Applied Mathematics & Information Sciences
*An International Journal*

http://dx.doi.org/10.12785/amis/090555

# Key Management Scheme for Controlling Access in Secure Authorization

*Tsung-Chih Hsiao*[1,*], *Tzer-Long Chen*[2], *Yu-Fang Chung* [3] *and Tzer-Shyong Chen*[4]

[1] College of Computer Science and Technology, Huaqiao University, China
[2] Department of Creative Product Design, Lingtung University, Taiwan
[3] Department of Electrical Engineering, Tunghai University, Taiwan
[4] Department of Information Management, Tunghai University, Taiwan

Received: 13 Feb. 2015, Revised: 16 May 2015, Accepted: 19 May 2015
Published online: 1 Sep. 2015

**Abstract:** With the rapid development of the Internet, on which many users start to take action in putting personal or corporate information and sharing them with everyone. The Internet is public as it were, if the limit of authority is not controlled to assure the security, it is possible that those attackers could illegally access to important information and destroy them. Not only is personal privacy invaded, but the mass properties are also damaged. Therefore, an effective access control system has been strongly emphasized in modern societies. To fight against these network attacks, it is necessary to establish an effective and secure access control system. Here, a scheme, a key management called Lagrange interpolation mainly takes an access control model as the framework, is proposed and Elliptic Curve Cryptography system is used for enhancing the security. The reason of choosing Lagrange interpolation is that the key used is randomized, no relationship between each key. With Elliptic Curve Cryptography system, it is expected to have attackers waste their time dealing with Elliptic Curve Discrete Logarithm Problem. Once the prime number is big enough, attackers will have trouble deciphering the key. An access control is comprehensive. For example, if the mobile agent technology is applied to an access control and key management, it would waste space and cause some flaws in the security. Moreover, there are still a lot of works to do on medical applications. Hence, these schemes are proposed for mobile agents in order to reach the improvement and then analyze the security and try to simulate what attackers will do. Four common attacks, namely External Collective Attack, Internal Attack, Collusion Attacks and Equation Breaking Attack are concluded. As results, attackers are hard to decipher the key because of no relationship between each key and will have to face Elliptic Curve Discrete Logarithm Problem. It is confirmed that the proposed schemes can be safer and more efficient in protecting mobile agents.

**Keywords:** Key Management; Mobile Agent; Elliptic Curve Cryptography; Lagrange Interpolation

## 1 Introduction

Access control has been applied quite a lot [1], like database management system, online pay-tv system and electronic subscription system, etc., where mobile agents are definitely one of the important applications. A mobile agent is a self-distributed computing program between a host and a switch information host to host on the Internet. Also, since it is autonomy, it can decrease delays of transmission, reduce network traffic and be applied to sorts of platforms. As its characters of fault-tolerance, adjustment and personalization [4], a mobile agent is wiser to send messages and can exchange the information with other individual resource systems or different mobile agents.

A mobile agent is functioned to take assigned tasks for users. It can be dispatched to the Internet or other relative services and platforms in order to search for or deal with information. When the mobile agent finishes the assigned tasks, it will return to the users. With these qualities, a mobile agent is suitable for being used in medical network systems, for example, transmitting or exchanging its contents from a particular hospital information system to another hospital host and executing the given tasks authorized by users to finish their works.

Fig. 1 is the basic structure and operation working on a medical system. When a patient goes to the medical department for a treatment, the doctor will access to the patients simple information and send a request to a mobile agent (such as searching for a patients illness

[*] Corresponding author e-mail: hsiaotc@hqu.edu.cn

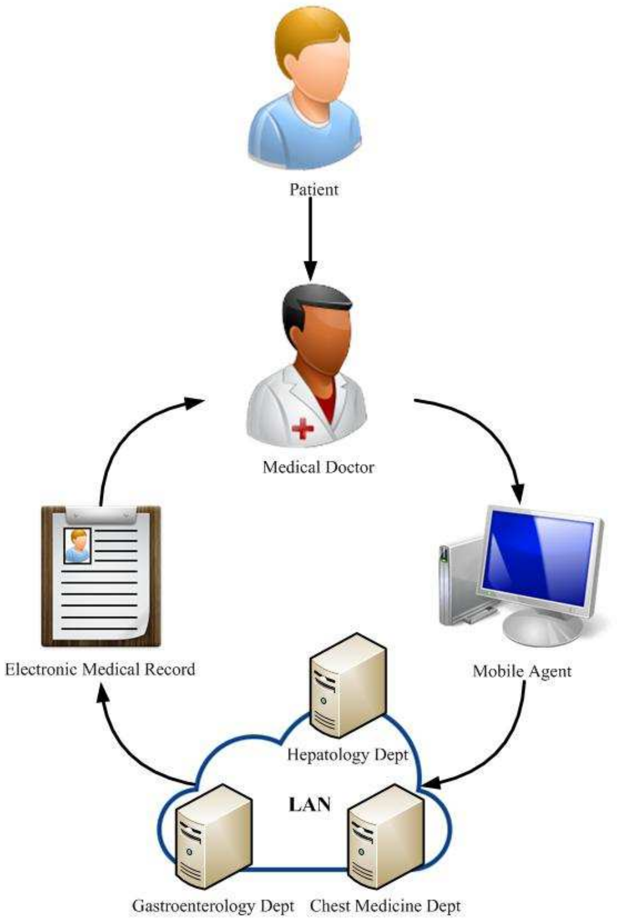


**Fig. 1:** Structure of Mobile Agent

history and medical records in every medical department). When the mobile agent gets the commission, it will quickly collect data or exchange information with other mobile agents to the specific host in the department according to the original process and automatically take different strategies and paths to search for information that patients and doctors want. These can enhance the efficiency and reduce time. Assuming that a mobile agent first searches for the liver department, it will find the patients related records there, access to the data, and send it to the next medical department for the integration until finishing searching for the data in all departments. It then returns to the original medical department and compiles all the information together into an electronic medical record for the doctor.

Although the mobile agent technology brings great convenience for medical or other businesses, it still needs to exchange information on the Internet. Concerning the Internet being public connecting with all countries, it is necessary to have a complete key management and access control to prevent attackers from illegal behaviors. The proposed key management and access control are based on 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, so that the access control mechanism becomes more secure and efficient. Meanwhile, the security against common attacks are analyzed. Like Internal attacks, the feasibility of an authentication mechanism, security and efficiency and the security of a mobile agent executing the commission, like accessing to a patients personal medical records in different hospitals, are tested. If it is secure enough, the efficiency on key management can definitely be promoted to protect the mobile agent system.

Many researchers have proposed some issues about access control mechanisms and solutions. However, these schemes still have some defects in the quality of safety and efficiency. The provided key management and access control mechanism emphasize the access control architecture. The mathematical theory and encryption technology different from the past ones are used, and the research motivation, purpose, and structure are introduced in next chapter.

Nowadays, most information systems have been used in network environments, as they have the feature of accessing to the public, that is not safe. Besides, the exchanged information is more likely to be stolen or destroyed in the transmission process. Fortunately, there is the solution. From previous literatures, people made use of encryption and decryption technology for protecting confidential documents or resources. The higher authority could load electronic files and documents from the lower authority according to the rule of access control. Therefore, the design of security access control technology is very important today, which not only protects the confidential information and resources, but ensures that only the higher authority can access to the lower sensitive information [1].

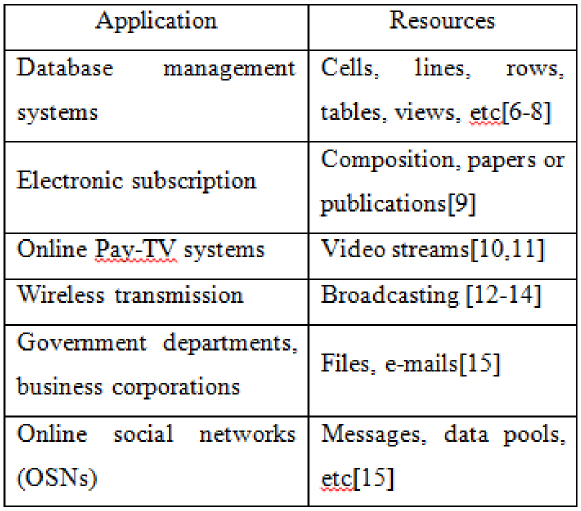
A mobile agent is an important application of access control mechanisms, which brings great convenience to medical institutions, but still has a lot to improve in the aspect of security and performance. From current medical conditions, the medical records are left after the diagnoses. However, no medical institution has all the medical records of patients to fully understand their patients situations. The following shows some problems with medical conditions [2]:

1. Traditional medical records could waste the space and time easily.
2. Unnecessary waste of resources.
3. Privacy issues.
4. Difficult to control statistics.
5. Real-time exchange of new types of medical researches.
6. Slowly retrieval of medical records.

Concerning security problems in the public network of mobile agents and those defects encountered, a completely safe access control mechanism is attempted to be established for correcting them. Lagrange interpolation polynomial and Elliptic curve cryptography are applied to the decryption key, and the access control mechanism is kept in the medical environment with mobile agents, which represent the doctors here. Though remote collection and prescription with mobile agents, it will be secure to exchange medical information. Applying mobile agents to electronic medical records tends to prove the following [17].

1.To reduce the waste of medical resources.
2.To complete and secure medical records.
3.To repeat key management.
4.To offer real-time information.
5.To provide high-quality medical information.
6.To be provided with statistics.

**Table 1:** Application on Access Control



| Application | Resources |
|---|---|
| Database management systems | Cells, lines, rows, tables, views, etc[6-8] |
| Electronic subscription | Composition, papers or publications[9] |
| Online Pay-TV systems | Video streams[10,11] |
| Wireless transmission | Broadcasting [12-14] |
| Government departments, business corporations | Files, e-mails[15] |
| Online social networks (OSNs) | Messages, data pools, etc[15] |

## 2 Related Work

1.Lagrange Interpolation

Lagrange interpolation, named after a French mathematician Joseph Louis Lagrange, is used for polynomial interpolation. There are many practical mathematic problems indicating its laws by function. The function can be proven by observation or experiments.

Lagrange interpolation gives a known polynomial function passing through the two-dimensional plane. Only one of $(x_0,y_0)$, $(x_1,y_1)$, $\ldots$, $(x_n,y_n)$ is under the $n$ of Lagrange polynomial.

In the numerical analysis and mathematical application, the supposed numbers $y$ and $x$ must be complex between each other. Its hard to understand their relationship by doing the experiment. A corresponding polynomial can be obtained by the Lagranges scheme, which will pass a finite set of points on the x-y plane. It is called Lagrange interpolation [5].

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

$\ell_j(x)$ is the Lagrange polynomial, also known as the interpolation base function. If it is set $x_i = 1$, other $x_j$ $(\mathrm{i} \neq \mathrm{j}) = 0$,

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

The Lagrange interpolation will be

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

2.Access Control

An access control is the selective restriction of access to a place or other resource, meaning to allow or ban the lower authority accessing to the resource. Being one of the control software or data access mechanisms, it uses key management for protecting the information from being illegally operated by hackers. The accessing act may mean consuming, entering, or using. The access control can be done by consuming or authorizing. The most common security risks of an access control system are unauthorized access, data destruction, wrong permission and privacy exposed.

For the information security, general access control includes authorization, authentication, access approval and audit. A narrower definition of access control only covers 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 the access is approved based on successful authentication or 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 [3].

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

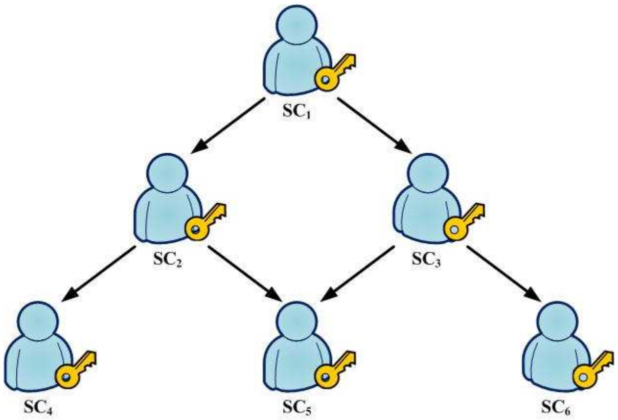


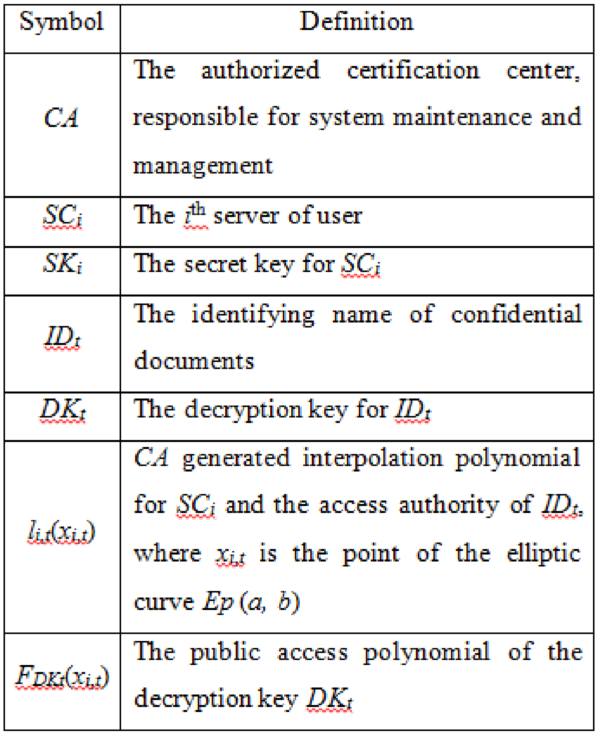
**Fig. 2:** Hierarchical Relationship Structure

Computer communication systems usually use a user hierarchy for solving the problems of access control. It contains different security levels, in which the data are allocated and ordered as Fig. 2.

As shown above, the algorithm applied in this paper is briefly induced. Under the structure, if the relationship of $SC_j \leq SC_i$ is valid, the public relational parameter $R_{ij}$ must be constructed to contain the security classs identification and encryption key. For example, when $SC_5 \leq SC_2$ is valid, SC2 is logically allowed to access to $SC_5$s data. Before $SC_2$ could obtain the access to $SC_5$s data, the public relational parameter, $R_{25}$, needs to be constructed, containing $ID_5$ (identity) and SK5 (secret key) of $SC_5$. Thus, $SC_2$ could use $R_{25}$ for calculating $SC_5$s secret key through the formula and then obtain the information from $SC_5$. The construction of the public relational parameter is essential to the proposed scheme. Because of the hierarchical relationship structure, it is possible to have the cross-relational class exist. In this case, a top-down approach is used for deriving the decryption key, $DK_s$. By assumption, $SC_1$ is permitted to access to the data of $SC_5$. The public relational parameter, $R_{15}$, must be constructed, but there is no direct link between SC1 and SC5. So, $SC_1$ must pass through either $SC_2$ in order to get the access to $SC_5$. The flow chart of the algorithm is shown as below [16].

With the increase of hierarchical relationship structure, the higher-security user needs a larger access storage to accept the lower secret key. Besides, its hard for the key security if there are too many secret keys. Hence, the new law needs to be set up to distribute the key to every user; through the key, they can calculate the key in the low hierarchy. Complex calculation should be prevented during the key-produced process. In other words, for $SC_j \leq SC_i, SC_i$ can use a private key for calculating $SK_j$ from $SC_j$.

**Table 2:** 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 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*) |
| $F_{DK_t}(x_{i,t})$ | The public access polynomial of the decryption key $DK_t$ |

In the consultation, medical staffs can use the key of the highest level permission, whose mobile agent can collect the patients information within the permission without causing the overload of the system or illegal access of outside permission. In writing the consultation data, the lowest common level of information of staffs can be written. The medical staffs can access to the data next time, when the loading of system will also not be caused.

## 3 Proposed Method

The application of the access control to the key generation is first introduced and then calculated. An example will be shown. Basically, Lagrange interpolation polynomial and Elliptic curve cryptography are used for encrypting and managing the key, and the mobile agent technology is used for collecting electronic medical records and leading the relationship structure into hospitals. It is divided to $SC_1$, $SC_2$, , and $SC_n$, which have different permission according to the relationship structure. The higher authority can access to the lower authority after going through the algorism. The parameters and the functions are listed in Table 2.

1.Key Generation Phase

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

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

Step 3.$CA$ chooses different decryption keys $DK_t(t = 1,2,\ldots,m; m$is the number of the mobile agent) for each confidential document.

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

Step 5.Establish an access polynomial.

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

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

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

In the above equation, $DK_t \leq SC_i$ means $SC_i$ being authorized by the confidential document $t$ while $x_{i,t} = (ID_t \| SK_i)G(\mathrm{mod}p)$. $ID_t$. $ID_t$ is the identity name, and $||$ is the connecting operator in the mathematical symbols.

2.Key Derivation Phase

Step 1 Set permission to the decryption key $DK_t$ to which $SC_i$ wants to access.

Step 2 $SC_i$ gets the decryption key $DK_t$ by the secret key $SK_i$ and the accessed polynomial $FDK_t(x)$.

In the mobile agent, every member and confidential document will obtain a key. A members key is to derive the lower hierarchy to obtain the access key they want from the relation. The confidential document key is called the decryption key 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 the storage space, and the mobile agent doesnt need extra calculation, but just to assure the security. The hospitals relationship structure is then put into the corresponding security class and server host or database being accessed to finally completing the mission. As shown in Fig. 3, a patients medical record has been separated to six parts, and each of it has its decryption key, $DK_1, DK_2, , DK_6$.$SC_4$ can access to $DK_1$ and $DK_2$, and $SC_5$ can access to $DK_3$ and $DK_4$. $SC_2$ is higher than $SC_4$ and $SC_5$, so that $SC_2$ can access to four decryption keys ($DK, DK_2, DK_3$ and $DK_4$).

## 4 Analysis of Security and performance

(1) External Collective Attack

An external collective attack is one of the familiar attacks. Usually, external attacks tend to grab important information to some specific institution that

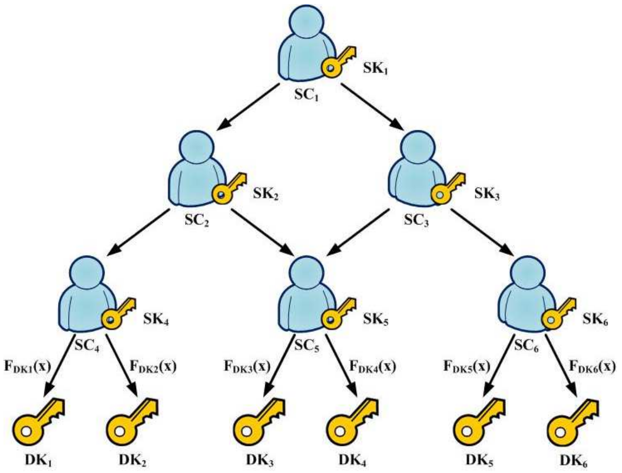


**Fig. 3:** Hierarchical Access Control Structure

is valuable, such as pivotal clients information in companies or patients medical records in hospitals. What they do can earn illegal profits that great property damage is caused to those institutions. Therefore, analyzing the standard of security is necessary.

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

If external attackers already have the public parameter and use it for getting the decryption key, it is safe enough as the decryption key is under protection of the equation $F_{DK_j}(x) = x \times DK_j \times \sum_{DK_j \leq SC_i} x_{i,j}^{-1} l_{i,j}(x)$. If attackers want to decipher the decryption key $DK_j$ from the equation, they need to insert the function into Lagrange interpolation polynomial to assure its security. The first function $l_{1,2}(x)$ is analyzed as below.

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

The attackers are found as unknown numbers, except $P$ and $G$. Although attackers obtain the equation $F_{DK_j}(x)$, they still cannot get $DK_2$ because of too many unknown numbers. Besides, external attackers

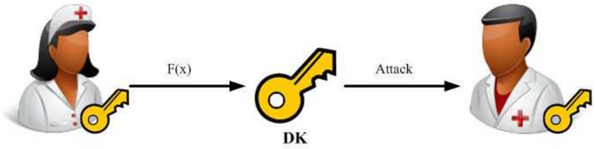


**Fig. 4:** Internal Attack

cant get the key $SK_i$ because they only have the public parameter; by contrast, they must get the key SKi 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, meaning that they have to face Elliptic Curve Discrete Logarithm Problem (ECDLP). Also, since $P$ is a big prime number, its hard to get the key. From above, it can prove that external attackers cannot obtain patients medical records and other important information by collective attacks.

(2) Internal Attack

An internal attack is a lower authorizer trying to illegally get the secret key from the higher one, like a nurse tending to decrypt important information from the doctors decryption key and get some secret materials. In Fig. 4, $SC_j$ represents the lower authorizer such as nurses and so on, and $SC_i$ represents the higher authorizer such as managers or doctors and so on. If a nurse gets the doctors decryption key, he or she could decrypt materials and other behaviors out of the authority like illegally retrieving or amending parts of patients medical records in the hospital from the doctors key. It could really cause great damage to the doctor who is being hacked and has bad feedback in the record.

For the proposed scheme in this research, $l_{i,j}(x)$ in the following equation can be referred

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

and $x_{i,t} = (ID_t||SK_i)G(\bmod p)$ . From the above, it is found that each $SK_i$ does not relate to each other, showing an advantage that there are not any equations between each key, each $SK_i$ is independent, and they do not rely on each other. Hence, the nurse wont have any equations or parameters to get the doctors 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 must face Elliptic Curve Discrete Logarithm Problem (ECDLP), which is highly challenged and difficult to decipher. Hence, an internal attack posts less threat to the system.

(3) Collusion Attack

In Fig. 4, $SC_j$ represents the lower authorizer such as nurses and so on, and $SC_i$ represents the higher authorizer such as managers or doctors and so on. A collusion attack is that the lower attackers together get the key from the higher authorizer; for example, nurses want to steal a doctors decryption key. It means many internal attackers gathering to attack, as in Fig. 5. Comparing internal attacks to collusion attacks, collusion attacks have chunk of member joint, thats why there are more keys as the reference. It means the better chance to decipher the system. Hence, a collusion attack is much more dangerous than an internal attack.

To solve the problem, the key used in this thesis is randomized, no relationship between each other. Even if lower authorized keys are combined together, the higher authorizers decryption key can still not be figured out. By the way, Lagrange interpolation polynomial is used as well. Each layer does not relate to each other; also, it takes risks away the layer being deciphered by attackers. Therefore, the higher authorizers key becomes safer. $SC_j$ is separated into an individual one. The good point is that there exist remote chances to get the higher authorizers private key either by internal attacks or collusion attacks.

From the equation $F_{DK_j}(x) = x \times DK_j \times \sum_{DK_j \leq SC_i} x_{i,j}^{-1} l_{i,j}(x)$ , $l_{i,j}(x)$ is the key point that it is taken as an example.

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

$SK_2 - SK_6$ are unknown numbers. If $SK_2$ represents the manager or the doctors key and the others represent the nurses keys, only $(ID_2||SK_2)G(\bmod p)$ in $SK_2$ is an unknown number. From above, the security is based on Elliptic Curve Discrete Logarithm Problem (ECDLP). From the former document, the security of Elliptic Curve Discrete Logarithm Problem (ECDLP) is according to a prime number. Once the prime number is big enough, the safer it would be that it is hard to decipher the key $SK_i$. Collusion attackers cannot figure out any clues related to the key $SK_i$ through this equation. That is why this proposed scheme can withstand collusion attacks.

(4) Equation Breaking Attack

An equation breaking attack is that attackers try to put up the decryption key they want by known equations and a few parameters. Whether the equation is safe or not is discussed in this section.

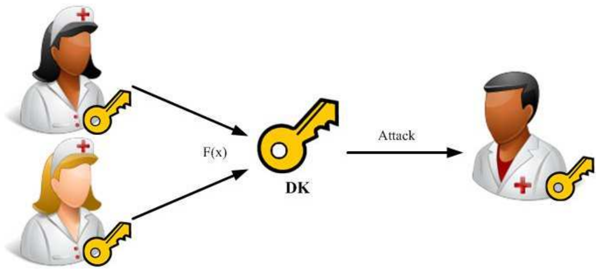


**Fig. 5:** Collusion Attack

Assuming that two legitimate users $SC_1$ and $SC_2$ can derive the key $DK_5$ from $F_{DK_5}(x)$ , it is feasible for $SC_2$ deriving another legitimate users secret parameters by public parameters, the secret parameter $SK_2$ and the access polynomial $F_{DK_5}(x)$ . If the secret parameters are successfully got, the key $SK_1$ is derived and $SC_1$'s important information is illegal accessed. In case of the possibility, the security of this equation needs to be analyzed.

$$F_{DK_5}(x_{2,5}) = x_{2,5} \times DK_5 \times \sum_{DK_j \le SC_i} x_{i,j}^{-1} l_{i,j}(x_{2,5})$$
$$\Rightarrow F_{DK_5}(x_{2,5}) \times DK_5^{-1} = x_{2,5} \times \sum_{DK_j \le SC_j} x_{i,j}^{-1} l_{i,j}(x_{2,5})$$
$$\Rightarrow F_{DK_5}(x_{2,5}) \times DK_5^{-1} = x_{2,5} \times \left\{ \begin{array}{c} (x_{1,5})^{-1} l_{1,5}(x_{2,5}) \times \\ (x_{2,5})^{-1} l_{2,5}(x_{2,5}) \times \\ (x_{4,5})^{-1} l_{4,5}(x_{2,5}) \end{array} \right\}$$

On the left side of the equation, $SC_2$ can legally use the polynomial $F_{DK_5}(x)$ to get the key $DK_5$ that $F_{DK_5}(x) = DK_5$.

$$\Rightarrow DK_5 \times DK_5^{-1} = x_{2,5}$$
$$\times \left\{ (x_{2,5})^{-1} \times \left( \frac{x_{2,5}-x_{1,5}}{x_{2,5}-x_{1,5}} \right) \left( \frac{x_{2,5}-x_{3,5}}{x_{2,5}-x_{3,5}} \right) \left( \frac{x_{2,5}-x_{4,5}}{x_{2,5}-x_{4,5}} \right) \left( \frac{x_{2,5}-x_{5,5}}{x_{2,5}-x_{5,5}} \right) \left( \frac{x_{2,5}-x_{6,5}}{x_{2,5}-x_{6,5}} \right) \times ... \right\}$$
$$\Rightarrow 1 = x_{2,5} \times \{0 + (x_{2,5})^{-1}$$
$$\times \frac{(ID_5||SK_2)G(\bmod P) - (ID_5||SK_1)G(\bmod P)}{(ID_5||SK_2)G(\bmod P) - (ID_5||SK_1)G(\bmod P)} \times ... + 0\}$$
$$\Rightarrow 1 = x_{2,5} \times x_{2,5}^{-1} \times 1$$

On the right side of the equation, a function $L_{2,5}(x_{2,5})$ in Lagrange interpolation polynomial equals 1, and the others are 0. Even if a legitimate user can successfully take the advantage of known parameters to this step, they cannot get the key because of failing to inverse polynomials or parameters from 1. In addition, equation breaking attackers must face Elliptic Curve Discrete Logarithm Problem (ECDLP) to get the secret key $SK_i$ from Lagrange interpolation polynomial, $x_{i,t} = (ID_t||SK_i)G(\mathrm{mod}\, p)$. Hence, this proposed scheme alike can withstand equation breaking attacks.

(5) Analysis of Performance In the following analysis of performance, the performance of the proposed scheme is compared with that of several published schemes. The computational complexity and the storage requirement of each scheme are investigated.

**Table 3:** Notation table

| Definition | Notation |
|---|---|
| $k$ | Number of the security classes |
| $m$ | Number of the files |
| $v_i$ | Degree of the polynomial $f(x)$ |
| $len$ | Bit-length of an integer $len$ |
| $T_{MUL}$ | Time for performing a modular multiplication |
| $T_{INV}$ | Time for performing a modular inversion |
| $T_{EC\_MUL}$ | Time for executing a scalar multiplication on the Elliptic curve E |
| $T_{EC\_ADD}$ | Time for executing an/a addition/subtraction on the Elliptic curve E |
| $T_{exp}$ | Time for executing a modular exponentiation |
| $T_{hash}$ | Time for evaluating a hash function |
| $T_{mod}$ | Time for executing a modular arithmetic operation |
| $T_l$ | Time for evaluating an interpolation polynomial |

Notations used in the performance analysis are listed in Table 3

In this subsection, the required computational overheads and storage are addressed. Most of the published schemes which actually utilize Lagrange interpolation do not follow an environment structure adopted by the proposed scheme. For this reason, the performance of the proposed scheme is compared with the schemes proposed by Chen et al. [21], Das et al. [19] and Chang et al. [20], because these three schemes follow a similar structure. Knuth [18] showed that the process of interpolation $(k+1)$ points using Newtons equation required $(k^2+k)/2$ division and $k^2+k$ subtractions, where k was the degree of the interpolating polynomial. Both Chens and this scheme apply interpolation polynomial. The main difference between Chens and this scheme is the encryption system used, where Chen adopts exponent encryption, while ECC is applied in this study. It has significant computation gap between this two different methods.

For the evaluation of the polynomial to derive the successors secret key, according to Knuth [18], $(2k-1)$ multiplications and $(2k)$ additions and one modular operation are needed by applying Horners rule.

The proposed scheme thus requires a computation time of $2T_{MUL} + \sum_{1 \le i \le k} v_i(T_l + T_{INV}) + kT_{EC\_MUL}$ to generate the access functions $F_{DKt}(x)$ in the key generation phase, where $T_l$ is the computation time for evaluating an interpolating polynomial. In the key derivation phase of this proposed scheme, a computation time of $v_i TEC\_MUL$ is required for computing ECC multiplication time and the computing time of $mT_l$ is required for evaluating $F_{DKt}(x)$. Hence, a computation time of $v_i T_{EC\_MUL} + mT_l$ is required in the key derivation phase. A computation time of $v_i TEC\_MUL$ is hence required for the key generation phase and the key derivation phase of this proposed scheme.

The scheme of Chang et al. [20], which utilizes Newtons interpolating equation, requires a computation time of $\sum\limits_{1\leq i\leq k} v_i T_l + (2 \sum\limits_{1\leq i\leq k} v_i + k)T_{\text{exp}} + kT_{INV}$ for creating the interpolating polynomials $H_i(x)$ and the parameters $V_i = E_i^{K_i^{-1}} (\bmod p)$ in the key generation phase. In the key derivation phase, a computation time of $v_i T_{\text{exp}} + kT_l$ is required for computing $x_j = K_i^{-ID_i} (\bmod p)$ and $y_j = H_i(x_j)$, and a computation time of $A_i T_{exp} + mT_{exp}$ is required for computing $+mT_{exp}$ and $E_j = V_j^{K_j} (\bmod p)$. Hence, a computation time of $(4 \sum\limits_{1\leq i\leq k} v_i + k + m)T_{\text{exp}} + ( \sum\limits_{1\leq i\leq k} v_i + k)T_l + kT_{INV}$ is required for both the key generation phase and the key derivation phase of the scheme of Chang et al. [20]. It is noticed that the most time-consuming operation used in constructing the scheme of Chang et al. is the modular exponentiation.

Following a same line of reasoning, the computation time for the key generation phase and the key derivation phase of the scheme of Das et al. [19] is given by, respectively, $( \sum\limits_{1\leq i\leq k} v_i)T_l + \sum\limits_{1\leq i\leq k} v_i T_{INV} + ( \sum\limits_{1\leq i\leq k} v_i)T_{hash}$ and $kT_l + v_i T_{hash}$. Hence, a computation time of $( \sum\limits_{1\leq i\leq k} v_i + k)T_l + \sum\limits_{1\leq i\leq k} v_i T_{INV} + (3 \sum\limits_{1\leq i\leq k} v_i)T_{hash}$ is required for the key generation phase and derivation phase of the scheme of Das et al. [19].

The scheme of Chen et al. [21] thus requires a computation time of $2T_{MUL} + \sum\limits_{1\leq i\leq k} v_i(T_l + T_{INV}) + kT_{MUL}$ for generating the access functions $F_{DKt}(x)$ in the key generation phase, where $T_l$ s the computation time for evaluating an interpolating polynomial. In the key derivation phase of this proposed scheme, a computation time of $v_i TMUL$ is required for computing, and a computing time of $mT_l$ is required for evaluating $F_{DKt}(x)$. Hence, a computation time of $v_i T_{MUL} + mT_l$ is required in the key derivation phase. A computation time of $(k + \sum\limits_{1\leq i\leq k} v_i)T_{MUL} + ( \sum\limits_{1\leq i\leq k} v_i + m)T_l + \sum\limits_{1\leq i\leq k} v_i T_{INV} + 2T_{MUL}$ is hence required for the key generation phase and the key derivation phase of this proposed scheme.

The storage space required by each of the four schemes under comparison is further considered. For the proposed scheme, a storage space of $(m+2)\,len$ is required for the public parameters, and a storage space of $len$ is required for each private key $SK_i$ of the user $SC_i$. For the scheme of Chang et al., a storage space of $(2k+1)len$ is required for the public parameters $V_i, H_i(x)$ and $p$, and a storage space of length $len$ is required for each private key $K_i$.

For the scheme of Chen et al. [21], a storage space of $(m+2)$ $len$ is required for the public parameters, and a storage space of $len$ is required for each private key $SK_i$ of user $SC_i$.

For the scheme of Das et al. [19], a storage space of $(k+m)$ $len$ is required for the public parameters $ID_j$, $H_i(x)$ and a storage space of $len$ is required for each private key. Since the number of security classes $(k)$ is usually larger than the number of confidential files $(m)$, the proposed scheme requires a smaller storage space than the other three schemes most of the time.

It is noticed that the key operation used for constructing the four schemes under comparison is the same, modular exponentiation. The computation complexity of the schemes by Chang et al. [20] and Das et al. [19] are $O(k^2)$ in the number of modular hashing and of the scheme by Chen et al[21] is $O(k^2)$ in the number of modular ECC. The computation complexity of the proposed scheme is $O(k^2)$ in the number of modular ECC. The complexity and the storage requirement of the four schemes under comparison are summarized in Table 1.

It now addresses a numerical experiment conducted to compare time performance in terms of the computation time required for the key generation phase and key derivation phase.

### 4.1 Numerical Experiment

A numerical experiment conducted to compare the performance in terms of the computation time required for the key generation phase and the key derivation phase is addressed. Plots of the computation time for the key generation phase of the three schemes under comparison versus the number of members in the hierarchy are given in Figure 6. The computation time for the proposed scheme, the scheme of Das, the scheme of Chen and the scheme of Chang are indicated by red line, green line, blue line, and pink line, respectively. As the number of members reaches 1200, the computation time for the proposed scheme, the scheme of Das, the scheme of Chen, and the scheme of Chang are, 7.39 seconds, 15.45 seconds, 17.66 seconds, and 22.67 seconds. The proposed scheme is better than the other three schemes.

The computation time required for the key derivation phase of the four schemes under comparison is further considered. The plots of the computation time, following a structure similar to that of Figure 12, are given in Figure 13. Again, the scheme of Chang always requires the most computation time. The proposed scheme is better than the other three schemes.

## 5 Conclusions

As the advance of technology rapidly grows, the Internet has become increasingly important for modern people. It brings lots of benefits to people; not only the exchange of

**Table 4:** Analysis of computation complexity

| | Key Generation/ Derivation | Complexity | Storage of public parameters | Storage of private keys |
|---|---|---|---|---|
| Chang et al. (2004) | $(4\sum_{1\le i\le k} v_i + k + m)T_{\exp}$<br>$+(\sum_{1\le i\le k} v_i + k)T_i + kT_{INV}$ | O($k^2$) in modular exponentiation | $(2k+1)len$ | $len$ |
| Das et al. (2005) | $(\sum_{1\le i\le k} v_i + k)T_i$<br>$+\sum_{1\le i\le k} v_i T_{INV} + (2\sum_{1\le i\le k} v_i)T_{hash}$ | O($k^2$) in hashing | $(k+m)len$ | $len$ |
| Chen et al. | $(k+\sum_{1\le i\le k} v_i)T_{\exp} + (\sum_{1\le i\le k} v_i + m)T_i$<br>$+\sum_{1\le i\le k} v_i T_{INV} + 2T_{MUL}$ | O($k^2$) in modular exponentiation | $(m+2)len$ | $len$ |
| The New Proposed | $(k+\sum_{1\le i\le k} v_i)T_{EC\_MUL} + (\sum_{1\le i\le k} v_i + m)T_i$<br>$+\sum_{1\le i\le k} v_i T_{INV} + 2T_{MUL}$ | O($k^2$) in modular exponentiation on Elliptic curve E | $(m+2)len$ | $len$ |

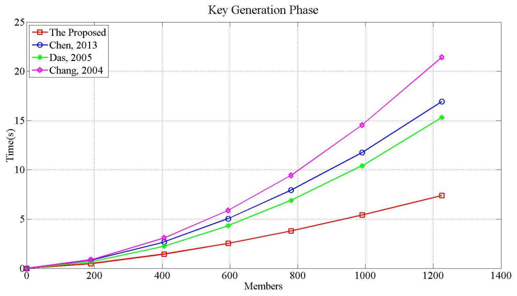


**Fig. 6:** Analysis of computation complexity

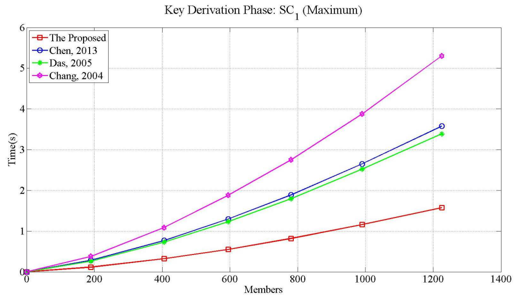


**Fig. 7:** Key derivation phase

knowledge and information is more convenient, but the operation of medical system is more digitized. Hence, a medical system is more effective now when traditional paper medical records gradually become electronic medical records. With that, quality medical services and up-to-date information are acquired. 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 being Intercepted or stolen by attackers can cause great property damage. Here, although the access control is widely applied, the security in the structure still needs to be improved. How to make mobile agents work better is the emphasis.

The key is encrypted by applying Lagrange interpolation polynomial and Elliptic Curve Cryptography to protecting its security, hiding it in the access polynomial to assure only legitimate users being able to access to the private files or resources, and analyzing whether the proposed scheme can withstand every common attacks or not. As a result, the fact of choosing Lagrange interpolation polynomial is the key being randomized, no relationship between each key, that it is relatively hard to be hacked. Moreover, since the key is under Elliptic Curve Cryptography system, attackers must encounter Elliptic Curve Discrete Logarithm Problem (ECDLP). This will greatly enhance the difficulty to crack the key.

The mobile agent technology, which is effective to access to the information immediately, is discussed in the thesis. Therefore, its security and integrity in the instable

Internet can be assured; also, it is combined with the access control in the internal structure as the control to make information more private and secure. The outcome will be obviously if being applied to the medical system or the cloud system of a company.

## Acknowledgement

The introduction of talents Huaqiao University Scientific Research Projects (Project No. 13BS412).

## References

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

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

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

[4] 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.

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

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

[7] 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.

[8] 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

[9] 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.

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

[11] 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..

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] D. E. Knuth, The Art of Computer Programming, 3rd Ed., Addison-Wesley, Reading, MA, 1998.

[19] M. L. Das, A. Saxena, V. P. Gulati and D. B. Phatak, Hierarchical Key Management Scheme Using Polynomial Interpolation, *SIGOPS Operating Systems Review*, Vol. 39, No. 1, pp. 40-47, 2005

[20] C. C. Chang, I. C. Lin, H. M. Tsai and H. H. Wang, A Key Assignment Scheme for Controlling Access in Partially Ordered User Hierarchies, *Advanced Information Networking and Application*, Vol. 2, pp. 376-379, 2004

[21] T. L. Chen, Y. F. Chung, J. M. Hong, J. H. Jhong, C. S. Chen and T. S. Chen, A Hierarchical Access Control Scheme Based on Lagrange Interpolation and ELGamal Algorithm with Numerical Experiments, *Applied Mechanics and Materials* , Vols. 385-386, pp. 1705-1707, 2013.

**Tsung Chih Hsiao** received the Ph.D. in the Department of Computer Science and Engineering, National Chung Hsing University, Taiwan. He is currently an instructor in the College of Computer Science and Technology at Huaqiao University, China. Research fields include Information Security, Cryptography, and Network Security.

**Tzer Long Chen** received the Ph.D. in the Department of Information Management, National Taiwan University, Taiwan. He is currently an assistant professor in the Department of Creative Product Design at Lingtung University, Taiwan. Research fields include Information Security, Cryptography, and Network Security.

**Yu Fang Chung** received a B.A. degree in English Language, Literature and Linguistics from Providence University in 1994, an M.S. degree from Dayeh University in 2003, and a Ph.D. degree from National Taiwan University in 2007, both in Computer Science, Taiwan. She is currently an associate professor in the Departments of Electronic Engineering and Information Management at Tunghai University, doing research, i.e., Information Security and Cryptography.

**Tzer Shyong Chen** received the Ph.D. in the Department of Electrical Engineering (Computer Science) at National Taiwan University, Taiwan. He is currently a professor in the Department of Information Management at Tunghai University, Taiwan. Research fields include Information Security, Cryptography, and Network Security.