Med Biol Eng Comput (2014) 52:449–457
DOI 10.1007/s11517-014-1147-9

ORIGINAL ARTICLE

An efficient forward-secure group certificate digital signature scheme to enhance EMR authentication process

Yao-Chang Yu · Ting-Wei Hou

Received: 2 May 2013 / Accepted: 3 March 2014 / Published online: 21 March 2014

Abstract The frequently used digital signature algorithms, such as RSA and the Digital Signature Algorithm (DSA), lack forward-secure function. The result is that, when private keys are renewed, trustworthiness is lost. In other words, electronic medical records (EMRs) signed by revoked private keys are no longer trusted. This significant security threat stands in the way of EMR adoption. This paper proposes an efficient forward-secure group certificate digital signature scheme that is based on Shamir's (t,n) threshold scheme and Schnorr's digital signature scheme to ensure trustworthiness is maintained when private keys are renewed and to increase the efficiency of EMRs' authentication processes in terms of number of certificates, number of keys, forward-secure ability and searching time.

Keywords Digital signature · Group certificate · Forward-secure · EMR

1 Introduction

Medical records actually store patients' medical histories; therefore, medical record management is one of the most important systems in a hospital. Advances in information technology and environmental concerns are motivating a transition from paper-based medical records to electronic medical records (EMRs). EMRs are prospective to bring wide range of advantages to healthcare provider. In order to increase the usage of EMR, many researches have been conducted [6, 7, 19, 20, 22].

The digitisation of medical records raises the issue of security. In 1998, Toyoda [25] mentioned that "ensuring the authenticity of the record" is one of the essential legal and administrative requirements of implementing EMR systems. HIPAA was enacted by the U.S. Congress in 1996 [26]. According to this Act, the digital signature cryptographic method is important to ensure the integrity and authenticity of EMRs. The Taiwanese Electronic Medical Record Produce and Management Act was passed by the Legislative Yuan of Republic of China in 2005. It also mandated that all EMRs be electronically signed by the doctors who composed them.

There is no doubt that digital signatures [28] are a good way to ensure the integrity and authenticity of EMRs, and it is used incorporated with smartcards [10, 12] in healthcare systems.

However, the current most frequently used digital signature scheme, the RSA public key system, suffers from efficiency and key renewing issues when used on EMRs in hospitals.

Consider this scenario: Dr. AAA and Dr. AAB are in the same department of a hospital. Dr. AAA wants to verify the digital signature of a medical record issued by Dr. AAB. According to the RSA algorithm, if Dr. AAA wishes to verify Dr. AAB's signature, then Dr. AAA has to search the key directory and find Dr. AAB's corresponding public key. This is because the RSA algorithm does not support the concept of a "group." On the other hand, if the doctors could share the same group public key in the department, the group public key could be used to verify both Dr. AAA's and Dr. AAB's digital signatures. Hence, Dr. AAA would not need

Y.-C. Yu (✉) · T.-W. Hou
Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan
e-mail: yuy0329@hotmail.com; n9895110@mail.ncku.edu.tw

T.-W. Hou
Department of Medical Informatics, National Cheng Kung University Hospital, College of Medicine, National Cheng Kung University, Tainan, Taiwan
e-mail: houtw@mail.ncku.edu.tw

to search for Dr. AAB's public key in the key directory. A group certificate digital signature scheme could be used in EMR systems to increase efficiency and reduce key search time and key directory size. However, simply enforcing the idea of a group is still not enough to solve the key renewal problem. A forward-secure function is also important for signature schemes. In 2010, Yu et al. [31] mentioned there are three reasons that a private key needs to be revoked and renewed: (1) loss of the private key (medical staff card), (2) expiration of the private key (medical staff card) and (3) retirement of the medical personnel. When any one of these three situations occurs, the EMRs are no longer verifiable. Hence, it is necessary to have a new "forward-secure" key that allows a medical staff to retain the trustworthiness of the previously signed medical records.

This research aims to develop an efficient forward-secure group certificate digital signature scheme for EMRs in hospitals. In this paper, we propose a "group certificate" signature scheme that supports forward-secure functionality and satisfies four principal requirements: (1) the private key is updatable to solve the key renewal problem; (2) private key lifetime is not predetermined; (3) only one public key certificate is needed in a group; and (4) each user should have a unique private key that can be used for generating individual signatures on behalf of the group.

This new forward-secure group certificate digital signature scheme is based on Shamir's (t,n) threshold scheme [23] and Schnorr's digital signature scheme [21] and includes four algorithms: key generation, key update, signing, and verifying. The proposed scheme has the following four advantages that fulfill the abovementioned four principles:

1. Forward-secure functionality is enabled.
2. There is no need to predetermine the lifetime of private key (T).
   Note: If the private key reaches the upper bound of the key lifetime T, then the whole group needs to be rekeyed. To prevent such a problem, the proposed scheme is designed with no need to predetermine private key lifetimes.
3. One group public key certificate is needed to authenticate the identity of the group and verify the individual digital signature.
4. Each member within a group holds an individual user private key that can be used to generate individual digital signatures on behalf of the group.

2 Background information

In this section, brief background information on group-oriented, group certificate and forward-secure signature schemes is provided.

2.1 Group-oriented and group certificate signature scheme

In 1994, Harn [8] first proposed a "group-oriented" threshold digital signature scheme. According to Harn, the group-oriented threshold digital signature scheme should satisfy five properties: (1) it is required to have at least t group users to mutually generate group signatures; (2) the group signature size is the same as the individual signature size; (3) the signature verification process is more efficient, because there is only one group public key; (4) the group signature is verifiable by any users who are outside the group; and (5) it is the group members' responsibility to sign the group signature. In the following years, several group-oriented threshold digital signature schemes were proposed [9, 15, 16, 18, 24, 27, 29, 30].

In Harn's scheme, the group secret key, SK, breaks into n different shadows, SK_1, SK_2, SK_3,…,SK_n, and these n shadows are distributed to n group members to generate a group signature. The limitation of the group-oriented threshold digital signature schemes is that all group members do not hold the individual secret key; therefore, individual group members are not able to generate individual signatures.

In 2004, Chen et al. [5] proposed the "group certificate" authentication scheme. The main difference between Chen et al.'s "group certificate" scheme and Harm's "group-oriented" scheme is that Chen et al.'s scheme enables each group member to hold a private key, and each group member is capable of generating an individual signature on behalf of the group. However, Chen et al.'s scheme does not support forward-secure functionality.

2.2 Forward-secure signature scheme

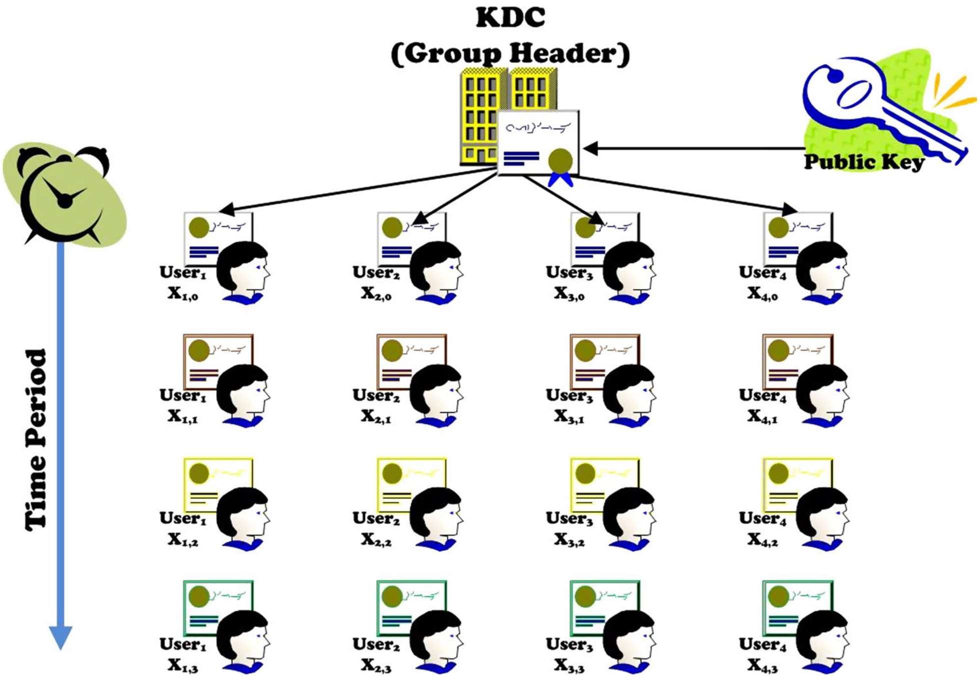
In 1999, Anderson [2] noted that the most frequently used digital signature algorithms, such as RSA and DSS, faced a serious security threat: if the private key of the signer is compromised, all signatures issued with the compromised private key are no longer trusted. Anderson proposed the concept of the forward-secure signature scheme. After Anderson presented this concept in 1999, Bellare and Miner [3] proposed the first forward-secure signature scheme. In the following years, several forward-secure digital signature schemes were developed [1, 4, 11, 13, 14, 17].

3 Methods

3.1 Description of the scheme

There is no doubt that currently there is no suitable forward-secure group certificate digital signature scheme

Fig. 1 Scheme model ($N = 4$)



that can be used in hospitals to solve the problems that we mentioned in the Introduction section. Therefore, in this section, the authors have decided to create a new forward-secure group certificate digital signature scheme, and it is suitable for hospital use.

Before the forward-secure group certificate digital signature scheme can be designed, we also need a forward-secure transformation model. In this section, we propose a new forward-secure transformation model and use the transformation model to create the forward-secure group certificate digital signature scheme.

3.2 The transformation model

To prevent the aforementioned shortcomings, we do not fully adopt Krawczky's scheme to achieve forward security in our proposed scheme. Instead, we look into the basic principle of forward security and decide to adopt hash chain technology to build a new Forward-Secure Pseudorandom Generator (FSPRG). FSPRG simply requires a seed (User $\mathrm{ID}_{i,t-1}$) to generate a new $\mathrm{ID}_{i,t}$ for time period t. This $\mathrm{ID}_{i,t}$ is then inputted to key generation process to get an updated private key, $x_{i,t}$. The algorithm is as follows;

$$\mathrm{FSPRG}\left(\mathrm{ID}_{i,t-1}\right) \rightarrow \mathrm{ID}_{i,t}$$

New private key at time period t, $x_{i,t} = f(\mathrm{ID}_{i,t})$.

Hence, the forward-secure functionality is enabled without extra public key certificates, and at each time period, extra storage is not needed and total lifetime of private key T is not predetermined.

3.3 Signature scheme

Our model contains three entities, the key distribution centre (KDC), group users and the verifier. The group header plays the role of a KDC, which is trusted by all users. In this scheme, it is assumed that all group users do not have the ability to generate private keys, so the KDC is responsible for generating private keys for all users, and all users share only one public key. When any group user's private key is compromised, the KDC also helps the specific user to update the compromised private key into a new private time. The proposed scheme is depicted in Fig. 1, which shows that in a group with 4 group members and each member owns a private key and there is only one public key owned by the group header.

There are four algorithms in the proposed scheme, including the key generation algorithm, the key update algorithm, the signing algorithm and the verifying algorithm.

Notations

p	Prime number
q	Prime number
β	$\beta < p$ and is a primitive root of p
z_q*	Finite field
Y	Group public key
$x_{i,n}$	User private key
$h()$	Collision-resistant one-way hash function
FDPRG()	Forward-Secure Pseudorandom Generator
k	Integer
s	Signature value
M	Message
m	Hash value, so $m = h(M)$

1. Key generation algorithm

The key generation algorithm is used to generate group public key ($Y = \beta^X \bmod p$) and user private key ($x_{i,0} = f(ID_{i,0})$, where i denotes the User i). Within a group, when the key generation algorithm is done, each group member will be assigned a user private key, and only public key is generated for the group.

2. Key update algorithm

As mentioned before, there are many reasons that a key holder requires key update, such key expiration, key leakage, etc. This algorithm is used to update the old key ($x_{i,t-1} = f(\mathrm{ID}_{i,t-1})$) into a new key ($x_{i,t} = f(\mathrm{ID}_{i,t})$).

3. Signing Algorithm

This algorithm is used to generate digital signature ($\sigma_{i,t} = (s_{i,t}, r_{i,t})$), where $\sigma_{i,t}$ represents the signature of the EMRs.

4. Verifying Algorithm

This algorithm is to prove that $\beta^{s_{\mathrm{i,t}}}$ equal to $Y^{h(m,r_{i,t})} \cdot r_{i,t} \bmod p$ If they are equal, then the digital signature is legitimate.

Because the private keys used in this scheme are not precomputed, it is not required to predetermine the time period (T), and there is no need to have secure storage to store the valuables. There is only one public key certificate used in this proposed scheme. The most important contribution in this scheme is that the each user's private key is updated individually. This means if a medical staff accidently lost his healthcare personnel card, only his private key is renewed. All other private keys used by medical staffs in the hospital remain the same.

3.4 Algorithms

1. Key Generation Algorithm

1.1 KDC first picks two large primes p and q, such that $q|p-1$. $|p|$ and $|q|$ denote the bit lengths of p and q respectively. $|p| \geq 512$, $|q| \geq 160$.

1.2 KDC selects β in z_q^* as a secret parameter.

1.3 KDC randomly generates an $n-1$ degree polynomial

$$f(z) = b_0 + b_1 z + b_2 z^2 + \cdots + b_{n-1} z^{n-1} \bmod q,$$
$$\text{where} \quad b_j \in Z_q \quad \text{for} \quad j = 1, \ldots, n-1$$

1.4 KDC generates

(i) Group public key: $y = \beta^X \bmod p$, where $X = b_0$
(ii) User I private key: $x_{i,0} = f(\mathrm{ID}_{i,0})$ for the initial stage

2. Key update Algorithm

A Forward-Secure Pseudorandom Generator is used to make the scheme capable of forward-secure function.

$\mathrm{FSPRG}(\mathrm{ID}_{i,t-1}) \rightarrow \mathrm{ID}_{i,t}$

New private key at time period t, $x_{i,t} = f(\mathrm{ID}_{i,t})$

3. Signing
There is a message M to be signed.

3.1. $m = h(M)$, where $h()$ denotes a collision-resistant one-way hash function.
3.2. User i at time t randomly selects an integer $k_{i,t} \in Z_p{}^*$
3.3. User I computes $r_{i,t} = \beta^{k_{i,t}} \bmod p$
3.4. User i computes

$$s_{i,t} = x_{i,t} \cdot h(m, r_{i,t}) + k_{i,t} - [x_{i,t} - b_0] \cdot h(m, r_{i,t}) \bmod p$$

3.5 The signature of message M is $\sigma_{i,t} = (s_{i,t}, r_{i,t})$

4. Verify

Check whether $\beta^{i,t}$ equals to $Y^{h(m,r_{i,t})} \cdot r_{i,t} \bmod p$

Theorem 1 *If the signatory and verifier follow the algorithm above, then the verifier will accept the signature as valid.*

Proof

$$\begin{aligned}
\beta^{s_{i,t}} \bmod p &= \beta^{x_{i,t} \cdot h(m,r_{i,t}) + k_{i,t} - \left[\sum_{j,j\neq 1}^{n-1} b_j (ID_{i,t})^i\right] \bmod p} \bmod p \\
&= \beta^{\left[b_0 + \sum_{j,j\neq 1}^{n-1} b_j (\mathrm{ID}_{i,t})^i \cdot \beta^{k_{i,t}}\right]} \Big/ \beta^{\sum_{j,j\neq 1}^{n-1} b_j (\mathrm{ID}_{i,t})^i \cdot h(m,r_{i,t})} \bmod p \\
&= \beta^{b_0 h(m,r_{i,t})} \cdot \beta^{\left[\sum_{j,j\neq 1}^{n-1} b_j \left(\mathrm{ID}_{i,t}^i\right)\right] \cdot h(m,r_{it})} \\
&\quad \cdot \beta^{k_{i,t}} / \beta^{\left[\sum_{j,j\neq 1}^{n-1} b_j \left(\mathrm{ID}_{i,t}^i\right)\right] \cdot h(m,r_{it})} \bmod p \\
&= Y^{h(m,r_{i,t})} \cdot r_{i,t} \bmod p
\end{aligned}$$

Lemma 1 (Reference to William [28])

For any integer t
If $g = h^{(p-1)/q} mod p$
Then $g^t \bmod p = g^{t \bmod q} \bmod p$

Proof By Fermat's theorem, because h is relatively prime to p, $h^{p-1} \bmod p = 1$

If we have a nonnegative integer n,

$$\begin{aligned} g^{\mathrm{nq}} \bmod p &= \left(h^{(p-1)/q} \bmod p\right)^{\mathrm{nq}} \bmod\ p \\ &= h^{((p-1)/q)^{\mathrm{nq}}} \bmod p \\ &= h^{(p-1)n} \bmod p \\ &= \left(\left(h^{p-1}\right) \bmod p\right)^{n} \bmod p \end{aligned}$$

So, for nonnegative integers n and z, we have

$$\begin{aligned} g^{\mathrm{nq}+z} \bmod p &= \left(g^{\mathrm{nq}} g^{z}\right) \bmod p \\ &= \left(\left(g^{\mathrm{nq}} \bmod p\right)\left(g^{z} \bmod p\right)\right) \bmod p \\ &= g^{z} \bmod p \end{aligned}$$

Any nonnegative integer t can be represented uniquely as $t = \mathrm{nq} + z$, where n and z are nonnegative integers, and $0 < z < q$. So, $z = t \bmod q$.

4 Results

In order to prove that the proposed scheme is workable, in this section, a scenario is provided to show how the proposed scheme can be used in EMR system.

4.1 Application scenario on EMR

In this section, a scenario is provided to explain how the proposed scheme works. Figure 2 shows a hierarchical structure, representing the organisational structure of a hospital. On the top of the structure is the hospital administration, which is responsible for administrative issues and manages public and private keys for the entire hospital. In other words, the administration plays the role of a KDC. This structure can be organized into five groups (G1 through G5). Also, Fig. 2 shows the corresponding keys for each group; for example, the members of G1 are hospital administration (Hospital A), Dept. AA, Dept. AB, Dept. AC and Dept. AD. Within G1, each member shares a group certificate (public key certificate), puk_A.

Dept. AA owns a private key, $\mathrm{pri}_{\mathrm{AA}}$, and a public key certificate, $\mathrm{puk}_{\mathrm{AA}}$. Dept. AB owns a private key, $\mathrm{pri}_{\mathrm{AB}}$, and a public key certificate, $\mathrm{puk}_{\mathrm{AB}}$. Dept. AA uses private key $\mathrm{pri}_{\mathrm{AA}}$ to generate signatures and Dept. AB uses private key $\mathrm{pri}_{\mathrm{AB}}$ to generate signatures. These signatures generated by Dept. AA and Dept. AB can be verified by Hospital A's public key, $\mathrm{puk}_{\mathrm{A}}$. In this structure, if RSA public key infrastructure is used, then 26 keys (including public and private keys) are needed. For our proposed scheme to work, only 17 keys are needed. In general, the total keys required is reduced by $m + 1$, where m is the total number of doctors in the hospital (the leaf nodes in the hierarchical structure). Therefore, our proposed scheme eases the problem of key management in the healthcare system structure.

Let's return to the scenario mentioned in the introduction. Dr. AAA and Dr. AAB are in the same department, Dept. AA. Dr. AAA wants to verify an EMR composed and signed by Dr. AAB. In the RSA public key infrastructure, Dr. AAA has to search the key directory and find Dr. AAB's public key. If we assume that the key directory is well sorted and the search algorithm is binary, then the

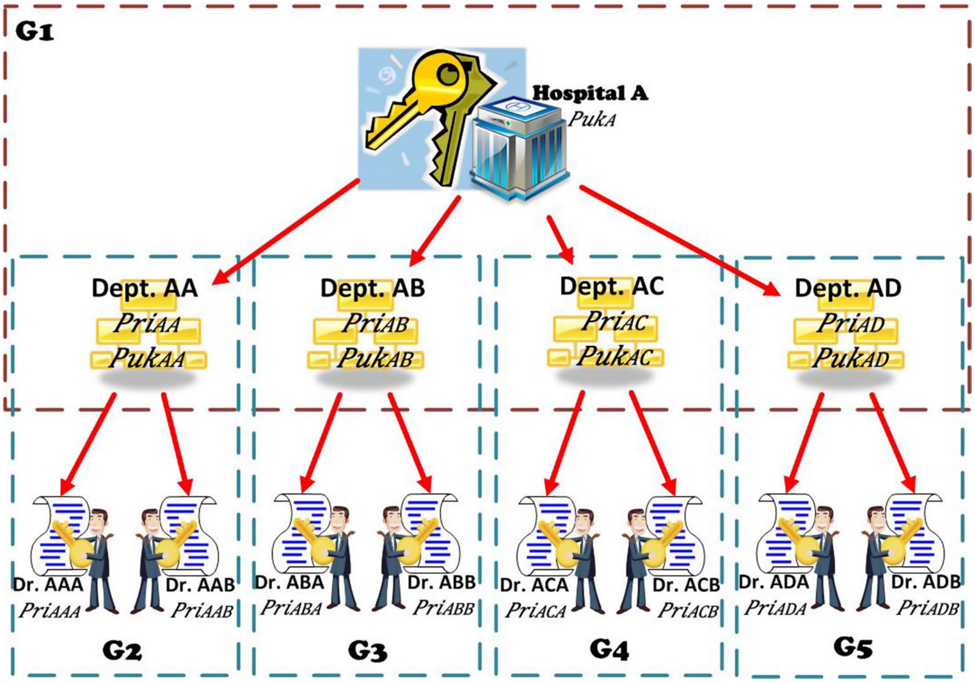


Fig. 2 Healthcare system structure

time needed to search Dr. AAB's public key from the key directory is O(log n), where n is the size of the key directory. In our scheme, Dr. AAA and Dr. AAB are in the same department, and they share the same public key certificate, puk_{AA}, so the search time is not required for Dr. AAA. Hence, our proposed scheme is more efficient than the RSA scheme.

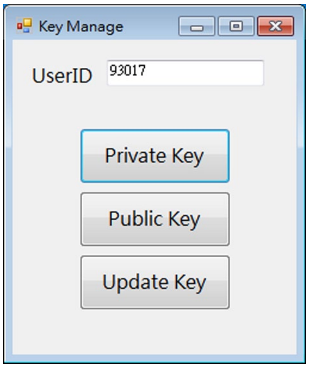
In another scenario, Dr. AAA wants to verify an EMR composed and signed by Dr. ABA. Because Dr. AAA and Dr. ABA are not in the same department, Dr. AAA has to search the public key directory and find the group key (puk_{AB}) belonging to Dep. AB. The public key search time in our scheme is O(log $n - m-1$), because there are only $n - m-1$ public keys in the public key directory. Therefore, our proposed scheme is still more efficient than the RSA scheme.

Also, the proposed scheme has the ability to update private keys, so if Dr. AAA's private key is lost or expires, Dr. AAA can file an application form to hospital administration and receive an updated private key. With forward-secure ability, although Dr. AAA's private key is updated, all the signed EMRs with private keys are still verifiable, which means their trustworthiness is maintained.

4.2 Simulated EMR system

In this section, a simulated EMR system is provided to show the proposed scheme can easily be programmed to perform the tasks. For the following, we use the implemented EMR system to simulate the scenario, which is mentioned in Sect. 4.1.

In the initialization step, all private keys and public keys are generated by the key generation tool, which is shown in Fig. 3, and then the private keys are distributed to all doctors in the hospital. Table 1 summarizes the simulated hospital information, and it shows the private key for each doctor in all departments and the public key for each department.

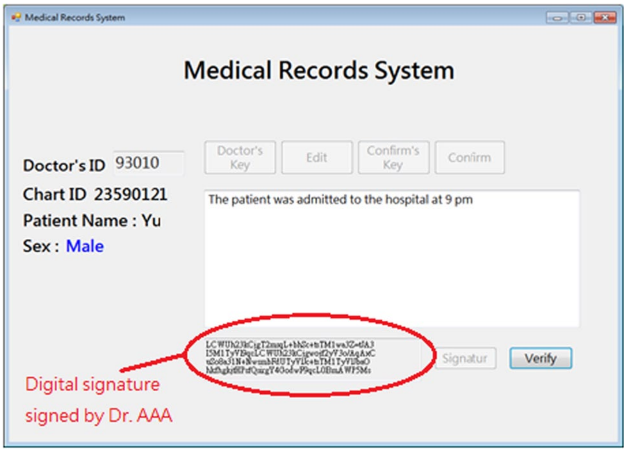


UserID 93017

Fig. 3 Key generation tool

Table 1 Simulated hospital information

Group	DR.	ID	Private Key	Public Key
G2 Dept. AA	Dr. AAA	93010	93010 Private Key	G2 Public Key
	Dr. AAB	93011	93011 Private Key	
G3 Dept. AB	Dr. ABA	93012	93012 Private Key	G3 Public Key
	Dr. ABB	93013	93013 Private Key	
G4 Dept. AC	Dr. ACA	93014	93014 Private Key	G4 Public Key
	Dr. ACB	93015	93015 Private Key	
G5 Dept. AD	Dr. ADA	93016	93016 Private Key	G5 Public Key
	Dr. ADB	93017	93017 Private Key	



Doctor's ID 93010

Chart ID 23590121

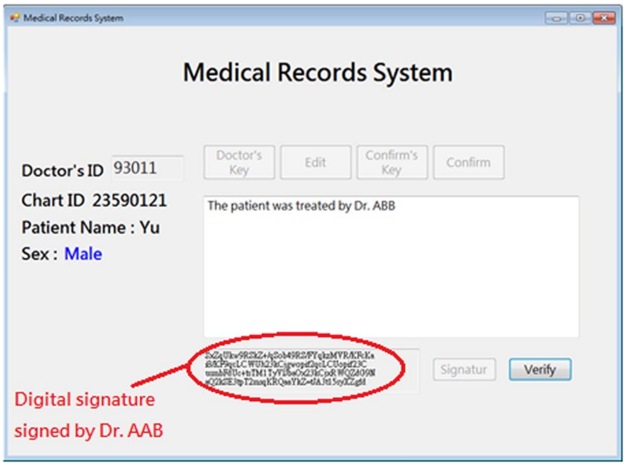
Patient Name : Yu

Sex : Male

The patient was admitted to the hospital at 9 pm

LCWUh23kCjgT2maqL+bhSc+tsTM1waJZ=tJA3
l5M1TyVEkqcLCWUh23kCjgwodf2yV3o/AqAxC
u2o8a31N+NwsmbRtUTyV1kc+tsTM1TyVLbaO
NdfbgkjdHPdQmrgY4OodwP9qcL0BmAWPSMs

Fig. 4 Patient record signed by Dr. AAA (ID: 93010)



Doctor's ID 93011

Chart ID 23590121

Patient Name : Yu

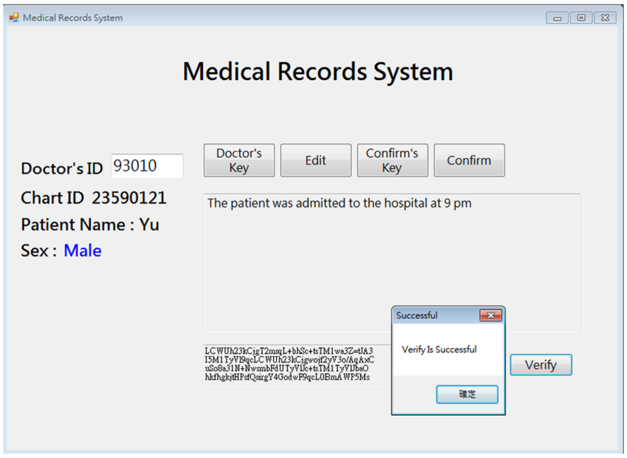
Sex : Male

The patient was treated by Dr. ABB

SxZqUkw9RSkZ+/qSob49RS/FYqkzMVR/KRcKa
sB/KP9qcLCWUh23kCjgwopdf2qcLCUopdf23C
umbRtUc+tsTM1TyVLbaOx23kCpdRWQZd09N
sQ2kSE3tpT2maqKRQaaYkZ=tJA3tl5oyJCZg6t

Fig. 5 Patient record signed by Dr. AAB (ID: 93011)

According to the following results, we have proved that the proposed scheme not only works theoretically but also it can be implemented and work in practical.



Medical Records System

Doctor's ID 93010

Chart ID 23590121

Patient Name : Yu

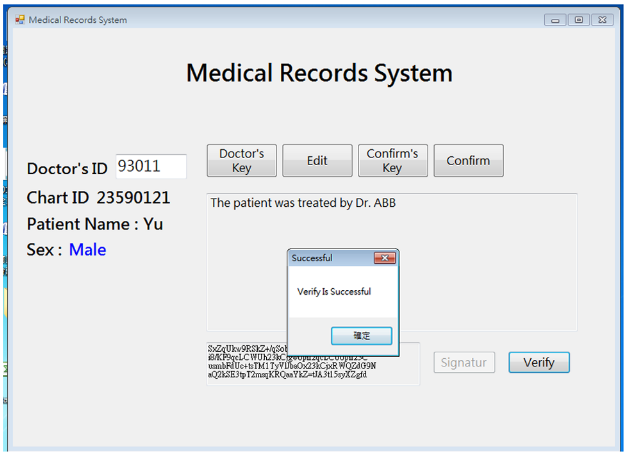
Sex : Male

The patient was admitted to the hospital at 9 pm

```
LCWUh23kCjgT2msqL+bhSc+tsTM1wa3Z=tJA3
I5M1TyVl9qcLCWUh23kCjgwojf2yV3o/AqAxC
uSo8a31N+NwsmbFdUTyVlJc+tsTM1TyVlJbaO
hkfhgkjtHPsfQsirgY4GodwF9qcL0BmAWP5Ms
```

Verify Is Successful

Fig. 6 Patient record verified by group public key (G2 Public Key)



Medical Records System

Doctor's ID 93011

Chart ID 23590121

Patient Name : Yu

Sex : Male

The patient was treated by Dr. ABB

```
SxZqUkw9RSkZ+/qSol
i8/KF9qcLCWUh23kCjgwopn2qcLC0opn23C
usmbFdUc+tsTM1TyVlJbaOx23kCjxRWQZdG9N
aQ2kSE3tpT2msqKRQaaYkZ=tJA3t15syXZgfd
```

Verify Is Successful

Fig. 7 Patient Record verified by group public key (G2 Public Key)

When doctors receive their own private key, they can use the private key to sign electronic records; for example, the Fig. 4 shows the electronic record was signed by Dr. AAA, and Fig. 5 shows the electronic record was signed by Dr. AAB. Because Dr. AAA and Dr. AAB are the same department, these two EMR can be verified by the same group public key (G2 Public Key); the result is shown in Figs. 6 and 7.

5 Discussion

In this section, in order to show the proposed scheme is more efficient than the currently used RSA scheme by providing the comparison between the proposed scheme and RSA scheme in Sect. 5.1. Also, a security analysis is provided in Sect. 5.2 to prove that the proposed scheme is strong enough to against the well know attacks.

Table 2 Comparisons

	RSA	Proposed scheme
Number of certificates	N	1
Number of keys	$2n$	$n+1$
Forward-secure ability	No	Yes
Search time	O(log n)	O(1)

5.1 Comparisons

In this section, a comparison will show the differences between currently used RSA signatures and our proposed signatures.

We assume there are n members in a group in the same department. If RSA public key infrastructure is used, then n public key certificates are needed, and $2n$ keys (public/private keys) are required. Also, RSA is not forward-secure. It is assumed that a binary search is used, so the time to search the public key directory is O(log n).

On the other hand, if our scheme is adopted, because our scheme introduces the concept of the group, only one public key certificate is needed, and only $n+1$ keys (n private keys and one public key) are necessary. In addition, our scheme is equipped with forward-security function to solve the re-key problem. A group of members share one public key; therefore, there is no need to search the public key directory for the corresponding public key to verify signatures. A summary of the comparisons is shown in Table 2.

5.2 Security analysis

An attacker can forge signatures either by finding the signer's private key x or by finding collisions in the hash function. Finding the signer's private key is equivalent to solving a discrete logarithm problem; however, it is computationally infeasible to find the collision, such that $h(M) = h(M')$. Therefore, both problems are considered difficult.

There are several possible attacks on our proposed scheme. The following shows that the proposed scheme is secure.

5.2.1 Attack 1

An outsider of the group can correct signatures, $\sigma_{i,t} = \left(s_{i,t}, r_{i,t}\right)$, issued by a particular User$_\mathrm{i}$ at time period 1 to t and use these signatures to derive this User$_i$'s corresponding private key, $x_{i,t}$.

Cryptanalysis of Attack 1 By giving the outsider the knowledge of signatures, $\sigma_{i,t} = (s_{i,t}, r_{i,t})$, attackers can compute $x_{i,t}$ from the equation $s_{i,t} = x_{i,t} \cdot h\left(m, r_{i,t}\right) + k_{i,t} - \left[x_{i,t} - b_0\right] \cdot h\left(m, r_{i,t}\right) \bmod p$ by first finding $k_{i,t}$; however, finding $k_{i,t}$ is a Discrete Logarithm Problem (DLP).

5.2.2 Attack 2

An outsider of the group can correct signatures $\sigma_{i,t} = \left(s_{i,t}, r_{i,t}\right)$ issued by User$_i$ at time period t, where $i = 1\ldots n$ and use these signatures to derive a particular User$_i$'s corresponding private key, $x_{i,t}$.

Cryptanalysis of Attack 2 By giving the outsider the knowledge of signatures $\sigma_{i,t} = (s_{i,t}, r_{i,t})$ issued by User$_i$ at time period t, where $i = 1\ldots n$ and use these signatures to derive a particular User$_i$'s corresponding private key $x_{i,t}$, the outsider still needs to find $k_{i,t}$; however, finding $k_{i,t}$ is a DLP.

5.2.3 Attack 3

An adversary tries to forge a signature $\sigma_{i,t} = (s_{i,t}, r_{i,t})$ for a given M' that has been delegates to a particular User$_i$ at time period t without knowing $x_{i,t}$.

Cryptanalysis of Attack 3 In equation $s_{i,t} = x_{i,t} \cdot h\left(m, r_{i,t}\right) + k_{i,t} - \left[x_{i,t} - b_0\right] \cdot h\left(m, r_{i,t}\right) \bmod p$, we assume that the $\sigma_{i,t} = (s_{i,t}, r_{i,t})$ is known and that it is difficult to forge a signature over message M' for a particular User$_\mathrm{i}$ at time period t. To achieve this attack, the adversary first has to find $k_{i,t}$; however, this is DLP. Secondly, the adversary needs to find collision to satisfy $h(M') =$ m; however, it is infeasible to find M' due to the non-invertible property of $h()$. Third, according to Shamir's (t,n) threshold scheme, it is required that at least t insiders work together to reconstruct $f(z) = b_0 + b_1 z + b_2 z^2 + \cdots + b_{n-1} z^{n-1} \bmod q$; therefore, it is not possible for the adversary to do so.

5.2.4 Attack 4

Fewer than t insiders try to derive the private keys of the other participants of the group.

Cryptanalysis of Attack 4 According to Shamir's (t,n) threshold scheme, it is required that at least t insiders work together to reconstruct $f(z) = b_0 + b_1 z + b_2 z^2 + \cdots + b_{n-1} z^{n-1} \bmod q$; therefore, it is not possible to reconstruct $f(x)$ with fewer than t insider.

5.2.5 Attack 5

Fewer than t insiders attempt to forge a signature on message M', which has been delegates to particular User$_i$ at time period t without the knowledge of $x_{i,t}$.

Cryptanalysis of Attack 5 For this attack to work, all the corrupt insider needs to do is either reconstruct User$_i$'s private key at time period t, $x_{i,t}$, or find the collision of $h()$. According to Shamir's (t,n) threshold scheme, which is based on Lagrange Interpolating Polynomial, the attacker needs t shadows to reconstruct all private keys for User$_i$, where $i = 1\ldots n - 1$ form the following equation.

$$H(x) = \sum_{s=1}^{t} k_{i_s} \prod_{j=j\neq s}^{t} \frac{x - x_{i_j}}{x_{i_s} - x_{i_j}} \bmod p$$

Therefore, fewer than t insiders are not capable of reconstructing the private key for Useri at time period t. Also, the insiders need to find the collision to satisfy $h(M) = m$ at time period $t - 1$.

5.2.6 Attack 6

A User can use the current private key $x_{i,t}$ to derive previous key $x_{i,t-1}$ at time period $t - 1$.

Cryptanalysis of Attack 6 Forward-Secure Pseudorandom Generator is a one-way function, so it is computationally infeasible to derive $x_{i,t-1}$ from $x_{i,t}$.

Although the strength of our proposed algorithm is not RSA rely on the factoring problem, in this section, we have successfully demonstrated how the proposed scheme can be attacked and how the proposed scheme can protect itself against all above-mentioned attack base on the mathematic properties.

6 Conclusions

Regulation, standardization, technology and security are key concerns in the development of a system of EMRs. When paper-based medical records are transformed into EMRs and put on the open Internet for exchange, security becomes a crucial topic. In this paper, we focused on the security problems of the current most frequently used digital signature scheme, RSA, and presented an efficient forward-secure group certificate digital signature scheme to manage EMR's security issues. We performed a security analysis, and its results showed that the proposed digital signature is robust against attacks. Comparisons between RSA and our proposed scheme are provided to show the advantages of our scheme. These advantages include the following: (1) only one group certificate is needed within a group, (2) fewer keys are needed, (3) forward security is enabled and (4) there is no search time needed in a group.

In summary, the proposed efficient forward-secure group certificate digital signature scheme does not only solve the security issues of the EMR but also increases the efficiency of the EMR authentication process and eases the problems of key directory management.

7 Future work

This newly proposed signature scheme creates a whole new signature system with better efficiency and forward-secure function, but this proposed scheme is not like current used RSA digital signature scheme; therefore, it is not compatible with HIS. Our future work is to discover a new digital signature scheme that not only contains the same advantages as the proposed scheme in this paper but also can be incorporated with HIS easily.

References

1. Abdalla M, Reyzin L (2000) A new forward-secure digital signature scheme. Advances in cryptology-ASIACRYPT00. Springer, Berlin, pp 116–129
2. Anderson R (1997) Two remarks of public key cryptology. Technical report UCAM-CL-TR-549, University of Cambridge, Computer Laboratory
3. Bellar M, Miner S (1999) A forward-secure digital signature scheme. Advances in cryptology-CRYPTO99. Springer, Berlin, pp 431–448
4. Canetti R, Halevi S, Katz J (2003) A forward-secure public key encryption scheme. Advances in Cryptology-EUROCRYPT03. Springer, Berlin, pp 255–271
5. Chen KY, Chang TW, Yu YC, Laih CS (2004) Efficient authentication scheme based on group certificate and its application on mobile communication systems. Appl Cryptogr Netw Secur pp 475–484
6. Fiol DG, Haug PJ (2009) Classification models for the prediction of clinicians' information needs. J Biomed Inform 42:82–89
7. Giakoumaki A, Pavlopoulos D, Koutsouris D (2006) Secure and efficient health data management through multiple watermarking on medical images. Med Biol Eng Comput 44:619–631
8. Harn L (1994) Group-oriented (t,n) threshold digital signature scheme and digital multisignature. IEE Proc Comput Dig Tech 141(5):307–313
9. Hsu CL, Wu TS, Wu TC (2004) Group-oriented signature scheme with distinguished signing authorities. Future Gen Comput Syst 20:865–873
10. Huang J-W, Hou T-W (2007) Design and prototype of a mechanism for active on-line emerging/notifiable infectious diseases control, tracking and surveillance, based on a national healthcare card system. Comput Methods Programs Biomed 86(2):161–170
11. Itkis G, Reyzin L (2001) Forward-secure signatures with optimal signing and verifying. Advances in cryptology-CRYPTO01. Springer, Berlin, pp 441–456
12. Kardas G, Tunali ET (2005) Design and implementation of a smart card based healthcare information system. Comput Methods Programs Biomed 81(1):66–78
13. Kozlov A, Reyzin L (2002) Forward-secure signatures with fast key update 3rd International conference on security in communication networks. Springer, Berlin, pp 341–356
14. Krawczyk H (2003) "Simple forward-secure signature schemes from any signature scheme: 7th ACM conference on computer and communications security, pp 108–115
15. Lee WB, Chang CC (1999) (t,n) threshold digital signature scheme with traceability property. J Inform Sci Eng 15:669–678
16. Li CM, Hwang T, Lee NY (1995) Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders. Proceedings of EUROCRYPT94, Springer, Berlin, pp 194–203
17. Malkin T, Micciancio D, Miner S (2002) Efficient generic forward-secure signatures with unbounded number of time periods. Advances in cryptology-EUROCRYPT02, Springer, Berlin, pp 400–417
18. Michels M, Horster P (1996) On the risk of disruption in several multiparty signature scheme. In: Advances in cryptology-ASIACRYPT96, Springer, Berlin, pp 334–345
19. Patel VL, Arocha JF, Kushniruk AW (2002) Patients' and Physicians' understanding of health and biomedical concepts: relationship to the design of EMR systems. J Biomed Inform 35:8–16
20. Rose AF, Schnipper JL, Park ER, Poon EG, Li Q, Middleton B (2005) Using qualitative studies to improve the usability of an EMR. J Biomed Inform 38:51–60
21. Schnorr CP (1990) Efficient identification and signatures for smart cards, Advances in Cryptology-CRYPTO89. Springer, Berlin, pp 339–351
22. Scholl J, Syed-Abdul S, Ahmed AL (2011) A case study of an EMR system at large hospital in India: challenges and strategies for successful adoption. J Biomed Inform 44:958–967
23. Shamir A (1979) How to share a secret. Commun ACM 24(11):612–613
24. Shao Z (2005) Cryptanalysis of Xia-You group signature scheme. J Syst Softw 75:89–94
25. Toyoda K (1998) Standardization and security for the EMR. Int J Med Inform 48:57–60
26. U.S. Department of Health & Human Services (1996) Health Insurance Portability and Accountability Act (HIPAA). http://www.hhs.gov/ocr/privacy/
27. Wang CT, Lin CH, Chang CC (1998) Threshold signature schemes with traceable signers in group communication. Comput Commun 21(8):771–776
28. William S (1999) Cryptography and network security-principles and practice, 2nd edn. Prentice Hall, Englewood Cliffs
29. Wu TS, Hsu CL (2003) Threshold signature scheme using self-certified public keys. J Syst Softw 67:87–97
30. Wu TS, Hsu CL (2004) "Cryptanalysis of group-oriented (t,n) threshold digital signature schemes with traceable signers. Comput Stand Interfaces 26:477–485
31. Yu YC, Huang TY, Hou TW (2012) Forward secure digital signature for electronic medical records. J Med Syst 36(2):399–406