3-2004

A smart-card-enabled privacy preserving E-prescription system

Yanjiang YANG
Singapore Management University, yjyang@smu.edu.sg

Xiaoxi HAN

Feng BAO
Singapore Management University, fbao@smu.edu.sg

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Published in IEEE Transactions on Information Technology in Biomedicine, 2004 March, Volume 8, Issue 1, Pages 47-58
https://doi.org/10.1109/TITB.2004.824731

A Smart-Card-Enabled Privacy Preserving E-Prescription System

Yanjiang Yang, Xiaoxi Han, Feng Bao, and Robert H. Deng

***Abstract*—Within the overall context of protection of health care information, privacy of prescription data needs special treatment. First, the involvement of diverse parties, especially nonmedical parties in the process of drug prescription complicates the protection of prescription data. Second, both patients and doctors have privacy stakes in prescription, and their privacy should be equally protected. Third, the following facts determine that prescription should not be processed in a truly anonymous manner: certain involved parties conduct useful research on the basis of aggregation of prescription data that are linkable with respect to either the patients or the doctors; prescription data has to be identifiable in some extreme circumstances, e.g., under the court order for inspection and assign liability. In this paper, we propose an e-prescription system to address issues pertaining to the privacy protection in the process of drug prescription. In our system, patients' smart cards play an important role. For one thing, the smart cards are implemented to be portable repositories carrying up-to-date personal medical records and insurance information, providing doctors instant data access crucial to the process of diagnosis and prescription. For the other, with the secret signing key being stored inside, the smart card enables the patient to sign electronically the prescription pad, declaring his acceptance of the prescription. To make the system more realistic, we identify the needs for a patient to delegate his signing capability to other people so as to protect the privacy of information housed on his card. A strong proxy signature scheme achieving technologically mutual agreements on the delegation is proposed to implement the delegation functionality.**

***Index Terms*—Anonymous, e-prescription, privacy, pseudonym, smart card.**

I. Introduction

EASY and instant access to electronically managed medical and insurance information is now a key factor determining the efficiency and quality of health care provision. However, the involvement of diverse parties in the process, together with the continuously increased mobility of patients, makes it practically infeasible to maintain such information in an unified and globally available manner. To be more specific, i) a number of parties get involved in the health care provision, such as hospitals, clinics, general practitioners (GPs), and external business associates including insurance companies, billing agencies, pharmacies, and so on, resulting in the heterogeneity of information infrastructures and business patterns; ii) the mobility of patients comes from the facts that people on frequent trips may need to visit doctors in different cities or even countries; some patients may need to seek appropriate medical treatment beyond local facilities. It is clear that it is hard to achieve the goal of "data availability at the point of care" with the current model of statically maintained information repositories. This difficulty can be resolved by *smart cards* [2] containing the latest personal medical and insurance information, carried by the patient themselves [1], [3].

Drug prescription is among the health care processes that frequently makes references to patients' medical and insurance information. Before issuing a prescription, a doctor needs to inspect a patient's medical records, complementing his diagnosis process as well as checking for possible allergies and harmful drug interactions pertaining to the patient; insurance information is consulted to determine whether the intended drugs are indeed covered by the patient's health plan. It is apparent that the introduction of smart card based *portable* personal information repository would significantly simplify the process of drug prescription, enabling the doctor to bypass several bureaucratic and time-consuming procedures if otherwise retrieving information from central databases. Moreover, the doctor would be relieved completely from the inconvenience and annoyance caused by the occasional blockage of network traffic.

In addition to being a data storage device, the smart card is capable of performing some "intelligent"work. We take advantage of this to entail the smart card digital signature signing capability to sign the electronic prescription pads, declaring the patient's authorization to the prescription so as to collect the prescribed medicine. This proof of authorization will be used by the pharmacy to collect payment from the patient's health plan account administrated by the corresponding insurance organization. Moveover, this aspect is further extended to include the delegation of prescription signing capability among users, which we refer to as *delegated signing*. Simply speaking, delegated signing is intended for a designated person (e.g., a relative or custodian who accepts the delegated signing right from the patient) who uses his own smart card to sign the prescription on behalf of the patient in collecting the medicine. Such an extension is motivated by the observation that, in practice, it is quite common that other people instead of the patient himself collect the prescribed medicine on his behalf. They may be his custodians, relatives, or friends who accompany him to visit the doctor. Although it offers the flexibility to be carried by someone else than the owner himself, passing the smart card to a delegatee would increase the likelihood of disclosing sensitive personal medical information stored in the card and expose the patient to potential threat

Manuscript received July 9, 2003; revised October 6, 2003. This work was supported by the IEEE.

Y. Yang, F. Bao, and R. H. Deng are with the Institute for Infocomm Research, Singapore 119613 (e-mail: yanjiang@i2r.a-star.edu.sg; baofeng@i2r.a-star.edu.sg; deng@i2r.a-star.edu.sg).

X. Han is with the Institute of Software, Chinese Academy of Sciences Beijing 100080, China (e-mail: hxx@ios.ac.cn).

Digital Object Identifier 10.1109/TITB.2004.824731

of unexpected abuses. From a technical point of view, it is obviously desirable to root out such drawbacks in an e-prescription system. Delegated signing avoids the passing of a patient's smart card to the people who actually sign the prescription pad. An additional fact that merits delegated signing is that it does not complicate the system, instead it simplifies the system design to avoid considering implementation particulars. A typical particular is that if the smart card is implemented as biometrics-based, then passing smart card to others for signing would be impossible.

Apart from bringing the flexibility and convenience in accessing personal health and insurance data, the adoption of smart cards in our system has many other advantages: the authenticity of the patients is automatically ensured by holding the cards, so that many processes would be automated and sped up, e.g., hospital admissions; it prevents patients from obtaining multiple prescriptions from different practitioners; smart cards can be used as a tool for tracking public health initiatives, e.g., vaccinations; with free access to the emergency data stored in the smart card, emergency treatment would be instant; to name a few.

Privacy concerns in health care prevail now. Notably, patients worry about their health information being disclosed. The medical community has long been recognizing the ethical and professional obligation to protect health care information, as stated in the Hippocratic oath: *Whatsoever I shall see or hear in the course of my dealing with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets*. As a matter of fact, privacy of health information goes beyond the ethical scope in the sense that compromising its privacy would harm patients' dignity, job acquisition, and health [4]–[6]. Legislation too has long recognized the importance and urgency in maintaining privacy of health care information. For instance, the Health Insurance Portability and Accountability Act in U.S. [7], Recommendation R (75) in Europe [32], and the Health Information Privacy Code in New Zealand [39] are all laws on the protection of health care information. As far as prescription is concerned, doctors have privacy concerns too. In particular, doctors' prescription patterns would be (and have been) collected, analyzed, and utilized by their affiliated organizations, drug companies, etc., [8]. For instance, the General Practice Research Database [35] maintained in the U.K. serves, among others, exactly this purpose. It is therefore crucially important to protect privacy of both the patients and the doctors in the course of prescription. We, in respondence, focus on addressing such privacy issues in the proposed system.

The remainder of the paper is organized as follows. We investigate the privacy issues regarding patients as well as doctors involved in the process of prescription in Section II. In Section III, we present a strong proxy signature scheme achieving mutual agreements between the delegator and the delegatee, to enable the delegated signing functionality in our system. In Section IV, we propose our protocol to implement a smart-card-based e-prescription system, meeting the identified needs of privacy protection. We also outline the aspects on protecting data in the smart card and review some works that are closely related to ours. Section V is a summary of the paper.

II. Privacy in Prescription

Electronic medical records (EMRs) are gradually substituting the traditional paper-based medical records in health care domain, providing more efficient and timely collaboration and information exchange among various health care organizations, as well as external business associates (e.g., pharmacies, insurance organizations, billing companies, etc.). Besides the direct impact on the quality and efficiency of health care provision, the wide use of EMRs eases medical research. For example, researchers in health care organizations normally conduct research on the basis of inspection of clinical data to find and evaluate new treatments; insurance companies and other health care providers frequently engage in extensive research on the cost effectiveness of certain medical treatments and practices, capitalizing on health care data. Although this type of research is important and beneficial, it is a potential threat to the privacy of health care information. From the privacy perspective, it seems enough to de-identify the EMRs prior to their statistical processing. However, there are frequent cases in which patients benefit from being traceable by the research, such as in the assessment of treatment safety [9].

Protecting health care information goes far beyond the basic ethical principle of respecting individuals' privacy in a civilized society. Inappropriate disclosure of an individual's health care information has varying consequences, ranging from inconvenience to ruin [41] (see http://www.healthprivacy.org for a number of concrete cases). The protection of security and privacy of the health care information is now under the jurisdiction of laws around the world. For example, U.S. enacted the Health Insurance Portability and Accountability Act (HIPAA) [7], [10]; European Union issued the Recommendation R (75) [32] and Privacy Directive [42], Japan has the Data Protection Bill [43], and South Korea has similar Acts [44].

Privacy protection of prescription information is relevant in the overall context of protecting health care information primarily due to the fact that prescription data are quite revealing of a patient's health history. In other words, it is by no means very hard to deduce one's health condition by inspecting his prescription information. In this sense, there is little difference between prescription data and other kinds of medical records in terms of privacy concern from the viewpoint of patients. On the other hand, doctors also have privacy concern in prescription data since their prescription habit is reflected there. This information can be then utilized for many purposes. Consider this example: a hospital, based on the comparison of doctors' prescription patterns, may issue guidelines on prescription of certain drugs, and doctors are then required to follow. Those failing to comply would be treated negatively. Another example: drug companies take advantage of doctors' prescription information for marketing purpose, tempting doctors to prescribe their drugs [8]. Patients' information regarding their drug purchasing can be used for a similar reason by drug companies.

The process of prescription is a little particular in the sense that it involves external business associates such as pharmacy and insurer other than medical related parties. The active involvement of several parties would inevitably cause multiple vulnerabilities in terms of privacy protection. Moreover,

while it is reasonable to presume medical personnel would be bound by strong ethical obligation and good professional faith in maintaining privacy of the prescription information, it seems baseless to assume the same for nonmedical parties such as pharmacies and insurance companies. Worse yet, law regulations do not suffice in stopping these organizations from leaking prescription information while it is being used for, say, aforementioned cost-effectiveness research. In the U.S., for instance, there is no federal law on the protection of medical records kept by pharmacies; on the contrary, pharmacies benefit financially from selling prescription information: over 99% of prescription claims are collected and processed by Pharmacy Benefits Management Systems (PBMs) [11].

The protection of privacy should not result in a pseudonymous process. If prescription pads were issued in a truly pseudonymous manner, a wide range of drug abuses could be expected. There is already a thriving black market on prescription medicines [12]. More importantly, laws and regulations require pharmacies to maintain records that can be identified for possible inspection and preventing drug interactions [13]. For example, Section 164.512(2)(d) of HIPAA states that disclosure of protected health information including audits may be made to health oversight agencies for authorized oversight activities. In addition, some current beneficial research based on prescription data would be rendered impossible once truly pseudonymous prescription is applied. As a consequence, it is desirable that prescription data i) achieves two-way *anonymity*, i.e., normally they are sustained *pseudonymous*, but allowed for feasible *pseudonymity revocation* [29]; ii) provides *linkability* to enable useful research on data aggregation. Note that linkability of prescription data is also conducive to fraud prevention of patients and doctors. To be more specific, i) prescription information of a patient should be identifiable to the insurer for billing purpose, pseudonymous be linkable to the pharmacies or PBMs for enabling research and fraud prevention, and pseudonymity be revocable under law provision; ii) pseudonymity of a doctor should be similarly revocable, and prescription from the same doctor should be pseudonymous to the health care organization as well as the pharmacy, but linkable to the insurer for fraud prevention.[1]

III. A Strong Proxy Signature Scheme

In Section II, we have identified the need for delegation of prescription signing rights (delegated signing). In this section, we propose a strong proxy signature scheme based on the Schnorr signature scheme [25]. Its extension to other DLP-like signature schemes is straightforward.

For ease of reference, we list below the notations to be used in this section:

O, Pr, V	the original signer, the proxy signer, and the verifier, respectively.
p, q	large primes with $q \mid (p-1)$.
g	an element of order q in Z_p^*.
x_u, y_u	key pair of user u for signing, with $y_u = g^{x_u} \bmod p$.
σ	a digital signature of a message m signed by a conventional DLP-like signature scheme.
$veri(\cdot)$	the verification algorithm of digital signature.
w_d	a delegation warrant.

In the proxy signature setting, the *original signer* (delegator) would delegate his signing capability to the *proxy signer* (delegatee), so the proxy signer is authorized to issue *proxy signatures* on behalf of the original signer. References [26], [27] are among the earliest work on the idea of proxy signature, and the concept was later systematically studied in [20] with three types of delegations, namely, *full delegation*, *partial delegation*, and *delegation by warrant*. In full delegation, the original signer O simply gives his secret signing key to the proxy signer Pr. This kind of delegation seems to have little practical significance as O loses complete control of his signature. In partial delegation, a new key pair is generated from O's secret, and the newly generated secret is delivered to Pr via a private channel. As the name implies, a delegation by warrant capitalizes on a policy warrant to certify Pr as entrusted. To satisfy the varying delegation requirements, combination of the last two types of delegation seems practical and viable. In fact, our scheme capitalizes on this combination. The schemes in [20] do not offer nonrepudiatability since both O and Pr know the proxy signing key. The work in [22] suffers from the same problem. To overcome this, Zhang proposed in [23] a nonrepudiable proxy signature scheme, which however was found not to be successful [24]. Lee *et al.*[18] first introduced the concept of strong proxy signature which represents both O's signature and Pr's signature. Nonrepudiatability regarding both O and Pr is thus implied in a strong proxy signature. An earlier scheme in [21] based on the Schnorr signature was in fact a strong proxy signature, whereas the role asymmetry of O and Pr is not well reflected from a valid signature itself. The strong proxy scheme in [18] and its application variant adaptable to mobile agent environment [28] offer asymmetry in roles, but they are found subject to O's forgery attack [19]. Our proposed scheme is a modification of this scheme to thwart the forgery attack by O. Moreover, in our modification, Pr becomes designated instead of originally nondesignated for mobile agent environments.

In summary, a strong proxy signature scheme should satisfy the following security requirements.

> **Strong Unforgeability:** No one else (including the original signer) except the designated proxy signer can generate a valid proxy signature.
> **Verifiability:** Anyone can verify the signature based on the publicly available parameters.
> **Strong Identifiability:** A proxy signer's identity can be determined from the proxy signature it generates.
> **Strong Undeniability:** The proxy signer cannot repudiate his signatures.
> **Prevention of Misuse:** The proxy key pair should not be used for purposes other than the designated ones.

To better understand our scheme, we first review the scheme in [18] and the attack proposed in [19], respectively.

[1]There may be controversies to this point. We may alternatively employ, e.g., a trusted third party under supervision from government agencies, to manage the linkability part of doctors. However, this would complicate the system.

The Scheme:

— **Delegation:**
In the delegation phase, the original signer O chooses randomly $k_o \in_R Z_q^*$, computes $r_o = g^{k_o} \bmod p$ and $s_o = x_o h(w_d, r_o) + k_o \bmod q$. Then O sends secretly to Pr the triple (w_d, r_o, s_o), which is in fact O's signature on w_d under Schnorr's signature scheme. Pr accepts the triple as long as $g^{s_o} = y_o^{h(w_d, r_o)} r_o \bmod p$ holds. Note that (x_o, y_o) is O's key pair.

— **Signing and Verification:**
The proxy signer Pr computes his proxy key pair (x_s, y_s) as

$$x_s = s_o + x_{pr} \bmod q$$

and

$$y_s = g^{x_s} = y_o^{h(w_d, r_o)} r_o y_{pr} \bmod p$$

where (x_{pr}, y_{pr}) is Pr's key pair. Pr then signs a message m conforming to w_d as $\sigma(x_s, m)$ using a conventional DLP-like signature scheme. The tuple $(m, \sigma, w_d, r_o, y_o, y_{pr})$ is then a valid proxy signature. To verify the tuple, the verifier V computes

$$y_s = y_o^{h(w_d, r_o)} r_o y_{pr}$$

and then checks

$$\text{veri}(m, \sigma, y_s) \stackrel{?}{=} \text{true}.$$

The scheme is, however, found to suffer from the *original signer's forgery* attack, failing to satisfy the so-called "strong unforgeability" property. The attack works as follows.

The Attack:

In the strong proxy signature scheme, a dishonest original signer computes $r'_o = y_{pr}^{-1} \bmod p$, thus

$$x'_s = x_o h(w_d, r'_o) \bmod q$$

is a valid proxy signature signing key and $(m, \sigma, w_d, r'_o, y_o, y_{pr})$ is a valid proxy signature because

$$\begin{aligned} y_s &= y_o^{h(w_d, r'_o)} * r'_o * y_{pr} \bmod p \\ &= g^{x_o h(w_d, r'_o)} * y'_{pr} * y_{pr} \bmod p \\ &= g^{x_o h(w_d, r'_o)} \bmod p \\ &= g^{x'_s} \bmod p. \end{aligned}$$

We are now ready to present our strong proxy signature scheme, which works as shown in the diagram at the bottom of the page.

In our scheme, both consents from O and Pr are demonstrated explicitly in the scheme itself. To see this, r is actually the signature from Pr and s_o is O's signature. For this reason, there is no need to include in the delegation warrant w_d the identities of O and Pr, as well as certain policy stating the acceptance of the delegation by the two sides. Recall that r is a signature from Pr on $r_o || y_o$, this is more notably a countermeasure against the above attack than demonstrating Pr's acceptance of the delegation.

Theorem 1: The proposed strong proxy signature scheme is secure against the original signer's forgery attack.

Proof: Intuitively, the original signer's forgery attack to the original scheme takes advantage of the fact that O is allowed to change r_o by substituting it with $r'_o = y_{pr}^{-1} \bmod p$. In our scheme, however, r_o (together with y_o) is signed by Pr to produce r. Since O cannot forge Pr's signature, thus, it cannot forge r. This avoids the attack. □

Theorem 2: The proposed strong proxy signature scheme fullfills all the security requirements listed above.

Proof (sketch):

1) Strong Unforgeability: From Theorem 1, O cannot forge valid proxy signatures. For other people, the private proxy signing key contains Pr's private key, therefore, only Pr can generate valid proxy signatures.

Delegation :

$O \longrightarrow Pr$:	$r_o = g^{k_o} \bmod p$, where $k_o \in_R Z_q^*$
$Pr \longrightarrow O$:	$(r_{pr},\ r)$, where $r_{pr} = g^{k_{pr}} \bmod p$ with $k_{pr} \in_R Z_q^*$, $r = x_{pr} h(y_o \| r_o, r_{pr}) + k_{pr} \bmod q$; O checks $g^r = y_{pr}^{h(y_o \| r_o, r_{pr})} r_{pr}$
$O \longrightarrow Pr$:	$(w_d,\ s_o)$, where $s_o = x_o h(w_d,\ r) + k_o \bmod q$; Pr accepts as long as $g^{s_o} = y_o^{h(w_d,\ r)} r_o \bmod p$ holds; Pr computes the private proxy signing key as $x_s = s_o + x_{pr}$; the proxy signing key held by Pr is thus $(x_s,\ y_s = g^{x_s})$

Signing:

$Pr \longrightarrow V$:	$(m,\ \sigma,\ w_d,\ r_o,\ y_o,\ r,\ r_{pr},\ y_{pr})$

Verification:

V checks:	$g^r \stackrel{?}{=} y_{pr}^{h(y_o \| r_o,\ r_{pr})} r_{pr},\ \text{veri}(m,\ \sigma,\ y_s) \stackrel{?}{=} \text{true}$

2) Verifiability: (r_o, s_o) demonstrates the consent of O on the delegation; (r_{pr}, r) shows Pr's acceptance of the delegation; verifiability of the signed message is obviously based on the underlying DLP-like digital signature scheme.
3) Strong Identifiability: The inclusion of Pr's public key y_{pr} in the public proxy signing key y_s implies that Pr is identifiable.
4) Strong Undeniability: The proxy signer cannot repudiate his signatures because only he can compute the private proxy signing key x_s used in the signature.
5) Prevention of Misuse: Expiration date of the proxy signing key can be readily checked against the validity of the keys held by O and Pr, from which the proxy signing key is derived. w_d serves practically to prevent abuses of the proxy signing key. In the context of our e-prescription system, proxy signing keys are intended for the mere use of prescription signing. □

An alternative method for generating proxy signing key is simply that the proxy signer chooses a key pair as the proxy signing key and the original signer certifies it using his signing key by issuing a certificate, and the certificate states the delegation policy. There exists a controversy on the practical significance of proxy signing schemes since they do not demonstrate convincing efficiency advantages over this alternative method. With no exception, our proposed scheme faces the same problem. However, one thing is clear regarding our scheme that both the original signer and the proxy signer are explicit from a valid proxy signature itself. This as we will see, is quite critical to make prescription data linkable with respect to the patients.

IV. Method and System Implementation

In this section, we present a detailed implementation of the e-prescription system, wherein privacy of the patients and the doctors are appropriately protected. In addition, we also address the problem of how to protect data in smart cards.

A. Basic Idea

We make specific the process of a typical e-prescription service in real world. A patient visits his doctor and on the basis of the diagnosis, the doctor prepares a prescription pad. To this end, the doctor normally connects to the central medical record database to check for allergies and possible harmful drug interactions or medical history concerning the patient. At the same time, the doctor may query an information system maintained by the patient's insurer to determine whether certain intended drugs are covered by the patient's health plan. Upon completion of the drug selection, the doctor signs the pad electronically, which would serve as evidence that the doctor vouches for the safe use of the medicine. The prescription is then directed to the pharmacy and added to the patient's medical records. The patient later goes to the pharmacy where the prescription pad is retrieved. The pharmacy collects enough evidence in filling the prescription to meet the requirements of law regulations. Then the pharmacy charges the insurer (or the patient) for the medicine upon the patient's authorization (signed by the patient) and delivers the medicine to the patient. The prescription pad may then be forward to the PBMs for statistical research.

To simplify this process, we introduce the smart card into our system. The smart card serves dual roles: one as a portable data repository, storing personal medical records and insurance information; the other as a signature generating tool to sign electronically the prescription pad when the patient goes to the pharmacy to collect the medicine. Yet another major characteristic of our system lies in the introduction of delegated signing, which allows patients to delegate their signing rights to other people. As a result, a patient does not need to pass his smart card to another party to sign prescription pads on his behalf. We leverage on the proxy signature scheme proposed in Section III to achieve delegated signing. To delegate his prescription signing right, the patient (the original signer) negotiates a proxy signing key with the intended person (the proxy signer) who stores the key in his own smart card. Theoretically, a patient can delegate to multiple proxy signers. The accommodation of delegated signatures makes our system efficient and practical.

Recall that a central objective of our e-prescription system is to protect the privacy of patients and doctors in medicine prescriptions, and such a protection should still support useful research on the basis of data aggregation. To this end, we adopt the following techniques. i) The patient applies for a pseudonym from his insurer, which links the pseudonym with the patient's real identity. This is crucial as the insurer pays the prescription on the absolute discretion of the patient. The patient then engages in the prescription process in the name of the pseudonym, thereby gaining pseudonymity. Transactions under the same pseudonym apparently offers linkability. Revocation of the pseudonymity can be done by the insurer when necessary. ii) The doctor joins a group of affiliated health care organization. Whenever the doctor issues a prescription, the *Group Manager* signs a group signature in the name of the group, so the pseudonymity of the doctor is achieved. Given a signed pad, only the group manager is able to identify the doctor who issued it. We assume the group manager is independent of the health care organization in the sense that he would not do anything in favor of the latter, e.g., help the organization to link a specific doctor's prescription data. We point out that an off-the-shelf group signature scheme seems more convenient to doctor pseudonymity. However, virtually all existing group signature schemes are ineffective in revocation of group members, thereby insufficient for a dynamic group. Considering this, we let the Group Manager sign on behalf of the doctors. The Group Manager issues each doctor a pseudonym, which serves to hide the real identity of the doctor. We point out that a pseudonym system [29] does not seem quite relevant in our case, many of whose properties, e.g., unlinkability of the pseudonyms, are unnecessary for our use.

It may be argued that the Group Manager computing group signatures for every doctor would become a bottleneck, affecting overall performance of the system. Referring to Fig. 1, there are two methods for the Group Manager to calculate group signatures. In case of Fig. 1(a), a prescription m is first passed to the Group Manager for signing $\sigma(m)$ before reaching the pharmacy. In case of Fig. 1(b), the doctor first delivers m to

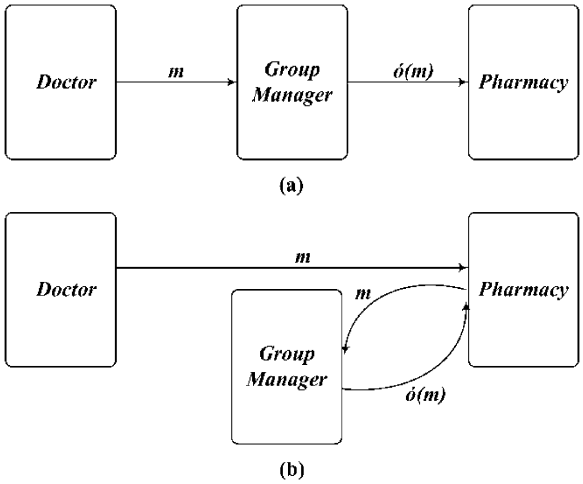


Fig. 1. Group signature modes.

the pharmacy which later relays m to the Group Manager for signing. This actually offers the flexibility that the prescription is signed at any point of time before the patient collects the medicine, alleviating to some extent the situation that the Group Manager becomes a bottleneck of our system.

We note that long-term linkable pseudonyms would risk the patients being identified. We, therefore, accommodate the flexibility to readily renew pseudonyms. In responding to this, the signing key of a patient is rendered short term. In other words, the signing key is certified to be valid within a short period of time, e.g., half a year; or once the patient senses his privacy is at risk, he is able to revoke his pseudonym and the associated signing key [in this case, the signing key is announced in a public certificate revocation list (CRL), and then applies for a new pseudonym and new a signing key]. The same applies to his proxy signing keys. In our system, a proxy signing key is derived from both sides' signing keys, governed by the strong proxy signature scheme in Section III. As a consequence, revoking either side's signing key results in the revocation of the proxy signing key. As a signing key is short termed and credited under the pseudonym, it is obviously insufficient to be used to identify the patient's real identity when needed. We then employ a long-term key, *master key*, to associate with the real identity of the patient. The master key is intended for authenticating real authority of the patient beyond the prescription context. As a result, there are three kinds of keys in a patient's smart card, namely, the master key (long term), the signing key (short term), and possibly proxy signing keys (short term).

Based on the above discussions, we now formally define the parties involved in our e-prescription system.

1) Definition of Entities:

- **Patient P**. The patient P is the entity to whom a prescription is issued. The patient needs to provide information pertaining to his health plan for drug prescription. To collect the prescribed medicine, the patient is required to sign the prescription pad to show his consent on the prescription. This authorization will be recognized by the insurer to pay the prescribed medicine.
- **Doctor DR**. The doctor DR is the entity that issues the prescription. The doctor signs the prescription pad to claim his assurance of the prescribed drugs benefiting the patient from medical perspective. The signature can as well be used as a nonrepudiatable evidence to assign liability if the prescribed medicine cause disputes.
- **Insurer I**. The insurer I is the entity to provide health benefits plan to the patient and pays for the prescription. The insurer may engage in certain statistical research. In our system, we designate I to be responsible for detection of fraud by the doctor. It issues pseudonyms to the patient, certifies public signing keys, and revokes pseudonymity of the patient when necessary.
- **Proxy Signer PxS**. The proxy signer PxS accepts delegated rights from the patient, signs the prescription, and collects the medicine on the patient's behalf.
- **Pharmacy PH**. The pharmacy PH is the entity to file the prescription. In filling a prescription, the pharmacy collects the payment from the insurer and delivers the medicine to the patient. The pharmacy must collect sufficient evidences on the sale of the medicine, including signatures from both the doctor and the patient. The pharmacy also engages in data aggregation for the purpose of statistical research to better manage medicine provision.
- **Group Manager GM**. The group manager GM manages privacy issues of the doctor. GM signs the prescription while keeps trail of the doctor who issued a particular prescription. GM is responsible for revoking pseudonymity of the doctor when required.
- **Certificate Authority CA**. The certificate authority CA issues public key certificates to related entities. A CA may be a medical board that qualifies and certifies the doctor's capability in issuing prescription.

There may be other entities involved in the process of prescription, such as law enforcement agencies overseeing medicine prescription. However, they are not directly related to our discussion.

Note that the introduction of group manager GM as a trusted party in our system is in fact under the jurisdiction of HIPAA, Section 164.512(f), where it is referred to as *privacy officer* GM, together with CA, constitutes the trusted infrastructure of our system.

A prescription system is said to be *privacy preserving* if it satisfies the following requirements.

2) Privacy Requirements:

1) **Pseudonymity.** Actual identities of the patient P and the doctor DR are hidden by means of pseudonyms; pseudonymity, however, can be revoked by designated trusted entities.
2) **Linkability of patients.** Under the pseudonymity provision, prescriptions to the same patient P are linkable to the pharmacy PH.
3) **Linkability of doctors.** Under the pseudonymity provision, prescriptions issued by the same doctor DR are linkable to the insure I.

TABLE I
NOTATIONS

L_P, L_{DR}	pseudonyms of P and DR, respectively
TH_i, i = 0,1,...	transaction header that minimally contains a transaction ID, inception & expiration date, insurance and health plan identifiers
k_i, i = 0,1,...	random session key
$E_U(m)$	encryption of m under entity U's public key by a semantically secure public key cryptosystem
$\{m\}_k$	symmetric encryption of m under CBC mode with key k
$EM_{k_1,k_2}(m)$	$\{m, MAC(k_2, m)\}_{k_1}$, where $MAC(k, m)$ is the cryptographic message digest of m with k
$S_U(m)$	digital signature on m under entity U's private key. We assume cleartext signatures, e.g., $S_U(m) = \sigma(m)\|\|m$, where $\sigma(m)$ is the exact signature of m
$GS(m)$	group signature on m produced by GM
GK	a secret key owned by GM for symmetric encryption
Rx	prescription pad
(mPR_U, mPU_U)	master key of entity U; mPR is private key and mPU is public key
(PR_U, PU_U)	signing key of entity U; PR is private key and PU is public key
$(pPR_{\succ U}, pPU_{\succ U})$	proxy signing key delegated to U from other people

4) **Unlinkability of doctors.** Prescriptions by the same doctor are pseudonymous and unlinkable by the pharmacy.
5) **Least data disclosure.** Unless absolutely necessary, prescription data is kept confidential.

B. Proposed Protocol

In this subsection, we present our protocols and methods to implement a smart card enabled e-prescription system. For the ease of references, we list the notations in Table I.

We then streamline the process of our e-prescription system with the following phases, and outline the interactions that are best relevant for electronic processing.

1) Initialization: At this stage, each involved entity gets itself prepared for the engagement into the prescription process, including establishing necessary keys and obtaining corresponding certificates.

P applies for a personal smart card from his primary health care organization storing initially the latest medical records, establishes his long-term master key (mPR_P, mPU_P), and gets the corresponding certificate under his real identity. P then enrolls in an insurer's health plan. To do this, he establishes his short-term signing key (PR_{L_P}, PU_{L_P}), contacts the insurer I, and directs to it the public part of the signing key PU_{L_P}. I generates a random pseudonym L_P for P,[2] issues a certificate for the signing key under the pseudonym, finalizes the health plan with P, and enters related information together with L_P into a private database for P. Relevant insurance information L_P and the certificate are delivered to P via a reliable channel, e.g., registered postal mail. P then negotiates with proxy signers PxS to delegate his prescription signing right to them and helps them generate proxy signing keys $(pPR_{\succ PxS}, pPU_{\succ PxS})$. P himself may be a proxy signer by accepting others' delegation and generates correspondingly proxy signing keys $(pPR_{\succ P}, pPU_{\succ P})$ that are delegated to him. Finally, public parts of the generated key materials, insurance information obtained from I are added to P's smart card. Note that secret parts of the keys are generated directly inside the smart card during their establishment. The above process is depicted as follows.

(M1) $P \rightarrow I$: $S_p = S_P(\text{Enroll\_Req}, PU_{L_P})$
(M2) $I \rightarrow P$: $Cert_{L_P} = S_I(PU_{L_P}, L_P, T)$, $E_P(k_1), \{S_I(\text{Insurance\_Info})\}_{k_1}$
(M3) $P \leftrightarrow PxS$: establish $(pPR_{\succ PxS}, pPU_{\succ PxS})$.

In M1, Enroll_Req is an enrollment request stating which plan to enrol and PU_{L_P} is the public part of the prescription signing key. Note that P computes S_p using his master key (mPR_P) to authenticate his real authority to I. In response, I returns to P the certificate $Cert_{L_P}$ under a pseudonym L_P for PU_{L_P} and the insurance information (Insurance_Info) under the enrolled health plan in M2. T, included in the certificate, is the expiration date of $Cert_{L_P}$. In order not to be leaked, the signed insurance information is encrypted by a random session key k_1. In M3, P exchanges information with a proxy signer PxS, establishing the proxy signing key $(pPR_{\succ PxS}, pPU_{\succ PxS})$ delegated to PxS. P may also set up for himself $(pPR_{\succ P}, pPU_{\succ P})$ by accepting delegations from other people. Recall that a proxy signing key is derived from both entities' short-term prescription signing keys under the strong proxy signature scheme introduced in Section III. P is the original signer O and PxS is the proxy signer Pr; (PR_{L_P}, PU_{L_P}) and (PR_{PxS}, PU_{PxS}) are key pairs (x_o, y_o) and (x_{pr}, y_{pr}), respectively. They collectively produce the proxy signing key $(pPR_{\succ PxS}, pPU_{\succ PxS})$. It is clear that $(pPR_{\succ PxS}, pPU_{\succ PxS})$ is valid only when both (PR_{L_P}, PU_{L_P}) and (PR_{PxS}, PU_{PxS}) are valid.

The doctor DR joins a group, such as his affiliated health care organization, where he is entailed and certified as to the capacity of issuing prescriptions. The group manager GM is the actual entity that computes digital group signatures on behalf of the group members. GM issues DR a random pseudonym L_{DR} and certifies DR's key material under his real identity.

GM chooses a group signing key and obtains the certificate, from related certificate authority CA, for committing group signatures to the prescription. GM chooses also a secret key GK known only to himself, for symmetric encryption and a key pair for asymmetric encryption.

2) Prescription Preparation: When the patient P visits the doctor DR, he presents his personal smart card and signs a random message on the fly to DR, proving his successful enrollment in a particular health plan. The process of diagnosis by DR may be complemented by the medical data stored in the smart card. Upon completion of the diagnosis, DR prepares the prescription. To do this, he makes references to the medical data in the smart card for checking drug allergies, drug interactions, and insurance information for determining whether certain intended drugs are indeed covered by P's health benefits plan and checking the account status under the plan.[3] DR then generates an electronic prescription pad including no identities of P and DR. Afterwards, DR concatenates the prescription pad with L_P and delivers the concatenation to the pharmacy

[2]Alternatively, P generates himself a random pseudonym and forwards it to I together with the signing key.

[3]To avoid leaking sensitive account information, the smart card tells only whether the balance in the account can cover the charges

PH. Note that DR is pseudonymous to PH. Finally, DR updates P's smart card by adding to it the particulars of current visit and prescription.

(M4) $P \rightarrow DR$: $S_{l_p} = S_{L_P}(Tstmp), Cert_{L_P}$
(M5) $DR \rightarrow PH$: $E_{PH}(k_2, k_3)$, $e = EM_{k_2,k_3}(TH_0, Rx, S_{l_p}), Cert_{L_P}$, $Pe = E_{GM}(L_{DR}, S = S_{DR}(TH_1, e))$.

In M4, P computes a signature S_{l_p} on $Tstmp$, the current time stamp, using his prescription signing key to show his successful enrolment in a health plan dictated by the insurer I. The prescription is forwarded by DR to PH in M5, where k_2 and k_3 are random session keys for PH to decrypt and check e, TH_0 and TH_1 are transaction headers as defined in Table I, Rx is the prescription pad including a serial number Prescription_Id, Pe is intended only for GM, S is a signature on e under the real identity of DR which serves to tell GM who issues the prescription. $Cert_{L_P}$ included in M4 and M5 is used to verify S_{l_p}.

3) Prescription Signing: The pharmacy PH transfers the prescription to the group manager GM for signing. To minimize the likelihood of leaking prescription information, it makes sense to hide the exact prescription content from GM. This, however, will not cause trouble because GM is in charge of pseudonymity revocation of doctors, so he is able to keep the scrambled message traceable; this would also prevent GM from otherwise substituting certain drugs for discriminative purposes against P. Therefore, in our system, GM issues a unlinkable group signature to the encrypted prescription. A cryptographic primitive, namely, blind digital signature [30], [31] does not meet our need here, simply because the entity (i.e., PH) requiring signing is not the actual originator of the message. GM includes in the group signature a linkable token in an attempt for the insurer I to link doctors' data. GM then returns the signed prescription to PH. The process is illustrated by the following interactions:

(M6) $PH \rightarrow GM$: $Pe, Cert_{L_P}$
(M7) $GM \rightarrow PH$: $Gs = GS(TH_2, e, \{DR, S\}_{k_4}$ $\{k_4\}_{GK}, \tilde{e} = E_I(L_{DR}))$.

In M6, PH relays Pe received in M5 to GM. GM then decrypts to get L_{DR} and S. Since S is a signature (under DR's actual identity) on e, GM verifies e. From L_{DR}, GM retrieves from his database the real identity corresponding to L_{DR}, and checks against the one indicated by S. In M7, GM returns to PH the group signature on e, where TH_2 is a transaction header, k_4 is a random session key, and GK is the symmetric key known only to GM so $\{DR, S\}_{k_4}$ can be opened only by GM, $\tilde{e}$ is the ciphertext by the insurer I's public key, thereby openable only to I, and $\tilde{e}$ is intended for I to link doctors' prescription data. Since PH keeps an original copy of e, he can detect GM's modification of e by comparing the returned signed e with the original copy. Apparently, PH has also no chance to substitute drugs in the prescription.

4) Prescription Filling: To collect the medicine, the patient P or a proxy signer PxS goes to the pharmacy PH, where he signs the prescription using his own smart card. Signatures of both P and DR are the evidences that must be collected by PH in compliance with law regulations for legal sale of medicine. PH gets the electronic payment from the insurer I by providing I the signed prescription information, and delivers the medicine to P or PxS. The prescription information is then passed to PBM for statistical research. The following interactions explain the process:

(M8) $PH \rightarrow P$: k_2, k_3, Gs
(M8′) $PH \rightarrow PxS$: k_2, k_3, Gs
(M9) $P \rightarrow PH$: $\tilde{S} = S_{L_P}(\text{Prescription\_Id}, S_{l_p})$
(M9′) $PxS \rightarrow PH$: $\tilde{S} = S_{PxS}(\text{Prescription\_Id}, S_{l_p})$
(M10) $ZPH \rightarrow I$: $E_I(k_2, k_3), Gs, \tilde{S}, Cert_{L_P}$
(M11) $I \rightarrow PH$: Electronic Payment, $S_i = S_I(\text{Prescription\_Id}, S_{l_p})$.

Before signing, P or PxS must verify the prescription. To this end, PH submits Gs to P's (PxS's) smart card in M8 (M8′), where k_2 and k_3 are the same session keys as in M5 for decrypting e included in Gs. Note that we assume the submission channel from PH's workstation to the smart card is secure, so k_2 and k_3 are in cleartext. Upon confirmation, P or PxS signs the prescription in M9 or M9′. The Prescription_Id, together with S_{l_p} obtained from e, uniquely identifies a prescription. To collect payment, PH forwards the signed prescription Gs, P's signature $\tilde{S}$, and the encrypted session keys k_2, k_3 to the insurer I. Upon validating the prescription, I pays the bill and returns a signature S_i to PH. At this point, a successful prescription session is completed. Gs, $\tilde{S}$, and S_i are a set of completed evidence of a prescription to be collected by PH. Note that we have avoided the prescription to be signed in a recursive fashion, i.e., one entity signs upon another entity's signature. Verifying such a recursively signed message must proceed in a sequential manner. Instead, Gs, $\tilde{S}$, and S_i can be verified independently and in parallel.

C. Analysis

In this subsection, we discuss how the above protocol meets the previously stated privacy requirements. Our proof is informal and intended only to offer an intuitive exposition. In fact, a formal proof would be quite involved, and would require more elaborated definitions of the privacy requirements as well as the cryptographic primitives relied on in the system.

Theorem 3: The proposed e-prescription system is privacy preserving, satisfying the privacy requirements.

Proof:

1) **Pseudonymity**. *Pseudonymity requires that actual identities of the patient P and the doctor DR are appropriately protected, but revocable to the designated entities*. In the system, P and DR engage in the process of prescription with respective pseudonyms, with the only exception in the *Initialization* phase. In particular, P interacts under his real name with the insurer I to apply for a pseudonym as well as the certificate for the prescription signing key, and to negotiate a health plan; DR communicates with the group manager GM to acquire his pseudonym and credentials for issuing prescriptions. Both cases, however, are deemed reasonable considering the fact that I and GM are designated entities taking the responsibility for pseudonymity revocation of I and DR, respectively. The real identity of DR is also included in messages exchanged in M5, M6, M7, M8 (M8′), and M10. But notice that in all cases, only GM can decrypt the corresponding ciphertexts to read the identity. In addition, no

identity information of P and DR is incorporated in the prescription pad Rx. With these, pseudonymity of both patients and doctors are achieved.

Pseudonymity revocation of P is clear in the sense that given any signed prescription data under the pseudonym L_P, only the insurer I can map L_P to the real identity of P. As to DR, in M7, GM includes in Gs $\{DR, S\}_{k_4}$ and $\{k_4\}_{GK}$, which are readable only to GM and thus pseudonymous to other entities. This means, given a valid prescription data Gs, only GM can tell who exactly issued the prescription.

2) **Linkability of patient**. *This property requires that under the pseudonymity provision, prescriptions to the same patient P are linkable to the pharmacy PH.* Linkability of patient to PH follows immediately if the prescriptions to P are signed by P himself in M9. If the prescriptions to P are signed by a proxy signer PxS in M9$'$, according to a property of our proposed strong proxy scheme, i.e., identities of both the original signer and the proxy signer are explicit in a valid proxy signature, linkability of the patient is also achieved.
3) **Linkability of doctor**. *This requires that under the pseudonymity provision, prescriptions issued by the same doctor DR are linkable to the insure I.* Prescriptions issued by the doctor are signed by the group manager GM in M7. GM includes $\tilde{e} = E_I(L_{DR})$ in the group signature Gs. Since the insurer I is able to decrypt $\tilde{e}$ using his private key, linkability of the doctor to I is thus achieved. $E(\,)$ is a semantically secure public key cryptosystem, by reading $\tilde{e}$ without decryption, no one can do the same linking.
4) **Unlinkability of doctor**. *This property requires that prescriptions by the same doctor are pseudonymous and unlinkable to the pharmacy PH.* Pseudonymity of the doctor to PH holds true as we already discussed in the first requirement. It then suffices for us to show that Gs is unlinkable to PH. Included in Gs are TH_2, e, $\{DR, S\}_{k_4}$, $\{k_4\}_{GK}$, and $\tilde{e}$: TH_2 is random; e and $\{DR, S\}_{k_4}$ are random dictated by random session keys; so is $\{k_4\}_{GK}$; and as we just discussed, from $\tilde{e}$ no one including PH can do the same linking as I does by decrypting $\tilde{e}$. Unlinkability of the doctor to PH is thus achieved. Interestingly, $\{DR, S\}_{k_4}$ and $\{k_4\}_{GK}$ cannot be simply replaced by $\{DR, S\}_{GK}$, as otherwise a portion of the ciphertext might be fixed, making the prescriptions by DR linkable to PH. To see this, consider the following scenario: suppose the symmetric cipher is the widely used DES (its block size is 64 bits) and the text length of DR exceeds 64 bits, then the first block of $\{DR, S\}_{GK}$ is always a fixed value.
5) **Least data disclosure**. *It requires that unless absolutely necessary, prescription data be kept confidential*. It would be quite hard to precisely define and then prove the implication of least data disclosure in the system. We, however, mention two outstanding facts of our system relating to this point. First, to protect the information including the prescription data stored in a patient's smart card, the patient delegates his signing right to other people to avoid the possibility of his card being carried by others. Second, to avoid unnecessarily disclosing information while without affecting its functionality, the group manager GM is designed to "blindly" sign prescriptions. □

D. Smart Card Aspects

Needless to say, security of the smart card is of paramount importance in our system. We consider the smart card as a tamper-resistant device that offers significant resistance to physical attacks. The smart card is equipped with a crypto-coprocessor for performing crypto-algorithms. The SLE66CX microcontroller family from Infineon Technologies [48] and the AT90SC microcontroller family [49] from Atmel seem to be sufficient for our use since they perform fast discrete logarithm computations by hardware. There are normally three types of memories constituting the storage system of a smart card, namely, working memory, program memory, and user memory. Working memory is made up of random access memory (RAM) chips, providing temporary storage for the data exchanged during program execution. Data in working memory will get lost when power is off. Program memory is a kind of nonerasible read only memory (ROM). The operating system and the security module that enforces security mechanisms resides in this area. The content of program memory is entered when the chip is manufactured, and any later attempt to modify it would ruin the card. User memory, taking advantage of EEPROM technology, is programmable in the sense that it can be erased and rewritten by electronic means. All personal data used in our system including medical records, insurance information, key materials (master key, signing key, and proxy signing keys from other people if any) are stored in this area.

We further organize the user memory into different sections to accommodate data requiring different maintenance and access control. Note that the allocation of space is theoretical, and the precise structure and the data access control will be implemented in accordance with existing standards [45]–[47]

- Secret Section
  This section is designed to be written only once and cannot be read from the outside by either physical or logical means [17]. The data in this area are retained throughout the life cycle of a smart card, and can only be read by its own microprocessor. The following data are archived in this section:
  — the card manufacture's PIN;
  — the card holder's long-term master key: The master key serves to authenticate the patient's actual identity, e.g., when the patient enrols in a health plan by interacting with the insurer.
- Sensitive Section
  This section is similar to the secret section, but allows for occasional updates. The following information is stored here:
  — the card issuer's PIN (CIN): The card issuer in our system is the patient's primary health care providing organization. CIN serves to protect the application data against unauthorized operations such as erase and write;
  — the card holder's PIN (CHN): The card holder is obviously the patient himself in our system. CHN is used to

activate certain functionalities of the smart card, e.g., to review the protected information.

- Working Section
  This section can be erased and rewritten, whereas such updates can be accomplished only by designated entities, the card issuer or holder in our case. The information in working section is read protected, write protected, or erase protected through appropriate access control codes (CIN or CHN), depending on the nature of the data. The following data are managed in this section:
  - private part of the card holder's short-term signing key: The signing key serves to sign electronically the prescription when the patient collects the medicine in the pharmacy;
  - private part of the short term proxy signing keys delegated to the card holder: The card holder may agree to be the proxy signer of other people in terms of prescription signing. If this is the case, the proxy signing keys are stored in this area;
  - medical information: The medical information set includes coded personal medical records, consultation details, and prescription information;
  - insurance information.
- Public Section
  Data in public section can be read free, requiring no protection. The following data are stored in this area:
  - serial number of the card;
  - pseudonym and related personal pseudonymous information;
  - emergency medical information: such information includes blood type, drug allergies, etc.;
  - public keys and their corresponding certificates: These include the delegation warrants stating delegation policy for the use of the proxy signing keys.

We summarize the data managed in the user memory in Table II.

TABLE II
DATA MANAGEMENT

Data (Section)	Size (bytes)	Reading	Erasing	Writing
Secret Sec.	40	Forbidden	Forbidden	Forbidden
Sensitive Sec.				
CHN	10	Forbidden	CHN	CHN
CIN	10	Forbidden	CIN	CIN
Working Sec.				
signing key	30	Forbidden	CIN	CIN
delegated keys	90 (30×3)	Forbidden	CIN	CIN
med. records	40	CHN	CIN	CIN
consul. info.	1,500 (50×30)	CHN	CIN	CHN
prescr. info.	1,200 (120×10)	CHN	CIN	CHN
insur. info.	250	CHN	CIN	CIN
Public Sec.				
pseud. info.	10	Free	CIN	CIN
emer. med. info.	20	Free	CIN	CIN
pub. sig. key	350	Free	CIN	CIN
pub. prox. keys	1,050 (350×3)	Free	CIN	CIN

In the following, we clarify some particulars presented in the table.

- By *Reading Forbidden*, the data can only be read through the microprocessor of the smart card.
- The design of the data structure for medical record is merely indicative instead of descriptive. In other words, we *code* the medical record using a well-structured template. As a result, most of the fields accept binary values "YES" or "NO." Reference [1] provides an example of such a structured template. For example, if a patient has "*Obsessive–compulsive disorder*," the corresponding field will be "1." Similarly, all fields are filled with either "1" or "0." In this way, the 40-B space allocated for the patient's medical records can accommodate 320 fields.
- We assume that discrete logarithm based public key cryptosystems are used to compute digital signatures and issue key certificates. This makes typically 160-b private keys, 212-B public keys, and 84-B digital signatures. A public key (short-term) certificate is simplified to contain minimally the user's name, CA's name, expiration date, and a digital signature on them. Other certificates, such as those for proxy signing keys, may contain a simplified version of policy. With these, the length of a public key together with its certificate is expected not to exceed 350 B.
- For the master key, as it is for long-term use, the public key certificate should be produced in a standard format. Because of space limitation, we do not include this certificate in the smart card, thereby not providing a verifier for the convenience to verify a signature off-line. This, however, does not degrade the efficiency of our e-prescription system, for the master key is used only once in the initialization phase.
- The area for consultation details and prescription information is writable under the card holder's PIN (CHN). With this, our system offers the flexibility that such information can be added to the smart card under the authorization of the patient. This is significant when the patient visits a doctor in other place than his primary health care organization.
- We allow information regarding the latest 30 consultations and 10 prescriptions being stored in the smart card. Removal of this kind of information is on a "first in, first out" basis. Because of space limitation, a card holder is permitted to be the proxy signer of at most three people. Therefore, maximally 1,050 (350×3) B of space is allocated for proxy signing keys and their certificates.
- The total space to accommodate all the data is estimated to be 5 kB. Therefore, a smart card with 8-kB memory suffices for our system.

As a final note, we point out some existing health card systems for comparison with ours. The Health Smart Card in Texas [33] serves mainly as a medical data container, and the Health Card in France [34], besides containing health care information, is intended more as a paying means for health services. The Health Professional Card (HPC) [36] has been standardized on European level as CEN prEVN 13 729 "Health Informatics—Secure User Identification—Strong Authentication using Microprocessor Cards" [37] as well as consistently on the German national level as the HPC Protocol [38]. HPC tends to provide identification services with security functionalities such as digital signature and encryption.

E. Related Work

The anonymous e-prescription system in [14] solves privacy protection problems in the following way. The privacy of a patient is reserved by applying for a pseudonym from his insurer and signing the prescription under the pseudonym. Linkability is achieved also with respect to the pseudonym. Apparently, revocation can be accomplished by the insurer. Anonymity of the doctor is achieved by the doctor joining a group and then issuing group signatures on the prescription pads (a group signature scheme [15] is employed for static groups and an online group signature scheme is designed for highly dynamic groups). Special care is given to make the group signatures linkable. The work in [16] is intended to protect doctors' identities in the prescription pads while at the same time allow data to be aggregated for the purposes of research and statistical analysis. The method utilized is to present prescription data in two distinct batches: one batch includes prescription information with scrambled doctor references and the other batch contains the scrambled doctor reference and the exact doctor information. The identity of the doctor could then be released or kept hidden, according to the doctor's preference. Another work related to ours is in [50]; it presents a clearing scheme for the Germany health care system, addressing the privacy issues among various parties such as physician, insurers, pharmacies, etc., in the overall context of medical processes.

V. Conclusion and Future Work

In this paper, we have introduced a smart card enabled e-prescription system with the following features distinguishing it from the system in [14]. First, the introduction of a smart card carrying personal health and insurance information greatly simplifies the process of diagnosis and medicine prescription, while smart card in [14] is intended only for signing purposes. Second, pre-approval for a prescription from the insurer in [14] is no longer deemed necessary in our case, because the doctor has enough information in the smart card to support his prescription, for which the patient can later get reimbursement from the insurer. Third, we identified and accommodated the need for the patients to delegate their prescription rights to other people, e.g., the custodians. This would protect the privacy of information stored in the smart cards, making our system more acceptable in practice. The work in [14] did not consider delegated signing. In addition, we explicitly pointed out that the prescription signing key of a patient to be short term, so the renewal of the patient's pseudonym, prescription signing key, and proxy signing keys can be facilitated easily.

We believe that our proposed system is quite practical considering smart cards have already been deployed in some health care systems [33], [34], [36]. Implementation of each step of our protocol at the smart card level within a real word e-prescription environment is our future work.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable suggestion, to improve the quality of this paper.

References

[1] C. Lambrinoudakis and S. Gritzalis, "Managing medical and insurance information through a smart-card-based information system," *J. Med. Syst.*, vol. 24, no. 4, pp. 213–234, 2000.

[2] J. L. Zoreda and J. M. Oton, *Smart Cards*. Norwood, MA: Artech House, 1994.

[3] T. S. Chan, "Integrating smart card access to web-based medical information system," in *Proc. ACM Symp. Applied Computing*, 2003, pp. 246–250.

[4] D. F. Linowes and R. C. Spencer. (1997) How empolyers handle employees' personal information. [Online]. Available: http://www.kentlaw.edu/ilw/erepj/v1n1/lino-main.htm

[5] N. Keene, W. Hobbie, and K. Ruccione, *Childhood Cancer Survivors: A Practical Guide to Your Future*: O'Reilly & Associates Inc., 2000.

[6] R. Weiss, "Ignorance undercuts gene tests' potential," *The Washington Post*, p. A1, 2000.

[7] National Standards to Protect the Privacy of Personal Health Information, Office for Civil Rights. (2001). [Online]. Available: http://www.hhs.gov/ocr/hipaa/

[8] T. Albert. (2000) Doctors ask AMA to assure some privacy for their prescription pads. [Online]. Available: http://www.ama-assn.org/sci-pubs/amnews/pick_00/prl11225.htm,

[9] Food and Drugs Administration. Medwatch: The FDA Safety Information and Adverse Event Reporting Program. [Online]. Available: http://www.fda.gov/medwatch/

[10] Standards for Privacy of Individually Identifiable Health Information, Office for Civil Rights. (2001). [Online]. Available: http://www.hhs.gov/ocr/hipaa/finalmaster.html

[11] Health Care Financing Administration. (2001) Study of Pharmaceutical Benefit Management. [Online]. Available: http://www.hcfa.gov/research/pharmbm.pdf

[12] J. Ledbetter. (1999) Is Buying Drugs on the Web too Easy?. [Online]. Available: http://www.cnn.com/TECH/computing/9906/29/drugs.idg/index.html

[13] California Board of Pharmacy, *California Pharmacy Laws* Sacramento, CA.

[14] G. Ateniese and B. Medeiros, "Anonymous e-prescriptions," in *Proc. ACM Workshop Privacy in the Electronic Society (WPES02)*, 2002.

[15] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure colalition-resistant group signature scheme, advances in cryptology," in *Proc. CRYPTO'00 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1880, pp. 255–270.

[16] V. Matuáš Jr, "Protecting doctor's identity in drug prescription analysis," *Health Informatics J.*, vol. 4, p. 4, 1998.

[17] B. Schneier and A. Shostack, "Breaking up is hard to do: Modeling security threats for smart cards," in *Proc. USENIX Workshop on Smart Card Technology*, 1999, pp. 175–185.

[18] B. Lee, H. Kim, and K. Kim, "Strong proxy signature and its applications," in *Proc. SCIS*, 2001, pp. 603–608.

[19] H. M. Sun and B. T. Hsieh, "On the security of some proxy signature schemes," Cryptology ePrint Archive no. 068, 2003.

[20] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature for delegating signing operation," in *Proc. 3rd ACM Conf. Computer and Comminications Security*, 1996.

[21] S. Kim, S. Park, and D. Won, "Proxy signatures, revisited," in *Proc. Int. Conf. Information and Communication Security (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1997, vol. 1334, pp. 223–232.

[22] H. Pertersen and P. Horster, "Sefl-certified keys-concepts and applications," in *Proc. Communications and Multimedia Security*, IFIP, 1997, pp. 102–116.

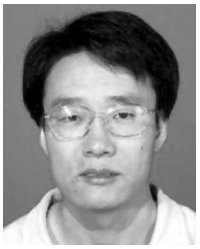
[23] K. Zhang, "Threshold proxy signature schemes," in *Proc. Information Security Workshop*, Japan, 1997, pp. 191–197.

[24] N. Y. Lee, T. Hwang, and C. H. Wang, "On Zhang's nonrepudiable proxy signature schemes," in *Proc. 3rd Australasian Conf. Information Security and Privacy*, 1998, pp. 415–422.

[25] C. Schnorr, "Efficient identification and signature for smart cards," in *Advances in Cryptology, CRYPTO'89 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1989, vol. 435, pp. 235–251.

[26] V. Varadharajan, P. Allen, and S. Black, "An analysis of the proxy problem in distributed systems," in *Proc. IEEE Symp. Research in Security and Privacy*, 1991, pp. 255–275.

[27] B. C. Neuman, "Proxy-based authorization and accounting for distributed systems," in *Proc. 13th Int. Conf. Distributed Computing Systems*, 1993, pp. 283–291.
[28] B. Lee, H. Kim, and K. Kim, "Secure mobile agent using strong non-designated proxy signature," in *Proc. ACISP (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2001, vol. 2119, pp. 474–486.
[29] A. Lysyanskaya, R. Rivest, A. Sahai, and S. Wolf, "Pseudonym systems," in *Selected Areas in Cryptography (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, vol. 1758.
[30] J. Camenisch, J. M. Piveteau, and M. Stadler, "Blind signatures based on the discrete logarithm problem," in *Advances in Cryptology, EUROCRYPT '94*, vol. 950, LNCS, 1994, pp. 428–432.
[31] D. Pointcheval and J. Stern, "Provably secure blind signature schemes," in *Advances in Cryptology, ASIACRYPT'96 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1996, vol. 1163, pp. 252–265.
[32] Council of Europe, "On the Protection of Medical Data," Recommendation R(75), 1997.
[33] Council of Europe. [Online]. Available: http://www.healthsmartcard.net/
[34] R. Neame, "Smart cardsCthe key to trustworthy health information systems," *BMJ*, vol. 314, pp. 573–577, 1997.
[35] Council of Europe. [Online]. Available: http://www.gprd.com
[36] B. Blobel and P. Pharow, "Security infrastructure of an oncological network using health professional cards," in *Health Cards '97 (Series in Health Technology and Informatics)*. Amsterdam, The Netherlands: IOS Press, 1997, vol. 49, pp. 323–334.
[37] "Health Informatics-Secure User Identification-Strong Authentication Using Microprocessor Cards (SEC-ID/CARDS)," report, CEN TC 251 prENV 13 729, 1999.
[38] (1999) The German HPC Specification for An Electronic Doctor's Licence, Version 0.81. HPC. [Online]. Available: http://www.hpc-protocol.de
[39] New Zealand Privacy Commissioner, "Health Information Privacy Code,", 1994.
[40] European Committee for Standardization. Technical Committee for Health Informatics. Rep. CEN/TC251. [Online]. Available: www.centc251.org
[41] Y. J. Yang, "Security Issues in Health Care,", Term Rep., 2003.
[42] "The European Union Privacy Directive," report, 95/46/EC.
[43] "Bill to Protect Personal Data,", Japan, 1999.
[44] "Act for the Protection of Personal Information Maintained by Public Agencies,", South Korea, 1994.
[45] ISO/IEC, "Information Technology-Identification Cards-Integrated Circuit(s) Cards With Contacts-Part 4:Interindustry Commands for Interchange," standard, Std. ISO/IEC 7816-4, 1995.
[46] ——, "Information Technology-Identification Cards-Integrated Circuit(s) Cards With Contacts-Part 8 Security Related Interindustry Commands," standard, Std. ISO/IEC 7816-8, 1999.
[47] ——, "Information Technology-Identification Cards-Integrated Circuit(s) Cards With Contacts-Part 9 Additional Interindustry Commands and Security Attributes," standard, Std. ISO/IEC 7816-9, 2000.
[48] [Online]. Available: http://www.infineon.com/
[49] [Online]. Available: http://www.atmel.com/
[50] G. Bleumer and M. Schunter, "Privacy oriented clearing for the german health care system," in *Personal Information Security, Engineering and Ethics*, I. R. Anderson, Ed. New York: Springer-Verlag, 1997, pp. 175–194.



Yanjiang Yang received the B.S. degree in computer science from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 1995 and the M.S. degree in biomedical imaging from National University of Singapore, Singapore, in 2001.

He is now working towards the Ph.D. degree at the School of Computing, National University of Singapore, attached to the Institute for Infocomm Research, A*STAR, Singapore. His research areas include information security, biomedical imaging.

Xiaoxi Han received the B.S. degree in mathematics and the M.S. degree in electronic engineering in 1992 and 1997, respectively. He is now working towards the Ph.D. degree at the Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, China.

His research areas include information security and smart card applications.

Feng Bao received the B.S. and M.S. degrees from Peking University, Beijing, China, and the Ph.D. degree from Gunma University, Gunma, Japan, in 1984, 1986, and 1996, respectively.

From 1990 to 1991, he was a Visiting Scholar at the Hamburg University, Hamburg, Germany, and from 1987 to 1993, an Assitant/Associate Professor at the Institute of Software, Chinese Academy of Sciences, Beijing. Currently he is a Lead Scientist and the Head of the Cryptography Lab of the Institute for Infocomm Research, Singapore. His research areas include algorithm, automata theory, complexity, cryptography, distributed computing, fault tolerance, and information security. He has published more than 80 international journal/conference papers and filed 16 patents.

Robert H. Deng received the B.Eng. degree from the National University of Defense Technology, Changsha, China, in 1981 and the M.Sc. and Ph.D. degrees from the Illinois Institute of Technology, Chicago, in 1983 and 1985, respectively.

He is currently the Principal Scientist and Manager of Infocomm Security Department, Institute for Infocomm Research, Singapore. He has 10 patents and more than 130 technical publications in refereed journals and conferences in the areas of error control coding, digital communications, computer networking, cryptographic techniques, and information security. He has served on the advisory, technical and program committees of numerous international conferences.

Dr. Deng received the Outstanding University Researcher Award from the National University of Singapore in 1999.