植基於混沌映射符合 HIPAA 安全規範並具授權註銷之金鑰管理機制

李添福[1*]、陳柏錡[2]、黃思翰[3]
慈濟大學醫學資訊學系
[1] jackytflee@mail.tcu.edu.tw、[2]103325115@gms.tcu.edu.tw、[3]102325109@gms.tcu.edu.tw

摘要

含個人健康資訊的病歷資料，對於個人而言是屬於相當機密的，需要有一個有效的存取控制作為管制手段，而金鑰管理是目前最常用且有效的方法。在 HIPAA 規範下，導入金鑰管理授權與註銷的機制，同時強化病人對於病歷資料的管控。

最近幾年，有許多符合 HIPAA 的金鑰管理機制陸續被提出來，用來保護病歷資料的安全，然而有些機制卻存在著授權下，可以獲得全部病歷資料，同時也需要大量的運算來產生金鑰。在一個階層式結構的病歷資料下，現有的金鑰管理機制是一個病人就一把金鑰保護病人的病歷資料，無法進行部分病歷資料的授權與保護的機制，進而無法發揮金鑰管理機制所要達成保護病歷資料的目的。因此需要低運算量的金鑰運算同時以不同的鑰匙來保護不同的病歷資料，擁有者則可以管理與控制不同病歷資料的金鑰。在這兩大項的考量，由於混沌映射在運算效能上比模指數運算或橢圓曲線點乘運算更好，同時也被證明符合半群以及其他數學上的特性，因此適合運用在複雜階層式資料存取控制上。本研究利用混沌映射之快速運算與數學上的優點，及其適合運用在階層式資料存取控制的特性，提出符合 HIPAA 規範與同時具有安全與效率的病歷資料存取控制的金鑰管理機制。

關鍵詞:存取控制、金鑰管理、混沌映射、HIPAA、病歷資料、病歷資料授權與註銷

An Extended Chaotic Map-based HIPAA-compliant Key Management Scheme with Revocation of Authorization

Tian-Fu Lee[1*], Po-Qi Chen[2], Shi-Han Hwang[3]
Department of Medical Informatics, Tzu Chi University
[1] jackytflee@mail.tcu.edu.tw, [2]103325115@gms.tcu.edu.tw, [3]102325109@gms.tcu.edu.tw

Abstract

Medical records containing personal health information are confidential for individual. Therefore, an effective method such as key management to control and access these files is needed. Health Insurance Portability and Accountability Act (HIPAA) is a standard regulation for medical records management. Under HIPAA specifications, the key management

mechanisms, such as authorization and revocation of access right for the medical records, are regulated. Additionally, accessing electronic medical records by medical staff requires authorization from patients.

In recent years, many HIPAA key management schemes were proposed in order to provide confidentiality protection of sensitive information for patient's medical record. However, there exist some security problems in these schemes. For example, an authorize person (medical staff) can access to all medical records, or the scheme need heavy computational cost in order to maintain a key management scheme. The structure of medical records may be regarded as hierarchical. However, some key management schemes protect one patient's medical records by using one set of secret key, may reveal partial unauthorized medical records. Additionally, most key management schemes require time-consuming modular exponential computations and scalar multiplications on the elliptic curve.

Recent studies showed that cryptography using chaotic maps was demonstrated to provide the semi-group property and commutative property. Additionally, cryptosystems using chaotic map operations were more efficient than cryptosystems using modular exponential computations and scalar multiplications on the elliptic curve. Therefore, this study develops a key management scheme using extended chaotic maps for HIPAA privacy/security regulations. The proposed key management scheme is not only more efficient than related approaches, but also has revocation of authorization and is suitable for complex hierarchical data structure in electronic medical records.

Keywords: Access control, key management, chaotic maps, HIPAA, personal health information, revocation, authorization

壹、前言

在資訊安全領域存取控制(Access Control)是一個非常重要的議題，而 HIPAA 中對於醫療安全上的存取控制有相當嚴謹的管控，尤其是對於使用病歷資料上的管控更是嚴格。病歷資料對於醫院而言在醫學研究上是相當重要的資產，對個人而言卻是極為隱私和機密的文件，即使是醫院的醫生或護理人員不能夠在未經授權下輕易地取得、觀看、增加和修改病歷資料,並且也須要避免相關的資料暴露在被竊取、竄改和洩漏的風險中。

1.1 研究背景

隨著網際網路與數位化的快速進行與發展，許多電子化、數位化的資料利用各種方

式進行傳輸，而各家醫院和醫療組織也隨著這個潮流將紙本病歷電子化，在這個背景下電子病歷在醫療服務系統擠身成為重要的研究對象。病歷資料對於個人而言屬於相當重要的隱私資料，因此建立一個可靠且安全的認證機制，同時也保護電子病歷資料不被竊取或者被竄改是相當重要的事。

醫院所持有的病歷資料是相當可觀，即便是小診所也有數千筆，地區醫院則動輒數萬筆，醫學中心就更不用說數十萬到數百萬都有，而且有許多不同類型的病歷資料，像超音波、X 光...，各式各樣的儀器所產生的病歷資料。

針對病歷存取的保護機制，雖然有許多不同的金鑰管理機制被提出，但是大多需要大量的運算才能達到病歷資料的安全，在運算量上對於部分的電腦而言是一大負擔。因此，設計出一個完善且具有低運算量的金鑰授權系統，用以保護病歷不被未授權的醫護使用者存取，於醫療服務系統之病歷資料保護是一個相當重要的資訊安全議題。[5][6][8][9][13][15][17]

1.2 研究動機與目的

電子病歷資料的存取控制一直是醫療領域中相當重要的議題。病歷存取時，必須在病人同意授權下，醫生方能存取這份病歷，以避免病歷被任意存取或竄改，以至於影響患者隱私。此外，當醫生存取某病患之病歷時，醫生應僅能存取進行醫療行為時，所需要使用之部分病歷資訊，而無法存取該患者其他病歷內容或資訊。

早期的病歷每一病患所有病歷資料存取都是透過一把認證金鑰控制，便可存取該病人所擁有的全部病歷的內容，而病人的就醫資訊與個人隱私只能憑藉著醫生的醫療道德和良知。病人的就醫資訊與個人隱私，未受到完整且完善的保護，可能將其暴露在不安全的環境中。因此必須提出一個安全的存取方法，讓醫生存取病歷時，只能存取他在進行醫療行為時，所需要的病歷資訊，以藉此來保障病人的就醫資訊與個人隱私，同時也可以避免醫生在不經意的情況下，破壞到病人的病歷完整性與機密性。

有許多的文獻針對病歷存取控制的環境，有提出相關或類似的解決方案，但大多需要耗時的模指數運算，如: 2008 年 Lee 和 Lee [8] ，或橢圓曲線點乘運算，如: 2011 年 Huang 和 Liu [6]，以及有安全問題，如: 2010 年 Hu、Chen 和 Hou [5]和 2014 年 Lee 和 Lee [9]。高運算量對於性能較差的電腦而言是一個沉重的負擔，尤其在病人在取得自己病歷或醫生在執行醫療行為時所需病歷，而在這分秒必爭的環境下，需要較長的時間對病歷進行解密，將會使病人的生命遭受威脅，所以需要一個可以確保病人隱私又高效率的存取控制，安全性保護不足則會讓病人病歷資料的隱私暴露在危險的環境。

由於電子病歷資料庫的存取環境中，涉及複雜運算的階層式存取控制架構，用在具有階層架構的環境下，以公開金鑰與公開參數即可推導下一個階層的金鑰，而不需要儲存多把金鑰來達到相同效果[1][3][4][7][10][11][12][16]，而渾沌映射由於其的數學特性[2][12][17]，相當適合運用在階層式存取控制，再加上其所需的運算量相當的低，以及他

已經在許多文獻中被證實具模指數運算或橢圓曲線點乘運算相似的安全特性，而運算效能遠優於耗時的模指數運算或橢圓曲線點乘運算[14][19][20][21]。在安全性與運算量上的考量下，混沌映射比其他的方法來的有優勢。此外，混沌映射滿足半群(Semi-group Property)的特性，並具有解離散對數問題(Discrete logarithm problem-DLP)與 Diffie-Hellman problem (DHP)的特性，以現行的硬體設備的運算效能計算上不可能破解。在許多文獻中也證實其的運算效率比較快速，安全性也不比現行的密碼系統差[17]。

本研究將發展植基於混沌映射技術之電子病歷金鑰管理授權與註銷機制，透過利用其低計算量及數學特性解決現行相關機制在效能上與安全上的缺點，並且符合 HIPAA 的安全規範。

貳、文獻探討

2.1 導入 HIPAA 的金鑰管理機制

在 1996 年美國通過 HIPAA(Health Insurance Portability and Accountability Act)法案[15]，屬於病人的個人病歷隱私就受到了法律的保障。近幾年來有許多論文針對符合 HIPAA 之電子病歷存取控制的金鑰管理，並提出解決方案。

2008 年 Lee 和 Lee[8]將 HIPAA 引入，提出用來保護病歷隱私的金鑰管理，並使用智慧卡(Smart Cards)儲存部分驗證資訊。同時亦根據 HIPAA 規範提出金鑰管理的五個面向，分別是病人知情同意、病歷保密性、病人控制、病歷資料完整性、例外同意，在這五個面向下發展的金鑰管理。2010 年 Hu 等人[5]提出了建立合約導向系統，並且提出了一套混和公開金鑰密碼為基礎架構解決方案(HPKI－Hybrid Public Key Infrastructure)，獨立且可信任的智慧卡中心(STC－Smartcard Trust Centre)負責簽署合約，而每個病人的病歷資料都留在了醫療中心伺服器(MCS－Medical Centre server)，同時也是首度提出在 HIPAA 下的跨醫院病歷資料的授權。2011 年 Huang 和 Liu [6]提出符合 HIPAA 的高效能金鑰管理機制，以橢圓曲線密碼(Elliptic Curve Cryptography)為基礎的智慧卡金鑰授權與管理，並利用他的最小鑰匙長度和計算成本，簽名驗證和加解密過程，即便如此他的計算量還是比其他金鑰產生的計算量大。這個金鑰管理機制的限制大致上和 2008 年 Lee 和 Lee 所提出的方法相同，除了病人更換密碼的機制有所更動外並無太大的改變。2014 年 Lee 和 Lee [9]指出 2011 年 Huang 和 Liu 的金鑰授權必須親自由病人完成的缺點，以及在 2010 年 Hu 等學者[5]針對金鑰授權提出系統允許病人授權合同在時間內一個指定的醫療保健機構，卻存在無法提前撤銷授權。因此 Lee 和 Lee [9]提出拉格朗日插值多項式(N-degree Lagrange Interpolating Polynomial)可以有效解決上述的兩個問題，其提出的解決方案是將病人與 MCS 的密鑰存放在各自的智慧卡，在金鑰產生時需要病人的密鑰與線性方程所產生的主密鑰，但是如果病人的智慧卡被攻擊者取得，可能造成金鑰安全

有所疑慮，威脅到病歷資訊的機密性。

綜合以上的論文，發現大多數的文獻在計算量上較為龐大，而且也被發現到在安全上有疑慮，同時也不能確保病歷資料的隱密性，部分的文獻並沒有遵守金鑰由病人所控制的 HIPAA 規範，且有病歷資料完整性的疑慮。

2.2 階層式存取控制金鑰管理機制

1983 年 AKL 和 Tylor [1]提出階層式金鑰管理機制，在這之後有許多針對階層式金鑰控管機制陸陸續續被提出來，但是許多被提出來的機制存在著安全上的問題，以及需要大量的運算量與龐大的儲存空間，當階層多和複雜時，效率較低且不易進行階層的金鑰動態管理。2006 年 Jeng 和 Wang [7]以及 2008 年 Chung 和 Lee [3]都提出基於多項式與橢圓曲線公開金鑰密碼系統的階層式存取控制金鑰管理機制。2012 年 Das 等人[4]，指出 Chung 和 Lee 等人提出的管理機制存在被外部攻擊者(External Attack)取得金鑰，因此提出改進的機制抵擋攻擊的階層式存取控制金鑰管理機制。2010 年 Nikooghadam [11]等人提出了不需要多項式，只基於橢圓曲線加密金鑰的階層式存取控制金鑰管理機制，因為只使用橢圓曲線加密金鑰系統，雖然可以讓效率變得比較好，但相對於對稱式加解密和混沌映射相較而言仍然是需要相當多的運算量。2012 年 Wu 和 Chen [16]指出 Nikooghadam 等人的方法缺少正式的安全性分析，而且使用了跟對稱式加解密運算速度上來得更慢的橢圓曲線加解密運算，為此提出應用於電子醫療系統上更有效率的混合式加密系統階層式存取控制，利用橢圓曲線與對稱式加解密，改善了機制的運算效率。同年，Nikooghadam 和 Zakerolhosseini [10]發現 Wu 的方法有中間人攻擊(Man-in-the-middle-attack)，為了改善這個問題使用了橢圓曲線簽章，但是需要花費大量的運算在驗證。2013 年 Odelu [12]等人提出使用對稱式加解密雜湊函數的機制，大量減少參數儲存與運算的複雜度，雖然減少了參數的使用，但在階層複雜的情況下仍需要許多的參數運算。

綜合以上的文獻中，可以發現現行的階層式金鑰管理系統，大多依賴複雜度高且運算量大的機制，而也有些文獻被發現有安全上的疑慮，因此本研究將利用低運算量且安全性高混沌映射技術來設計適用於電子病歷之階層式金鑰管理機制。

2.3 Chebyshev(切比雪夫) Chaotic Maps

本節將簡單介紹切比雪夫混沌映射[2]，描述延伸的混沌映射，以及解離散對數問題與 Diffie-Hellman 問題。

定義 1 (切比雪夫多項式): 令 $n \in N$，$x \in N$，則切比雪夫$T_n(x)$: $Z_n \to Z_n$使用下列遞迴關係:

$$T_0(x) = 1，T_1(x) = x，T_n(x) = 2xT_{n-1} - T_{n-2}(x)，$$

$n \geqq 2$，並滿足交換律:

$$T_r(T_s(x)) = T_s(T_r(x)) = T_{sr}(x)。$$

定義 2 （Chaotic Map-based 離散對數問題）：給定的 x 和 y，很難找到一整數 s，滿足 $T_s(x)=y$。

定義 3 （Chaotic Map-based Diffie-Hellman 問題）：給定的 x、$T_r(x)$和$T_s(x)$，很難找到 $T_{rs}(x)$。

2005 年，Bergamo 等人[2]指出 Chaotic maps 有安全上的問題，這個攻擊是攻擊者可以利用 x、$T_r(x)$等資訊，計算出一個整數 r'，滿足$T_{r'}(x) = T_r(x)$，進而讓通訊者的一方事先決定通訊金鑰。2006 年，Zhang [18] 提出 Extended Chaotic Maps，證明將 x 定義在區間 $[-\infty,+\infty]$ 可以解決安全上的問題，且擁有相同的特性，本研究在機制中使用 Extended chaotic maps:

$$T_n(x)=(2xT_{n-1}(x)- T_{n-2}(x))(\text{mod } p),\ n \geqq 2，$$

其中 $x \in [-\infty,+\infty]$，p 大質數。

定義 4 （Extended Chaotic Map-based 離散對數問題）：給定 x、$T_r(x) \bmod p$，很難找到一個整數 r，使得$T_r(x) \bmod p = r$, 其中 $r \in N$。

定義 5 （Extended Chaotic Map-based Diffie-Hellman 問題）：給定的 x、大質數 p、$T_r(x) \bmod p$ 和$T_s(x) \bmod p$，很難找到$T_{rs}(x) \bmod p$。

參、所提植基於混沌映射之金鑰管理機制

本節將說明利用低運算量的混沌映射建構階層式病歷資料金鑰加密機制，並說明研究架構與方法，表一為本研究使用符號表。

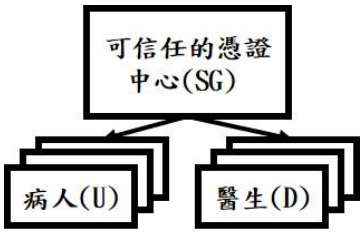
表一：使用符號表

符號	敘述
U	病人的代表符號
D	醫生的代表符號
SG	可信任的憑證中心的代表符號
MCS	醫學中心伺服器的代表符號
PHI_i	病歷資料的代表符號
u/d	前者代表病人的 ID，後者代表醫生的 ID
p	SG 產生的大質數
R_i	在每個病歷用以產生授權金鑰的參數

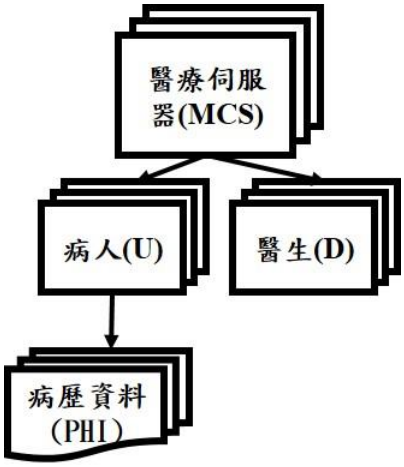
K_i	由每個病歷參數和SK_p計算出的授權金鑰
$T_s(x)$	切比雪夫多項式
s	可信任的憑證中心的密鑰
sk	個人密鑰
$E_K(.)/D_K(.)$	用授權金鑰進行加/解密
f	表示全部的病歷個數
e	表示全部的病人個數

3.1 研究架構

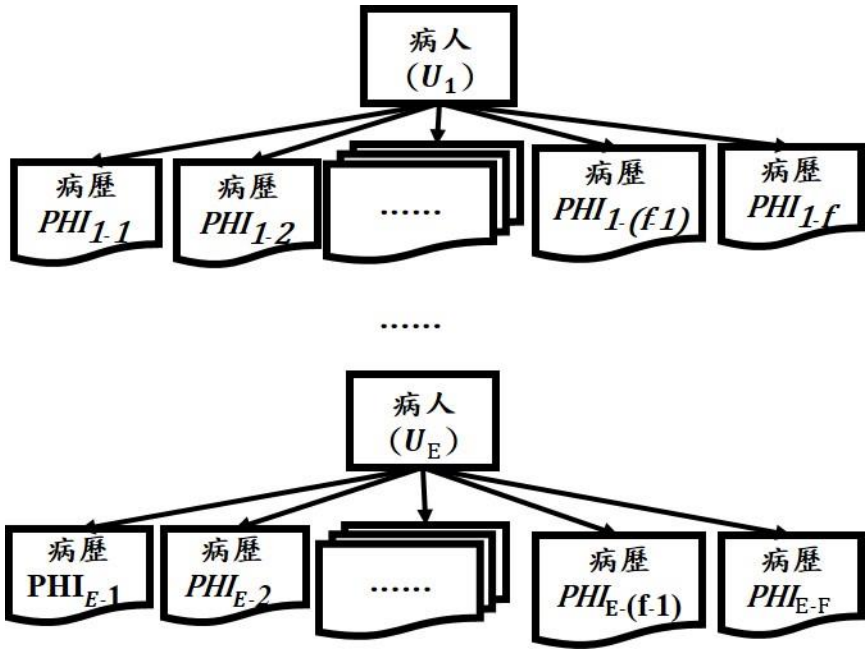
圖一說明每位病人或醫生都可以向信任憑證中心取得自己的私鑰; 圖二說明醫學中心伺服器與病人和醫生之間的關係，單一病人有許多份的病歷; 圖三說明有許多不同的病人，而每個病人都有各自不同的病歷資料。



圖一: 病人和醫生金鑰授權

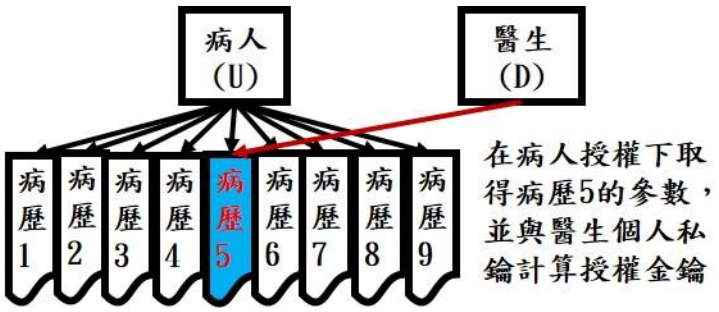


圖二: 醫學伺服器與病人和醫生的關係圖



圖三: 病人與病歷的關係圖

並不是該病人所有的病歷都和這次的診斷有關，因此只需要給予本次診斷所需的病歷資料，而和本次診斷無關的病歷資料，這兩者在這次診斷所需的機密性要求是不一樣的，因此在金鑰管理上必須有所區別，藉由不同病歷有不同金鑰來管理，單一份病歷的金鑰授權如圖四，病人提供病歷 5 的參數給醫生，醫生藉由病歷 5 的參數和醫生 A 自己本身所的參數產生一把授權的鑰匙。



圖四: 病歷金鑰授權示意圖

管理不同的病歷會有不同的參數，經由對金鑰參數的變更，對金鑰產生管控，同時對病歷資料進行重新加解密，來確保病歷的機密性，病人需要提供可以授權給醫生的病歷資料的參數，醫生才可以根據參數獲得金鑰。

3.2 角色描述

本研究有以下幾個角色 可信任的憑證中心(SG)、醫學中心服務器(MCS)、病人(P)、醫生(D)、病歷(PHI)。

(1) 可信任的憑證中心(SG)

通常是政府或由其他可以信任的組織提供的憑證中心，以台灣為例，通常 SG 通常指的是衛生福利部所提供的 SG，管理與驗證病人和醫生的身分確認，註冊時核發個人的金鑰。

(2) 醫學中心伺服器(MCS)

醫學中心伺服器通常是指在各個醫院中存放病歷資料的伺服器，有許多不同種類的病歷資料，同時也是該醫院管理病歷資料的伺服器，不論是醫生或病人都必須通過該伺服器取得所需的病歷資料，MCS 是病歷資料的保管者。

(3) 病人(U)

病人是病歷資料的持有者，他有權力可以決定病歷資料是否可以給予他人觀看，同時他也有權力知道病歷資料要被如何使用，病歷資料必須是完整保存的，不可以有所竄改和遺失，否則資料完整性會有疑慮，而病歷資料的獲得必須要有一定的隱密性，並且確保病歷資料不被不相關的第三人所取得，因此必須要有嚴謹保護機制來保護病歷資料不被取得。

(4) 醫生(D)

醫生是最主要的病歷資料的使用者，但卻是有極高風險會洩漏病歷資料的人，因此醫生取得病歷資料時，必須要有一套有效且嚴謹的管制機制，所以必須要取得參數產生金鑰來進行解密病歷資料，而這把金鑰也必須要有嚴謹的核發與產生機制。

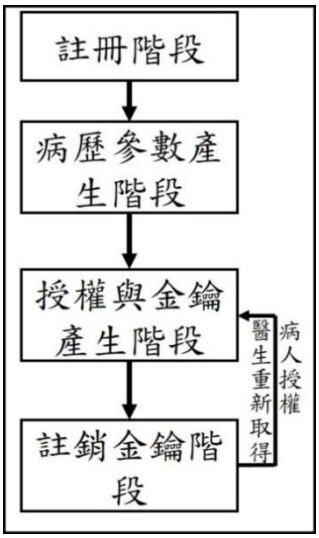
(5) 病歷(PHI)

病歷資料存放在 MCS，MCS 是它的保管者，病人是它的擁有者，醫生則是它的使用者，因此不管它在哪個使用情況，都是有可能會有洩漏的情況，因此要有相當嚴謹的管控機制來確保它的隱密性，否則會被不相關的第三人所取得，所以有許多不同的方法來進行保護,其中對它進行加密是最常見也是最好的方式,而且要適當管制金鑰的機制。

本研究之流程主要分為四個部分，第一部分病人的每分病歷給予一個參數，第二部分是醫生在獲得病人的授權下，可以取得獲得授權的病歷的參數，第三部分利用這些參數產生一把金鑰，第四部分藉由參數的控管來限制金鑰可以開啟的病歷資料。

3.3 方法描述

本研究所提之機制主要分成註冊階段、病歷參數產生階段、授權與金鑰產生階段、註銷金鑰階段，共四個階段，如圖五。



圖五: 研究方法四個階段

(1) 註冊階段

在這個階段，SG 產生一個隨機大質數 p，SG 在收到各人金鑰請求時，會分別驗證每個病人和每個醫生身分的合法性，驗證身份合法後給予每個病人和醫生各自的金鑰，如圖六。

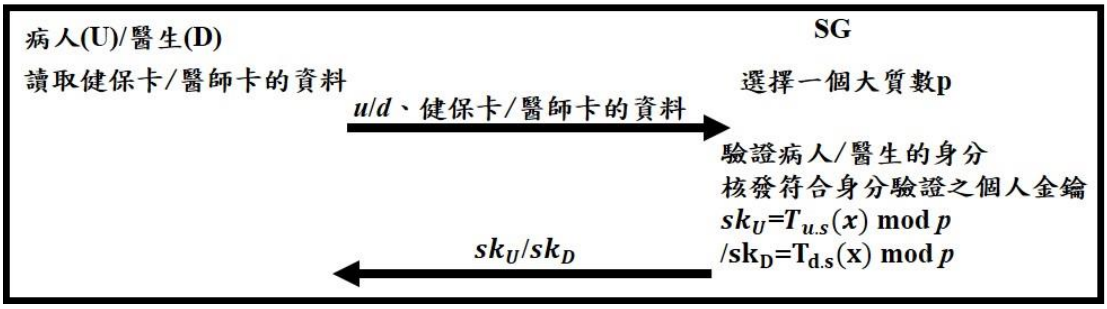
Step 1: 病人(U)/醫生(D)產生各自各自傳送其的 u 和 d 以及讀取各自的健保卡或醫師卡內的身分資料，並對 SG 請求產生屬於自己的金鑰，同時 SG 產生一個隨機數 p。

Step 2: SG 驗證病人/醫生的身分。

Step 3: SG 驗證符合身分核發個人金鑰。

Step 4: 病人/醫生取得個人金鑰 $sk_u=T_{u.s}(x) \bmod p$ / $sk_d=T_{d.s}(x) \bmod p$，

其中 s 為 SG 之私密金鑰，p 為 SG 產生的公開大質數。



圖六、註冊階段

(2) 病歷參數產生階段

此階段，由健保卡驗證是否為合法使用者，確認為合法使用者本人後，對其所屬的病歷資料產生各自的參數，這些參數是為下一階段產生的授權金鑰做準備，如圖七。

Step 1: 驗證病人身分。

Step 2: 產生病歷參數，為產生下一階段的授權金鑰做準備。

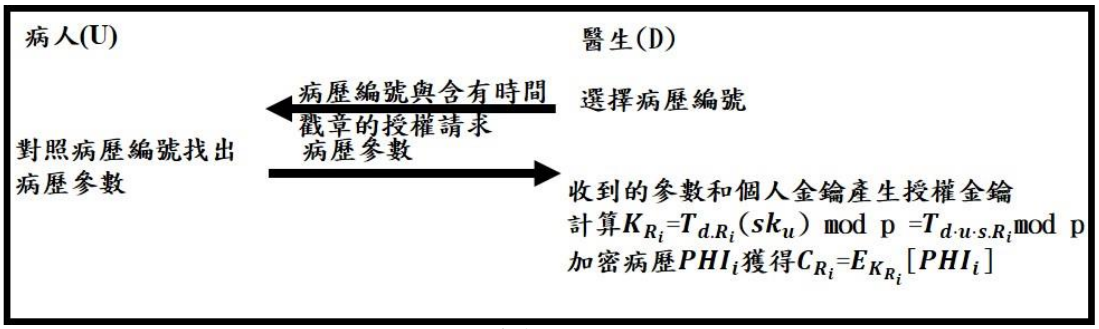
圖七、病歷參數產生階段

(3) 授權與金鑰產生階段

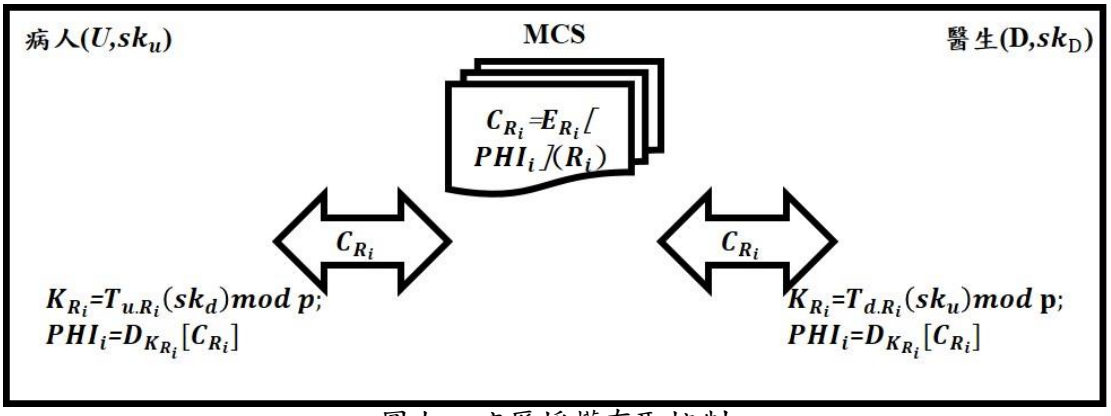
授權與金鑰產生階段，醫生會對病人發出病歷資料的授權請求，病人在確認醫生的請求後，在同意授權下在其所屬的病歷編號目錄中，查找醫生所請求的病歷的參數，並將對應的R_i提供給 MCS，MCS 在收到R_i後，利用參數計算獲得授權金鑰K_{R_i}，並利用金鑰對PHI_i進行加密，醫生和病人本身可以使用自己的私鑰和R_i推導出授權金鑰K_{R_i}， 從而解密被 MCS 加密的病歷資料。

Step 1: 醫生對病人發出具有時間戳章的病歷授權請求。

Step 2: 病人(U)其私鑰SK_u，而其一所屬之病歷資料PHI_i的參數R_i，醫生(D)獲其授權存取，MCS 藉由其參數計算出病歷授權金鑰$K_{R_i}=T_{d.u.s}(R_i) \bmod p = T_{d\cdot u\cdot s.R_i}(x) \bmod p$，並加密病歷$PHI_i$獲得$C_{R_i}=E_{K_{R_i}}[PHI_i]$。病人(U)可利用本身之私鑰$SK_u$與公開參數計算出$K_{R_i}=T_{d\cdot R_i}(SK_u) \bmod p = T_{d\cdot R_i}(T_{u.s}(x)) \bmod p$；另一方面，醫生(D)向 MCS 存取$C_{R_i}$後，可利用本身之私鑰與公開參數計算出病歷授權金鑰$K_{R_1}=T_{u\cdot R_i}(SK_d) \bmod p = T_{u\cdot R_i}(T_{d.s}(x)) \bmod p$。因此，病歷擁有者病人(U)與病歷授權者醫生(D)皆有能力算出病歷授權金鑰$K_{R_i}=T_{d\cdot u\cdot s\cdot R_i}(x) \bmod p$，進而解出病歷$PHI_i = D_{k'R_i}[C_{R_i}]$，如圖八、圖九。



圖八、授權與金鑰產生階段



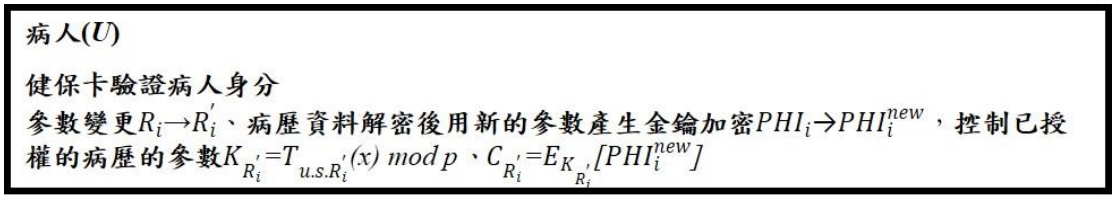
圖九、病歷授權存取控制

(4) 註銷金鑰階段

註銷金鑰階段，以健保卡驗證是否為合法使用者，確認為合法使用者本人後，使用者才可以對病歷資料的參數進行更新，以確保病歷資料的安全性，參數更新後如要再次使用該病歷，需要取得病人的再次授權，並重新產生授權金鑰，如圖十。

Step 1: 驗證病人身分。

Step 2: 病人針對特定病歷資料的參數進行變更，$R_i \rightarrow R_i'$、對病歷資料解密後用新的參數產生金鑰加密$PHI_i \rightarrow PHI_i^{new}$，控制已授權的病歷的參數$K_{R_i'}=T_{u.s.R_i'}$(x) mod p、$C_{R_i'}=E_{K_{R_i'}}[PHI_i^{new}]$。如果醫生還要再使用該病歷，就必須重新取得授權，重新產生授權金鑰。



圖十: 註銷金鑰階段

肆、效能與安全性分析

綜合文獻的所提的方法與安全分析，發現 Lee 和 Lee 的機制[8]與本研究所提方法較為相近，在接下來的分析將會以 Lee 和 Lee 作為最主要的安全分析與比較。

本研究中授權行為是發生在授權與金鑰產生階段，每次醫生需要病歷資料時，都需要獲得病人的授權後才能取得病歷參數並計算出授權金鑰，而且不同的病歷有不同的金鑰所保護。然而 Lee 和 Lee 機制[8]的病人授權行為是在註冊階段，一經註冊就可以使用相同的授權資訊，同時使用這個授權資訊作為金鑰的一部分，雖然所有的病歷資料都受這把金鑰保護，但在單一病歷資料的保護上較為不易。

表二: 安全特性比較表

攻擊名稱	Lee 和 Lee	本研究所提金鑰管理機制
身分驗證	●	●
內部攻擊	●	●
偽冒攻擊	●	●
重送攻擊	●	●
中間人攻擊	●	●
反向攻擊	●	●
外部蒐集攻擊	●	●
合作攻擊	●	●
已知金鑰安全性	●	●

●: 可抵擋/有 ○:不可抵擋/無

所提金鑰管理機制以 Extended Chaotic Maps 建構階層式病歷資料金鑰加密系統。在註銷授權金鑰後，曾獲得授權的人員是不能夠計算出任何病歷資料的金鑰。Lee 和 Lee 機制[8]雖然也有註銷機制，但沒有提供單一病歷資料的保護機制，在取得金鑰後，會讓沒有被授權的病歷資料也可以被解密，使得其的機密性會有所疑慮，表二說明本研究與 Lee 和 Lee 機制之安全特性比較表。

在表三中，Lee 和 Lee 機制在病人控制上是以全部的病歷資料一起授權，且在註冊階段授權，而不是採取病歷資料單一授權的方法進行。在本研究中，醫生每次要取得病歷資料，都需要病人的重新授權才可以計算出合法的授權金鑰，並透過註銷病歷參數對加密病歷資料從新加密，也因此需要取得授權，才可獲得授權金鑰，以此加大病人對病歷資料的控制。Lee 和 Lee 機制和本研究所提機制都有達到 HIPAA 的四個原則，但是 Lee 和 Lee 機制在病歷保密性上，以一把金鑰對全部的病歷資料加密，而醫生取得金鑰後解密病歷，會使得和這次就診無關的病歷資料的保密性造成危害。在本研究中不同的病歷資料，有不同的病歷參數，以這些病歷參數所產生的金鑰對病歷資料加密，且存放

在 MCS 中的病歷資料也是加密狀態,而醫生要取得授權才可以獲得授權金鑰進行解密,使得病歷資料在保密性獲得比較好的保障。

表三: HIPAA 規範比較表

HIPAA 安全規範	Lee 和 Lee	本研究所提金鑰管理機制
病人知情同意	●	●
病人控制	●	●
病歷保密性	●	●
病歷資料完整性	●	●

● : 有 ○:無

在本研究中儲存空間可以分為兩個部分，第一個部分 SG 需要儲存密鑰 s:128bit，病人、醫生的密鑰則是要經過 SG 的密鑰加上自己產生的隨機數 U/D，隨機數的大小是 128bit，總合為 256bit，各個病歷的金鑰由於是由病歷參數計算得來所以無需儲存；第二部分為儲存病歷參數空間，一個病人不同份的病歷資料皆有不同的參數，每份病歷所需的空間為 128bit。

表四說明本研究與 Lee 和 Lee 機制[8]在 SG 與病人/醫生儲存空間在金鑰與參數的差別，由於 Lee 和 Lee 並不是使用階層式架構，所以沒有病歷參數的資料空間。

表四: 儲存空間比較表

儲存單位	空間名稱	Lee 和 Lee	本研究所提金鑰管理機制
可信任的憑證中心(SG)	可信任的憑證中心的密鑰(s)	128bit	128bit
病人(U)/醫生(D)	個人私鑰(SK_U/SK_D)	384bit(僅病人個人私鑰)	256bit
病人(U)	病歷參數(R_i)	無	128 bit

以下將分析 Lee 和 Lee 機制與本研究所提金鑰管理機制每個階段所需的時間，其中T_h表一 one-way hash 運算所需的時間; T_e表一 exponentiation 運算所需的時間; T_i表一 inverse 運算所需的時間; T_m表一 modular multiplication 運算所需的時間; T_S表一 symmetric encryption/ decryption 運算所需的時間; T_c: 表一 extend chaotic maps 運算所需的時間。

在註冊階段，SG 計算病人或醫生的個人私鑰，需要 $1T_c$；授權與金鑰產生階段(含病歷參數產生階段)，需要 $3T_c$+$2T_S$；註銷金鑰階段則是將已經授權的病歷資料的參數進行變更，要 $1T_c$+$1T_S$。表五說明本研究和文獻在各個不同的階段所需要的時間比較。

表五: 運算量比較表

階段名稱	Lee 和 Lee	本研究所提金鑰管理機制
註冊階段	$3T_h$+$3T_e$+$2T_i$+$5T_m$	$1T_c$
授權與金鑰產生階段	$6T_h$+$2T_S$/$7T_h$+$1T_i$+$1T_m$	$3T_c$+$2T_S$(含病歷參數產生階段)
註銷金鑰階段	$3T_h$+$3T_e$+$2T_i$+$2T_m$	$1T_c$+$1T_S$

藉由實機模擬在相同的軟體執行環境、相同的硬體設備以及相同的金鑰 bit 長度進行模擬測試。表六為實機模擬的環境，表七為 Lee 和 Lee 及本研究所提金鑰管理機制各個階段效率模擬獲得的時間。

表六: 實機模擬的環境

作業系統: windows 7 企業版 Service Pack 1 64 位元
開發語言: Scala 2.12.2-JAVA1.8.0_131 平台運行
金鑰 bit 長度: 256
中央處理器(CPU): Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz 3.30GHz
記憶體(RAM): 4G

表七: 各個階段效率模擬的時間

階段名稱	Lee 和 Lee	本研究所提金鑰管理機制
註冊階段	0.38032 Sec	0.0024Sec
授權與金鑰產生階段	0.004/0.0324 Sec	0.0232Sec
註銷金鑰階段	0.38032 Sec	0.0104Sec

伍、結論

本研究使用 HIPAA 安全規範中的四個原則為基礎，並以混沌映射的特性和運算速度快的優點，提出具有授權與註銷之金鑰管理機制，有效的管制醫生使用病歷資料需要病人的授權。病歷資料的安全性與完整性會受到進一步的保障，為達到以上目的，讓不同的病歷資料使用不同的病歷參數。由病歷參數產生授權金鑰對病歷資料進行保護，迫使醫生必須合法的請求病人授權，產生合法的授權金鑰進行病歷資料的解密。同時，在授權結束後，病人藉由病歷參數的更新來保障病歷資料的完整性。

本研究改善部份的安全問題，也增進了 HIPAA 的四個原則，此外儲存空間的比較，雖然較其他相關研究的方法多出了病歷參數所需的儲存空間；相較於一把金鑰即可對所有的病歷加密病歷進行相關的操作，其的安全性與完整性是有疑慮的。因此在本研究中，不同病歷使用不同的病歷參數，並且由這些病歷參數產生授權金鑰。而病人可對病歷參

數進行調整，其對於病歷資料的管控會更強，也更加符合 HIPAA 規範中的四原則裡病人控制的規範，可以達到不同病歷之間加密的保密性與病人授權不同資料完整性的需求，而在本研究中運算效能上也比相關的研究來的好。

未來計畫將本研究的結果應用於實際的電子病歷資料庫系統中，在實機環境也可以達到與本研究相同的高效能和安全性，並且符合 HIPAA 四個原則的安全規範。

Acknowledgement

本研究由科技部贊助，計畫編號 MOST 105-2221-E-320-003; 慈濟大學，計畫編號 TCRPP105004。

參考文獻

[1] S. G. Akl and P.D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," *ACM Transactions on Computer System*, vol. 1, no. 3, pp. 239-248, 1983.

[2] P. Bergamo, P. D'Arco, A.D. Santis and L. Kocarev, "Security of public-key cryptosystems based on chebyshev polynomials," *IEEE Transactions on Circuits and Systems—I: Regular Papers*, vol. 52, no. 7, pp. 1382-1393, 2005.

[3] Y. F. Chung, H.H. Lee and T.S. Chen, "Access control in user hierarchy based on elliptic curve cryptosystem," *Information Sciences*, vol. 178, no. 1, pp. 230-243, 2008.

[4] A. K. Das, N.Y. Paul and L. Tripathy, "Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem," *Information Sciences*, vol. 209, no. 20, pp. 80-92, 2012.

[5] J. Hu, H. Chen and T. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations," *Computer Standards & Interfaces* , vol. 32, no. 5-6, pp. 274-280, 2010.

[6] H. F. Huang and K.C. Liu, "Efficient key management for preserving HIPAA regulations," *Journal of Systems and Software*, vol. 84, no. 1, pp. 113-119, 2011.

[7] F. G. Jeng and C.M. Wang, "An efficient key-management scheme for hierarchical access control based on elliptic curve cryptosystem," *Journal of Systems and Software*, vol. 79, no. 8, pp. 1161-1167, 2006.

[8] W. B. Lee and C.D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 1, pp. 34-41, 2008.

[9] W. B. Lee, C.D. Lee and K.I.J. Ho, "A HIPAA-compliant key management scheme with revocation of authorization," *Computer Methods and Programs in Biomedicine*, vol. 113, no. 3, pp. 809-814, 2014.

[10] M. Nikooghadam and A. Zakerolhosseini, "Secure communication of medical information using mobile agents," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3839-3850, 2012.

[11] M. Nikooghadam, A. Zakerolhosseini and M.E. Moghaddam, "Efficient utilization of elliptic curve cryptosystem for hierarchical access control," *Journal of Systems and Software*, vol. 83, no. 10, pp. 1917-1929, 2010.

[12] V. Odelu, N.Y. Das and A. Goswami, "An efficient and secure key-management scheme for hierarchical access control in e-medicine system," *Journal of Medical Systems*, vol. 37, no. 2, pp. 1-18, 2013.

[13] H. Qian, J. Li, Y. Zhang and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation," *International Journal of Information Security*, vol. 14, no. 6, pp. 487-497, 2014.

[14] Y. Sun, H. Zhu and X. Feng, "A novel and concise multi-receiver protocol based on chaotic maps with privacy protection," *International Journal of Network Security*, vol. 19, no. 3, pp. 371-382, 2017.

[15] The USA government. HIPAA, 1996a; HIPAA, 1996b, pp. 104-191.

[16] S. Wu and K. Chen, "An efficient key-management scheme for hierarchical access control in E- medical system," *Journal of Medical Systems* vol. 36, no. 4, pp. 2325-2337, 2012.

[17] Q. Xie, B. Hu and T. Wu. "Improvement of a chaotic maps-based three-party password-authenticated key exchange protocol without using server's public key smart card," *Nonlinear Dynamics*, vol. 79, no. 4, pp. 2345-2358, 2015.

[18] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic system," *Chaos, Solitons and Fractals*, vol. 37, no. 3, pp. 669-674, 2006.

[19] L. Zhang, S. Zhu and S. Tang, "Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme," *IEEE Biomedical and Health Informatics*, vol. 21, no. 2, pp. 465-475, 2016.

[20] Y. Zhou, J. Zhou, F. Wang and F. Geo, "An efficient chaotic map-based authentication scheme with mutual anonymity," *Applied Computational Intelligence and Soft Computing*, vol. 2016, no. 1, pp. 1-10, 2016.

[21] H. Zhu, Y. Zhang, Y. Zhang and H. Li, "A novel and provable authenticated key agreement protocol with privacy protection based on chaotic maps towards mobile network," *International Journal of Network Security*, vol. 18, no. 1, pp. 116-123, 2016.

Biography

李添福，2008 年於國立成功大學資訊工程學系取得博士學位，目前為慈濟大學醫學資訊學系教授。研究興趣包含: 密碼學、網路安全、醫學資訊安全、無線網路、感測網路與認證金鑰協定等領域。

陳柏錡，2014 年於慈濟大學醫學院醫學資訊學系取得學士學位，目前為慈濟大學醫學院醫學資訊學系碩士班研究生。研究興趣包含: 醫學資訊安全、電子病歷金鑰管理機制與 HIPAA 的安全規範等領域。

黃思翰，2013 年於慈濟大學醫學院醫學資訊學系取得學士學位; 2015 年於慈濟大學醫學院醫學資訊學系取得碩士學位。研究興趣包含: 網路安全、醫學資訊安全、使用者認證與認證金鑰協定等領域。