DESIGN AND IMPLEMENTATION OF A SECURED PERSONAL IDENTITY BASED ECC AND ECDSA: AN INPATIENT SYSTEM

Mike Yuliana , ST, MT
Ghandra Awaludinsyah
Aries Pratiars , ST, MT
Amang Sudarsono , ST, PhD
Electronic Engineering Polytechnic Institute of Surabaya, Indonesia

Abstract

In this research, we developed an e-health system for cases of patient's hospitalization. This system was integrated with an e-id based RFID. E-id contains patient's id, secret key, and personal identity that consist of strong and weak attributes. Strong attributes will be encrypted using ECC Method, while the authentication process will verify the validity of the patient's personal identity using ECDSA method. The results show that the system which was developed has been able to protect the patient's personal identity. This is because strong attributes have been successfully encrypted. During the authentication process, the received message was authenticated. Therefore, the system that was developed is expected to increase the trust and confidence of patients.

Keywords: E-health, authentication, e-id, ECC, ECDSA

Introduction

Nowadays, the ease of accessing e-health or medical care system plays an important role in our daily lives. The rapid development of wireless communications and computing technologies had an impact on the displacement of the health services from paper-based to the e-health service system. However, this also has a significant impact through increased efficiency, reduced storage costs and medical errors, increase data availability, and the ease of sharing data (Tan *et al.,* 2008). Consequently, its convenience also assists in the reduction of the privacy of personal identity and the medical records of patients. Thus, there is an urgent need for the development of architectures to ensure that the issue of privacy and security

are imperative in safeguarding confidential information wherever it digitally resides (Kreps and Neuhauser, 2010).

Moreover, some researches focus on the security of EHR (Electronic Health Record), whereas privacy in health services must meet the requirements of anonymity and unlinkability (Ray and Wimalasiri, 2006). Anonymity is required if personal identity in the EHR (Electronic Health Record) needs to be hidden from the other party, such that the EHR cannot be associated with a particular patient (Guo *et al.*, 2012). Other parties include insurance companies, researchers, staff management, and other parties who have no access or the appropriate privileges. On the other hand, the hospital caregivers such as doctors, nurses, and the emergency medical technicians (Kou-Hui *et al.*, 2013) should be able to obtain the personal identity of patients. Furthermore, unlinkability indicates that multiple EHRs cannot be linked to the same owner. This requirement is necessary because it prevents the profiling of a patient by the insurance companies or the central servers which stores the patient's data (Krummenacher *et al.*, 2007).

In this paper, we focus on the security of personal identity in the case of an inpatient system. System which would be developed includes the patient registration protocol in obtaining e-id and hospitalization protocol. In addition, patients' registers by filling out their personal identity such as name, address, birthdate, blood type, marriage, religion, gender, and phone number. After receiving the personal identity of the patient, the receptionist would generate a public key and a secret key. Therefore, the e-id will contain the id of patient, secret key, and patient's personal identity which has been encrypted. Hence, this will be used during the authentication process when the process of hospitalization and the patient's personal identity cannot be known by unauthorized parties. Thus, researchers should open up the eyes, give insight, and make a commitment to the security of e-health system in Indonesia. However, this would increase the trust and confidence of the public

Methods

ECC (Elliptic Curve Cryptography)

Elliptic curve cryptography is a public key cryptography system that bases its security on elliptic curve mathematical problems. Unlike Discrete Logarithm Problem (DLP) and Integer Factorization Problem (IFP), there is no sub-exponential time algorithm that is known to solve Elliptic Curve Discrete logarithm problem (ECDLP). Elliptic curve cryptography algorithms have advantages when compared with other public-key cryptography algorithm. In those algorithms, the key length is shorter but it has the same security level. Subsequently, there are three protocols of ECDLP which is well-known today: Elliptic Curve Digital Signature

Algorithm (ECDSA), Elliptic Curve Diffie-Hellman (ECDH), and Elliptic Curve ElGamal (ECElgamal). Elliptic Curve Cryptography (ECC) is one approach of public-key cryptography algorithm that is based on the algebraic structure of elliptic curves on finite area.

The use of elliptic curves in cryptography was triggered by Neal Koblitz and Victor S. Miller in 1985. Elliptic curves are also used in some integer factoring algorithm that also has applications in cryptography, such as Elliptic Curve Lenstra Factorization. Furthermore, public key algorithms based on mathematical calculations variations are fairly difficult to resolve without specific knowledge of how the calculations were made. Therefore, algorithm maker stores the private key and spreads the public key. Public key algorithm used to encrypt messages whereby only the algorithm maker would be able to solve it. Public key system such as RSA algorithm uses two very large prime numbers. Hence, the user chooses two random large prime numbers as the private key and publish the results of the calculation as the public key (Bangerter *et al.*, 2004). Furthermore, factoring large numbers that is very difficult will maintain the confidentiality of the private key. Another issue concerns the algebraic calculations $ab = c$, where a and c are known. The calculations which involve complex numbers or estate could be easily solved using logarithms. Nevertheless, in a large finite set of numbers, to find a solution from such calculation is very difficult. Thus, this is often known as "discrete logarithm problem". Elliptic curve can be written with mathematical calculations as follows (Randhawa and Singh, 2011):

$$y^2 = x^3 + ax + b \quad (1)$$

Every changes in the value of 'a' and 'b' will produce different elliptic curve. Elliptic Curve example can be seen in Fig. 1. Thus, Fig. 1(a) is a representation of elliptic curve $y^2 = x^3 - 12x + 3$, while Fig. 1(b) is a representation of another elliptic curve $y^2 = x^3 - 2x + 1$. Every elliptic curve usually defines a set of points on the field and can form albelian collection (collection of point with point infinite as an identity element). If the value of x and y that is selected is a large finite area, the solution will generate a finite albelian. However, the elliptic curve cryptography that is used in elliptic curve is defined by two finite fields.

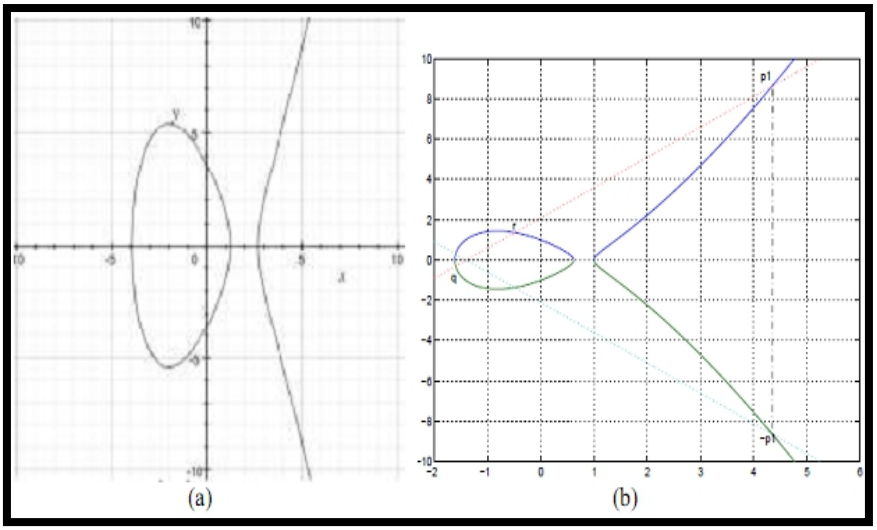

Figure 1. Some representations of elliptic curves[6]

ECDSA (Elliptic Curve Digital Signature Algorithm)

ECDSA is an analog elliptic curve of Digital Signature Algorithm (DSA). ECDSA is one of the ECC digital signatures which provide data authentication, data integrity, and non-repudiation. ECDSA was first introduced in 1992 by Scott Vanstone. In 1998, ECDSA got a standard ISO (International Standards Organization) as ISO 14888-3. In 1999, they were accepted as standard ANSI (American National Standards Institute): ANSI X9.62. In 2000, they were accepted as standard IEEE (Institute of Electrical and Electronics Engineers): IEEE 1363-2000 and standard NIST (National Institute of Standards and Technology) FIPS 186-2. In ECDSA protocol, the parties that will make the digital signature have domain parameters elliptic curve *D = {q, FR, a, b, G, n, h}*, key pair secret key *dA*, and public key *QA*. Then the party that will verify the signatures have an authentic copy of *D* document and public key of *QA*. Therefore, the processes that occurs are as follows (Randhawa and Singh, 2011):

1. Key Generation

a. Select random integer d, whose value is between $[1, n-1]$

b. Calculate $Q = dG$

c. Secret key = d and public key = Q

2. Signing

a. Select random integer k, whose value is between $[1, n-1]$.

b. Calculate $kG = (x_1, y_1)$

c. Calculate $r = x_1 mod\ n$, if $r = 0$, back to step a.

d. Calculate $k^{-1}\ mod\ n$.

e. Calculate SHA-1(m) and convert the result from string to integer e.

f.Calculate $s = k^{-1}(e + dr)\ mod\ n$.

g. Signature for message m are (r, s).

3. Verifying

a. Verify that r and s are integer between $[1, n-1]$

b. Calculate SHA-1(m) and convert the result from string to integer e.

c. Calculate $w = s^{-1} \, mod \, n$.

d. Calculate $u_1 = ew \, mod \, n$ and $u_2 = rw \, mod \, n$.

e. Calculate $X = u_1 G + u_2 Q$.

f.If $X = 0$, then the signature is incorrect. Conversely, inverse the coordinates-xx_1 from X, and calculate $v = \bar{x}_1 mod \, n$.

g. Signature valid if $v = r$.

Secure E-health System Design

In this research, we proposed a secured e-health application for the cases of inpatient which include:

1. Patient's registration

2. Data storage and processing of patient medical record information

3. Placement of patients based on the needs of the patients.

Privacy Requirements

Patient will enter their personal identity such as name, address, and their phone number at the time of registering to become a member of e-health. Personal identity is divided into two parts, namely: strong and weak attributes. Hence, the purpose of the division is to provide greater security to the strong attributes. Before being put on the e-id, strong attributes such as address, phone number will be encrypted using ECC algorithm. At the time of authentication, strong attributes will not be revealed. Thus, patient's privacy will be maintained.

Security Requirements

Some security requirements of secured e-health system are listed as follows.

Authentication: E-health system can realize the authentication of messages. For example, when a patient sends the message *M* and its signature β that was made from the patient's private key, doctor can authenticate the messages by verifying the signature using public key β. The message will be authenticated if verifying process returns true value.

Data Integrity: Besides message authentication, e-health system can also realize the integrity of data through the verification process. For example, patient signs the message *M* and send it to the doctor. Thus, to maintain the integrity of the message, patient can use hash function and obtain signatures β by calling sign algorithm with input digest *M*:

β sign(h(M),Skpatient)

Patient sends (*M,* β) to the doctor. After receiving (*M,* β), the doctor verifies the digest *M* as follows:

Accept Verify (h(M), β, Pkpatient)
If it accept true value, then the data integrity was maintained and accepted.
Non Repudiation: Security services are also provided by e-health system to prevent the rejection of the message that has been signed. For examples, if patient denies that he had signed a document which he actually signed, then the doctor could prove that the patient ever signed that document. Therefore, achieving non-repudiation service requires trusted party to be an intermediary between doctors and patients.

Patient's Registration Protocol

Patients' registers by filling out personal identity such as name, address, birthdate, blood type, marriage, religion, gender, and phone numbers. Personal identity is also regarded as attribute. Thus, there are two types of attributes, namely strong and weak attributes. Strong attributes are usually unique identity for each user, while weak attributes could be the same for each user. Example of strong attributes are address, birthdates, and phone number; while weak attributes are name, gender, blood type, marriage, and religion. After receiving the personal identity of patient, receptionist will make the process of generating public and secret key. Public key are used to scramble strong attributes, so that they cannot be known by unauthorized parties. Also, secret key are used for signing personal identity. E-id contains the id of the patient, secret key, and personal identity that contain strong and weak attributes. Therefore, the scheme of the registration protocol can be seen in Fig.2.

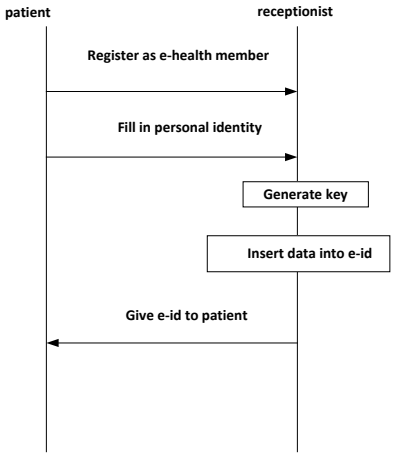

Figure 2. Issuing of e-id

Hospitalization Protocol

After getting inpatient referral from a doctor, the patient will go to the receptionist. Patients performs authentication during the authentication,

signing, and the verifying process. However, if the authentication is successful, then the receptionist will check if the rooms were empty. The allocation of rooms is in accordance with the needs of the patient which is based on the illness and the request of the patient. After finding an empty room in accordance with the above conditions, receptionist gives a message/ notification to the nurse in charge. If the room is ready, then the receptionist tells the patients to go into the room. Therefore, the scheme of hospitalization protocols can be seen in Fig. 3.

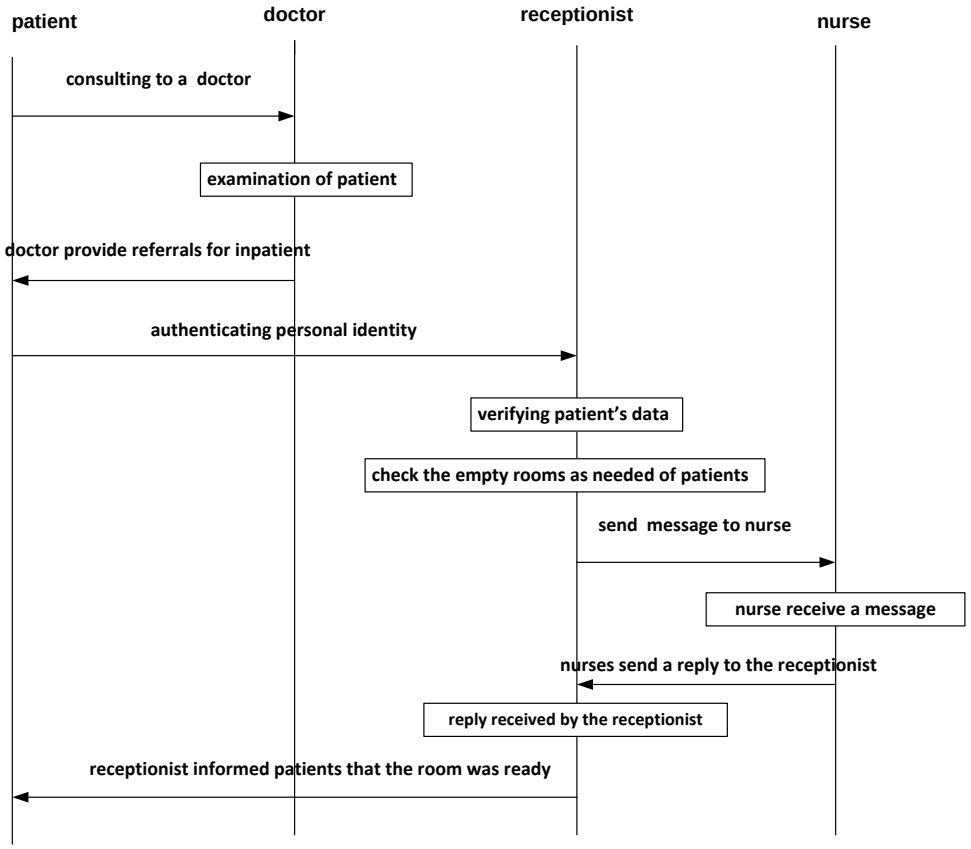

Figure 3. Flow interaction between patient and doctor

Experimental Result

In this research, secured personal identity will be tested using PC with specification as shown in Table 1. In addition, RFID reader/writer and tag with specification as shown in Table 2 and 3 would also be employed. Fig. 4 shows the RFID reader/writer and the tags that were used.

Table 1. Specifications of PC used in experiment

Specification	Remarks
Software	Java
O/S	Windows 8 (64 bit)
CPU	Intel Core™ i5-3317U Processor (1.70 GHz)
RAM	4 GB

Table 2. Specifications of RFID reader/writer used in experiment

Specification	Remarks
Microcontroller	ATmega328
Operating Voltage	5V
Input Voltage (recommended)	7-12V
Flash Memory	32 KB (ATmega328) of which 0.5 KB used by bootloader
SRAM	2 KB (ATmega328)
EEPROM	1 KB (ATmega328)

Table 3. Specifications of RFID tag used in experiment

Specification	Remarks
Model	MIFARE™ Classic 4K
Frequency	13.56MHz
Protocol	ISO14443A
Unique ID	32 bits
EEPROM Size	4096 Bytes
Material	PVC
Temperature	-20°C ~ +50°C
Dimension	85.6 × 54 × 0.86 (mm)
Data transfer	106 kbit/s
4 kB	organized in 32 sectors of 4 blocks and 8 sectors of 16 blocks (one block consists of 16 byte)
Write endurance	100000 cycles

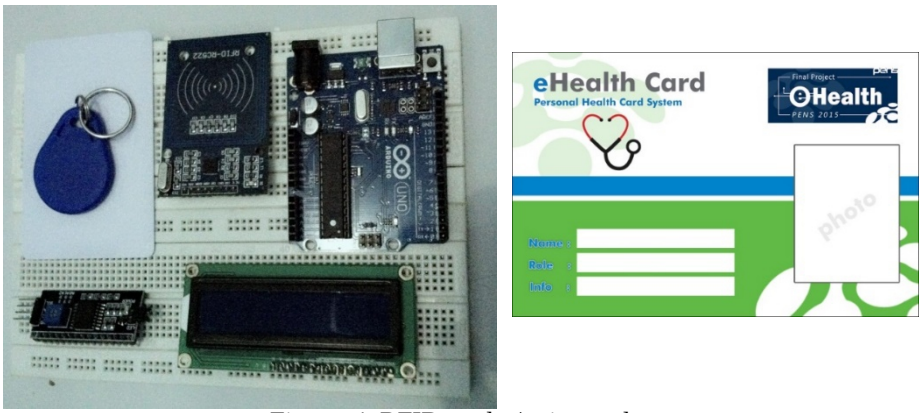

Figure 4. RFID reader/writer and tag

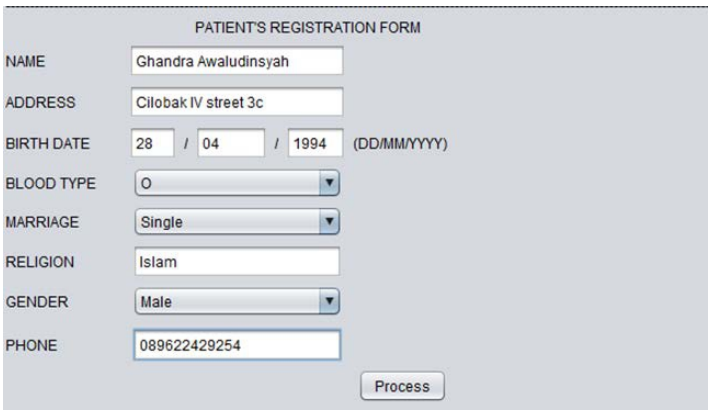

Figure 5. Patient's registration form

Fig. 5 shows a registration form that must be completed by patients when registering as a member of e-health. Thus, the address, birthdate, and phone are strong attributes. Fig. 6 shows the process of making e-id. However, this process occurs when the patient's personal identity entered during registration have been received by the server. When performing the write process, the sequence of steps to be taken includes the selection of patient ID, generate key, process, COM3, and write tags. E-id contains the id of the patient, the secret key, and personal identity that includes strong and weak attributes. Strong attributes will be encrypted using ECC methods. Thus, it cannot be identified by unauthorized parties.

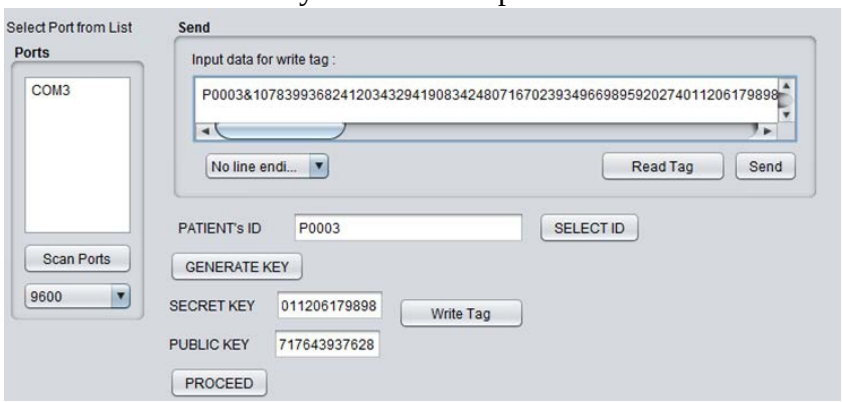

Figure 6. Write RFID form

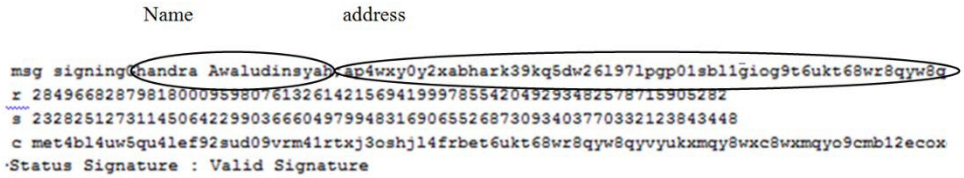

Figure 7. Authentication Result

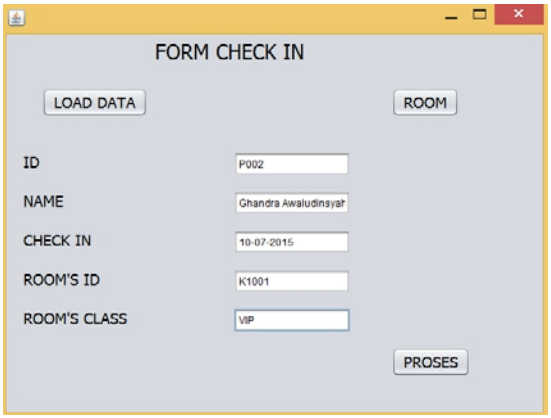

Figure 8. Check in form

Fig. 7 shows the results of the authentication process when consulting a doctor or at the time of hospitalization. During this time, patient's personal identity is been signed and verified using ECDSA. The experimental results showed that signing and verifying patient's personal identity was performed on strong attributes that had been encrypted. This is because patient's name as a weak attribute was revealed. Thus, address as a strong attributes was not revealed because it has been encrypted. Fig. 8 shows a check-in form. If the patient must be hospitalized, a room is found according to their needs.

Conclusion

In this research, we have presented the protection of the patient's personal identity using ECC and ECDSA. ECC methods are used to scramble the strong attributes, so that the data could not be known by unauthorized parties. ECDSA method is used during the authentication process of consulting a doctor and when the hospitalization to ascertain whether the messages that was received is true. The results show that the systems made has been able to protect the patient's personal identity, because the strong attributes have been successfully encrypted. During the authentication process, the received message was authenticated. Therefore, the system that was developed is expected to increase the trust and confidence of patients.

Acknowledgments

This works was supported by Grant from Kementrian RISTEK dan DIKTI.

References:

A. Randhawa, L. Singh., A Systematic Way to Provide Security for Digital Signature Using Elliptic Curve Cryptography, IJCST Vol.2, Issue 3, , 185-188, Sep-2011.

C.C. Tan, H. Wang, S. Zhong, Q. Li, Body sensor network security: an identity-based cryptography approach, The ACM Conference on Wireless Network Security (WiSec'08), April 2008.

E. Bangerter, J. Camenisch, and A. Lysyanskaya. A cryptographic framework for the controlled release of certified data. Security Protocols Workshop, volume 3957 of Lecture Notes in Computer Science, pp. 20–42. Springer, 2004.

G. L. Kreps and L. Neuhauser. New directions in eHealth communication: opportunities and challenges. Patient Education and Counseling, vol. 78, no. 3, pp. 329–336, 2010.

Kou-Hui Y., Nai-Wei L., Tzong-Chen W., and Chieh W. Secure E-Health System on Passive RFID : Outpatient Clinic and Emergency Care. International Journal of Distributed Sensor Networks, Article ID 752412, 2013.

P. Ray, J. Wimalasiri, The need for technical solutions for maintaining the privacy of EHR, in: Proc. 28th IEEE EMBS Annual International Conference, September 2006, pp. 4686–468.

R. Krummenacher, E. P. B. Simperl, L. J. B. Nixon, D. Cerizza, and E. Della Valle. Enabling the european patient summary through triplespaces. In CBMS, pages 319–324, 2007.

L.Guo, C. Zhang, J.Sun, Y.Fang, A Privacy-Preserving Attribute-Based Authentication System for eHealth Networks. Proceeding of ICDCS, pp 224-233, 2012.