Regular Paper

Communications of the CCISA
Vol. 28 No. 4 Nov. 2022

# 適用於 5G 智慧救護車之植基於切比雪夫混沌映射聯合匿名身分管理協定

林子煒 [1*]
[1] 逢甲大學創能學院、[1] 逢甲大學資訊總處資訊安全中心
[1]tweilin@fcu.edu.tw

## 摘要

5G 網路為最新的行動通訊標準，而 5G 網路與物聯網結合，可提供即時、隨選、隨時連結、可重組計算的網路應用服務，而 5G-IoT 環境已被視為下個世代的智慧醫療健康照護的重要元素。緊急醫療照護系統已成為所有專業都在一台救護車裡的複雜系統，需要在第一時間對病患進行及時處置與反應，並在病患到院前與目的醫院聯繫，以便病患到院時可以接受即時的適當處置。醫療資料隱私，包含病患的身分，是醫療健康照護系統中至關重要的議題之一，一旦遭到破壞，不僅造成醫療院所的損失，還會對病患造成難以估計的損害。本研究設計一個適用於 5G 智慧救護車的聯合匿名身分管理協定，不僅可以允許救護車與目的醫院間安全地傳輸資料，亦可藉由匿名機制保護病患身分。

**關鍵詞：5G 網路、物聯網、緊急醫療照護系統、智慧救護車、聯合匿名身分管理**

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 28 No. 4 Nov. 2022

# Federal Anonymous Identity Management for 5G-Based Smart Ambulance based on Chebyshev Chaotic Maps

Tzu-Wei Lin[1*]
[1]iSchool, Feng Chia University, [1]Information Security Office, Office of Information Technology, Feng Chia University
[1]tweilin@fcu.edu.tw

## Abstract

5G is the newest mobile communication standard, and 5G can be applied in Internet of Things environment to provide real time, on-demand, linkable, and re-computable applications. 5G-IoT has become one of the important parts of next generation smart medical healthcare services. Emergency medical system (EMS) has already become a complex system which content all professionals in an ambulance. EMS is required to take immediately reaction and response to patients at accident cites, and EMS staff has to communicate with destinate hospital while transporting patients. By doing so, patients can have proper treatment once arriving destination hospital. Privacy of medical data, including patients' personal data, is an important issue in medical healthcare system. Otherwise, damage to hospital and patient will be caused seriously if privacy is compromised. This paper designs a federal anonymous identity management for 5G-based smart ambulance based on Chebyshev chaotic maps which provides secure communication between ambulance and destination hospital and privacy preservation of patients' identity through anonymity mechanism.

**Keywords: 5G, IoT, Emergency Medical System, Smart Ambulance, Federal Anonymous Identity Management**

# 壹、前言

5G 網路已是最新的行動通訊標準，提供高速傳輸、大容量與可延展性的網路服務[4][5]。5G 網路亦可連結虛擬網路系統，連結至擁有人工智慧 (Artificial Intelligence，以下簡稱為 AI) 技術的雲端運算服務，進行不同需求的運算[3]。物聯網 (Internet of things，以下簡稱為 IoT) 乃是利用數種科技與網路連結網路中的物與人，形成一個「物物相連」的概念，並可讓設備之間彼此分享及傳送訊息。物聯網已被應用於各種領域，諸如工業、物流、智慧環境、醫療健康照護等等。結合 5G 與 IoT 的網路環境 (即 5G-IoT 環境)，可提供即時、隨選、隨時連結、可重組計算的網路應用服務，而相關應用正如雨後春筍般快速成長。然而，5G-IoT 環境中傳送資訊的安全與隱私議題，亦逐漸受到重視。

現今醫療健康照護系統正面臨諸多挑戰，而 5G-IoT 環境被預期能有效改善服務品質、資源最佳化等，因此 5G-IoT 環境已被視為下個世代的智慧醫療健康照護的重要元素，包括緊急醫療照護系統[4]。緊急醫療照護系統 (Emergency Medical System，以下簡稱為 EMS) 已今非昔比，如今已成為所有專業都在一台救護車裡的複雜系統[6]。EMS 面對各種傷患，包含車禍、天然災害、恐怖攻擊、流行性傳染病 (例如 COVID-19)，都需要在第一時間對病患進行及時處置與反應，並在病患到院前與目的醫院聯繫，以便病患到院時，目的醫院的醫療團隊可以即時做出接續的適當處置。5G-IoT 環境預期可讓救護車快速傳輸即時救護資料及病患生理資訊給目的醫院。然而，醫療資料隱私，包含病患的身分，是醫療健康照護系統中至關重要的議題之一，一旦遭到破壞，不僅造成醫療院所的損失，還會對病患造成難以估計的損害。

本研究設計一個適用於 5G 智慧救護車的聯合匿名身分管理協定，不僅可以允許救護車與目的醫院間安全地傳輸資料，亦可藉由匿名機制保護病患身分。

# 貳、文獻探討

本研究針對 EMS、車聯網於 EMS、以身分為基底之密碼系統及切比雪夫混沌映射進行文獻回顧與探討。

## 2.1 EMS

EMS 已成為所有專業都在一台救護車裡的複雜系統[6]，需要第一時間對病患進行及時處置與反應，並在病患到院前與目的醫院聯繫，目的醫院的醫療團隊即可在病患到院時做適當處置。為了提升相關效率，許多科技技術亦被應用於 EMS，例如千葉大學醫學院中田教授成立的「Smart119 公司」，利用語音辨識，將通話語音轉成文字，讓急救人員能直接觀看內容，減少來回溝通時間，讓搬送病患花費時間比起以往減少八成，有

效提高急救效率[27]。

### 2.2 車聯網於 EMS

車聯網 (Vehicular ad hoc networks，VANETs) 有助於提升交通安全、交通管理、意外防止及即時車輛定位等[2]。車聯網為一種自組無線隨選網路系統，其元件包含了車上單元 (Onboard Unit，OBU)、路側單元 (Road Side Unit，RSU) 以及可信任單位 (Trusted Authority，TA) [1][2][12]。EMS 已成為所有專業都在一台救護車裡的複雜系統[6]，面對各種傷患都需要在第一時間對病患進行及時處置與反應，並在病患到院前與目的醫院聯繫，以便病患到院時，目的醫院的醫療團隊可以即時做出接續的適當處置。美國加州緊急醫療服務機構在 2017 年發展了一套模型以達成 EMS 與健康資訊系統 (Health Information Exchange，HIE) 以改善到院前處置與決策及其紀錄[16]。5G-IoT 結合車聯網環境預期將可達到上述目標，並讓救護車快速傳輸即時救護資料及病患生理資訊給目的醫院[15]。

### 2.3 以身分為基底之密碼系統

學者 Shamir 於 1985 提出以身分為基底之密碼系統 (Identity-Based Cryptosystem，ID-based Cryptosystem)，其概念為利用使用者的可識別公開資訊作為公鑰[18]。2002 年，學者 Gentry 等人提出階層式以身分為基底之密碼系統 (Hierarchical ID-based Cryptography， 以下簡稱為 HIDC)，該方法降低私鑰產生中心的負荷，亦降低金鑰託管的風險[8]，而 Yan 等人認為 HIDC 適用於雲端運算環境，並改善其方法以因應聯合身分管理議題[23]。近十年亦已有許多研究提出適用於車聯網、物聯網或雲端運算環境之 HIDC 聯合身分管理機制[7][17][19][20]，但尚未有針對醫療健康照護環境或 5G-IoT 環境之 HIDC 聯合身分管理機制之相關研究。

### 2.4 切比雪夫混沌映射

混沌系統 (Chaotic System) 擁有對初始值敏感、偽亂數及遍歷性 (Ergodicity) 的特性，而這些特性與密碼學的分散性 (Diffusion) 與混淆性 (Confusion) 有相似之處[24][25]。混沌映射密碼系統已被多位學者應用與討論[10][11][13][14][21][24][25]。切比雪夫混沌映射(Chebyshev Chaotic Maps)的數學定義如下[13][14][24][25]。

定義 1：切比雪夫多項式 (Chebyshev Polynomial)。定義 $n$ 為正整數，$x$ 為區間[−1, 1]裡的變量，切比雪夫多項式在自由度 (Degree) $n$ 情形下，可表示為：

$$T_n(x) = cos(ncos^{-1}(x)) \quad (1)$$

定義 2：在$n \geq 2$的情形下，切比雪夫多項式$T_n(x)$的遞迴關係可表示為方程式(2)。$n = 0$ 時，$T_0(x) = 1$；$n = 1$ 時，$T_1(x) = x$。

$$T_n(x) = 2xT_{n-1}(x)-T_{n-2}(x) \quad (2)$$

定義 3：$s$ 與 $r$ 屬於整數，且 $s$ 在區間-1 到 1 之間，切比雪夫多項式$T_n(x)$的半群性 (Semi-Group Property) 可表示為：

$$T_r(T_s(x)) = T_{rs}(x) = T_s(T_r(x)) \quad (3)$$

定義 4：學者 Zhang 證明 $x$ 在區間$(-\infty, +\infty)$的情形下，仍可符合半群性[26]。本研究使用學者 Zhang[26]提出的切比雪夫多項式，其定義如方程式(4)，其中$n \geq 2$、$x \in (-\infty, +\infty)$且 $N$ 為大質數。

$$T_n(x) = (2xT_{n-1}(x)-T_{n-2}(x)) \bmod N \quad (4)$$

其半群性可表示為：

$$T_r(T_s(x)) \bmod N = T_{rs}(x) \bmod N = T_s(T_r(x)) \bmod N \quad (5)$$

定義 5：基於混沌映射之離散對數問題 (Chaotic Maps-Based Discrete Logarithm Problem，以下簡稱為 CMDLP)。即使知道 $x$ 與 $y$，計算上很難從$T_n(x) \bmod N = y$得到 $n$。

定義 6：基於混沌映射之 Diffie-Hellman 問題 (Chaotic Maps-Based Diffie-Hellman Problem，以下簡稱為 CMDHP)。即使知道 $x$、$T_r(x) \bmod N$ 與$T_s(x) \bmod N$ $y$，計算上很難得到$T_{rs}(x) \bmod N$。

## 參、方法

本研究提出適用於 5G 智慧救護車之植基於切比雪夫混沌映射聯合匿名身分管理協定，包含使用者 $U_i$ 與伺服器 $S_j$，並有五個階段：初始化階段、路側單元註冊階段、車上單元註冊階段、雙向驗證與金鑰協議階段及匿名分配階段。表一為本研究提出之方法所使用之符號表。

### 3.1 初始化階段

醫院伺服器於初始化階段決定系統公開參數與私密參數，詳細步驟如下所述。

步驟一：醫療憑證中心核發憑證$Cert_{HCA \rightarrow HS}$給醫院伺服器$HS$。

步驟二：醫院伺服器$HS$產生秘密參數$hs_0 \in Z_p^*$、大質數$p$及隨機亂數$x \in (-\infty, +\infty)$並計算，其方程式為：

$$B_0 = T_{hs_0}(x) \bmod p \quad (6)$$

步驟三：醫院伺服器$HS$決定對稱式加密演算法$E_k(.)$、對稱式解密演算法$D_k(.)$、抗碰撞單向雜湊函數$(H_0(.), H_1(.), H_2(.))$及抗碰撞單向混沌雜湊函數$h_k(.)$。

步驟四：醫院伺服器 *HS* 產生公開參數$\{B_0, p, x, H_0(.), H_1(.), H_2(.), h_k(.), E_k(.), D_k(.)\}$與私密參數$hs_0$。

表一：符號表

| 符號 | 定義 |
|---|---|
| $RID_i$ | 路側單元$RSU_i$的識別符(Identity)。 |
| $OID_{ij}$ | 車上單元$OBU_{ij}$的識別符。 |
| $aOID_{ij}$ | 車上單元$OBU_{ij}$的匿名識別符。 |
| $k$ | 加解密金鑰 |
| $sk_{RSU_i \leftrightarrow OBU_{ij}}$ | 路側單元與車上單元的交談金鑰。 |
| $H_0(.),\ H_1(.),\ H_2(.)$ | 抗碰撞單向雜湊函數。 |
| $E_k(.)/D_k(.)$ | 對稱式加/解密演算法。 |
| $p$ | 大質數。 |
| $x,\ e_i,\ d_i$ | 隨機整數。 |
| $h_k(.)$ | 抗碰撞單向混沌雜湊函數。 |
| $\oplus$ | 互斥或運算。 |
| $MAC_A$ | $A$ 的訊息驗證碼。 |
| $Cert_{A \to S}$ | $A$ 發給 $S$ 的憑證。 |

### 3.2 路側單元註冊階段

路側單元$RSU_i$於此階段向醫院伺服器 *HS* 註冊為合法身分，詳細步驟如下所述。

步驟一：路側單元$RSU_i$選擇識別符$RID_i$，並傳送給醫院伺服器*HS*。

步驟二：醫院伺服器*HS*計算$A_i$與$B_i$如下列方程式：

$$A_i = H_0(RID_i) \tag{7}$$

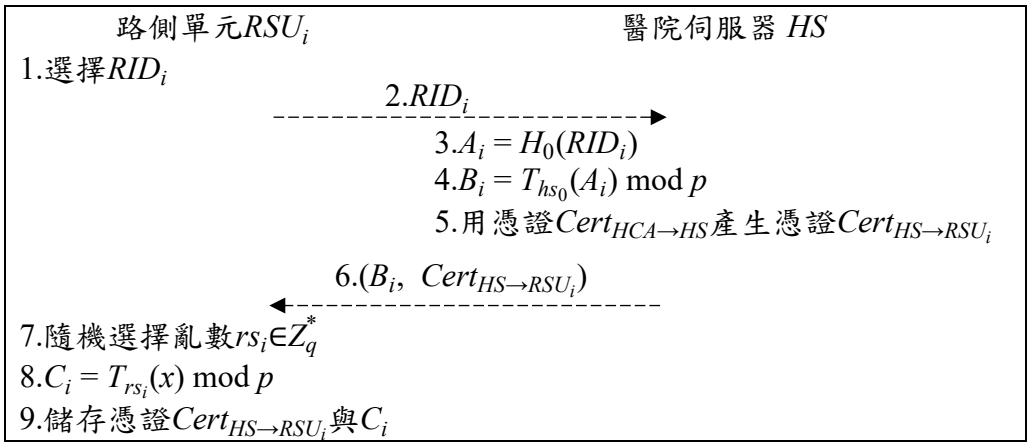
$$B_i = T_{hs_0}(A_i) \bmod p \tag{8}$$

步驟三：醫院伺服器 *HS* 用憑證$Cert_{HCA \to HS}$產生憑證$Cert_{HS \to RSU_i}$，並將$(B_i, Cert_{HS \to RSU_i})$傳送給路側單元$RSU_i$。

步驟四：路側單元$RSU_i$隨機產生$rs_i \in Z_q^*$並利用以下方程式計算$C_i$後，儲存憑證$Cert_{HS \to RSU_i}$與$C_i$。

$$C_i = T_{rs_i}(x) \bmod p \tag{9}$$

圖一為路側單元註冊階段之流程圖。




圖一：路側單元註冊階段

### 3.3 車上單元註冊階段

車上單元$OBU_{ij}$於此階段向路側單元$RSU_i$註冊為合法身分，詳細步驟如下所述。

步驟一：車上單元$OBU_{ij}$選擇識別符$OID_{ij}$，隨機選擇亂數隨機選擇亂數$os_{ij} \in Z_q^*$後，計算$D_{ij}$並傳送($OID_{ij}$, $D_{ij}$)給路側單元$RSU_i$。

$$D_{ij} = T_{os_{ij}}(x) \bmod p \tag{10}$$

步驟二：路側單元$RSU_i$計算$E_{ij}$與$F_{ij}$如下列方程式：

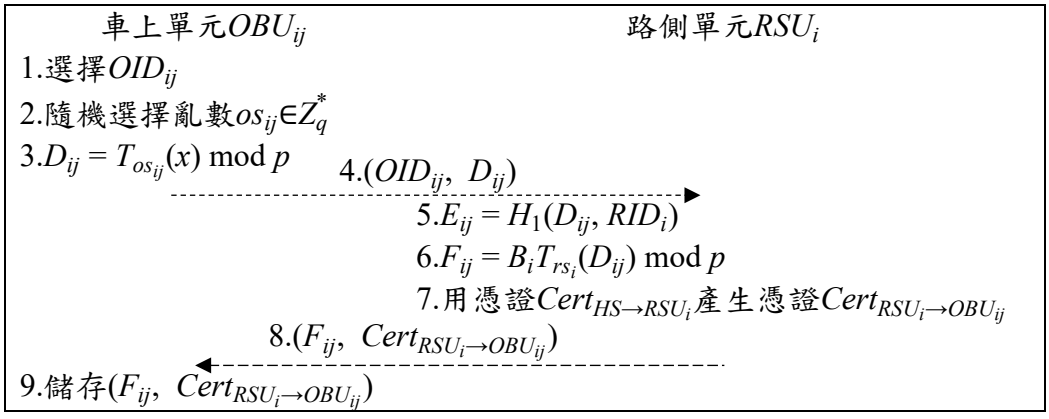
$$E_{ij} = H_1(D_{ij}, RID_i) \tag{11}$$

$$F_{ij} = B_i T_{rs_i}(D_{ij}) \bmod p \tag{12}$$

步驟三：路側單元$RSU_i$用憑證$Cert_{HS \to RSU_i}$產生憑證$Cert_{RSU_i \to OBU_{ij}}$，並將($F_{ij}$, $Cert_{RSU_i \to OBU_{ij}}$)傳送給車上單元$OBU_{ij}$。

步驟四：車上單元$OBU_{ij}$儲存憑證$Cert_{RSU_i \to OBU_{ij}}$與$F_{ij}$。

圖二為車上單元註冊階段之流程圖。




圖二：車上單元註冊階段

### 3.4 雙向驗證與金鑰協議階段

車上單元$OBU_{ij}$與路側單元$RSU_i$於此階段進行雙向驗證並建立交談金鑰，詳細步驟如下所述。

步驟一：車上單元$OBU_{ij}$隨機選擇亂數隨機選擇亂數$a_{ij} \in Z_q^*$後，計算$\mu_{ij}$與$C_i$並傳送($C_i$, $OID_{ij}$)給路側單元$RSU_i$。

$$\mu_{ij} = T_{os_{ij}}(a_{ij}) \bmod p \tag{13}$$

$$C_i = (T_{e_i}(\mu_{ij} \| a_{ij} \| Cert_{RSU_i \to OBU_{ij}}) \bmod p) P_i \tag{14}$$

步驟二：路側單元$RSU_i$利用$P_i$將$C_i$解密如下列方程式並驗證憑證$Cert_{RSU_i \to OBU_{ij}}$：

$$(\mu_{ij} \| a_{ij} \| Cert_{RSU_i \to OBU_{ij}}) = (T_{d_i}(C_i) \bmod p)/P_i \tag{15}$$

步驟三：當憑證$Cert_{RSU_i \to OBU_{ij}}$驗證成功，路側單元$RSU_i$利用$a_{ij}$計算$\omega_i$與交談金鑰$sk_{RSU_i \leftrightarrow OBU_{ij}}$如方程式：

$$\omega_i = T_{rs_i}(a_{ij}) \bmod p \tag{16}$$

$$sk_{RSU_i \leftrightarrow OBU_{ij}} = H_2(T_{rs_i}(\mu_{ij}) \bmod p) \tag{17}$$

步驟四：路側單元$RSU_i$計算($A_i$, $E_{ij}$, $K$)後，利用前述結果計算$MAC_{RSU_i}$並傳送($MAC_{RSU_i}$, $\omega_i$)給車上單元$OBU_{ij}$。

$$A_i = H_0(RID_i) \tag{18}$$

$$E_{ij} = H_1(D_{ij}, RID_i) \tag{19}$$

$$K = (A_i \| Q_0) \oplus (E_{ij} \| B_i) \oplus (sk_{RSU_i \leftrightarrow OBU_{ij}} \| \omega_i) \tag{20}$$

$$MAC_{RSU_i} = h_K(A_i, E_{ij}, \mu_{ij}) \tag{21}$$

步驟五：車上單元$OBU_{ij}$利用$\omega_i$計算$sk'_{RSU_i \leftrightarrow OBU_{ij}}$後，再計算$K'$，之後驗證$MAC_{RSU_i}$的正確性，若正確則進行下一步，否則終止此階段。

$$sk'_{RSU_i \leftrightarrow OBU_{ij}} = H_2(T_{os_{ij}}(\omega_i) \bmod p) \tag{22}$$

$$K' = (A_i \| Q_0) \oplus (E_{ij} \| B_i) \oplus (sk'_{RSU_i \leftrightarrow OBU_{ij}} \| \omega_i) \tag{23}$$

$$h_K(A_i, E_{ij}, \mu_{ij}) \stackrel{?}{=} MAC_{RSU_i} \tag{24}$$

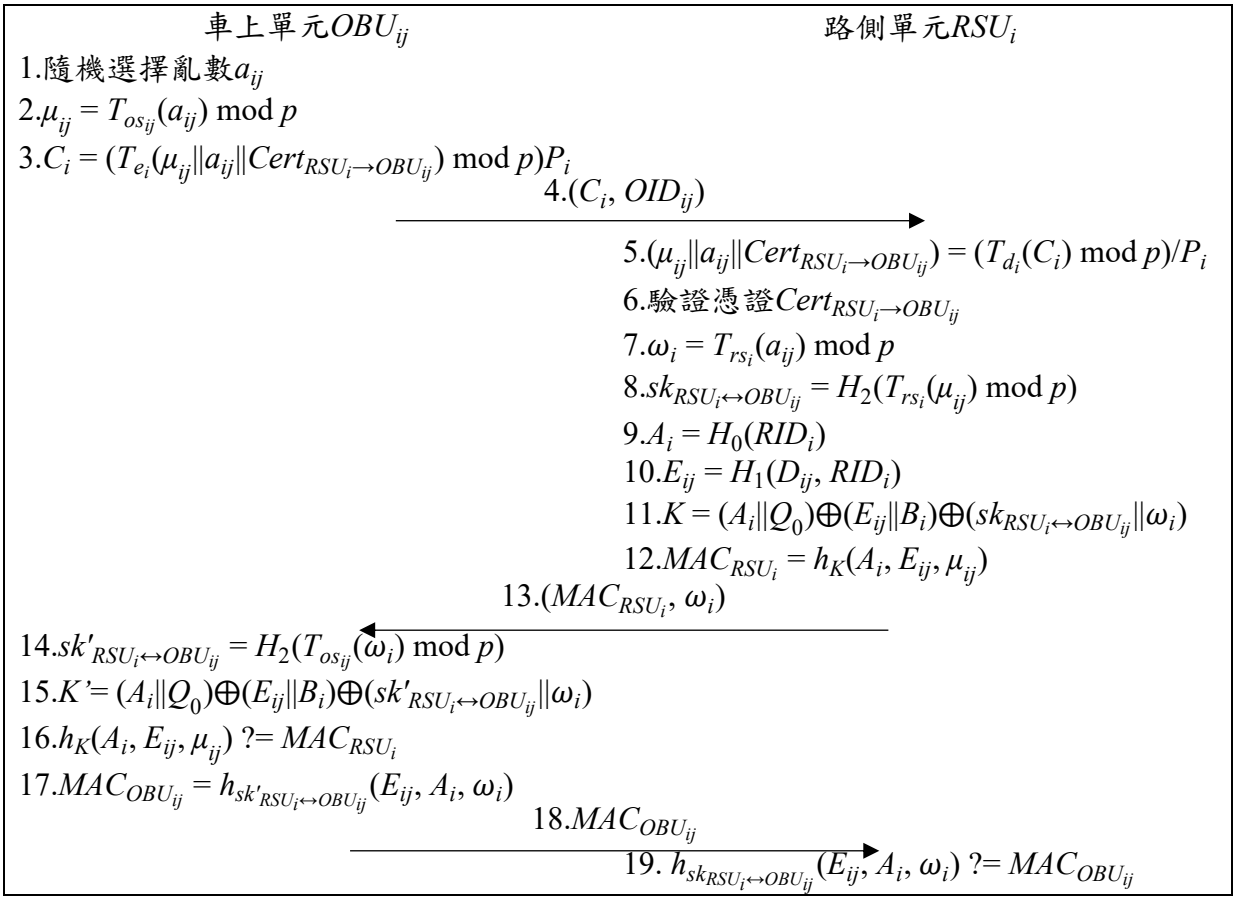
步驟六：車上單元$OBU_{ij}$計算$MAC_{OBU_{ij}}$後傳給路側單元$RSU_i$。

$$MAC_{OBU_{ij}} = h_{sk'_{RSU_i \leftrightarrow OBU_{ij}}}(E_{ij}, A_i, \omega_i) \tag{25}$$

步驟七：路側單元$RSU_i$驗證$MAC_{OBU_{ij}}$的正確性，若正確則確定$sk_{RSU_i \leftrightarrow OBU_{ij}}$為本次的交談金鑰，否則終止此階段。

$$h_{sk_{RSU_i \leftrightarrow OBU_{ij}}}(E_{ij}, A_i, \omega_i) \stackrel{?}{=} MAC_{OBU_{ij}} \tag{26}$$

圖三為雙向驗證與金鑰協議階段之流程圖。




圖三：雙向驗證與金鑰協議階段

### 3.5 匿名分配階段

路側單元$RSU_i$於此階段分配匿名給車上單元$OBU_{ij}$，詳細步驟如下所述。

步驟一：路側單元$RSU_i$隨機選擇亂數$t_i$並計算$aOID_{ij}$後傳給車上單元$OBU_{ij}$。

$$aOID_{ij} = E_{sk_{RSU_i \leftrightarrow OBU_{ij}}}(OID_{ij}||t_i) \tag{27}$$

步驟二：車上單元$OBU_{ij}$計算$P_{aOID_{ij}}$與$Q_{aOID_{ij}}$後，回傳$Q_{aOID_{ij}}$給路側單元$RSU_i$。

$$P_{aOID_{ij}} = H_0(RID_i||aOID_{ij}) \tag{28}$$

$$Q_{aOID_{ij}} = E_{sk_{RSU_i \leftrightarrow OBU_{ij}}}(RID_i||P_{aCID_{ij}}) \tag{29}$$

步驟三：路側單元$RSU_i$用交談金鑰$sk_{RSU_i \leftrightarrow OBU_{ij}}$將$Q_{aOID_{ij}}$解密後驗證$P_{aOID_{ij}}$的正確性，驗證成功方進行下一步，否則終止此階段。

$$(RID_i||P_{aCID_{ij}}) = D_{sk_{RSU_i \leftrightarrow OBU_{ij}}}(Q_{aOID_{ij}}) \tag{30}$$

$$H_0(RID_i||aOID_{ij}) \text{ ?= } P_{aOID_{ij}} \tag{31}$$

步驟四：路側單元$RSU_i$計算$(aF_{ij}, C)$後，再計算$MAC'_{RSU_i}$後傳給車上單元$OBU_{ij}$。

$$aF_{ij} = B_i T_{rs_i}(A_i) \bmod p \tag{32}$$

$$C = E_{sk_{RSU_i \leftrightarrow OBU_{ij}}}(aF_{ij}) \tag{33}$$

$$MAC'_{RSU_i} = E_{sk_{RSU_i \leftrightarrow OBU_{ij}}}(C, A_i) \tag{34}$$

步驟五：車上單元$OBU_{ij}$用交談金鑰$sk_{RSU_i \leftrightarrow OBU_{ij}}$將$MAC'_{RSU_i}$解密後驗證$A'_i$的正確性，驗證成功方進行下一步，否則終止此階段。

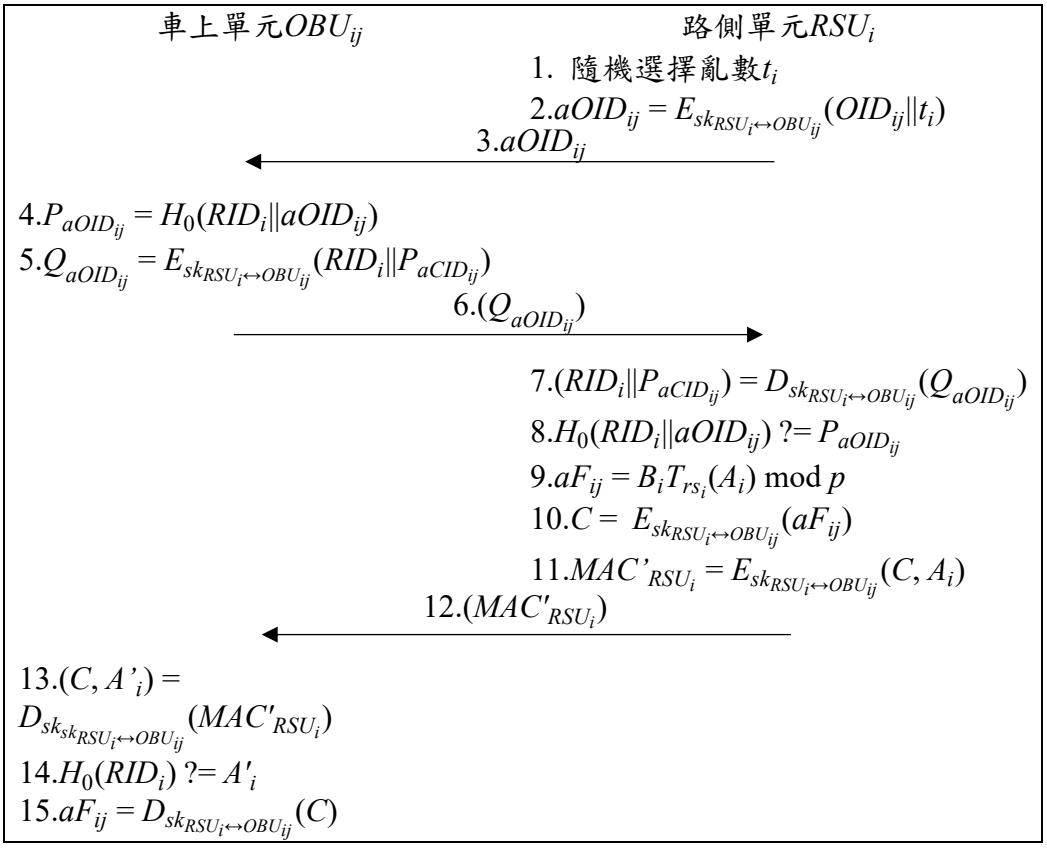
$$(C, A'_i) = D_{sk_{sk_{RSU_i \leftrightarrow OBU_{ij}}}}(MAC'_{RSU_i}) \tag{35}$$

$$H_0(RID_i) \text{ ?= } A'_i \tag{36}$$

步驟六：車上單元$OBU_{ij}$用交談金鑰$sk_{RSU_i \leftrightarrow OBU_{ij}}$將$C$解密後取得配發的$aF_{ij}$。

$$(aF_{ij} = D_{sk_{RSU_i \leftrightarrow OBU_{ij}}}(C) \tag{37}$$

圖四為匿名分配階段之流程圖。




圖四：匿名分配階段

## 肆、安全性分析

### 4.1 秘密金鑰安全性

醫院伺服器的秘密金鑰為$B_0 = T_{hs_0}(x) \bmod p$，路側單元的秘密金鑰為$B_i = T_{hs_0}(A_i) \bmod p$。倘若攻擊者欲非法取得$B_0$或$B_i$，攻擊者將面臨 CMDLP。

### 4.2 交談金鑰確認及其安全性

此方法利用訊息驗證碼$MAC_{RSU_i}$與$MAC_{OBU_{ij}}$，提供交談金鑰確認功能以確保對稱式加密金鑰的正確性。倘若攻擊者想非法獲得交談金鑰$sk_{RSU_i \leftrightarrow OBU_{ij}}$，攻擊者會面臨 CMDHP；此外，因其包含隨機亂數$a_{ij}$，故每次通訊使用的交談金鑰皆不同。

### 4.3 匿名功能

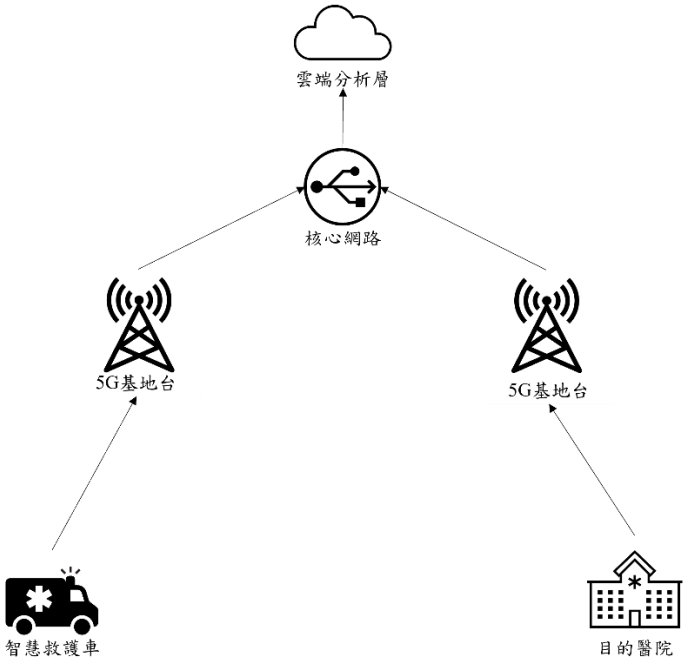
車上單元$OBU_{ij}$會在完成雙向驗證與金鑰協議階段後，獲得假名$aOID_{ij}$及其關聯私鑰$aF_{ij}$。因假名$aOID_{ij}$內包含時間戳記$t_i$，故每次車上單元$OBU_{ij}$會獲得不同的假名，使其無法與真實身分產生明顯關聯，確保通訊身分隱私。

### 4.4 無須註冊中心

學者 Ying 與 Nayak[22]及學者 Haq 等人[9]皆提出需要註冊中心的 5G 網路架構相關協定，通訊雙方須先向註冊中心申請為合法身分，後續雙方通訊亦須透過註冊中心。然而，註冊中心會面臨特權攻擊(Privilege Attack)或惡意內部攻擊 (Malicious Insider Attack)的風險。此研究使用階層式網路架構，而此架構適用於現行 5G 網路架構。

## 伍、使用情境

當 5G 智慧救護車運送病患，救護車上的緊急醫療團隊可以與目的醫院進行視訊通話，而通話期間的訊息都使用交談金鑰加密；緊急醫療團隊亦可傳送到院前診療紀錄給目的醫院。如此可以達到病患隱私保護以及提升整體緊急醫療服務品質。圖五為其系統架構示意圖。




圖五：系統架構示意圖

## 陸、結論

本研究提出適用於 5G 智慧救護車之植基於切比雪夫混沌映射聯合匿名身分管理協定，此協定利用階層式網路架構進行有效的匿名身分管理，並利用匿名及交談金鑰建立，達到醫療隱私保護，減少病患資料外洩風險。

## 參考文獻

[1] J.S. Alshudukhi, Z.G. Al-Mekhlafi, B.A. Mohammed, “A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography,” IEEE Access Vol. 9, pp.15633–15642, 2019.

[2] M. Al Shareeda, A. Khalil, W. Fahs, “Realistic heterogeneous genetic-based RSU placement solution for V2I networks,” International Arab Journal of Information Technology Vol. 16, No. 3A, pp.540–547, 2019.

[3] S. Anwar, R. Prasad, “Framework for future telemedicine planning and infrastructure using 5G technology,” Wireless Personal Communications Vol. 100, No. 1, pp.193–208, 2018.

[4] A. Ahad, M. Tahir, K.L.A. Yau, "5G-based smart healthcare network: architecture, taxonomy, challenges and future research directions," IEEE Access Vol. 7, pp.100747–100762, 2019.

[5] L. Chettri, R. Bera, "a comprehensive survey on Internet of things (IoT) toward 5G wireless systems," IEEE Internet of Things Journal Vol. 7, No. 1, pp.16–32, 2020.

[6] EMS Agenda 2050 Technical Expert Panel, "EMS agenda 2050: a people-centered vision for the future of emergency medical services (Report No. DOT HS 812 664)," Washington, DC: National Highway Traffic Safety Administration, 2019.

[7] P. Fremantle, B. Aziz, "Cloud-based federated identity for the Internet of Things," Annales des Telecommunications/Annals of Telecommunications Vol. 73, No. 7-8, pp.415–427, 2018.

[8] C. Gentry, A. Silverberg, "Hierarchical ID-based cryptography," 8th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2002), New Zealand (Queenstown), pp.548–566, 2002.

[9] I.U. Haq, J. Wang, Y. Zhu, "Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks," Journal of Network and Computer Applications Vol. 161, 2020.

[10] L. Kocarev, "Chaos-based cryptography: a brief overview," IEEE Circuits and Systems Magazine Vol. 1, No. 3, pp.6–21, 2001.

[11] L. Kocarev, S. Lian, Chaos-Based Cryptography: Theory, Algorithms and Applications, Springer, Germany (Berlin/Heidelberg), 2011.

[12] A.K. Leaby, A. Yassin, M. Hasson, A. Rashid, "Towards design strong emergency and COVID-19 authentication scheme in VANET," Indonesian Journal of Electrical Engineering and Computer Science Vol. 21, No. 3, pp.1808–1819, 2021.

[13] T.F. Lee, C.H. Hsiao, S.H. Hwang, T.H. Lin, "Enhanced smartcard-based password-authenticated key agreement using extended chaotic maps," PLoS ONE Vol. 12, No. 7, 2017.

[14] H.Y. Lin, "Improved chaotic maps-based password-authenticated key agreement using smart cards," Communications in Nonlinear Science and Numerical Simulation Vol. 20, No. 2, pp.482–488, 2015.

[15] A. Mukhopadhyay, S. Sreekumar, B. Xavier, M. Suraj, "A cloud-based smartphone solution for transmitting bio-signals from an emergency response vehicle," International Journal of E-Health and Medical Communications Vol. 10, No. 3, pp.22–38, 2019.

[16] Office of the National Coordinator for Health Information Technology, "Emergency medical services (EMS) data integration to optimize patient care: an overview of the search, alert, file, reconcile (SAFR) model of health information exchange," URL:

https://www.healthit.gov/sites/default/files/emr_safer_knowledge_product_final.pdf (存取時間： 2022/04/23).

[17] Y. Park, C. Sur, K.H. Rhee, "A privacy-preserving location assurance protocol for location-aware services in VANETs," Wireless Personal Communications Vol. 61, No. 4, pp.779–791, 2011.

[18] A. Shamir, "Identity-based cryptosystems and signature schemes," Annual International Cryptology Conference (CRYPTO 1984), United States (Santa Barbara), pp.47–53, 1985.

[19] M.L.B.A. Santos, J.C. Carneiro, A.M.R. Franco, F.A. Teixeira, M.A.A. Henriques, L.B. Oliveira, "FLAT: federated lightweight authentication for the Internet of Things," Ad Hoc Networks Vol. 107, 2020.

[20] V.R.L. Shen, W.C. Huang, "A time-bound and hierarchical key management scheme for secure multicast systems," Wireless Personal Communications Vol. 85, No. 4, pp.1741–1764, 2015.

[21] D. Solev, P. Janjic, L. Kocarev, "Introduction to chaos," Studies in Computational Intelligence Vol. 354, pp.1–25, 2011.

[22] B. Ying, A. Nayak, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography," Journal of Network and Computer Applications Vol. 131, pp. 66-74, 2019.

[23] L. Yan, C. Rong, G. Zhao, "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography," 1st International Conference on Cloud Computing (CloudCom 2009), China (Beijing), pp. 167–177, 2009.

[24] E.J. Yoon, I.S. Jeon, "An efficient and secure Diffie–Hellman key agreement protocol based on Chebyshev chaotic map," Communications in Nonlinear Science and Numerical Simulation Vol. 16, No. 6, pp.2383–2389, 2011.

[25] E.J. Yoon, K.Y. Yoo, "Cryptanalysis of group key agreement protocol based on chaotic hash function," IEICE Transactions on Information and Systems Vol. E94-D, No. 11, pp.2167–2170, 2011.

[26] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," Chaos, Solitons and Fractals Vol. 37, No. 3, pp.669–674, 2008.

[27] 中田孝明，織田成人，羽石秀昭，山尾恭生，鈴木哲也，近藤針次，《實現及時正確急救醫療之智慧急救系統及裝置開發(早く正しい救急医療実現のためのスマートな救急情報システム・装置の開発)》，第 26 次全國急救隊員論壇，2017。

**[作者簡介]**

林子煒先生分別於2013年與2021年取得長庚大學資訊管理系碩士學位與企業管理研究所博士班博士學位，自2021年8月起擔任逢甲大學創能學院助理教授，並於2022年8月起兼任逢甲大學資訊總處資訊安全中心主任。研究領域包括資訊安全、網路安全、密碼學、物聯網應用安全、雲端運算應用安全、醫療資訊系統、健康照護系統、行動商務、人工智慧等。