心遺失其手機，而被攻擊者拾獲，當攻擊者想要存取服務時，由於不知道合法用戶之密碼，因此無法通過基地台認證，進而存取行動漫遊服務的，且主基地台與外部基地台並不會存放驗證表，當攻擊者攻擊主基地台時無法竊取行動用戶驗證過程的相關資訊，根據上述理由，我們的方法能夠抵擋驗證表竊取攻擊。

計算成本分析

在本節中，我們將分析 Mun 等學者的方法與本文所提出的方法之計算成本。表 3 顯示出行動用戶與主基地台方面之計算成本，根據表 3 可以顯示出我們所提出的方法相對於 Mun 等學者的方法，其計算成本降低許多。我們的方法並無使用橢圓曲線加密法或是非對稱式加密法，而是採用運算量較低的互斥或運算以及單向雜湊函數來保護驗證資訊，所以我們的方法更加的有效率。

表 3、兩種方法之計算成本比較

方法 / 參與者	MUN 等學者的方法	我們的方法
行動用戶	5*Hash* + 2*XOR* + 1*Asym* + 2*ECDH*	5*Hash* + 4*XOR*
外部基地台	4*Hash* + 2*XOR* + 1*Asym* + 2*ECDH*	12*Hash* + 4*XOR*
主基地台	5*Hash* + 3*XOR*	13*Hash* + 4*XOR*
總計	14*Hash* + 7*XOR* +2*Asym.* + 4*ECDH*	30*Hash* + 12*XOR*

Asym:非對稱式加密法
ECDH:橢圓曲線加密法
Hash:單向雜湊函數
XOR:互斥或運算

5. 結論

於本篇論文中，我們提出了一個全新的行動網路服務匿名性認證機制，主基地台不需要儲存行動用戶認證過程的驗證表，能降低設備負擔，也能夠避免驗證表被竊取的風險。行動用戶於漫遊時，外部基地台並不會直接取得用互相關資訊，能夠保障行動用戶之隱私，且我們的方法有著低計算成本的優勢，因為它不需要作橢圓曲線系統或公開金鑰系統的加解密運算。因此相較於先前學者所提出的相關方法，本文所提出之方法更符合現實環境且更有效率，可應用於網路服務提供者所提供之服務，且認證方式更適用於行動裝置之使用。

參考文獻

[1] S. Suzuki, and K. Nakada, “An authentication technique based on distributed security management for the global mobility network”, *IEEE Journal on Selected Areas in Communications.* , Vol. 15, No. 8, pp. 1608-1617, Oct. 1997.

[2] K. F. Hwang and C. C. Chang, “A self-encryption mechanism for authentication of roaming and teleconference services”, *IEEE Transactions on Wireless Communications*, Vol. 2, No. 2, pp. 400-407, Mar. 2003.

[3] J. Zhu and J. Ma, “A new authentication scheme with anonymity for wireless environments”, *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 1, pp. 231-235, Feb. 2004.

[4] X. Yi, C. K. Siew, and C. H. Tan, “A secure and efficient conference scheme for mobile communications”, *IEEE Transactions on Vehicular Technology*, Vol. 52, No. 4, pp. 784-793, Jul. 2003.

[5] T. F. Lee and T. Hwang, “Provably secure and efficient authentication techniques for the global mobility network”, *The Journal of Systems and Software*, Vol. 84, No. 10, pp. 1717-1725, Oct. 2011.

[6] C. C. Wu, W. B. Lee and W. J. Tsaur, “A secure authentication scheme with anonymity for wireless communications”, *IEEE Communications Letters*, Vol. 12, No. 10, pp. 722-723, Oct. 2008.

[7] P. Zeng, Z. F. Cao, K. K. Choo and S. B. Wang, “On the anonymity of some authentication schemes for wireless communications”, *IEEE Communications Letters*, Vol. 13, No. 3, pp. 170-171, Mar. 2009.

[8] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun and H. H. Choi, “Enhanced secure anonymous authentication scheme for roaming service in global mobility networks”, *Mathematical and Computer modeling*, Vol. 55, No. 1–2, pp. 214-222, Jan. 2012.

[9] D. Hankerson, A. J. Menezes and S. Vanstone, “Guide to elliptic curve cryptography”, Springer-Verlag Inc., Berlin, Germany, 2004.