東海大學電機工程研究所

碩士學位論文

# 經由金鑰管理機制控制存取之安全授權

Secure Authorization for Controlling Access

Via Key Management Scheme

指導教授：鐘玉芳 博士

研 究 生：劉智銘 撰

中華民國 102 年 6 月

# 誌　謝

即將結束這兩年的研究所生涯，在這兩年當中，遇到了很多的貴人，也受到了很多學業及生活上的幫助，因此，要感謝的人有很多；首先，感謝學校提供學生良好的學習環境，以及優良的師資陣容，讓學生得以在實驗室中無後顧之憂的做研究。

本論文可以順利的完成，首先要先感謝我的指導教授鐘玉芳老師，以及資訊管理系陳澤雄老師，這兩年來對本研究用心的指導及包容，讓我從錯誤中學習，培養我獨立思考的研究能力，及團隊學習的合作能力，在此向老師致上最深的謝意。

此外，我還要感謝口試委員賴飛羆教授、陳志賢教授、陳澤龍教授以及吳鎮宇教授對本論文提出許多寶貴的建議，對本論文有很大的幫助；接著，還要感謝同學健貿、峰祺與政宏在研究上總給予我適時的幫助，感謝學弟妹翰昱、富勝、坤昊、耀民與岱倫幫忙分擔我學校的相關事務及口試的相關事宜，使我能順利的口試並完成碩士論文。

最後，我還要感謝給我最大支持的家人，父母多年來對我的栽培，在我遇到挫折時總是給予我鼓勵與支持，讓我對研究能更有動力，以順利取得碩士學位，感謝你們。

劉智銘 謹誌

中華民國 102 年 6 月 1 日

# 摘　要

在資訊網路如此發達的社會中，有眾多使用者開始將個人或公司的重要資訊存放於網路環境中，以進行網路資源的分享，而網路環境屬於公開的環境，若是沒有對這些重要資訊的權限加以控管，保護其安全性，將可能會誘使網路上的惡意攻擊者對重要資料進行非法的存取，資料遭到侵入及破壞，不僅個人的隱私可能遭到侵犯，還可能會造成大量的財產損失，因此，在現今的社會，有效的存取控制系統已越來越為受到人們的重視。

為了防範這些惡意的網路攻擊，必須要建立一個有效且安全的存取控制系統，本論文提出一種基於 Lagrange 插值法的金鑰管理方式，以最為常見的存取控制模型作為主要的架構，再以橢圓曲線密碼系統來加強密鑰的安全性，採用 Lagrange 插值法的目的主要是為了讓各個密鑰間沒有相對的關係存在，且各密鑰的產生方式皆為隨機產生，因此要破解出密鑰是相對困難的，而採用橢圓曲線密碼系統主要則是為了讓網路攻擊者在破解的過程中遭遇橢圓曲線的離散對數問題，只要所採用的質數夠大，將會大大增加此系統的安全性，導致攻擊者難以破解出密鑰的相關資訊。

存取控制的應用也相當廣泛，例如：電子化公文、線上電視系統及無線網路等，由先前的文獻得知，行動代理人技術在存取控制與金鑰管理機制所提出的方法上，將會有耗費行動代理人的空間，以及安全性仍稍有缺陷等問題，而且應用於醫療系統上也是還存有改善的空間，因此，本論文將研究方法套用於此行動代理人環境，期望能將以上問題加以改善，接著在對本研究方法進行安全性的分析，嘗試以網路攻擊者的角度探討可能使用的攻擊，分析網路上較為常見的四種攻擊方式：外部攻擊、內部攻擊、協同攻擊以及方程式攻擊，由分析的

結果顯示，以上四項攻擊皆會因為密鑰間沒有存在相對關係或是橢圓曲線上的離散對數問題，而造成網路攻擊者破解密鑰的難度過高，也大為增加密鑰的安全性，證實本論文所提出的方法可以更為有效率且安全地保護行動代理人。

**關鍵字**：存取控制、金鑰管理、行動代理人、橢圓曲線密碼系統、Lagrange 插值法

# Abstract

With the rapid development of the Internet, many users start to take action putting personal or company information on it, and share with everyone. The Internet is public as it were, if we do not control its limit of authority to assure security, it's possible that those attackers do illegal access of important information and destroy them. Not only personal privacy is invaded, but the mass property damage. Therefore, effective access control system has been more and more emphasized these days.

To fight against these network attacks, it is necessary to establish an effective and safe access control system; here we proposed a scheme, a key management which called Lagrange interpolation mainly takes access control model as framework, and use Elliptic Curve Cryptography system to enhance security. The fact we choose Lagrange interpolation is the key we use is randomized, no relationship between each key, so is relatively hard. As Elliptic Curve Cryptography system, we want attackers to encounter Elliptic Curve Discrete Logarithm Problem. Once the prime number is big enough, attackers will have trouble deciphering the key.

Access control is so comprehensive, such as electronic documents, online television systems and wireless networks and so on, from previous literature; mobile agent technology applied in access control and key management would waste space and do exist some flaws in security, also we still have a lot of works to do on medical application. Hence, we propose these schemes in mobile agent in order to reach improvement, and then analyze of security and try to simulate what attackers will do. We conclude four common attacks: External Collective Attack, Internal

Attack, Collusion Attacks and Equation Breaking Attack. As results, attackers are hard to decipher the key because of no relationship between each key and will face Elliptic Curve Discrete Logarithm Problem. We confirm that the proposed schemes can be more efficiently and safety to protect mobile agent.

**Keywords:** Access Control, Key Management, Mobile Agent, Elliptic Curve Cryptography, Lagrange Interpolation

# Contents

# List of Figures

# List of Tables

# Chapter 1 — Introduction

## 1.1 Overview

The Internet is so prosper and has been widely use today, it's so common that lots of entrepreneur upload their important information to free web such as client's data, rather than traditional paper records. Despite digital era, people have already changed the traditional operation and turn them into digitalize and network-transmitted system to achieve exchanging of information and knowledge. In this era, we pay a lot of attention on computer cryptography and information security, computer network and technology rapidly grow that generally be applied to a multi-user environment. Therefore, the sharing of resources and access has become very common in today's society. Academic and business need to have ways to protect information from unauthorized access, so access control gradually becomes more and more important [2].

Access control has applied quite a lot as well, like database management system, online pay-tv system and electronic subscription system, etc. mobile agent is definitely one of the important applications. Mobile agent is a self-distributed computing program between each host and switch information host to host on Internet, also it is autonomy that can decrease delays of transmission, reduce network traffic and apply in sorts of platform. As its character of fault-tolerance, adjustment and personalization [6], mobile agent is more wisdom to send message and can exchange with other individual resource systems or different mobile agents.

Mobile agent's function is to take assigned tasks by users. It can be

dispatched to the Internet or other relates services and platforms in order to search or deal with information, when mobile agent finish assigned tasks, it will return to users; with these qualities, the mobile agent is very suitable to be used in medical network system. Like transmit or exchange its contents from a particular hospital information system to another hospital host, and execute the given tasks authorized by users to finish their works.

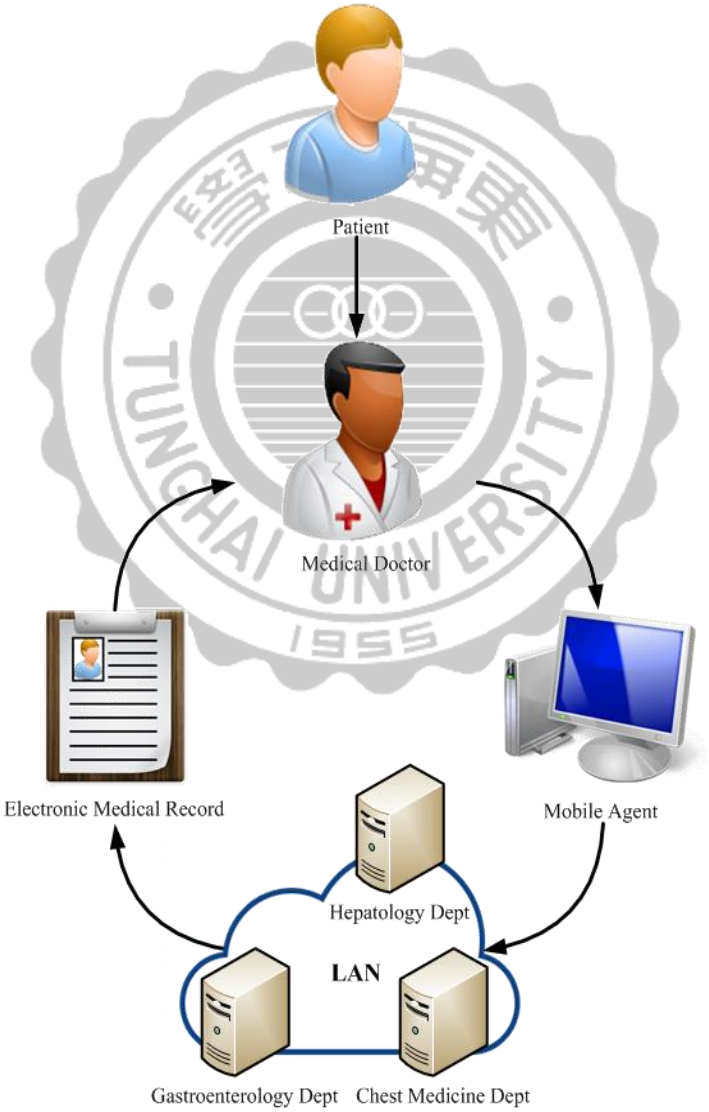


Figure 1: Structure of Mobile Agent

Figure 1 is basic structure and operation working on medical system. If the patient goes to the medical department for treatment, the doctor will enter the patient's simple information and send request to mobile agent (such as searching a patient's illness history and medical records in every medical department), when mobile agent gets the commission, it will quickly collect data or exchange information with other mobile agent to specific host in department according to the original process, and automatically take different strategy and path to search information patients and doctors' want, these can gain efficiency and reduce time. Assume that mobile agent search to liver department first; it will find the patient's relate records there and access the data, and send it to the next medical department to integrate until finish searching the data of all departments, and then back to the original medical department. Finally, compile all the information together into an electronic medical record to the doctor.

Although the mobile agent technology brings great convenience for medical or other business, it still needs to exchange information on the Internet. Concerning the Internet is public that every areas or countries are connected, so it is necessary to have complete key management and access control to prevent illegal behaviors from attackers. Key management and access control are based on the Lagrange interpolation polynomial and Elliptic curve cryptography. Because Lagrange interpolation polynomial is not difficult to compute and Elliptic curve cryptography is hard to be deciphered, access control mechanism becomes more secure and efficient. Meanwhile, we do analysis of security to common attacks. Like internal attack, we act as attackers to

assure the feasibility of the authentication mechanism, security and efficiency, and whether can guarantee its safety or not when the mobile agent is executing the commission like access patients' personal medical record in different hospitals. If so, we definitely can promote efficiency on key management and protect mobile agent system.

Many researchers have proposed some issues about access control mechanisms and solutions, however, these schemes still have some defects in the safety and efficiency of them. The key management and access control mechanism we provide here emphasized on access control architecture. We use mathematical theory and encryption technology different from the past, next chapter will be introduced in research motivation, purpose, and structure.

## 1.2 Research Motivation

Nowadays, most of the information system has been used in the network environment, but it has the feature of accessing to the public, so it's not safe. And in the transmission process, the exchange of information is more likely to be stolen or destroyed, fortunately we have the solution. From previous literature; people make use of encryption and decryption technology to protect confidential documents or resources, the higher authority can load electronic files and documents from the lower authority according to the rule of access control. Therefore, the design and security access control technology is very important today, not only protect the confidential information and resources, but ensure that only the higher authority can access the lower's sensitive information [2].

Mobile agent is an important application of access control mechanisms,

and brings great convenience to medical institutions, but it still has a lot to improve in aspect of security and performance. From current medical condition, after the diagnosis they would leave medical records, however, no medical institutions have all the medical records of patients that they are not enough to fully understand their situation.

There are some problems with medical condition as following [4]:

1. Traditional medical records could easily waste of space and time: most of traditional medical records are hand written; they are hard to identify and easily be destroyed. In addition, traditional medical records really waste of space.
2. Unnecessary waste of resources: like repeated check and waiting time lead to waste of medical resources, increase investment in health care information software, hardware equipment and manpower, that's why medical costs increase every year.
3. Privacy issues: traditional medical records are easily taken that the privacy had been infringed.
4. Difficult to control statistics: in efficient to grasp of the statistics of various diseases, especially in factious diseases.
5. Real-time exchange of new types of medical researches: for cannot reflect medical reports, will exchange medical information and solution.
6. Retrieve medical records slowly: when there is emergency, traditional medical records take more time to diagnose than electronic medical records.

## 1.3 Research Target

Concerning security problems in public network of mobile agent and those deflects we encounter, to correct them, what we mentioned here is to establish the completely safe access control mechanism. We applied Lagrange interpolation polynomial and Elliptic curve cryptography in decryption key and try to keep the access control mechanism in medical environment with mobile agent. And mobile agent here represented the doctor, though remote collection and prescription, with mobile agent, it will be secure to exchange medical information. The example here we mentioned about mobile agent applied in electronic medical records just want to prove that [19]:

1. To reduce the waste of medical resources: directly access in database after medical records digitalized, it won't waste any space and it's easy to retrieve medical records. Meanwhile we do not need too much manpower; instead, we can make use of them in other purposes just to increase efficiency.
2. To complete and secure medical records: doctors and patients can quickly find the basic personal state and inspection report that doctors take priority to diagnose accurately, and through identity authentication and authorized to protect the privacy of personal health.
3. To repeat key management: it will effectively lower number of access because of the structure and provide secure key management.
4. To offer real-time information: doctors and patients can immediately obtain complete medical records when they need.

5. To provide good medical information: provide new medical research to disease solutions to nurses.
6. To be provided with statistics: statistics for various diseases in order to make public understand and academic research purposes.

## 1.4 Structures

This thesis divided to five sections. First part is introduction in background of overview, motivation, purpose of study, described the importance of information security and access control and mobile agent. Second part is mathematical background and relevant research, including key management, access control, Elliptic curve cryptography and Lagrange interpolation polynomial. Then is the core values of thesis, it proposed scheme how to generate and derive key based on Lagrange interpolation polynomial. In the fourth section we did analysis of security, hold four attacks and prove they are safe enough. Finally we give it a conclusion.

# Chapter 2 — Mathematical Backgrounds and Correlation Research

We mainly discuss correlation research and mathematical backgrounds, including Lagrange interpolation polynomial, access control and Elliptic curve cryptosystem.

## 2.1 Public-Key Cryptosystem

Public-Key cryptosystem is also called Asymmetric Cryptosystem or Two-Key Cryptosystem. See as Figure 2. Public-Key cryptosystem is proposed by two scholars, Diffie and Hellman in 1976. It can deal with key-distribute and manage in Private-Key Cryptosystems and need less encryption key. So there are a lot of information security program adopt to Public-Key cryptosystem. In the system, the key used to encrypt a message is not the same as the key used to decrypt, each user has a pair of keys, a public encryption key and a private decryption key, and they are related mathematically that calculate the private key from the public key is impossible [1].

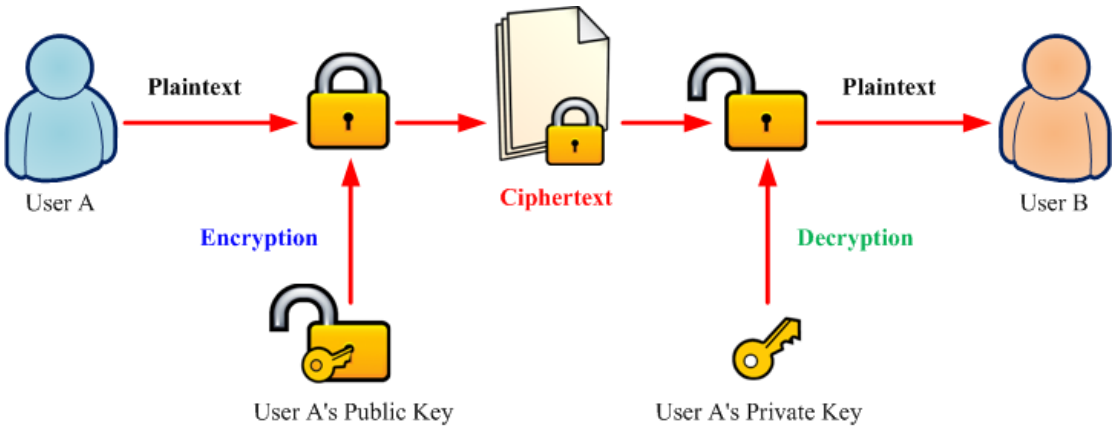


Figure 2: Public-Key Cryptosystem

Advantages of Public-Key cryptosystem:

1. Protect the privacy of the information: anyone can use public key to encrypt the plaintext. It does not require the Internet to exchange of one (or more) secret keys between the sender and receiver. They own their keys, so it's more secure.
2. Non-repudiation: if we use private-key to deal with plaintext, everyone can get signature with correlated public key. But only users themselves have private key that we can assure the signatures are done by them. It's also called Digital signature.
3. Simplify key-distribution and management: just a pair of keys which must be shared and kept private by both the sender and the receiver, so this encryption system is very suitable to apply in the distributed network environment.

Although the Public-Key cryptosystem has these advantages, the encryption and decryption process is so inefficient, the common public-key cryptosystem have RSA, ElGamal, and Elliptic Curve [3].

Public Key Infrastructure, $PK_i$ is the structure based on the cryptography, in Public-Key cryptosystem; the private key is a secret. Others cannot know whether the public key is correlated with the private key or not, and no authentication. Hence, the public key generates the certificate that it can execute the data's privacy.

Certificate works as a personal electronic card, including serial number, user name, public key and the expiration date. But it's impossible that they all published by one single certificate center, through public key infrastructure, we can organize every single certificate center to verify and rely on each other by certification service.

## 2.2 Lagrange Interpolation

Lagrange interpolation is named after a French mathematician Joseph Louis Lagrange, which used for polynomial interpolation. There are many practical mathematic problems indicate its laws by function, we can prove the function by observation or experiment.

Lagrange interpolation gives a known polynomial function pass through the two-dimensional plane. $(x_0, y_0)$, $(x_1, y_1)$, …, $(x_n, y_n)$ , only one will under to the n of Lagrange polynomial.

In numerical analysis and mathematical application, suppose that a number *y* and another is *x*, they must be complex between each other. And it's hard to understand their relationship by experiment; we can get a corresponding polynomial by the Lagrange's scheme, it will pass a finite set of points on the x-y plane, then we called it Lagrange interpolation [7].

$$\ell_j(x) = \prod_{i=0, i\neq j}^{n} \frac{x - x_i}{x_j - x_i} = \left(\frac{x - x_0}{x_j - x_0}\right) \cdots \left(\frac{x - x_{j-1}}{x_j - x_{j-1}}\right) \left(\frac{x - x_{j+1}}{x_j - x_{j+1}}\right) \cdots \left(\frac{x - x_n}{x_j - x_n}\right), \quad 1 \le j \le n$$

$\ell_j(x)$ is the Lagrange polynomial, also known as the interpolation bases function, if we set $x_i = 1$, other $x_j$ $(i \neq j) = 0$, then:

$$\ell_j(x) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

So the Lagrange interpolation will be:

$$L(x) = \sum_{j=0}^{n} y_j \ell_j(x)$$

Let's take an example, assume that a two-order polynomial pass through three points on the plane, they are (3, 7), (4, 9) and (5, 12), so the Lagrange bases function:

$$\ell_1(x)=\left(\frac{x-4}{3-4}\right)\left(\frac{x-5}{3-5}\right)$$

$$\ell_2(x)=\left(\frac{x-3}{4-3}\right)\left(\frac{x-5}{4-5}\right)$$

$$\ell_3(x)=\left(\frac{x-3}{5-3}\right)\left(\frac{x-4}{5-4}\right)$$

Then use Lagrange interpolation to get the only two-order polynomial $L(x)$, as below:

$$\begin{aligned}L(x) &= f(3)\ell_1(x)+f(4)\ell_2(x)+f(5)\ell_3(x)\\ &=7\times\left(\frac{x-4}{3-4}\right)\left(\frac{x-5}{3-5}\right)+9\times\left(\frac{x-3}{4-3}\right)\left(\frac{x-5}{4-5}\right)+12\times\left(\frac{x-3}{5-3}\right)\left(\frac{x-4}{5-4}\right)\\ &=\frac{1}{2}x^2-\frac{3}{2}x+7\end{aligned}$$

From above we know f (3) = 7, f (4) = 9, f (5) = 12, and use the formula to calculate predicted values, such as f (12), we bring $x$ = 12 into $L(x)$, then we can find f (12) =$L$ (12) =61.

## 2.3 Access Control

Access control is the selective restriction of access to a place or other resource, which means to allow or ban the lower authority to access the resource, is one of the control software or data access such as use key management to protect illegal operation of information from hackers. The act of accessing may mean consuming, entering, or using. Access control can be done by consuming or authorizing, the most common security risk of an access control system is unauthorized access, data destruction, wrong permission and privacy exposed.

In information security, general access control includes authorization, authentication, access approval and audit, a more narrow definition of access control is to only cover access approval, where the system makes a decision to grant or reject an access request from an already authenticated subject; based on what the subject is authorized to access. Authentication and access control are often combined into a single operation, so that access is approved based on successful authentication, or based on an anonymous access token. Authentication methods and tokens include passwords, biometric scans, physical keys, electronic keys and devices, hidden paths, social barriers, and monitoring by humans and automated systems [5].

The first applications of access control in hierarchies appeared in information systems. Typical applications for such systems are access rights management of file systems and databases. It has been widely adopted by the military communications fields, government departments and private corporations for a long time. Nowadays, access control is also applied in various fields. When access control happens, there exist different access rights between users and resources. Therefore, access control is indispensable in many fields. That is why the application field of access control is very large and includes applications from many domains [2]. Table 1 shows some interesting applications of access control, and the resources to secure in each application.

Table 1: Application on Access Control

| Application | Resources |
|---|---|
| Database management systems | Cells, lines, rows, tables, views, etc[8-10] |
| Electronic subscription | Composition, papers or publications[11] |
| Online Pay-TV systems | Video streams[12, 13] |
| Wireless transmission | Broadcasting [14-16] |
| Government departments, business corporations | Files, e-mails[17] |
| Online social networks (OSNs) | Messages, data pools, etc[17] |

Computer communication systems usually use a user hierarchy to solve problems of access control, it contains different security level and the data will be allocated and ordered. See as Figure 3.

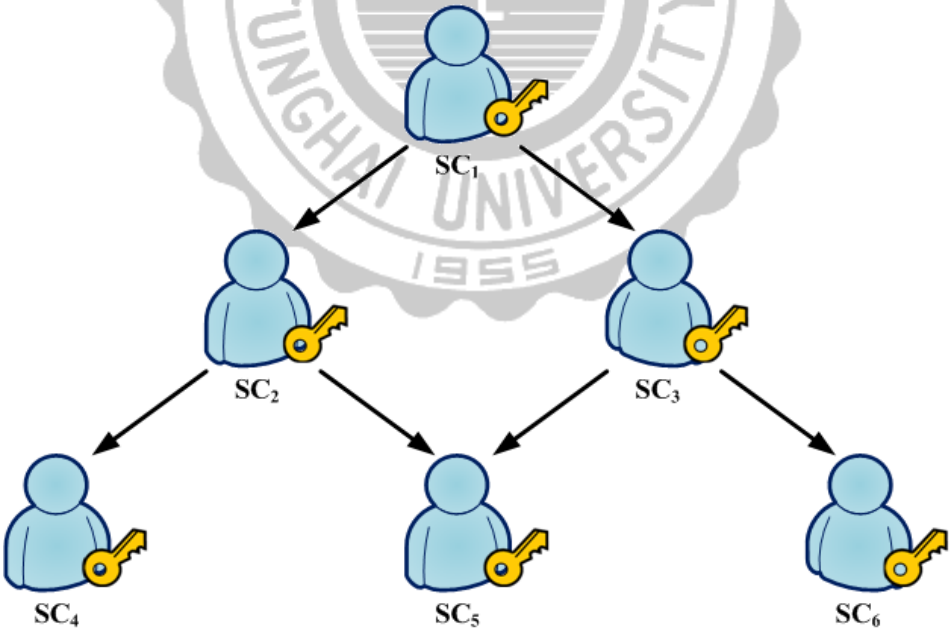


Figure 3: Hierarchical Relationship Structure

As shown above, the brief induction about the algorithm applied in this

paper. Under the structure, if the relationship of $SC_j \leq SC_i$ is valid, public relational parameter $R_{ij}$ must be constructed to contain security class's identification and encryption key. For example, when $SC_5 \leq SC_2$ is valid, $SC_2$ is logically allowed to access $SC_5$'s data. Before $SC_2$ could obtain access to $SC_5$'s data, the public relational parameter, $R_{25}$, needs to be constructed and which would contain $ID_5$ (identity) and $SK_5$ (secret key) of $SC_5$. Thus, $SC_2$ could use $R_{25}$ to calculate $SC_5$'s secret key through the formula and then obtain information from $SC_5$. The construction of the public relational parameter is essential to the proposed scheme. Because of hierarchical relationship structure, it is possible to have cross-relational class existed. In this case, we may use a top-down approach to derive the decryption key, $DK_s$. By assumption, $SC_1$ is permitted to access the data of $SC_5$. The public relational parameter, $R_{15}$, must be constructed, but there is no direct link between $SC_1$ and $SC_5$. So, $SC_1$ must get passed through either $SC_2$ in order to get the access to $SC_5$. The flow chart of algorithm is as shown below [18].

With increasing of hierarchical relationship structure, the higher-security user needs the bigger access storage to accept lower's secret key. Besides that, it's hard to key security if there are too many secret keys. So we need to set up the new law to distribute the key to every user, through the key, they can calculate the key in low hierarchy. We have to prevent complex calculation during the key-produced. In other words, for $SC_j \leq SC_i$, $SC_i$ can use own private key to calculate $SK_j$ from $SC_j$.

In the consultation, medical staffs can use the key of the highest level permission, the highest permission of mobile agent can collect the

patient's information within the permission, and it will not cause the overload of system or the illegal access of outside the permission. In writing the consultation data, it can write the lowest common level of information of staffs. The medical staffs can access the data next time, and it also will not cause the loading of system.

## 2.4 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz [20] and Victor S. Miller [21] in 1985.

The primary benefit promised by ECC is a smaller parameters, smaller key size, reducing bandwidth, transmission requirements and less processing unit [22]. In some cases, ECC provides smaller key size than other methods such as ECC are more secure compare to RSA. RSA and ElGamal system need 1024 bits to achieve enough security standards, and ECC only needs 160 bits. Because of high security and efficient EC provided, it's a worth to weight in the system [23, 24].

Elliptic curves can be divided into two families: prime curves and binary curves. $Z_p$ is suitable for software's application, because it doesn't need to expand spare for useless bits, but ($GF$ (2$n$)) is not. ($GF$ (2$n$)) is more suitable for hardware's application, because just a few logic gates can establish a intact cryptography. Variable, and the coefficient of the elliptic curve are derived from the finite field element, with that, it gains efficient of calculating on ECC.

In the finite field $Z_p$, defined modulo a prime $p$, an Elliptic curve is

represented as $E_p(a,b): y^2 = x^3 + ax + b \pmod{p}$ , where $a, b$ and $4a^3 + 27b^2 \pmod{p} \neq 0$ . The condition, $4a^3 + 27b^2 \pmod{p} \neq 0$ , is necessary to ensure that $y^2 = x^3 + ax + b \pmod{p}$ is smooth algebraic plane curve, has no repeated factors, and only one solution. So we can follow this principle to define a finite Abelian group, including a point at infinity, denoted by *O*, which is also the additive identity. The point at infinity *O* is the third point of intersection of any straight line with the curve, so that this line contains the points (*x*, *y*), (*x*, -*y*) and *O*.

For points on an Elliptic curve, an addition operation, denoted by +, is defined. Some of the basic properties of this operation are given below.

（1）$O + B = B$ and $B + O = B$, $O$ is the additive identity

（2）$- O = O$

（3）$B + (- B) = (- B) + B = O$, $(x, -y)$ is negative point of $(x, y)$

（4）$(B + Q) + R = B + (Q + R)$

（5）$B + Q = Q + B$

（6）n$B = B + B + ... + B$（n times）

Two points $B = (x_p, y_p)$ and $Q = (x_q, y_q)$, sum $R = (x_r, y_r) = B + Q$ defined as below:

$$\begin{aligned} x_r &= \lambda^2 - x_p - x_q \pmod{p} \\ y_r &= \lambda(x_p - x_r) - y_p \pmod{p} \end{aligned}$$ , where $$\lambda = \begin{cases} \dfrac{y_q - y_p}{x_q - x_p} \pmod{p}, & \text{if } B \neq Q \\ \dfrac{3x_p^2 + a}{2y_p} \pmod{p}, & \text{if } B = Q \end{cases}$$

Consider as an example the Elliptic curve

$E_{23}(3, 2): y^2 = x^3 + 3x + 2 \pmod{23}$ , $a = 3, b = 2 \in Z_{23}$ and $4a^3 + 27b^2 = 216 \pmod{23} = 9 \neq 0$, points over the Elliptic curve $E_{23}(3, 2)$ are shown in Table 2 [25].

Table 2: Points on Elliptic Curve $E_{23}(3, 2)$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| (0, 5) | (0, 18) | (1, 11) | (1, 12) | (2, 4) | (2, 19) | (4, 3) | (4, 20) |
| (5, 8) | (5, 15) | (6, 4) | (6, 19) | (8, 8) | (8, 15) | (9, 9) | (9, 14) |
| (11, 3) | (11, 20) | (12, 8) | (12, 15) | (13, 9) | (13, 14) | (15, 8) | (15, 15) |

Example:

Let $B = (x_p, y_p) = (0, 5)$ and $Q = (x_q, y_q) = (1, 11)$ in $E_{23}(3, 2)$. Since $B \neq Q$, we obtain $\lambda$ as follows:

$$\lambda = \frac{11-5}{1-0} \pmod{23} \equiv 6$$

We now obtain $R = (x_r, y_r) = B + Q$ as follows:

$x_r = \lambda^2 - x_p - x_q \pmod{p} = 6^2 - 0 - 1 \pmod{23} \equiv 13$

$y_r = \lambda(x_p - x_r) - y_p \pmod{p} = 6(0 - 13) - 5 \pmod{23} \equiv -83 \pmod{23} \equiv 9$

Thus, $B + Q = R = (13, 9)$.

To calculate $2B$ with $B = (0, 5)$, we must first derive $\lambda$ as follows:

$$\lambda = \frac{3x_p^2 + a}{2y_p} \pmod{p} = \frac{3 \times 0^2 + 3}{2 \times 5} \pmod{23} \equiv \frac{3}{10} \pmod{23} \equiv 3$$

Now $x_r$ and $y_r$ can be derived as below:

$x_r = \lambda^2 - x_p - x_q \pmod{p} = (3^2 - 0 - 0) \bmod 23 \equiv 9 \bmod 23 \equiv 9$

$y_r = \lambda(x_p - x_r) - y_p \pmod{p} = (3(0 - 9) - 5) \bmod 23 \equiv -32 \bmod 23 \equiv 14$

Thus, $B + B = 2B = (9, 14)$.

$B$ and $Q$ are two points on the Elliptic curve cryptosystem, and n is a constant value, such that $B = n \times Q$. If n is very large, then when the two points, $B$ and $Q$ are made public, people who attempt to guess n face some difficulty. This problem is known as the Elliptic Curve Discrete Logarithm Problem (ECDLP) [26].

# Chapter 3 — Research Method

In this section, we introduce applications on access control of key generation first, and then it's calculating. We will show an example. We basically use Lagrange interpolation polynomial and Elliptic curve cryptography to encrypt and manage the key and use of mobile agent technology to collect electronic medical record and lead the relationship structure into hospitals. We divided it to $SC_1$, $SC_2$, …,$SC_n$ they have different permission according to the relationship structure, the higher authority can access from the lower authority after going through the algorism we use here. As for parameter and function, see Table 3.

Table 3: Table of Parameter System

| Symbol | Definition |
|---|---|
| *CA* | The authorized certification center, responsible for system maintenance and management |
| $SC_i$ | The $i^{th}$ server of user |
| $SK_i$ | The secret key for $SC_i$ |
| $ID_t$ | The identifying name of the confidential documents |
| $DK_t$ | The decryption key for $ID_t$ |
| $l_{i,t}(x_{i,t})$ | *CA* generated interpolation polynomial for $SC_i$ and the access authority of $ID_t$, where $x_{i,t}$ is the point of the elliptic curve $Ep\ (a, b)$ |
| $F_{DKt}(x_{i,t})$ | The public access polynomial of the decryption key $DK_t$ |

### 3.1 Key Generation Phase

Step 1. *CA* define Elliptic curve in a finite field $Z_p$, $E_p(a,b):y^2=x^3+ax+b(\text{mod } P)$, and it must make sure $4a^3+27b^2(\text{mod } P)\neq 0$, $P$ is the big prime number.

Step 2. *CA* select a reference point $G=(x, y)$ in Elliptic curve.

Step 3. *CA* choose different decryption keys $DK_t$ ($t$=1, 2, …, $m$; $m$ is the number of the mobile agent) to each confidential document.

Step 4. *CA* choose different secret keys $SK_i$ ($i$=1, 2, …, $n$; $n$ is the mobile agent visits to hosts ) where $SK_i$ keeps private.

Step 5. Establish a access polynomial:

$$F_{DK_t}(x) = x \times DK_t \times \sum_{DK_t \le SC_i} x_{i,t}^{-1} l_{i,t}(x)$$

And $l_{i,t}(x)$ is a Lagrange interpolation polynomial

$$l_{i,t}(x) = \prod_{s=1, s\neq i}^{n} \frac{x - x_{s,t}}{x_{i,t} - x_{s,t}} = \left(\frac{x - x_{1,t}}{x_{i,t} - x_{1,t}}\right) \cdots \left(\frac{x - x_{s-1,t}}{x_{i,t} - x_{s-1,t}}\right) \left(\frac{x - x_{s+1,t}}{x_{i,t} - x_{s+1,t}}\right) \cdots \left(\frac{x - x_{n,t}}{x_{i,t} - x_{n,t}}\right)$$

The formula above, $DK_t \le SC_i$ means $SC_i$ has been authorized by the confidential document $t$ while $x_{i,t} = (ID_t \| SK_i)G(\text{mod } p)$. $ID_t$ is the identity name, and $\|$ is the connecting operator in the mathematical symbols.

### 3.2 Key Derivation Phase

Step 1. Set permission to the decryption key $DK_t$ that $SC_i$ want to access.

Step 2. $SC_i$ get the decryption key $DK_t$ by the secret key $SK_i$ and the access polynomial $F_{DKt}(x)$.

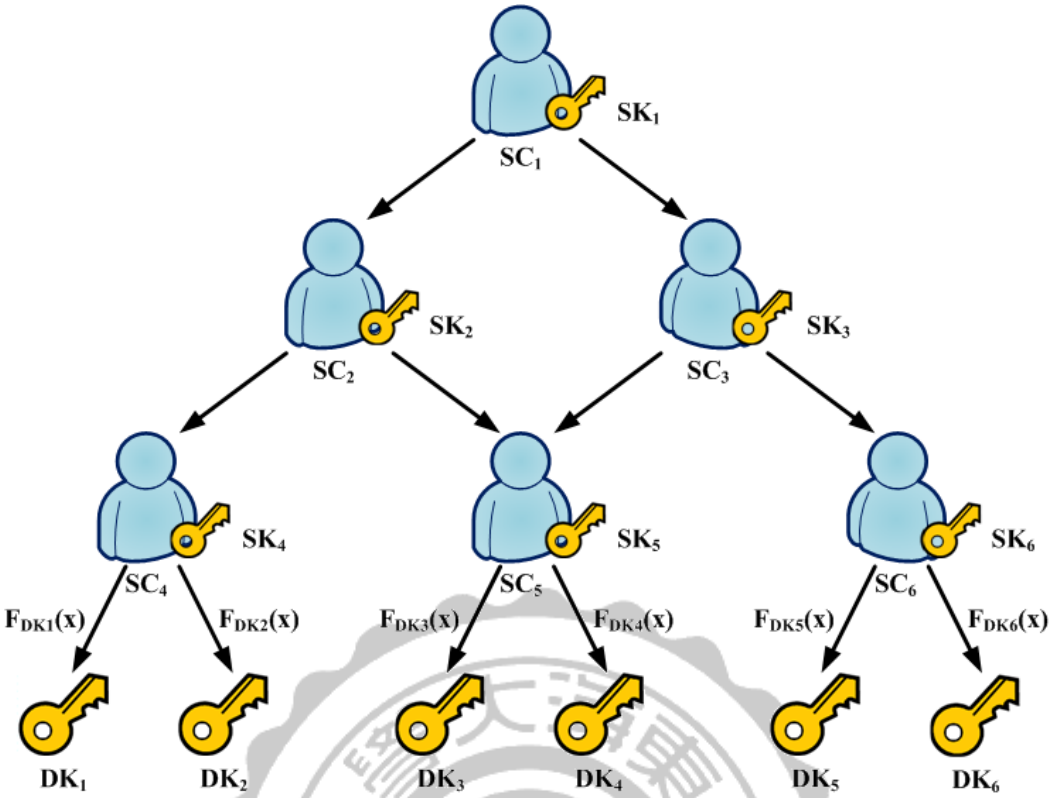


Figure 4: Hierarchical Access Control Structure

In mobile agent, every member and confidential document will obtain the key. Member's key is to derive of the lower hierarchy to obtain access key they want from relation. Confidential document' key is called the decryption key; it is to decrypt decryption files or documents. The advantage of the method is that each member needs only one key to decrypt all permission documents, it can save storage and mobile agent doesn't need extra calculation just to assure the security; and then we must put hospital's relationship structure into corresponding security class and server host or database that we want to access, finally mission completed. Like in Figure 4, patient's medical record has been separated to six parts, each of it has its decryption key, it is $DK_1$, $DK_2$, …, $DK_6$, $SC_4$ can access $DK_1$ and $DK_2$; $SC_5$ can access $DK_3$ and $DK_4$. $SC_2$ is higher than $SC_4$ and $SC_5$, so $SC_2$ can access four decryption keys ($DK_1$, $DK_2$, $DK_3$ and

$DK_4$) and so on.

### 3.3 Example

Propose that the key of a confidential document is $DK_t$, decrypt it and then send it to each designate department; if a user has the permission to decrypt the key, and then put the secret key $SK_i$ into the Lagrange interpolation polynomial so that the corresponding decryption key $DK_t$ will be generated.

In the process of encryption, CA will establish a public access polynomial $F_{DKt}(x)$, finally bring $x_{s,t} = (ID_t \| SK_s) G (\mathrm{mod}\, p)$ into Lagrange interpolation polynomial to find decryption key. We pretend $SC_1$ would like to get the decryption key $DK_2$, the detail of encryption and decryption are here as below:

$$
\begin{aligned}
l_{1,2}(x) &= \left(\frac{x-x_{2,2}}{x_{1,2}-x_{2,2}}\right)\left(\frac{x-x_{3,2}}{x_{1,2}-x_{3,2}}\right)\left(\frac{x-x_{4,2}}{x_{1,2}-x_{4,2}}\right)\left(\frac{x-x_{5,2}}{x_{1,2}-x_{5,2}}\right)\left(\frac{x-x_{6,2}}{x_{1,2}-x_{6,2}}\right) \\
&= \frac{x-(ID_2 \| SK_2)G(\mathrm{mod}\, P)}{(ID_2 \| SK_1)G(\mathrm{mod}\, P)-(ID_2 \| SK_2)G(\mathrm{mod}\, P)} \times \frac{x-(ID_2 \| SK_3)G(\mathrm{mod}\, P)}{(ID_2 \| SK_1)G(\mathrm{mod}\, P)-(ID_2 \| SK_3)G(\mathrm{mod}\, P)} \\
&\quad \times \frac{x-(ID_2 \| SK_4)G(\mathrm{mod}\, P)}{(ID_2 \| SK_1)G(\mathrm{mod}\, P)-(ID_2 \| SK_4)G(\mathrm{mod}\, P)} \times \frac{x-(ID_2 \| SK_5)G(\mathrm{mod}\, P)}{(ID_2 \| SK_1)G(\mathrm{mod}\, P)-(ID_2 \| SK_5)G(\mathrm{mod}\, P)} \\
&\quad \times \frac{x-(ID_2 \| SK_6)G(\mathrm{mod}\, P)}{(ID_2 \| SK_1)G(\mathrm{mod}\, P)-(ID_2 \| SK_6)G(\mathrm{mod}\, P)}
\end{aligned}
$$

$$
\begin{aligned}
l_{2,2}(x) &= \left(\frac{x-x_{1,2}}{x_{2,2}-x_{1,2}}\right)\left(\frac{x-x_{3,2}}{x_{2,2}-x_{3,2}}\right)\left(\frac{x-x_{4,2}}{x_{2,2}-x_{4,2}}\right)\left(\frac{x-x_{5,2}}{x_{2,2}-x_{5,2}}\right)\left(\frac{x-x_{6,2}}{x_{2,2}-x_{6,2}}\right) \\
&= \frac{x-(ID_2 \| SK_1)G(\mathrm{mod}\, P)}{(ID_2 \| SK_2)G(\mathrm{mod}\, P)-(ID_2 \| SK_1)G(\mathrm{mod}\, P)} \times \frac{x-(ID_2 \| SK_3)G(\mathrm{mod}\, P)}{(ID_2 \| SK_2)G(\mathrm{mod}\, P)-(ID_2 \| SK_3)G(\mathrm{mod}\, P)} \\
&\quad \times \frac{x-(ID_2 \| SK_4)G(\mathrm{mod}\, P)}{(ID_2 \| SK_2)G(\mathrm{mod}\, P)-(ID_2 \| SK_4)G(\mathrm{mod}\, P)} \times \frac{x-(ID_2 \| SK_5)G(\mathrm{mod}\, P)}{(ID_2 \| SK_2)G(\mathrm{mod}\, P)-(ID_2 \| SK_5)G(\mathrm{mod}\, P)} \\
&\quad \times \frac{x-(ID_2 \| SK_6)G(\mathrm{mod}\, P)}{(ID_2 \| SK_2)G(\mathrm{mod}\, P)-(ID_2 \| SK_6)G(\mathrm{mod}\, P)}
\end{aligned}
$$

$$l_{4,2}(x)=\left(\frac{x-x_{1,2}}{x_{4,2}-x_{1,2}}\right)\left(\frac{x-x_{2,2}}{x_{4,2}-x_{2,2}}\right)\left(\frac{x-x_{3,2}}{x_{4,2}-x_{3,2}}\right)\left(\frac{x-x_{5,2}}{x_{4,2}-x_{5,2}}\right)\left(\frac{x-x_{6,2}}{x_{4,2}-x_{6,2}}\right)$$
$$=\frac{x-(ID_2\|SK_1)G(\text{mod }P)}{(ID_2\|SK_4)G(\text{mod }P)-(ID_2\|SK_1)G(\text{mod }P)}\times\frac{x-(ID_2\|SK_2)G(\text{mod }P)}{(ID_2\|SK_4)G(\text{mod }P)-(ID_2\|SK_2)G(\text{mod }P)}$$
$$\times\frac{x-(ID_2\|SK_3)G(\text{mod }P)}{(ID_2\|SK_4)G(\text{mod }P)-(ID_2\|SK_3)G(\text{mod }P)}\times\frac{x-(ID_2\|SK_5)G(\text{mod }P)}{(ID_2\|SK_4)G(\text{mod }P)-(ID_2\|SK_5)G(\text{mod }P)}$$
$$\times\frac{x-(ID_2\|SK_6)G(\text{mod }P)}{(ID_2\|SK_4)G(\text{mod }P)-(ID_2\|SK_6)G(\text{mod }P)}$$

Access polynomial will be seeing as follow:

$$F_{DK_2}(x)=x\times DK_2\times\left\{\left(x_{1,2}\right)^{-1}l_{1,2}(x)+\left(x_{2,2}\right)^{-1}l_{2,2}(x)+\left(x_{4,2}\right)^{-1}l_{4,2}(x)\right\}$$

Then, $SC_1$ would like to get the decryption key $DK_2$ through access polynomial. Hence, we need to put $x_{1,2}=(ID_2\|SK_1)G(\text{mod }p)$ into Lagrange interpolation polynomial one by one.

Then we bring the result calculated with Lagrange interpolation polynomial into access polynomial to obtain decryption key $DK_2$. Here is the detailed process:

$$l_{1,2}(x_{1,2})=\left(\frac{x_{1,2}-x_{2,2}}{x_{1,2}-x_{2,2}}\right)\left(\frac{x_{1,2}-x_{3,2}}{x_{1,2}-x_{3,2}}\right)\left(\frac{x_{1,2}-x_{4,2}}{x_{1,2}-x_{4,2}}\right)\left(\frac{x_{1,2}-x_{5,2}}{x_{1,2}-x_{5,2}}\right)\left(\frac{x_{1,2}-x_{6,2}}{x_{1,2}-x_{6,2}}\right)$$
$$=\frac{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_2)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_2)G(\text{mod }P)}\times\frac{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_3)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_3)G(\text{mod }P)}$$
$$\times\frac{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_4)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_4)G(\text{mod }P)}\times\frac{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_5)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_5)G(\text{mod }P)}$$
$$\times\frac{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_6)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_6)G(\text{mod }P)}$$
$$=1$$

$$l_{2,2}(x_{1,2}) = \left(\frac{x_{1,2}-x_{1,2}}{x_{2,2}-x_{1,2}}\right)\left(\frac{x_{1,2}-x_{3,2}}{x_{2,2}-x_{3,2}}\right)\left(\frac{x_{1,2}-x_{4,2}}{x_{2,2}-x_{4,2}}\right)\left(\frac{x_{1,2}-x_{5,2}}{x_{2,2}-x_{5,2}}\right)\left(\frac{x_{1,2}-x_{6,2}}{x_{2,2}-x_{6,2}}\right)$$

$$= \frac{(ID_2 \| SK_1)G(\text{mod } P)-(ID_2 \| SK_1)G(\text{mod } P)}{(ID_2 \| SK_2)G(\text{mod } P)-(ID_2 \| SK_1)G(\text{mod } P)} \times \frac{x_{1,2}-(ID_2 \| SK_3)G(\text{mod } P)}{(ID_2 \| SK_2)G(\text{mod } P)-(ID_2 \| SK_3)G(\text{mod } P)}$$

$$\times \frac{x_{1,2}-(ID_2 \| SK_4)G(\text{mod } P)}{(ID_2 \| SK_2)G(\text{mod } P)-(ID_2 \| SK_4)G(\text{mod } P)} \times \frac{x_{1,2}-(ID_2 \| SK_5)G(\text{mod } P)}{(ID_2 \| SK_2)G(\text{mod } P)-(ID_2 \| SK_5)G(\text{mod } P)}$$

$$\times \frac{x_{1,2}-(ID_2 \| SK_6)G(\text{mod } P)}{(ID_2 \| SK_2)G(\text{mod } P)-(ID_2 \| SK_6)G(\text{mod } P)}$$

$$= 0$$

$$l_{4,2}(x_{1,2}) = \left(\frac{x_{1,2}-x_{1,2}}{x_{4,2}-x_{1,2}}\right)\left(\frac{x_{1,2}-x_{2,2}}{x_{4,2}-x_{2,2}}\right)\left(\frac{x_{1,2}-x_{3,2}}{x_{4,2}-x_{3,2}}\right)\left(\frac{x_{1,2}-x_{5,2}}{x_{4,2}-x_{5,2}}\right)\left(\frac{x_{1,2}-x_{6,2}}{x_{4,2}-x_{6,2}}\right)$$

$$= \frac{(ID_2 \| SK_1)G(\text{mod } P)-(ID_2 \| SK_1)G(\text{mod } P)}{(ID_2 \| SK_4)G(\text{mod } P)-(ID_2 \| SK_1)G(\text{mod } P)} \times \frac{x_{1,2}-(ID_2 \| SK_2)G(\text{mod } P)}{(ID_2 \| SK_4)G(\text{mod } P)-(ID_2 \| SK_2)G(\text{mod } P)}$$

$$\times \frac{x_{1,2}-(ID_2 \| SK_3)G(\text{mod } P)}{(ID_2 \| SK_4)G(\text{mod } P)-(ID_2 \| SK_3)G(\text{mod } P)} \times \frac{x_{1,2}-(ID_2 \| SK_5)G(\text{mod } P)}{(ID_2 \| SK_4)G(\text{mod } P)-(ID_2 \| SK_5)G(\text{mod } P)}$$

$$\times \frac{x_{1,2}-(ID_2 \| SK_6)G(\text{mod } P)}{(ID_2 \| SK_4)G(\text{mod } P)-(ID_2 \| SK_6)G(\text{mod } P)}$$

$$= 0$$

Finally will be able to get the decryption key $DK_2$ by accessing the polynomial $F_{DK_2}(x)$:

$$F_{DK_2}(x_{1,2}) = x_{1,2} \times DK_2 \times \left\{ \left(x_{1,2}\right)^{-1} l_{1,2}(x) + \left(x_{2,2}\right)^{-1} l_{2,2}(x) + \left(x_{4,2}\right)^{-1} l_{4,2}(x) \right\}$$

$$= (ID_2 \| SK_1)G(\text{mod } P) \times DK_2 \times \begin{Bmatrix} [(ID_2 \| SK_1)G(\text{mod } P)]^{-1} \times 1 \\ +[(ID_2 \| SK_2)G(\text{mod } P)]^{-1} \times 0 \\ +[(ID_2 \| SK_4)G(\text{mod } P)]^{-1} \times 0 \end{Bmatrix}$$

$$= (ID_2 \| SK_1)G(\text{mod } P) \times DK_2 \times [(ID_2 \| SK_1)G(\text{mod } P)]^{-1}$$

$$= DK_2$$

Assume that the value of $ID_2$ is 3, each value of secret key $SK_i$.

| | $SK_1$ | $SK_2$ | $SK_3$ | $SK_4$ | $SK_5$ | $SK_6$ |
|---|---|---|---|---|---|---|
| Value | 5 | 7 | 2 | 6 | 1 | 9 |

We bring values of $ID_2$ and secret key $SK_i$ into Lagrange interpolation polynomial to get:

$$
\begin{aligned}
l_{1,2}(x_{1,2}) &= \left(\frac{x_{1,2}-x_{2,2}}{x_{1,2}-x_{2,2}}\right)\left(\frac{x_{1,2}-x_{3,2}}{x_{1,2}-x_{3,2}}\right)\left(\frac{x_{1,2}-x_{4,2}}{x_{1,2}-x_{4,2}}\right)\left(\frac{x_{1,2}-x_{5,2}}{x_{1,2}-x_{5,2}}\right)\left(\frac{x_{1,2}-x_{6,2}}{x_{1,2}-x_{6,2}}\right) \\
&= \frac{(3\|5)G(\text{mod } P)-(3\|7)G(\text{mod } P)}{(3\|5)G(\text{mod } P)-(3\|7)G(\text{mod } P)} \times \frac{(3\|5)G(\text{mod } P)-(3\|2)G(\text{mod } P)}{(3\|5)G(\text{mod } P)-(3\|2)G(\text{mod } P)} \\
&\quad \times \frac{(3\|5)G(\text{mod } P)-(3\|6)G(\text{mod } P)}{(3\|5)G(\text{mod } P)-(3\|6)G(\text{mod } P)} \times \frac{(3\|5)G(\text{mod } P)-(3\|1)G(\text{mod } P)}{(3\|5)G(\text{mod } P)-(3\|1)G(\text{mod } P)} \\
&\quad \times \frac{(3\|5)G(\text{mod } P)-(3\|9)G(\text{mod } P)}{(3\|5)G(\text{mod } P)-(3\|9)G(\text{mod } P)} \\
&= 1
\end{aligned}
$$

$$
\begin{aligned}
l_{2,2}(x_{1,2}) &= \left(\frac{x_{1,2}-x_{1,2}}{x_{2,2}-x_{1,2}}\right)\left(\frac{x_{1,2}-x_{3,2}}{x_{2,2}-x_{3,2}}\right)\left(\frac{x_{1,2}-x_{4,2}}{x_{2,2}-x_{4,2}}\right)\left(\frac{x_{1,2}-x_{5,2}}{x_{2,2}-x_{5,2}}\right)\left(\frac{x_{1,2}-x_{6,2}}{x_{2,2}-x_{6,2}}\right) \\
&= \frac{(3\|5)G(\text{mod } P)-(3\|5)G(\text{mod } P)}{(3\|7)G(\text{mod } P)-(3\|5)G(\text{mod } P)} \times \frac{x_{1,2}-(3\|2)G(\text{mod } P)}{(3\|7)G(\text{mod } P)-(3\|2)G(\text{mod } P)} \\
&\quad \times \frac{x_{1,2}-(3\|6)G(\text{mod } P)}{(3\|7)G(\text{mod } P)-(3\|6)G(\text{mod } P)} \times \frac{x_{1,2}-(3\|1)G(\text{mod } P)}{(3\|7)G(\text{mod } P)-(3\|1)G(\text{mod } P)} \\
&\quad \times \frac{x_{1,2}-(3\|9)G(\text{mod } P)}{(3\|7)G(\text{mod } P)-(3\|9)G(\text{mod } P)} \\
&= 0
\end{aligned}
$$

$$
\begin{aligned}
l_{4,2}(x_{1,2}) &= \left(\frac{x_{1,2}-x_{1,2}}{x_{4,2}-x_{1,2}}\right)\left(\frac{x_{1,2}-x_{2,2}}{x_{4,2}-x_{2,2}}\right)\left(\frac{x_{1,2}-x_{3,2}}{x_{4,2}-x_{3,2}}\right)\left(\frac{x_{1,2}-x_{5,2}}{x_{4,2}-x_{5,2}}\right)\left(\frac{x_{1,2}-x_{6,2}}{x_{4,2}-x_{6,2}}\right) \\
&= \frac{(3\|5)G(\text{mod } P)-(3\|5)G(\text{mod } P)}{(3\|6)G(\text{mod } P)-(3\|5)G(\text{mod } P)} \times \frac{x_{1,2}-(3\|7)G(\text{mod } P)}{(3\|6)G(\text{mod } P)-(3\|7)G(\text{mod } P)} \\
&\quad \times \frac{x_{1,2}-(3\|2)G(\text{mod } P)}{(3\|6)G(\text{mod } P)-(3\|2)G(\text{mod } P)} \times \frac{x_{1,2}-(3\|1)G(\text{mod } P)}{(3\|6)G(\text{mod } P)-(3\|1)G(\text{mod } P)} \\
&\quad \times \frac{x_{1,2}-(3\|9)G(\text{mod } P)}{(3\|6)G(\text{mod } P)-(3\|9)G(\text{mod } P)} \\
&= 0
\end{aligned}
$$

Finally, we still are able to obtain the decryption key $DK_2$ by accessing the polynomial, see as below:

$$
\begin{aligned}
F_{DK_2}(x_{1,2}) &= x_{1,2} \times DK_2 \times \left\{ \left(x_{1,2}\right)^{-1} l_{1,2}(x) + \left(x_{2,2}\right)^{-1} l_{2,2}(x) + \left(x_{4,2}\right)^{-1} l_{4,2}(x) \right\} \\
&= (3 \| 5)G(\text{mod } P) \times DK_2 \times \left\{ \begin{array}{l} [(3 \| 5)G(\text{mod } P)]^{-1} \times 1 \\ +[(3 \| 7)G(\text{mod } P)]^{-1} \times 0 \\ +[(3 \| 6)G(\text{mod } P)]^{-1} \times 0 \end{array} \right\} \\
&= (3 \| 5)G(\text{mod } P) \times DK_2 \times [(3 \| 5)G(\text{mod } P)]^{-1} \\
&= DK_2
\end{aligned}
$$

From the example we know the method in different key value still can prove security of decryption key. Each key does not have relationship in Lagrange interpolation polynomial and the key generate randomly, so it's hard to calculate the key. Moreover, the key is under Elliptic curve cryptography, so attackers must encounter Elliptic Curve Discrete Logarithm Problem (ECDLP). This will greatly enhance the difficulty to crack the key $DK_t$.

# Chapter 4 — Analysis of Security

In this section, we will do analysis of security from common external collective attack, internal attack, collusion attacks and equation breaking attack, to show how much we can withstand these attacks, analyze whether to be cracked easily or not and we consider several potential attacks from attackers in order to prove that our proposed scheme is secure against these attacks.

## 4.1 External Collective Attack

External collective attack is one of us familiar with; usually they do external attack to grab important information to some specific institution which is valuable, such as pivotal client's information in companies or patient's medical records in hospital, what they do can earn illegal profit that cause great property damage to those institutions. Therefore, analyzing standard of security is necessary.

We take mobile agents as example, external attackers will intercept mobile agents in the first place, because attackers obtain internal important information through illegal process, they do not have authority to access, except public parameter and other unimportant information. If they want to get useful material, they must decipher the decryption key by public parameter, and use it to decrypt to get important information and medical records.

If external attackers already has public parameter, then use it to get the decryption key, but the decryption key is under protection on formula $F_{DK_j}(x) = x \times DK_j \times \sum_{DK_j \le SC_i} x_{i,j}^{-1} l_{i,j}(x)$, so it must be safe enough. If attackers

want to decipher the decryption key $DK_j$ from formula, they need to insert function into the Lagrange interpolation polynomial, to assure its security, we analyze the first function $l_{1,2}(x)$ as below:

$$l_{1,2}(x)=\left(\frac{x-x_{2,2}}{x_{1,2}-x_{2,2}}\right)\left(\frac{x-x_{3,2}}{x_{1,2}-x_{3,2}}\right)\left(\frac{x-x_{4,2}}{x_{1,2}-x_{4,2}}\right)\left(\frac{x-x_{5,2}}{x_{1,2}-x_{5,2}}\right)\left(\frac{x-x_{6,2}}{x_{1,2}-x_{6,2}}\right)$$
$$=\frac{x-(ID_2\|SK_2)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_2)G(\text{mod }P)}\times\frac{x-(ID_2\|SK_3)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_3)G(\text{mod }P)}$$
$$\times\frac{x-(ID_2\|SK_4)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_4)G(\text{mod }P)}\times\frac{x-(ID_2\|SK_5)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_5)G(\text{mod }P)}$$
$$\times\frac{x-(ID_2\|SK_6)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_6)G(\text{mod }P)}$$

We find attackers as unknown number, except $P$ and $G$, although attackers obtain formula $F_{DK_j}(x)$, they still cannot get $DK_2$ because of too much unknown number. Besides that, external attackers can't get the key $SK_i$ because they only have public parameter, by contrast, they must to get the key $SK_i$ from Lagrange interpolation polynomial $x_{i,j}=(ID_j\|SK_i)G(\text{mod }p)$, but the key $SK_i$ is protected under Elliptic Curve Cryptography system, which means they have to face Elliptic Curve Discrete Logarithm Problem (ECDLP), also $P$ is a big prime number, so it's hard to get the key, form above we can prove external attackers cannot obtain patient's medical records and other important information by collective attack.

### 4.2 Internal Attack

Internal attack is lower authorizer would like to get secret key illegally from those higher. Like the nurse want to decrypt important information form the doctor's decryption key and get some secret materials. As Figure

5, $SC_j$ represents lower authorizer such as nurses and so on. $SC_i$ represents higher authorizer such as managers or doctors and so on. If the nurse gets the doctor's decryption key, he or she could decrypt materials and other behavior out of authority like illegally retrieving or amending parts of patient's medical records in hospital from doctor's key, it really cause great damage to the doctor who is being hacked and has bad feedback in the record.

The proposed scheme in this research, we can refer to $l_{i,j}(x)$ in the following

$$l_{i,j}(x) = \prod_{t=1,t\neq i}^{n} \frac{x - x_{t,j}}{x_{i,j} - x_{t,j}} = \left(\frac{x - x_{1,j}}{x_{i,j} - x_{1,j}}\right)\cdots\left(\frac{x - x_{i-1,j}}{x_{i,j} - x_{i-1,j}}\right)\left(\frac{x - x_{i+1,j}}{x_{i,j} - x_{i+1,j}}\right)\cdots\left(\frac{x - x_{n,j}}{x_{i,j} - x_{n,j}}\right)$$

and $x_{i,t} = (ID_t \,||\, SK_i)G(\text{mod } p)$, from above we find each $SK_i$ do not relate to each other, it shows an advantage that key and key do not exist any formula, each $SK_i$ is independent, and they do not rely on each other. So that the nurse won't have any formula or parameter to get doctor's decryption key, if attackers still want to decipher Lagrange interpolation polynomial $x_{i,t} = (ID_t \,||\, SK_i)G(\text{mod } p)$ to get the key $SK_i$, they still must to face Elliptic Curve Discrete Logarithm Problem (ECDLP). It's a highly challenging and difficult to decipher. Hence, internal attack posts less threat to the system.

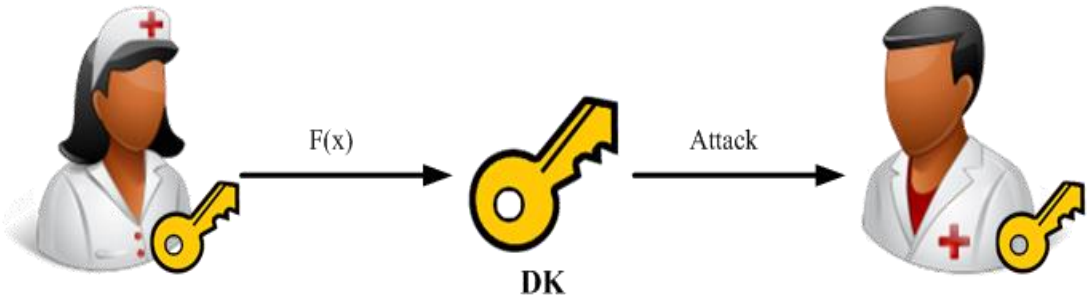


Figure 5: Internal Attack

### 4.3 Collusion Attack

As Figure 5, $SC_j$ represents lower authorizer such as nurses and so on. $SC_i$ represents higher authorizer such as managers or doctors and so on. Collusion attack is that lower authorizer attack together to get the key form higher authorizer, like nurses wants to steal doctor's decryption key, which means many internal attacks gathering to attack. Compare internal attack to collusion attack, collusion attack have chunk of member joint, that's why there are more key as reference. It's mean the better chance to decipher the system. So we know collusion attack is much more dangerous than internal attack.

To solve the problem, the key we use in this thesis is randomized, no relationship between each other. Even if we combine lower authorized keys together, we still cannot figure out higher authorizer's decryption key. By the way, we use the Lagrange interpolation polynomial, too. Each layer do not relate to each other, also, it take risk away that layer being deciphered by attackers, so higher authorizer's key become more safely. We separate $SC_j$ into individual one, the good point is no matter internal attack or collusion attack, there is remote chance to get higher authorizer's private key.

See formula $F_{DK_j}(x) = x \times DK_j \times \sum_{DK_j \le SC_i} x_{i,j}^{-1} l_{i,j}(x)$, we find $l_{i,j}(x)$ the

key point, we take $l_{i,j}(x)$ as an example, let's bring $l_{1,2}(x)$ in.

$$l_{1,2}(x)=\left(\frac{x-x_{2,2}}{x_{1,2}-x_{2,2}}\right)\left(\frac{x-x_{3,2}}{x_{1,2}-x_{3,2}}\right)\left(\frac{x-x_{4,2}}{x_{1,2}-x_{4,2}}\right)\left(\frac{x-x_{5,2}}{x_{1,2}-x_{5,2}}\right)\left(\frac{x-x_{6,2}}{x_{1,2}-x_{6,2}}\right)$$
$$=\frac{x-(ID_2\|SK_2)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_2)G(\text{mod }P)}\times\frac{x-(ID_2\|SK_3)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_3)G(\text{mod }P)}$$
$$\times\frac{x-(ID_2\|SK_4)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_4)G(\text{mod }P)}\times\frac{x-(ID_2\|SK_5)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_5)G(\text{mod }P)}$$
$$\times\frac{x-(ID_2\|SK_6)G(\text{mod }P)}{(ID_2\|SK_1)G(\text{mod }P)-(ID_2\|SK_6)G(\text{mod }P)}$$

$SK_2$-$SK_6$ are unknown number, if $SK_2$ represented the manager or the doctor's key, other represented nurses' key, the only $(ID_2\|SK_2)G(\text{mod }p)$ in $SK_2$ is unknown number. From above we can see security is based on Elliptic Curve Discrete Logarithm Problem (ECDLP). From former document we find security of Elliptic Curve Discrete Logarithm Problem (ECDLP) is according to prime number. Once the prime number is big enough, the more safety it is, so it's hard to decipher the key $SK_i$. Collusion attacker can't figure out any clue relate to the key $SK_i$ through this formula, that's why this proposed scheme can withstand collusion attack.

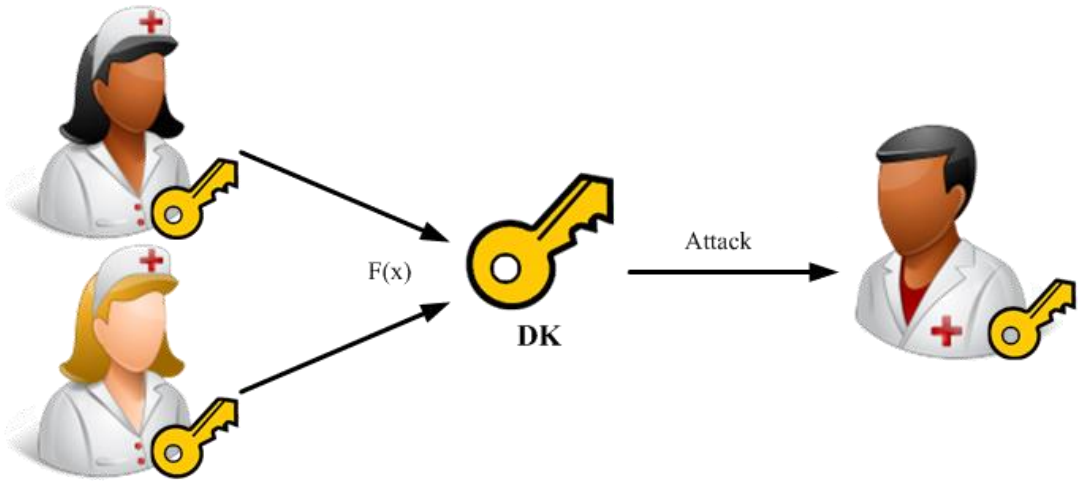


Figure 6: Collusion Attack

### 4.4 Equation Breaking Attack

Equation breaking attack is attackers try to put up the decryption key they want by known formula and a few parameters. We discuss whether the formula is safe or not in this section.

Assume that two legitimate user $SC_1$ and $SC_2$ can derive the key $DK_5$ from $F_{DK_5}(x)$. For $SC_2$, by public parameters, secret parameters $SK_2$ and access polynomial $F_{DK_5}(x)$ to derive another legitimate user's secret parameters is feasible. If successfully get the secret parameters, we will derive the key $SK_1$ and illegal access $SC_1$'s important information. In case the possibility, we need to analyze the security of this formula.

$$F_{DK_5}(x_{2,5}) = x_{2,5} \times DK_5 \times \sum_{DK_j \le SC_i} x_{i,j}^{-1} l_{i,j}(x_{2,5})$$

$$\Rightarrow F_{DK_5}(x_{2,5}) \times DK_5^{-1} = x_{2,5} \times \sum_{DK_j \le SC_j} x_{i,j}^{-1} l_{i,j}(x_{2,5})$$

$$\Rightarrow F_{DK_5}(x_{2,5}) \times DK_5^{-1} = x_{2,5} \times \left\{ \left(x_{1,5}\right)^{-1} l_{1,5}(x_{2,5}) \times \left(x_{2,5}\right)^{-1} l_{2,5}(x_{2,5}) \times \left(x_{4,5}\right)^{-1} l_{4,5}(x_{2,5}) \right\}$$

On the left side of the equation, $SC_2$ can legally use the polynomial $F_{DK_5}(x)$ to get the key $DK_5$, therefore we take $F_{DK_5}(x) = DK_5$ into:

$$\Rightarrow DK_5 \times DK_5^{-1} = x_{2,5} \times \left\{ \ldots \left(x_{2,5}\right)^{-1} \times \left( \frac{x_{2,5} - x_{1,5}}{x_{2,5} - x_{1,5}} \right) \left( \frac{x_{2,5} - x_{3,5}}{x_{2,5} - x_{3,5}} \right) \left( \frac{x_{2,5} - x_{4,5}}{x_{2,5} - x_{4,5}} \right) \left( \frac{x_{2,5} - x_{5,5}}{x_{2,5} - x_{5,5}} \right) \left( \frac{x_{2,5} - x_{6,5}}{x_{2,5} - x_{6,5}} \right) \times \ldots \right\}$$

$$\Rightarrow 1 = x_{2,5} \times \{0 + \left(x_{2,5}\right)^{-1} \times \frac{(ID_5 \| SK_2)G(\mathrm{mod}\, P) - (ID_5 \| SK_1)G(\mathrm{mod}\, P)}{(ID_5 \| SK_2)G(\mathrm{mod}\, P) - (ID_5 \| SK_1)G(\mathrm{mod}\, P)} \times \ldots + 0\}$$

$$\Rightarrow 1 = x_{2,5} \times x_{2,5}^{-1} \times 1$$

On the right side of the equation, a function $L_{2,5}(x_{2,5})$ in Lagrange interpolation polynomial will equal 1, others are 0. Even if a legitimate user can successfully take advantage of known parameters to this step,

they cannot get the key because fail to inverse polynomials or parameters from 1. In addition, equation breaking attackers want to get the secret key $SK_i$ from Lagrange interpolation polynomial, $x_{i,t} = (ID_t \| SK_i)G(\text{mod } p)$, they still must to face Elliptic Curve Discrete Logarithm Problem (ECDLP), hence, this proposed scheme alike can withstand equation breaking attack.

# Chapter 5 — Conclusion

Advancement in technology rapidly growth, the Internet has become increasingly important for modern people. And it brings lots of benefit to us, not only the exchange of knowledge and information is more convenient, but the operation of medical system is more digitized, so medical system is more effective now when traditional paper medical records gradually become electronic medical records. With that, we have quality medical service and fresh information. Also because of the Internet, many important personal data or medical records are out of security without great measures. Especially confidential information with unreliable key be Intercepted or stolen by attackers can cause great property damage. Here, although the application of access control is widely use, we still have to improve its security in the structure. How to make mobile agent work better is what we put emphasize on.

We encrypt the key by Lagrange interpolation polynomial and Elliptic Curve Cryptography to protect its security, hide it in the access polynomial to assure only legitimate users can access to the private files or resources and did analysis of security whether the schemes we proposed can withstand every common attacks or not. As the result, the fact we choose Lagrange interpolation polynomial is the key we use is randomized, no relationship between each key, so is relatively hard. Moreover, the key is under Elliptic Curve Cryptography system, so attackers must encounter Elliptic Curve Discrete Logarithm Problem (ECDLP). This will greatly enhance the difficulty to crack the key.

We discuss mobile agent technology in the thesis; it is effective to

access information immediately. Therefore, we still can assure its security and integrity in the instable Internet, also it combined with access control in the internal structure as control to make information more private and secure. The outcome will be obviously if applied to the medical system or the cloud system of a company.

# Reference


[1] 黃明祥、林詠章，資訊與網路安全概論，高立圖書出版有限公司，2009。

[2] T. L. Chen, “Private Key Management Schemes for Mobile Agents,” Doctoral Dissertation, National Taiwan University, Taipei, 2012.

[3] T. C. Lin, “Secure Dynamic Access Control Scheme of PHR in Cloud Computing,” Master Thesis, Tunghai University, Taichung, 2012.

[4] M. H. Kao, “The Study of Agent-based Secure Schemes on Electronic Medical Records System,” Master Thesis, Tunghai University, Taichung, 2010.

[5] Wikipedia, http://en.wikipedia.org/wiki/Access_control.

[6] T. S. Chen, Y. F. Chung, and C. S. Tian, “A Novel Key Management Scheme for Dynamic Access Control in a User Hierarchy,” *In Proceedings of the IEEE Annual International Computer Software and Applications Conference (COMPSAC)* , Vol. 162, No. 1, pp. 396-401, 2004.

[7] Wikipedia, http://en.wikipedia.org/wiki/Lagrange_polynomial.

[8] B. Thuraisingham, “Security and Privacy for Multimedia Database Management Systems,” *Multimedia Tools and Applications*, Vol. 33, No. 1, pp. 13-29, 2007.

[9] T. Chen, H. Chen, and Y. Liu, “Three-layer Application System for Database Encryption,” *Journal of Huazhong University of Science and Technology*, Vol. 33, No. 7, pp. 41-44, 2005.

[10]Z. Zhao, B. Liu, and J. Li, “Research and Design of Database Encryption System Based on External DBMS,” *Computer Engineering and Design*, Vol. 29, No. 12, pp. 3030-3032, 2008.

[11]J. Yeh, “An RSA-based Time-bound Hierarchical Key Assignment Scheme for Electronic Article Subscription,” *ACM International Conference on Information and Knowledge Management*, pp. 285-286, 2005.

[12]H. M. Sun, “An Efficient Authentication Scheme for Access Control in Mobile Pay-TV Systems,” *IEEE Transactions on Multimedia*, Vol. 11, No. 5, pp.947-959, 2009.

[13]T. Jiang, and S. Zheng, “Key Distribution for Conditional Access System in DTV Broadcasting,” *The Ninth International Conference on Communications Systems*, pp. 326-330, 2004.

[14]P. Xiao, J. H. He, and Y. F. Fu, “Distributed Group Key Management in Wireless Mesh Networks,” *International Journal of Security and Its Applications*, Vol. 6, No. 2, pp. 115-120, 2012.

[15]K. V. Babu, O. S. Rao, and Dr. M. K. Prasad, “Secured Tree Based Key Management in Wireless Broadcast Services,” *International Journal of Engineering Science and Technology*, Vol. 4, No. 2, pp. 523-529, 2012.

[16]E. Bertino, N. Shang, and S. S. Wagstaff, “An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting,” *IEEE Transactions on Dependable and Secure Computing*, Vol. 5, No. 2, pp. 65-70, 2008.

[17]H. Hu, G. Ahn, and J. Jorgensen, “Multiparty Access Control for

Online Social Networks: Model and Mechanisms: Networks Model, and Mechanisms," *IEEE Transactions on Knowledge and Data Engineering*, No. 99, pp. 1-14, 2012.

[18]C. H. Liu, Y. F. Chung, T. S. Chen and S. D. Wang, "Mobile Agent Application and Integration in Electronic Anamnesis System," *Journal of Medical Systems*, Vol. 36, No. 3, pp. 1009-1020, 2012.

[19]T. L. Chen, Y. F. Chung and F. Y. S. Lin, "Deployment of Secure Mobile Agents for Medical Information Systems," *Journal of Medical Systems*, Vol. 36, No. 4, pp. 2493-2503, 2012.

[20]W. Stallings, Cryptography and Network Security: Principles and Practice, 4th Ed., Prentice Hall, 2005.

[21]N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, Vol. 48, No. 177, pp. 203-209, 1987.

[22]V. S. Miller, "Use of Elliptic Curves in Cryptography," *Advances in Cryptology: Proceedings of Crypto'85*, Vol. 218, pp. 417-426, 1986.

[23]H. B. Chen, W. B. Lee, C. W. Liao, and C. H. Huang, "Efficient Hierarchical Access Control and Key Management for Mobile Agents," *The First International Workshop on Privacy and Security in Agent-based Collaborative Environments*, pp. 120-127, 2006.

[24]S. T. Wu, "Authentication and Group Secure Communications Using Elliptic Curve Cryptography," Doctoral Dissertation, National Taiwan University of Science and Technology, Taipei, 2005.

[25]C. W. Shieh, "An Efficient Design of Elliptic Curve Cryptography Processor," Master Thesis, Tatung University, Taipei, 2006.

[26]D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve

Digital Signature Algorithm (ECDSA),” *International Journal of Information Security*, Vol. 1, No.1, pp. 36-63, 2001.