SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth Systems

Xiaodong Lin, *Member, IEEE,* Rongxing Lu, Xuemin (Sherman) Shen, *Fellow, IEEE,* Yoshiaki Nemoto, *Senior Member, IEEE,* and Nei Kato, *Senior Member, IEEE*

***Abstract*—The eHealth system is envisioned as a promising approach to improving health care through information technology, where security and privacy are crucial for its success and large-scale deployment. In this paper, we propose a strong privacy-preserving Scheme Against Global Eavesdropping, named SAGE, for eHealth systems. The proposed SAGE can achieve not only the content oriented privacy but also the contextual privacy against a strong global adversary. Extensive analysis demonstrates the effectiveness and practicability of the proposed scheme.**

***Index Terms*—eHealth system, security and privacy, content oriented privacy, contextual privacy, strong global eavesdropping**

I. Introduction

TIME is crucial when dealing with acute diseases, such as heart disease and stroke. By statistics, in the United States alone stroke kills 150,000 people each year. The patients' lives could be saved if they are transported quickly to a hospital and receive immediate treatment and expeditious care. However, before a patient can receive crucial medical treatment on time, he or she needs to get early and rapid diagnosis. Many approaches have been developed to reduce the fatalities due to acute diseases, such as angioplasty, life-saving defibrillators installed in popular areas, but there are still tremendous losses. Over the last twenty years, the miraculous evolution of wireless technology has imposed a major impact on the revolution of human's lifestyle by providing the best ever convenience and flexibility in accessing the Internet services and various types of personal communication applications. Recently, Body Area Networks (BANs) (or Body Sensor Networks (BSNs)) are emerging and envisioned to be a promising approach for helping improve health care by effectively monitoring patient health and disease progression [1].

In BANs, wearable, implantable, or portable medical wireless sensors are deployed in patients to monitor the physiological conditions within the body and then send these patient information to a remote healthcare provider over the Internet for receiving high quality healthcare from their physicians on time but without seeing their physicians in person [1], [2]. It could avoid patients' lengthy waiting times and hospital stay. The patient information may include blood pressure (BP), heart failure status, heart rhythms, and blood oxygen level etc. This leads to an eHealth system shown in Fig. 1, which consists of three components: BSNs at home, wireless transmission network and eHealth center. With the rapid increase of elderly people in our societies, the eHealth system has been widely accepted by the healthcare communities. For example, over the last decade, European Commission activities in eHealth have devoted to a series of patient-centered health delivery systems across all stages of care including prevention, diagnosis, treatment and followup [2], [3].

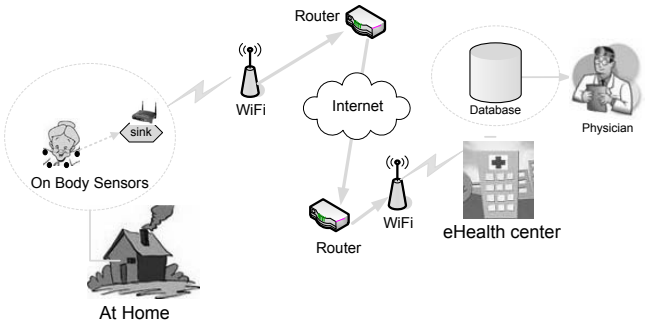


Fig. 1. Typical scenario of an eHealth system

The new wireless technology has offered many advantages over the conventional healthcare system from efficiencies in the hospital clinic to new ways monitoring patient health and disease progression. However, the design of eHealth system comes with a set of newly emerged challenges. One of the main challenges is on how to ensure the security and privacy of the patients' Personal Health Information (PHI) from various threats [4]–[10]. Most of the patients are concerned about the privacy of their PHI, such as unauthorized collection, disclosure or other uses of PHI. Without the proper protection of patients' PHI, they may refuse for any treatment since they are afraid of the loss of their PHI including information about their illness or disability. The government has also established stringent regulations to ensure that the security and privacy of patients' PHI are properly protected, for example HIPAA [11]. A healthcare provider is subject to severe civil and criminal penalties if regulations are not followed exactly, for example, fines up to $250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information. Therefore, it is crucial to protect the security and privacy of patients' PHI before eHealth system reaches its full flourish and puts into practice. However, just keeping the

Manuscript received 27 July 2008; revised 5 December 2008.

X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, 2000 Simcoe Street North, Oshawa, Ontario, Canada L1H 7K4 (e-mail: Xiaodong.Lin@uoit.ca).

R. Lu and X. Shen are with the Centre for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1 (e-mail: {rxlu,xshen}@bbcr.uwaterloo.ca).

Y. Nemoto and N. Kato are with the Graduate School of Information Sciences, Tohoku University, Sendai, 980-8579, Japan (e-mail: nemoto @nemoto.ecei.tohoku.ac.jp; kato@it.ecei.tohoku.ac.jp).

Digital Object Identifier 10.1109/JSAC.2009.090502.

patients' PHI secret is not enough for patient privacy since it could be disclosed by other means. For example, if an observer knows that a patient often sends his/her PHI to a specific physician, then based on the medical treatment domain of the physician, the observer can correctly guess the patient's disease with a high probability. Therefore, besides preventing the PHI from eavesdropping, how to cut off the relation between the patient and his/her physician is also crucial to patient privacy.

To address the patient privacy issues lying in eHealth systems, in this paper, we propose a strong privacy-preserving **S**cheme **A**gainst **G**lobal **E**avesdropping for eHealth systems, called SAGE. Firstly, we formally define the patient privacy issues in eHealth systems. Specifically, we divide patient privacy into content oriented privacy and contextual privacy. For the contextual privacy threats in eHealth systems, we further categorize the eavesdroppers into three classes: non global adversary, weak global adversary and strong global adversary. Secondly, the proposed SAGE can achieve not only the content oriented privacy but also the contextual privacy against the strong global adversary, which is the most powerful attack model against patient privacy. Furthermore, both of these two privacies are formally proved with provable security technique. Thirdly, since the time is crucial when dealing with some acute diseases in eHealth systems, we discuss the SAGE's transmission delay with extensive performance evaluation, which further convinces its practicality.

The remainder of this paper is organized as follows. We first formalize the problem in Section II, and then describe the related work in Section III. The proposed SAGE is presented in Section IV. Section V presents the security analysis, followed by the performance evaluation in Section VI. Finally, conclusions remarks are given in Section VII.

II. Problem Formalization

In this section, we provide a concise problem formalization, including system model, adversary model and privacy problem statement.

A. System Model

The emergence of eHealth system can be accredited to the development of two promising techniques: body sensor devices and wireless communications networks. Body sensor devices can collect patient's health information, while the wireless communication networks can deliver the information to a physician, so that the patient could get quick and accurate healthcare from the physician. Here, we define the system model by dividing the eHealth system into three parts: body sensor network at home, wireless transmission network and eHealth center, as shown in Fig. 1.

1) Body sensor network at home: As in other BSNs [12]–[17], a body sensor network at home consists of many body sensor devices as well as a powerful data sink device. These sensor devices could be accelerometer, blood pressure and oxygen saturation (SpO2) and temperature sensors, and continuously report the patient health information to the data sink. Then, the data sink transmits these information to the physician at eHealth center via wireless communication networks. Since the body sensor network is deployed at home, its security should be guaranteed.

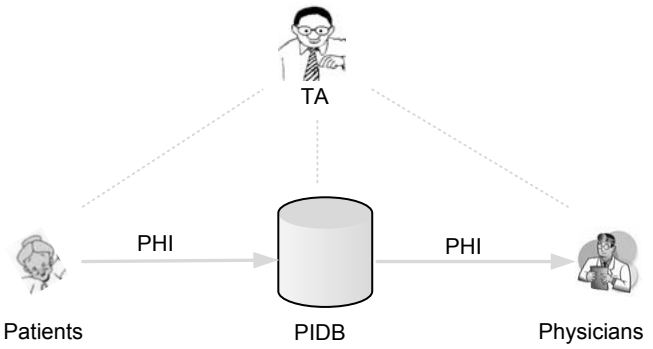


Fig. 2. eHealth center in a typical eHealth system

2) Wireless transmission network: WiFi is a globally used wireless networking technology that uses the 802.11 standard [18]. In our eHealth system, we adopt WiFi technology. Then, the data sink with a WiFi card can transmit patient health information over Internet to the physician via accessing the access point within a radius of 200 feet. However in a WiFi enabled work environment, anyone, within an accessible distance, can access the information. Therefore, the security of transmitted data can't be guaranteed if they are lack of necessary precautious measures.

3) eHealth center: eHealth center is organized by a trusted authority (TA), and includes registered patients (PAs), physicians (PHs) and patient information database (PIDB), as shown in Fig. 2. A patient, after registering himself/herself to TA, can get some body sensor devices suitable to him/her, and then deploy a body sensor network at home so that PHI can be collected and sent to the PIDB and physicians at eHealth center. We assume both patients and physicians are secure, while the PIDB may be compromised by a strong adversary due to some sophisticated attacks. However, the secret keys in PIDB are still secure due to some tamper proof devices being employed [19], [20]. For example, those secret keys and key-related operations are executed in the tamper proof devices, and an adversary can't access these keys.

B. Adversary Model

We divide the adversaries based on their capacities into three types: *non global adversary*, *weak global adversary* and *strong global adversary*.

1) Non global adversary: A non global adversary doesn't compromise the patients or the physicians but trying to eavesdrop the messages transmitting from the patients to the physicians. However, the capability of the non global adversary is limited, and he cannot gain the whole transmission path information from the patient to the physician.

2) Weak global adversary: The capability of an adversary highly depends on what skills it has. Compared with the non global adversary, the weak global adversary has the ability to monitor all traffic. Therefore, when a message transmits from a patient to a physician, the adversary can log the whole path information that the message passed by. Fig. 3 shows such a weak global adversary. Here "weak" means the adversary only passively eavesdrops all the communications in the network.

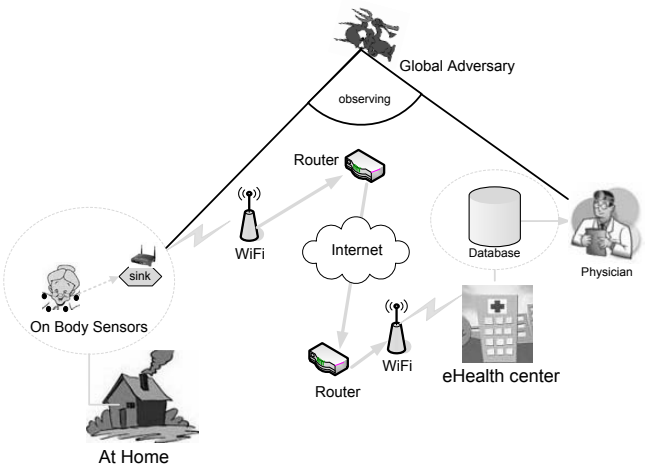


Fig. 3. An eHealth system with a global adversary

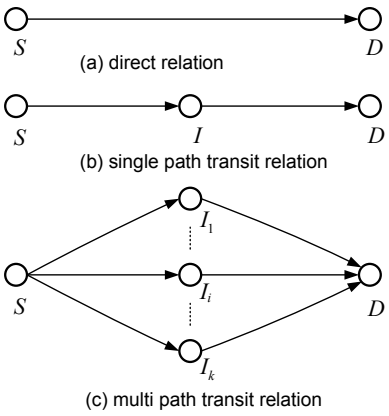


Fig. 4. Observed relations

As noted in [21], the global passive adversary is perhaps the most popular threat model for evaluating the anonymity.

3) Strong global adversary: In Fig. 3, if the global adversary can also compromise the intermediate nodes along with the path, then such a global adversary is called a strong global adversary. For example, the strong global adversary may implant some malicious Trojan horse programs in PIDB, so that he can monitor the inside data flows in PIDB while without being detected. (Note that the strong global adversary still can't access the secret keys due to the secret keys being protected by tamper proof devices.) Obviously, the strong global adversary is a stronger threat model than what needed in most realistic scenarios. However, if the eHealth system can withstand this type of adversary, then it is necessarily secure against the non global adversary and weak global adversary.

Note that, since the goal of the strong global adversary is to disclose the patient privacy, other active attacks that are irrelative to the patient privacy, such as some denial-of-service (DoS) attacks are outside the scope of this paper.

C. Privacy Problem Statement

eHealth systems have many characteristics that make them more vulnerable to the privacy attack than other scenarios. For example, communication between a patient and a physician could indicate the patient's disease and sickness to health. Simply providing the content oriented privacy is insufficient. Therefore, we divide the privacy issues in eHealth systems into two categories: *content oriented privacy* and *contextual privacy* [22], [23]. If an eHealth system can withstand not only the content oriented privacy attacks but also the contextual privacy attacks, then it is said to be a secure eHealth system.

1) Content oriented privacy: Content oriented privacy concerns whether an adversary has the capability in disclosing the patients' PHI that he cares about by observing and manipulating the data transmitted over the communication networks. In an eHealth system, if any adversary has no ability to reveal the patient PHI, then the content oriented privacy is achieved. Although the content oriented privacy is pivotal for eHealth systems, it is not difficult to address due to many cryptographic techniques such as available authentication and encryption algorithms [24].

2) Contextual privacy: Contextual privacy means an adversary has the ability to link the source and the destination of a message. In eHealth systems, if an adversary can link the patient with a specific physician, then the patient privacy will be disclosed. (See the example below).

EXAMPLE: Let E_1 be the event that a patient PA has some kind of disease and E_2 be the event that PA sees a specific physician PH. By statistics, the following conditions are available.

1) If PA has the disease, then the probability that he will see the specific PH is ρ_1, i.e., $\Pr[\mathrm{E}_2|\mathrm{E}_1] = \rho_1 = 98\%$
2) If PA does not have the disease, then the probability that he will see the specific PH is ρ_2, i.e., $\Pr[\mathrm{E}_2|\neg\mathrm{E}_1] = \rho_2 = 1\%$
3) Suppose that only 5% of the population in a region has the disease, i.e., $\Pr[\mathrm{E}_1] = 5\%$

INFERENCE: When the PHI of the patient PA reaches the specific physician, based on the Bayesian inference, we have

$$\Pr[\mathrm{E}_1|\mathrm{E}_2] = \frac{\Pr[\mathrm{E}_2|\mathrm{E}_1]\cdot\Pr[\mathrm{E}_1]}{\Pr[\mathrm{E}_2|\mathrm{E}_1]\cdot\Pr[\mathrm{E}_1] + \Pr[\mathrm{E}_2|\neg\mathrm{E}_1]\cdot\Pr[\neg\mathrm{E}_1]} = \frac{\rho_1\cdot 5\%}{\rho_1\cdot 5\% + \rho_2\cdot 95\%} = 83.76\%$$

From the above example, we can see, even though the content oriented privacy is well protected, the contextual privacy still largely affects patient privacy. To subtly consider the contextual privacy, we define *relations* and *observed relation depths* as follows.

Relations & observed relation depths. We consider the relation between the source S and the destination D by two ways: 1) if S can directly send a message m to D by one hop, the direct relation can be established; 2) if the message m sent by S requires more than one hops to reach D, the transit relation between S and D will also be established. (See Fig. 4 for these relations).

- *Direct relation:* As shown in Fig. 4 (a), if a message m transmitting from the sender S to receiver D only requires one hop, the relation $\mathcal{R}(S, D)$ is called *direct relation*. In the direct relation $\mathcal{R}(S, D)$, we determine the observed relation depth, denoted as $\mathcal{RD}(S, D) =$

$\Pr[\mathcal{R}(S,D)]$, by three factors: {*observed transmission*, *inside data flow*, *outside data flow*}. In general,

- *Observed transmission* refers to that S transmiting a message to D is observed by an observer with a probability ϑ. We denotes this event as F1. If F1 occurs, then $\Pr[\mathrm{F1}] = \vartheta$.
- *Inside data flow* refers to that receiver D executes some inside operations on the received message or drops it. We define F2 the event that D's inside data flow is observed.
- *Outside data flow* refers to that receiver D runs some outside operations on the received message such as responding or forwarding. We define F3 the event that D's outside data flow is observed.

Then, we define the value of $\mathcal{RD}(S,D)$ as

$$\mathcal{RD}(S,D) = \begin{cases} 0, & \textbf{case 1} \quad \text{if } \neg\mathrm{F1}; \\ \vartheta \cdot \varepsilon, & \textbf{case 2} \quad \text{if } (\mathrm{F1} \wedge \neg\mathrm{F2} \wedge \neg\mathrm{F3}); \\ 0 \text{ or } \vartheta, & \textbf{case 3} \quad \text{if } (\mathrm{F1} \wedge \mathrm{F2}); \\ \vartheta, & \textbf{case 4} \quad \text{if } (\mathrm{F1} \wedge \neg\mathrm{F2} \wedge \mathrm{F3}). \end{cases} \tag{1}$$

where $0 \le \varepsilon \le 1$ is the observer's guess probability that D has some interests in the received message in the case 2, since he can't observe neither inside nor outside data flow. In the case 3, since the inside data flow is observed, the observer can determine the value of $\mathcal{RD}(S,D)$. In the case 4, since the outside data flow is observed, $\mathcal{RD}(S,D)$ is clearly equal to ϑ. $\mathcal{RD}(S,D)$ captures the observed tightness of $\mathcal{R}(S,D)$. When $\mathcal{RD}(S,D) = 0$, the transmission of message m from S to D is hidden; $\mathcal{RD}(S,D) = 1$, the transmission is fully observed.

- *Single path transmit relation:* When a message m is transmitted from S to D through an intermediate node I, as shown in Fig. 4 (b), the relation $\mathcal{R}(S,I,D)$ is called *single path transmit relation*, and the *observed relation depth* of $\mathcal{R}(S,D)$ is defined as

$$\begin{aligned} \mathcal{RD}(S,D) &= \Pr(\mathcal{R}(S,D)) = \Pr(\mathcal{R}(S,I,D)) \\ &= \Pr(\mathcal{R}(S,I) \cap \mathcal{R}(I,D)) \\ &= \Pr(\mathcal{R}(S,I)) \cdot \Pr(\mathcal{R}(I,D)) \\ &= \mathcal{RD}(S,I) \cdot \mathcal{RD}(I,D) \end{aligned} \tag{2}$$

- *Multi path transmit relation:* In the multi path routing environments, a message m could reach D via different intermediate nodes $I_1, I_2, \cdots, I_k$, then there exist more than one path transmit relations between S and D. For example, in Fig. 4 (c), $\mathcal{R}(S,I_1,D)$, $\mathcal{R}(S,I_2,D)$, $\cdots$, $\mathcal{R}(S,I_k,D)$ are valid path transmit relations. In this case, we define the *observed relation depth* of $\mathcal{R}(S,D)$ as follows,

$$\begin{aligned} \mathcal{RD}(S,D) &= \sum_{i=1}^{k} \eta_i \Pr(\mathcal{R}(S,I_i,D)) \\ &= \sum_{i=1}^{k} \eta_i \Pr(\mathcal{R}(S,I_i)) \cdot \Pr(\mathcal{R}(I_i,D)) \\ &= \sum_{i=1}^{k} \eta_i \mathcal{RD}(S,I_i) \cdot \mathcal{RD}(I_i,D) \end{aligned} \tag{3}$$

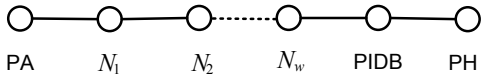


Fig. 5. Transmission path of patient PHI

where

$$\eta_i = \frac{\mathcal{RD}(S,I_i) \cdot \mathcal{RD}(I_i,D)}{\sum_{j=1}^{k} \mathcal{RD}(S,I_j) \cdot \mathcal{RD}(I_j,D)} \tag{4}$$

Note that in the multi path routing environments, if an observer's capability is limited, he can't observe all paths simultaneously, then it is not difficult to prove that the $\mathcal{RD}(S,D)$ will decrease. However, for the global observer, the multi path routing environments can't reduce the $\mathcal{RD}(S,D)$ due to the adversary's powerful capability.

Patient-physician relation & its observed relation depth. Let the routing information of the patient PHI be $\mathrm{PA} - N_1 - N_2 - \cdots - N_w - \mathrm{PIDB} - \mathrm{PH}$, as shown in Fig. 5. Here we won't discuss the multi path transmission, since a global adversary can identify all traffic information even though the multi path transmission is employed.

From the routing information, we can compute the observed relation depth $\mathcal{RD}(\mathrm{PA},\mathrm{PH})$ as follows,

$$\begin{aligned} \mathcal{RD}(\mathrm{PA},\mathrm{PH}) &= \Pr(\mathcal{R}(\mathrm{PA},N_1,N_2,\cdots,N_w,\mathrm{PIDB},\mathrm{PH})) \\ &= \Pr(\mathcal{R}(\mathrm{PA},N_1) \cap \mathcal{R}(N_1,N_2) \cap \cdots \cap \\ &\quad \mathcal{R}(N_w,\mathrm{PIDB}) \cap \mathcal{R}(\mathrm{PIDB},\mathrm{PH}) \\ &= \Pr(\mathcal{R}(\mathrm{PA},N_1)) \cdot \Pr(\mathcal{R}(N_1,N_2)) \cdot \cdots \cdot \\ &\quad \Pr(\mathcal{R}(N_w,\mathrm{PIDB})) \cdot \Pr(\mathcal{R}(\mathrm{PIDB},\mathrm{PH})) \\ &= \mathcal{RD}(\mathrm{PA},N_1) \cdot \prod_{i=1}^{w-1} \mathcal{RD}(N_i,N_{i+1}) \cdot \\ &\quad \mathcal{RD}(N_w,\mathrm{PIDB}) \cdot \mathcal{RD}(\mathrm{PIDB},\mathrm{PH}) \end{aligned} \tag{5}$$

According to the relation model, $\mathcal{RD}(\mathrm{PA},\mathrm{PH})$ is tightly related to each sub-relation depth along with the routing path. Only if one sub-relation depth equals or tends to 0, for example, $\mathcal{RD}(N_1,N_2)$ equals or tends to 0, then $\mathcal{RD}(\mathrm{PA},\mathrm{PH})$ also equals or tends to 0 immediately, which subsequently means the contextual privacy is protected. Based on this observation, we further discuss the relation between the contextual privacy and the adversaries with different capabilities.

- *Non global adversary:* Since the capability of non global adversary is limited, at least one F1 event doesn't occur between two neighboring nodes, for example N_1 and N_2. Then, from Eqs. (1) and (5), we have $\mathcal{RD}(\mathrm{PA},\mathrm{PH}) = 0$, which means the non global adversary has no ability to launch the contextual privacy attack. As a result, the contextual privacy is secure against the non global adversary.
- *Weak global adversary:* A weak global adversary can monitor all traffics over the communication network, i.e., he can observe not only the transmission but also all intermediate nodes' outside data flows. Then, we have $\mathcal{RD}(\mathrm{PIDB},\mathrm{PH}) = \vartheta \cdot \varepsilon$ for the last hop between PIDB and PH and ϑ for any other sub-relation depth. As a result, we have $\mathcal{RD}(\mathrm{PA},\mathrm{PH}) = \vartheta^{w+2} \cdot \varepsilon$ from

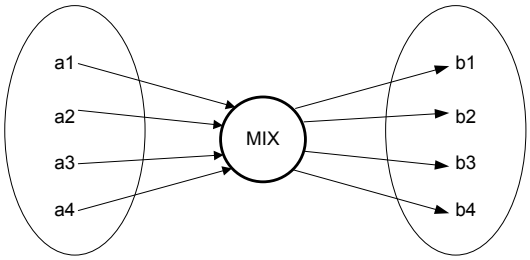


Fig. 6. Mix technique to achieve anonymity communications

Eq. (5). Since the adversary has global eavesdropping ability, ϑ can be assumed to be 1. At the same time, PH is the exclusive destination, then the adversary's guess probability ε could be 1. Concluding with these, we have $\mathcal{RD}(\mathrm{PA}, \mathrm{PH}) = 1$. This result indicates that the contextual privacy is not secure against the weak global adversary.

Fortunately, many mix techniques after Chaum's seminal paper [25] have been proposed to achieve anonymity communications [26]–[30]. For clarity, we outline the mix technique as follows and refer to [25] for more details. The main idea of the mix technique, as shown in Fig. 6, is to cut off the relation between the input and the output. Then, an adversary has no idea on the link relation, especially on the link relation between the source and the destination. For example, when the mix technique is applied in the PIDB, the weak global adversary can't observe the link relation from PIDB 's outside data flows. Then, for n possible physicians, the probability of adversary's observation is only $\mathcal{RD}(\mathrm{PIDB}, \mathrm{PH}) = \frac{1}{n}$ and $\mathcal{RD}(\mathrm{PA}, \mathrm{PH}) = \frac{1}{n}$ subsequently. As a result, the contextual privacy against the weak global adversary can be achieved in this case. However, in any mix technique, the parameter n should be large. Otherwise, the level of anonymity will decrease quickly. In an extreme case, when $n = 1$, no matter what mix technique is adopted, it is impossible to achieve the receiver anonymity.

- *Strong global adversary:* Compared with the weak global adversary, a strong global adversary can also observe all intermediate nodes' inside data flows. In this case, the pure mix technique cannot cut off the link relation against this type of adversary. Accordingly, the contextual privacy cannot be guaranteed, and finally the patient privacy will be disclosed.

Based on the privacy issues existing in the strong global adversary model, the goal of the SAGE is to achieve not only the context oriented privacy but also the contextual privacy. Thus, the patient privacy can be protected against strong global eavesdropping in eHealth systems.

III. Existing Approaches

Besides the mix techniques [25]–[30], many of the privacy techniques adopted in other scenarios such as the sensor networks are also not appropriate for protecting the patient privacy in eHealth systems. The reason is partially due to the fact that the problems considered are not same, and partially due to the fact that the adversary's capabilities are also different. In this section, we review some of these existing works [22], [23], [31]–[38]. Generally, to achieve contextual privacy, the existing approaches can be categorized into two types: one is *by protecting the source location privacy*, and the other is *by protecting the destination location privacy*.

By protecting the source location privacy, the relation between the source and the destination can be cut off, and then the contextual privacy is achieved. The design goals of [22], [23], [31]–[37] are to protect the source location privacy. Kamat et al. [22] observed the facts that both baseline flooding routing [32]–[34] and single-path routing [36], [37] cannot achieve privacy protection, and provided two new techniques to provide efficient source location privacy. One technique is called *routing with fake sources*, and the other is called *phantom single path routing*. In the routing with fake sources, when a source wants to send data, several fake sources, which are away the real source, are involved. Then, both the real and fake sources send data at the same time. Clearly, this technique can provide location privacy against local eavesdropping. However, it is not suitable for eHealth systems. In real life, since the locations of different patients are scattered, when a patient wants to send data, it is not reasonable to assume that he can inform other patients to participate. In *phantom single-path routing*, after a data is generated by the source, it will walk a random path before reaching the destination. By walking a random path, the source data can prevent the local eavesdropping. Another technique, called cyclic entrapment [31], is very similar to the phantom single-path routing, which deals with the local eavesdropping by creating looping pathes at various places. Although the above techniques can deal with non global eavesdropping, they are still not suitable for the defined eHealth system, since the tricks used in these techniques are not effective to a strong global eavesdropper. To deal with the global eavesdropping, Mehta et al. [23] proposed two new techniques: *periodical collect* and *source simulation*. However, the *periodical collect* should send dummy packets and thus could cause large data delivery latency. Therefore, it is not suitable for the real eHealth system. Although the source simulation method provides practical tradeoffs between privacy, communication cost and latency, it will bring inconvenience to the patient since a set of virtual objects should be simulated. On the other hand, the global eavesdropping they considered is confined to the weak global adversary.

Protecting the destination privacy is another alternative to achieve contextual privacy. In 2007, Jian et al. [38] proposed a location privacy routing protocol, call LPR, to achieve path diversity. By combining LPR with fake packet injection, the location privacy of the receiver can be protected, and subsequently, the contextual privacy is achieved. In this paper, similar to [38], we deal with the contextual privacy also from protecting the receiver's location privacy.

IV. The Proposed SAGE Scheme

In this section, we present the proposed SAGE, including system setting, patient registration, patient health information transmission and patient health information receiving. The basic idea of SAGE is quite straightforward: when the PIDB receives the PHIs from patients, it broadcasts the PHIs to all physicians. Then, only the potential physicians will be aware

of the PHIs of their patients. Obviously, due to the nature of broadcast, the SAGE can achieve unconditional receiver anonymity. As a consequence, the patient privacy can be guaranteed in SAGE. Before describing the SAGE in detail, we first review the bilinear pairing technique [39], which serves as the basis of the proposed SAGE.

A. Bilinear Pairing Technique

Let $\mathbb{G}$, $\mathbb{G}_T$ be two cyclic groups of the same prime order q. Let e be a computable bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, which satisfies the following three properties: 1) bilinear: $e(aP, bP) = e(P, P)^{ab}$, where $P, Q \in \mathbb{G}$ and $a, b \in \mathbb{Z}_q^*$; 2) non-degenerate: there exists $P, Q \in \mathbb{G}$ such that $e(P, Q) = 1_{\mathbb{G}_T}$; and 3) computability: there exists an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}$. We call such a bilinear map e as an admissible bilinear pairing, and the modified Weil or Tate pairing in elliptic curve can give a good implementation of the admissible bilinear pairing [39].

Definition 4.1 (Bilinear Parameter Generator): A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter k as input and outputs a 5-tuple $(q, \mathbb{G}, \mathbb{G}_T, e, P)$ as the bilinear parameters, including a prime number q with $|q| = k$, two cyclic groups $\mathbb{G}$, $\mathbb{G}_T$ of the same order q, an admissible bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ and a generator P of $\mathbb{G}$.

Definition 4.2 (Bilinear Diffie-Hellman (BDH) Problem): Let $(q, \mathbb{G}, \mathbb{G}_T, e, P)$ be a 5-tuple generated by $\mathcal{G}en(k)$. The BDH problem is stated as follows: given $aP, bP, cP \in \mathbb{G}$ with unknown a, b, $c \in \mathbb{Z}_q^*$, compute $e(P, P)^{abc} \in \mathbb{G}_T$. The success probability of any polynomial-time adversary $\mathcal{A}$ against the BDH problem is defined to be

$$\mathbf{Succ}_{\mathcal{A}}^{\mathrm{BDH}} = \Pr[\alpha = e(P, P)^{abc} : \alpha \leftarrow \mathcal{A}(aP, bP, cP)].$$

The BDH assumption holds if for all polynomial-time adversary $\mathcal{A}$, the success probability $\mathbf{Succ}_{\mathcal{A}}^{\mathrm{BDH}}$ is negligible.

B. System Setting

To establish an eHealth system, TA first initializes all required system parameters. Given the security parameters k, l_1, l_2, TA generates a 5-tuple $(q, \mathbb{G}, \mathbb{G}_T, e, P)$ by running $\mathcal{G}en(k)$. Then, TA picks up a random number $s \in \mathbb{Z}_q^*$ as a *master-key*, and computes the corresponding public key $P_{pub} = sP$. TA also chooses three secure cryptographic hash functions H, H_1, H_2, where $H : \{0,1\}^* \rightarrow \mathbb{G}$, $H_1 : \mathbb{G}_T \rightarrow \{0,1\}^{l_1}$ and $H_2 : \{0,1\}^* \times \mathbb{G}_T \rightarrow \{0,1\}^{l_2}$, and a secure symmetric encryption algorithm $\mathbf{Enc}_{\mathrm{k}}()$, i.e., DES [24]. In the end, TA publishes the public system parameters $(q, \mathbb{G}, \mathbb{G}_T, e, P, P_{pub}, H, H_1, H_2, \mathbf{Enc}_{\mathrm{k}}())$ and keeps the *master-key* s secretly. In the eHealth system, all PHIs are stored in PIDB at eHealth center. To achieve access control, i.e., only registered patients can store their data and only legal physicians can retrieve patients' data, TA implants a programmable daemon program (DP) in database, which owns a private key $S_{\mathsf{DP}} = sH(\mathrm{ID}_{\mathsf{DP}})$ derived from its identifier $\mathrm{ID}_{\mathsf{DP}}$. As discussed in Section II, many physicians are enrolled in the eHealth system. When they register themselves, each of them will get a private key $S_{\mathsf{PH}} = sH(\mathrm{ID}_{\mathsf{PH}})$ from TA based on his/her identity $\mathrm{ID}_{\mathsf{PH}}$.

C. Patient Registration

To take the benefits from the eHealth system, a patient will register himself/herself to the eHealth system. When the patient with identity $\mathrm{ID}_{\mathsf{PA}}$ registers to TA, TA will execute the following steps.

Step 1. Check the identity $\mathrm{ID}_{\mathsf{PA}}$ and compute the pseudo-identity $\mathrm{PID}_{\mathsf{PA}} = \mathbf{Enc}_s(\mathrm{ID}_{\mathsf{PA}})$ with the *master-key* s;

Step 2. Compute the private key $S_{\mathsf{PA}} = sH(\mathrm{PID}_{\mathsf{PA}})$;

Step 3. Choose the appropriate body sensors $\mathcal{S}$ and designate a physician with $\mathrm{ID}_{\mathsf{PH}}$ based on the patient's requirement.

Step 4. Send $(\mathrm{PID}_{\mathsf{PA}}, S_{\mathsf{PA}}, \mathcal{S}, \mathrm{ID}_{\mathsf{PH}})$ to the patient and $\mathrm{PID}_{\mathsf{PA}}$ to the physician. (Note that since the patient doesn't want the physician to know his/her real identity, the pseudo-identity $\mathrm{PID}_{\mathsf{PA}}$ can guarantee the identity privacy).

After receiving $(\mathrm{PID}_{\mathsf{PA}}, S_{\mathsf{PA}}, \mathcal{S}, \mathrm{ID}_{\mathsf{PH}})$, the patient deploys these sensor nodes at home to form a BSN. Through the BSN, the patient can periodically report his/her health data to the eHealth system.

Static shared key: With the patient registration procedure, the patient gets $(S_{\mathsf{PA}}, \mathrm{ID}_{\mathsf{PH}})$ and the physician holds $(S_{\mathsf{PH}}, \mathrm{PID}_{\mathsf{PA}})$. Then, based on the properties of bilinear pairing, the non-interactive static shared key K_{PP} can be conveniently computed in advance as follows,

$$\begin{aligned} K_{\mathsf{PP}} &= e(H(\mathrm{PID}_{\mathsf{PA}}), H(\mathrm{ID}_{\mathsf{PH}}))^s \\ &= \begin{cases} e(sH(\mathrm{PID}_{\mathsf{PA}}), H(\mathrm{ID}_{\mathsf{PH}})) = e(S_{\mathsf{PA}}, H(\mathrm{ID}_{\mathsf{PH}})) \\ e(H(\mathrm{PID}_{\mathsf{PA}}), sH(\mathrm{ID}_{\mathsf{PH}})) = e(H(\mathrm{PID}_{\mathsf{PA}}), S_{\mathsf{PH}}) \end{cases} \end{aligned} \quad (6)$$

Due to the static shared key, the subsequent content oriented privacy between the patient and the physician can be achieved when employing a secure symmetric encryption algorithm. The formal proof will be presented in Section V.

D. Patient Health Information Transmission

When the patient's BSN gathers the health data m and is ready to report it to the eHealth system and the physician, it first runs the Algorithm 1, and sends the returned C to the eHealth system via Internet (ref. Fig. 1). Note that the form of $\Delta = \mathbf{Enc}_{\mathsf{k}}(m)$ can provide the content oriented privacy. At the same time, since the static shared key $K_{\mathsf{PD}} = e(H(\mathrm{PID}_{\mathsf{PA}}), S_{\mathsf{DP}}) = e(S_{\mathsf{PA}}, H(\mathrm{ID}_{\mathsf{DP}}))$ is only known by the patient and the DP, the authentication on C at the side of DP is achieved. In addition, the self-encryption technique [40] encrypts the patient identity, $C = \mathcal{IBC}_{\mathrm{ID}_{\mathsf{DP}}}\{\mathrm{PID}_{\mathsf{PA}} || \Theta || H_2(\Theta, K_{\mathsf{PD}})\}$ won't disclose the identity privacy to the non-global adversary, although it may not prevent the global adversary from eavesdropping.

Upon receiving an incoming ciphertext C, DP runs the following operations.

Step 1. DP first invokes the Algorithm 2 with the private key $S_{\mathsf{DP}} = sH(\mathrm{ID}_{\mathsf{DP}})$. If the returned value is $\perp$, DP terminates the operation and discards the incoming message. Otherwise, DP continues to the next step.

Step 2. DP stores the entry $(\mathrm{PID}_{\mathsf{PA}}, \Theta)$ into PIDB for backup and puts the PHI Θ into a Patient Information Report

Algorithm 1: ReadySend()

Input: Gathered patient health data m
Result: Ciphertext C ready for transmission

begin
  Obtain the current timestamp T ;
  Compute the temporary key $\mathsf{k} = H_1(T \cdot K_{\mathsf{PP}})$;
  Compute $\Delta = \mathbf{Enc}_{\mathsf{k}}(m)$ and $H_2(T||\Delta, K_{\mathsf{PP}})$, where $||$ denotes the concatenation ;
  Compute $H_2(\Theta, K_{\mathsf{PD}})$ where

$$\Theta = T||\Delta||H_2(T||\Delta, K_{\mathsf{PP}})$$

  and $K_{\mathsf{PD}} = e(S_{\mathsf{PA}}, H(\mathrm{ID}_{\mathsf{DP}}))$ is static shared key between the patient and the daemon program DP ;
  Employ a chosen-plaintext secure identity-based encryption algorithm, for example $\mathcal{IBC}$ in [39], and use self encryption technique [40] with DP's identity $\mathrm{ID}_{\mathsf{DP}}$ to compute the ciphertext

$$C = \mathcal{IBC}_{\mathrm{ID}_{\mathsf{DP}}}\{\mathrm{PID}_{\mathsf{PA}}||\Theta||H_2(\Theta, K_{\mathsf{PD}})\} \quad (7)$$

  return C ;
end

$\mathrm{ID}_{\mathsf{DP}}$	n	δ
$1 \cdots n$	valid patient health information	

Fig. 7. Format of patient information report (PIR) for PHIs

(PIR), which serves a container for PHIs' aggregating and broadcasting. The format of PIR is illustrated in Fig. 7, and each field is as follows: *the header* is fixed as the DP's identity $\mathrm{ID}_{\mathsf{DP}}$; *the second field* n specifies the number of encapsulated PHIs; *the third field* σ is the identity-based signature on all n encapsulated PHIs, and *the fourth field* is the payload of PIR that contains n valid PHIs.

When the PIR is full of n valid PHIs, DP uses the private key $S_{\mathsf{DP}} = sH(\mathrm{ID}_{\mathsf{DP}})$ to compute the signature

$$\sigma = \mathcal{IBS}_{S_{\mathsf{DP}}}\{\Theta_1||\cdots||\Theta_n\} \quad (8)$$

where $\mathcal{IBS}$ is an efficient identity-based signature algorithm presented in [41], and as shown in Fig. 8, DP also broadcasts the PIR so that all physicians in eHealth center can receive these valid PHIs.

E. Patient Health Information Receiving

Each physician in eHealth center first checks the validity of the signature σ, after he receives the PIR broadcasted by DP. If the signature is invalid, he discards the PIR. Otherwise, he tries to recover his patients' information.

Assume that a physician $\mathrm{ID}_{\mathsf{PH}}$ has α patients with pseudo IDs $\{\mathrm{PID}_{\mathsf{PA1}}, \mathrm{PID}_{\mathsf{PA2}}, \cdots, \mathrm{PID}_{\mathsf{PA}\alpha}\}$, he can compute α static shared keys $\{K'_{\mathsf{PP1}}, K'_{\mathsf{PP2}}, \cdots, K'_{\mathsf{PP}_\alpha}\}$ in advance, where $K'_{\mathsf{PP}_i} = e(H(\mathrm{PID}_{\mathsf{PA}i}), S_{\mathsf{PH}})$, for $1 \le i \le \alpha$. Then, for n PHIs $\{\Theta_1, \Theta_2, \cdots, \Theta_n\}$ in the PIR, he invokes the Algorithm 3. If the returned set $\mathcal{M}^*$ is not vacant, the physician can efficiently retrieve his patents' PHIs in the current broadcast.

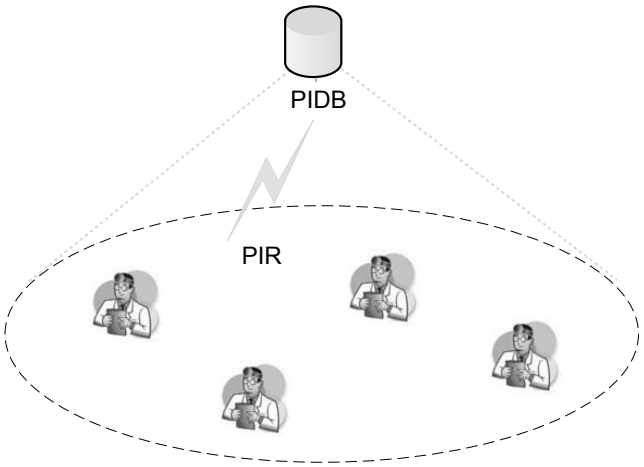


Fig. 8. Broadcasting the PIR to all physicians in eHealth center

Algorithm 2: AuthConvert()

Input: DP's private key S_{DP} and an incoming ciphertext $C = \mathcal{IBC}_{\mathrm{ID}_{\mathsf{DP}}}\{\mathrm{PID}_{\mathsf{PA}}||\Theta||H_2(\Theta, K_{\mathsf{PD}})\}$
Result: $\perp$ or converted ciphertext Θ

begin
  Use S_{DP} to recover M from C and parse M as

$$\mathrm{PID}_{\mathsf{PA}}||\Theta||H_2(\Theta, K_{\mathsf{PD}})$$

  Based on the pseudo ID $\mathrm{PID}_{\mathsf{PA}}$, compute static shared key $K'_{\mathsf{PP}} = e(H(\mathrm{PID}_{\mathsf{PA}}), S_{\mathsf{DP}})$ or get it from the cache if existing, and check

$$H_2(\Theta, K_{\mathsf{PD}}) \stackrel{?}{=} H_2(\Theta, K'_{\mathsf{PD}}) \quad (9)$$

  if *it doesn't hold* **then**
    return $\perp$;
  else
    parse the item Θ as $T||\Delta||H_2(T||\Delta, K_{\mathsf{PP}})$ and check whether T is a valid timestamp ;
    if *it is not valid* **then**
      return $\perp$;
    else
      return $\Theta = T||\Delta||H_2(T||\Delta, K_{\mathsf{PP}})$;
    end
  end
end

V. Security Analysis

In this section, we first prove that the proposed SAGE has the content oriented privacy, then show that it is also secure against global eavesdropping in terms of contextual privacy. Finally, we discuss the robustness of the SAGE against several known attacks.

A. Content Oriented Privacy

In the proposed SAGE, the content oriented privacy can be guaranteed by the security of $\mathbf{Enc}_{\mathsf{k}}(m)$. If the ciphertext $\mathbf{Enc}_{\mathsf{k}}(m)$ is provably secure, so does the content oriented privacy in SAGE. Therefore, we will prove the semantic security property of $\mathbf{Enc}_{\mathsf{k}}(m)$ by using the techniques from provable security [42], [43].

The semantic security of $\mathbf{Enc}_{\mathsf{k}}(m)$ in SAGE is defined using a game between a challenger and an adversary. Both

Algorithm 3: RecoverValidRecord()

Input: $\{K'_{\mathsf{PP}1}, K'_{\mathsf{PP}2}, \cdots, K'_{\mathsf{PP}\alpha}\}$ and $\{\Theta_1, \Theta_2, \cdots, \Theta_n\}$
Result: valid $\mathcal{M}^*$

```
begin
    set M* = {φ} ;
    for i = 1 to α do
        for j = 1 to n do
            parse Θ_j as T_j||Δ_j||H_2(T_j||Δ_j, K_PPi);
            check H_2(T_j||Δ_j, K'_PPi) ?= H_2(T_j||Δ_j, K_PPi);
            if it does hold then
                recover m_j from Δ' = Enc_k(m_j) with
                temporary key k, where k = H_1(T_j · K'_PPi) ;
                M* = M* ∪ {m_j} ;
            end
        end
    end
    return M* ;
end
```

the challenger and adversary are given the system parameters, and the game proceeds as follows:

- Define the adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that runs in the following two stages.
- In the first stage:
  - $\mathcal{A}_1$ is allowed to make extraction queries on identities he chooses so that he can gain some private keys of other patients and physicians, which is similar to the Identity-based cryptography in [39].
  - $\mathcal{A}_1$ is also allowed to make some random oracles' queries if the game is running in the random oracle model [42].
  - At some time, $\mathcal{A}_1$ terminates the query and sends two equal length messages m_0, m_1, a fresh timestamp $T^\star$, unextracted patient's pseudo-id $\mathrm{PID}^\star_{\mathsf{PA}}$ and unextracted physician's identity $\mathrm{ID}^{\star'}_{\mathsf{PH}}$ to the challenger.
- In the second stage:
  - The challenger picks a random bit $b \in \{0,1\}$ and sends $C^\star = \mathbf{Enc}_{\mathsf{k}}(m_b)$, where $\mathsf{k} = H_1(T^\star \cdot K_{\mathsf{PP}})$, as the challenge to $\mathcal{A}_2$.
  - At the end, $\mathcal{A}_2$ returns a guess $b' \in \{0,1\}$ on b and and wins the game if $b' = b$.

We define that the advantage of $\mathcal{A}$ breaking the semantic security of $\mathbf{Enc}_{\mathsf{k}}(m)$ is

$$\mathbf{Adv}^{\mathrm{SAGE}}_{\mathcal{A}} = 2 \cdot \Pr[b = b'] - 1$$

If for all adversaries $\mathcal{A}$, the advantage $\mathbf{Adv}^{\mathrm{SAGE}}_{\mathcal{A}}$ is negligible, we say $\mathbf{Enc}_{\mathsf{k}}(m)$ in SAGE is semantic security under adaptively chosen plaintext attacks. In the following theorem, we will formally prove that the $\mathbf{Enc}_{\mathsf{k}}(m)$ in SAGE is semantic security within the random oracle model, where H, H_1 behave as the random oracles [42].

Theorem 5.1: Let $\mathcal{G}en$ be a bilinear parameter generator, and $\mathcal{A}$ be an adversary against the semantic security of $\mathbf{Enc}_{\mathsf{k}}(m)$ in SAGE in the random oracle model. Assume that $\mathcal{A}$ has advantage $\epsilon = \mathbf{Adv}^{\mathrm{SAGE}}_{\mathcal{A}}$, within running time τ, making q_H, q_{H_1}, and $2q_E$ queries to the random oracles $\mathcal{O}_H$, $\mathcal{O}_{H_1}$, and the extraction oracle $\mathcal{O}_E$. Then, there exist $\epsilon' \in [0,1]$ and $\tau' \in \mathbb{N}$ as follows

$$\epsilon' \geq \frac{\epsilon}{\exp(1)^2 \cdot q_{H_1} \cdot (1+q_E)^2}$$
$$\tau' \leq \tau + (q_H + q_{H_1} + q_E) \cdot \mathbb{T}$$

such that BDH problem can be solved with probability ϵ', within time τ', where $\mathbb{T}$ denotes the average time required by each query.

Proof: We define a sequence of games Game_0, Game_1, $\cdots$ of modified attacks starting from the actual adversary $\mathcal{A}$ [43]. All the games operate on the same underlying probability space: the system parameters and master key, the coin tosses of $\mathcal{A}$ and the random oracles. Let $X = xP, Y = yP, Z = zP$ be a random instance of BDH. We will use $\mathcal{A}$ to compute $e(P,P)^{xyz} \in \mathbb{G}_T$, and starred letter $C^\star = \mathbf{Enc}_{\mathsf{k}}(m_b)$ to represent the challenge ciphertext.

Game_0: This is the real attack game in the random oracle model. TA chooses the *master keys* $s \in \mathbb{Z}^*_q$ and computes $P_{pub} = sP$. Then the system parameters $(q, \mathbb{G}, \mathbb{G}_T, e, P, P_{pub}, H, H_1, H_2, \mathbf{Enc}_k())$ are published. The adversary $\mathcal{A}$ is fed with these system parameters and queries the oracles $\mathcal{O}_H$, $\mathcal{O}_{H_1}$ and $\mathcal{O}_E$, and outputs two equal length messages (m_0, m_1), a fresh timestamp $T^\star$ and $(\mathrm{PID}^\star_{\mathsf{PA}}, \mathrm{ID}^{\star'}_{\mathsf{PH}})$. The challenger then flips a coin $b \in \{0,1\}$ and produces a ciphertext $C^\star = \mathbf{Enc}_{\mathsf{k}}(m_b)$ as the challenge to the adversary, where $\mathsf{k} = H_1(T^\star \cdot K_{\mathsf{PP}})$ with K_{PP} the static shared key between $\mathrm{PID}^\star_{\mathsf{PA}}$ and $\mathrm{ID}^{\star'}_{\mathsf{PH}}$. Finally, the adversary outputs a bit $b' \in \{0,1\}$ as the guess of b. In any Game_j, we denote by Guess_j the event $b = b'$ and Adv_j the guess advantage in Guess_j. Then, by definition, we have

$$\mathrm{Adv}_0 = \epsilon = 2\Pr[b = b'] - 1 = 2\Pr[\mathrm{Guess}_0] - 1 \quad (10)$$

$$\Pr[\mathrm{Guess}_0] = \frac{1}{2} + \frac{\mathrm{Adv}_0}{2} \quad (11)$$

Game_1: In this game, we modify the simulation by replacing the system public key $P_{pub} = sP$ by $X = xP$. Since the distribution of system public key is unchanged, we have

$$\mathrm{Adv}_1 = \mathrm{Adv}_0; \qquad \Pr[\mathrm{Guess}_1] = \Pr[\mathrm{Guess}_0] \quad (12)$$

Game_2: In this game, we simulate the random oracles $\mathcal{O}_H$ and $\mathcal{O}_{H_1}$ as follows.

- Simulate q_H queries on $\mathcal{O}_H$:
  - for any fresh query, we uniformly pick a random number $r \in \mathbb{Z}^*_q$;
  - pick one bit $c \in \{0,1\}$ with $\Pr(c = 0) = \delta$, where δ, $0 < \delta < 1$, is a parameter to be determined later [44];
  - If the fresh query is on a patient pseudo-id $\mathrm{PID}_{\mathsf{PA}}$, then
    1) if $c = 0$, sets $u = rP$, otherwise sets $u = rY = ryP$;
    2) store $(\mathrm{PID}_{\mathsf{PA}}, c, r, u)$ in the $\mathcal{H}$-list, which is initially empty, and return $H(\mathrm{PID}_{\mathsf{PA}}) = u$ as the answer to the oracle query.
  - If a fresh query is on a physician identity $\mathrm{ID}_{\mathsf{PH}}$, then
    1) if $c = 0$, sets $v = rP$, otherwise sets $v = rZ = rzP$;

2) store $(\mathrm{ID_{PH}}, c, r, v)$ in the $\mathcal{H}$-list and return $H(\mathrm{ID_{PH}}) = v$ as the answer to the oracle query.

- Simulate q_{H_1} queries on $\mathcal{O}_{H_1}$: For any fresh query $R \in \mathbb{G}_T$, we pick up a random number $h \in \{0,1\}^{l_1}$, store (R, h) in the $\mathcal{H}_1$-list, which is also initially empty, and return $H_1(R) = h$ as the answer to the oracle query.

Clearly, in the random oracle model, this game is identical to the previous one. Hence,

$$\mathrm{Adv}_2 = \mathrm{Adv}_1; \qquad \Pr[\mathrm{Guess}_2] = \Pr[\mathrm{Guess}_1] \tag{13}$$

Game_3: In this game, we simulate total $2q_E$ extraction oracle $\mathcal{O}_E$ queries as follows.

- Simulate q_E queries with patient pseudo-id $\mathrm{PID_{PA}}$:
  - look up $(\mathrm{PID_{PA}}, c, r, u)$ in $\mathcal{H}$-list ;
  - if $c = 0$, we compute $S_{\mathrm{PA}} = rY = ryP$ as the private key and return it to $\mathcal{A}$;
  - if $c = 1$, we have to terminate the game and report the failure.
- Simulate q_E queries with physician identity $\mathrm{ID_{PH}}$:
  - look up $(\mathrm{ID_{PH}}, c, r, v)$ in $\mathcal{H}_1$-list ;
  - if $c = 0$, we compute $S_{\mathrm{PH}} = rZ = rzP$ as the private key and return it to $\mathcal{A}$;
  - if $c = 1$, we have to terminate the game and report the failure.

In Game_3, only if the event $c = 1$ occurs during any query, we terminate the game. Therefore, after total $2q_E$ queries, the probability that the game is not terminated (i.e., $c = 0$ in all queries) is

$$[\Pr(c = 0)]^{2q_E} = \delta^{2q_E}$$

and we have

$$\mathrm{Adv}_3 = \delta^{2q_E} \cdot \mathrm{Adv}_2; \tag{14}$$

$$\Pr[\mathrm{Guess}_3] = \frac{1}{2} + \frac{\mathrm{Adv}_3}{2} \tag{15}$$

Game_4: In this game, we observe $(\mathrm{PID}^{\star}_{\mathrm{PA}}, \mathrm{ID}^{\star'}_{\mathrm{PH}})$ that $\mathcal{A}$ submitted at the end of the first stage.

- look up $(\mathrm{PID}^{\star}_{\mathrm{PA}}, c^{\star}, r^{\star}, u^{\star})$ in $\mathcal{H}$-list with $\mathrm{PID}^{\star}_{\mathrm{PA}}$; if $c^{\star} = 0$, terminate the game and report failure.
- look up $(\mathrm{ID}^{\star'}_{\mathrm{PH}}, c^{\star'}, r^{\star'}, v^{\star'})$ in $\mathcal{H}_1$-list with $\mathrm{ID}^{\star}_{\mathrm{PH}}$; if $c^{\star'} = 0$, terminate the game and report failure.

In Game_4, we will also terminate when the event $c^{\star} = 0$ or $c^{\star'} = 0$ occurs. Thus, the probability that Game_4 is not terminated (i.e., $c^{\star} = 1$ and $c^{\star'} = 1$ in two irrelevant cases) is

$$[\Pr(c^{\star} = 1 \wedge c^{\star'} = 1)] = (1-\delta)^2$$

and we have

$$\mathrm{Adv}_4 = (1-\delta)^2 \cdot \mathrm{Adv}_3; \tag{16}$$

$$\Pr[\mathrm{Guess}_4] = \frac{1}{2} + \frac{\mathrm{Adv}_4}{2} \tag{17}$$

Let AskH_4 denote the event that the adversary $\mathcal{A}$ has asked $H_1(T^{\star} \cdot e(\mathrm{PID}^{\star}_{\mathrm{PA}}, \mathrm{ID}^{\star'}_{\mathrm{PH}})^x)$. Thus, if the event AskH_4 doesn't occur, $C^{\star}$ is independent on b, we have

$$\Pr[\mathrm{Guess}_4 | \neg \mathrm{AskH}_4] = \frac{1}{2}$$

and

$$\begin{aligned}\Pr[\mathrm{Guess}_4] &= \Pr[\mathrm{Guess}_4|\mathrm{AskH}_4] \cdot \Pr[\mathrm{AskH}_4] \\ &\quad + \Pr[\mathrm{Guess}_4|\neg\mathrm{AskH}_4] \cdot \Pr[\neg\mathrm{AskH}_4] \\ &\le \frac{1}{2} \cdot \Pr[\neg\mathrm{AskH}_4] + 1 \cdot \Pr[\mathsf{AskH}_4] \\ &= \frac{1}{2} \cdot (1 - \Pr[\mathrm{AskH}_4]) + 1 \cdot \Pr[\mathsf{AskH}_4] \\ &= \frac{1}{2} + \frac{1}{2} \cdot \Pr[\mathrm{AskH}_4]\end{aligned} \tag{18}$$

When the event AskH_4 occurs, the entry $(R = T^{\star} \cdot e(\mathrm{PID}^{\star}_{\mathrm{PA}}, \mathrm{ID}^{\star'}_{\mathrm{PH}})^x, h)$ is in the $\mathcal{H}_1$-list. We can randomly pick an entry (R, h) from the $\mathcal{H}_1$-list and compute

$$\left(\frac{R}{T^{\star}}\right)^{\frac{1}{r^{\star}r^{\star'}}} = [e(\mathrm{PID}^{\star}_{\mathrm{PA}}, \mathrm{ID}^{\star'}_{\mathrm{PH}})^x]^{\frac{1}{r^{\star}r^{\star'}}} = e(r^{\star}yP, r^{\star'}zP)^{\frac{x}{r^{\star}r^{\star'}}}$$

and output it as the challenge $e(P,P)^{xyz}$ with the probability $1/q_{H_1}$. Therefore, we have

$$\frac{\Pr[\mathrm{AskH}_4]}{q_{H_1}} = \epsilon' = \mathbf{Succ}^{\mathrm{BDH}}_{\mathcal{A}} \tag{19}$$

By combining Eqs. (10)-(19), we have

$$\epsilon' \ge \frac{1}{q_{H_1}} \cdot \delta^{2q_E} \cdot (1-\delta)^2 \cdot \epsilon \tag{20}$$

When minimizing the function $\delta^{q_E} \cdot (1-\delta)$, we find the optimal value

$$\delta = \frac{1}{1+q_E} \tag{21}$$

and the overall probability of $\delta^{2q_E} \cdot (1-\delta)^2$ is at least

$$\frac{1}{\exp(1)^2 \cdot (1+q_E)^2} \tag{22}$$

Then, from Eqs. (20)-(22), we have

$$\mathbf{Succ}^{\mathrm{BDH}}_{\mathcal{A}} = \epsilon' \ge \frac{\epsilon}{\exp(1)^2 \cdot q_{H_1} \cdot (1+q_E)^2} \tag{23}$$

Also, based on the time costs in all oracle queries, we can obtain the claimed bound for

$$\tau' \le \tau + (q_H + q_{H_1} + q_E) \cdot \mathbb{T} \tag{24}$$

This completes the proof. ■

B. Contextual Privacy

In this subsection, we further demonstrate that the proposed SAGE is secure against the strong global eavesdropping in terms of contextual privacy. As discussed in section II, the strong global adversary has the ability to monitor not only all traffic over the communication network but also all inner traffic in each intermediate node along the routing. Therefore, the contextual privacy, i.e., $\mathcal{RD}(\mathrm{PA}, \mathrm{PH}) = 0$, cannot be achieved by pure mix technique, since an adversary always has ways to link the patient to a specific physician.

In the proposed SAGE, to gain $\mathcal{RD}(\mathrm{PA}, \mathrm{PH}) \to 0$, the key trick is to ensure $\mathcal{RD}(\mathrm{PIDB}, \mathrm{PH}) \to 0$ by DP's broadcasting. Due to the broadcasting, the PIR can be received by all physicians. At the same time, since the adversary can't observe any physician's inner operations, each physician is then equal suspicious by the adversary.

In the following, the link privacy between PIDB and PH is formally defined using a game between a challenger and an adversary. Both the challenger and the adversary are fed with system parameters, and the game proceeds as follows.

- Define the adversary $\mathcal{A}$ that runs in the following two stages.
- In the first stage:
  - A set of physicians $\mathcal{D} = \{\mathsf{PH}_1, \mathsf{PH}_2, \cdots, \mathsf{PH}_\gamma\}$ are available to both the adversary $\mathcal{A}$ and the challenger. The adversary knows that there is only one patient PA in the game, and the challenger knows the PA's private key.
  - At some time, the challenger picks at random a number $j \in \{1, 2, \cdots, \gamma\}$, generates an $\Theta = T||\Delta||H_2(T||\Delta, K_{\mathsf{PP}j})$, and broadcasts Θ.
- In the second stage:
  - After receiving the message Θ, the adversary $\mathcal{A}$ returns a guess $j' \in \{0, 1\}$ on j and wins the game if $j' = j$.

We define that the advantage of $\mathcal{A}$ breaking the link privacy property of Θ is

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{SAGE}} = \gamma \cdot \Pr[j = j'] - 1$$

For all adversaries $\mathcal{A}$, if the advantage $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{SAGE}}$ is negligible, we say the link privacy of Θ in SAGE is achieved. If the advantage $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{SAGE}}$ is exactly 0, then the link privacy is unconditional. A standard way of proving that SAGE in this game enjoys the unconditional link privacy is by showing that Θ's destination $\mathsf{PH}_{j'}$, guessed by the adversary $\mathcal{A}$ in the game, follows the same probability distribution for any possible physician in $\mathcal{D} = \{\mathsf{PH}_1, \mathsf{PH}_2, \cdots, \mathsf{PH}_\gamma\}$. If it can be proved, then in the second phase of the game defined above, the adversary $\mathcal{A}$ cannot obtain any information about which $\mathsf{PH}_{j'} \in \mathcal{D}$ is actually Θ's destination from Θ and his observations, and therefore its success probability $\Pr[j = j']$ is limited to $\frac{1}{\gamma}$. In the following theorem, we prove that the information Θ achieves the unconditional link privacy by broadcasting.

Theorem 5.2: The information Θ in SAGE achieves unconditional link privacy by broadcasting.

Proof: Since the content oriented privacy of Θ has been protected, the only way for the adversary $\mathcal{A}$ to find the Θ's destination is by using all traffic information he obtained from global eavesdropping. However, in the eye of the adversary, each physician is equal suspicious by broadcasting mechanism. Therefore, in the second stage, $\Pr[j = j'] = \frac{1}{\gamma}$. Then, by definition, we have

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{SAGE}} = \gamma \cdot \Pr[j = j'] - 1 = \gamma \cdot \frac{1}{\gamma} - 1 = 0 \qquad (25)$$

and the proof is completed. ■

From theorem 5.2, the information Θ in SAGE achieves unconditional link privacy. Unconditional link privacy means $\mathcal{RD}(\mathrm{PIDB}, \mathrm{PH}) = \Pr[j = j'] = \frac{1}{\gamma}$, and $\mathcal{RD}(\mathrm{PA}, \mathrm{PH}) = \frac{1}{\gamma}$ for a strong global eavesdropper. However, similar to the mix technique [25], if the set size $|\mathcal{D}| = 1$, i.e., $\gamma = 1$, then $\mathcal{RD}(\mathrm{PA}, \mathrm{PH})$ still equals 1. Therefore, to achieve high contextual privacy, γ should be a large number. Fortunately, from the view of practice, it is reasonable to assume that an eHealth center involves many physicians.

TABLE I
TIME COSTS OF REQUIRED OPERATIONS

Operation	Time
pairing (without precompution)	6.7 ms
pairing (with precompution)	3.0 ms
point multiplication	2.9 ms

C. Robustness

In this subsection, we discuss the robustness of SAGE. Concretely, we show how the SAGE prevents other known attacks, such at the replaying attack and the forging attack. Although these two attacks are not relevant to the patient privacy, they will affect the performance of SAGE.

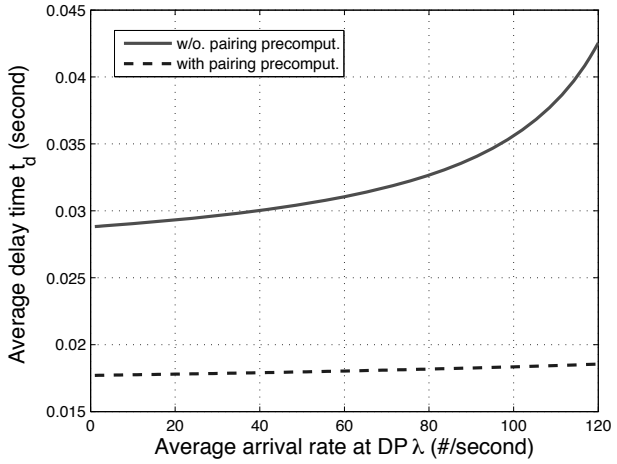
1) Resistance against the replaying attack.: One possible attack launched by an adversary is the replaying attack, which refers to the adversary maliciously replaying some valid but old messages. However, the replaying attack doesn't affect the proposed SAGE because the DP will check the validity of timestamp in the Algorithm 2. If the timestamp is outdated, it will be directly discarded.

2) Resistance against the forging attack.: Another attack could be launched by an adversary is the forging attack. In a forging attack, the adversary can inject forged messages in transmission. Fortunately, the forging attack can be also prevented by SAGE, since the message authentications based on the static shared key and digital signature techniques have been integrated in the proposed SAGE.

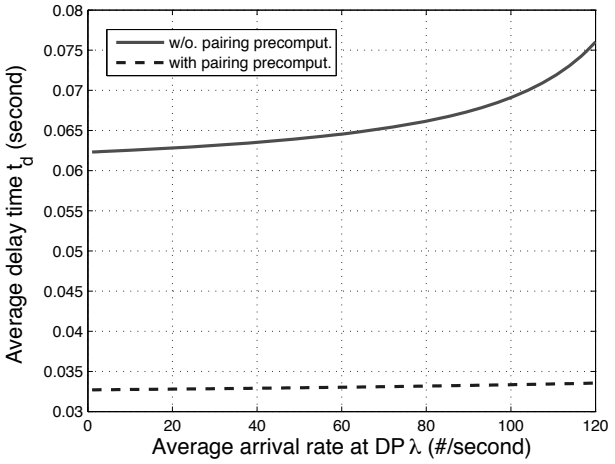
VI. PERFORMANCE EVALUATION

An important performance matric in eHealth systems is how long it takes for a patient PHI to reach its specific physician. Thus, in this section, to evaluate the performance of SAGE, we focus on the transmission delay of SAGE at the eHealth center. First, we estimate the computation costs of SAGE.

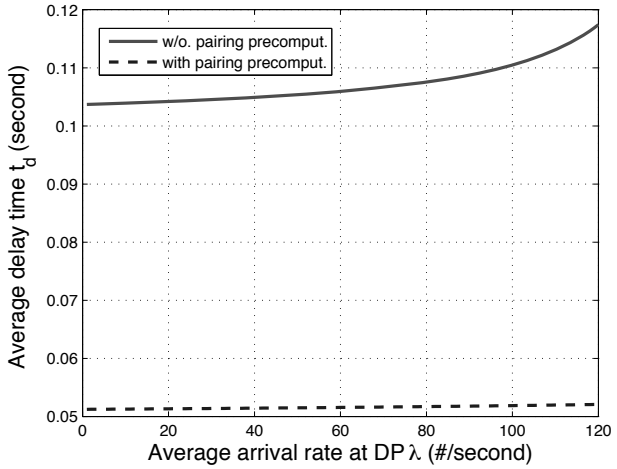
Roughly, the computation costs of SAGE include PHI authentication, PIR signing and verification, which mainly involve the following cryptographic operations: pairing, point multiplication, multiplication in $\mathbb{Z}_q^*$ and hash operations. Since the time costs of the latter two can be negligible compared with that of the first two, we only consider pairing and point multiplication when measuring the performance. We implement the Tate pairing with an embedding degree $k = 2$ Cocks-Pinch curve [45]. The curve is over $\mathbb{F}_p$ with 512-bit prime p and a subgroup of 160-bit prime q. Benchmarks for the selected pairing were running on a modern workstation, where the processor is 32 bits, 3GHz Pentium 4. The measured result are given in Table I. Based on these benchmark numbers and the adopted $\mathcal{IBE}$ [39] and $\mathcal{IBS}$ [41], we can estimate the computation costs in SAGE, and the relevant results are given in Table II [45].



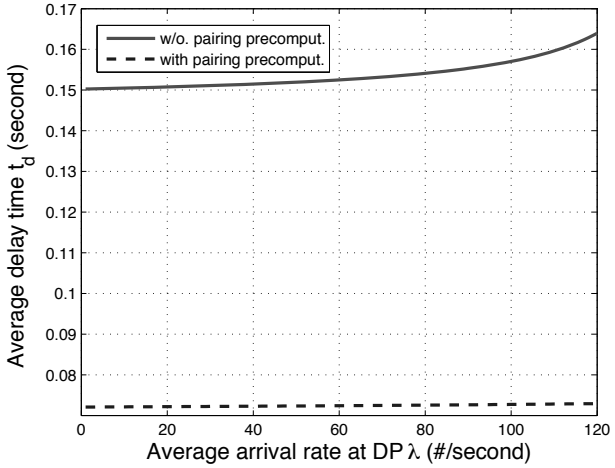
(a) T v.s. λ with $n = 1$, $p = 0$



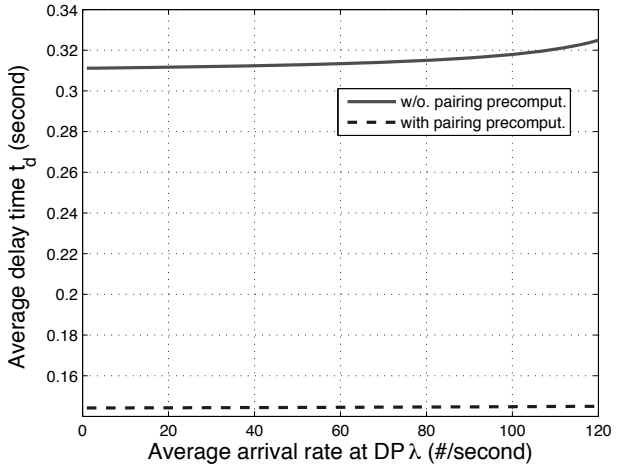
(b) T v.s. λ with $n = 10$, $p = 10\%$



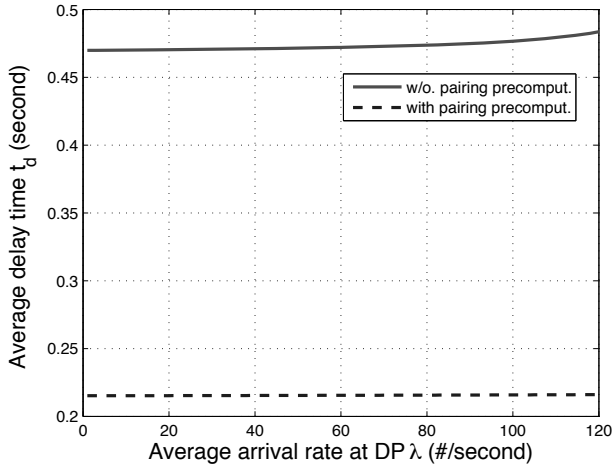
(c) T v.s. λ with $n = 20$, $p = 15\%$



(d) T v.s. λ with $n = 40$, $p = 20\%$



(e) T v.s. λ with $n = 60$, $p = 25\%$



(f) T v.s. λ with $n = 80$, $p = 40\%$

Fig. 9. Average transmission delay t_d varies with the average arrival rate λ, where $1 \leq \lambda \leq 120$

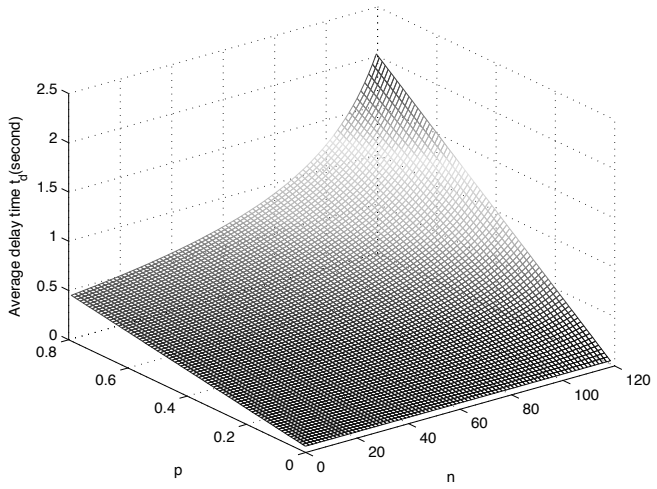
Next we evaluate the transmission delay of SAGE. We consider the average arrival of PHI at DP is a Poisson process with rate λ. In addition, each fixed-length PHI packet has the same authentication time estimated in Table II. Then, we have

$$\mu = \begin{cases} 149.3/\text{sec, w/o pairing precomputation;} \\ 333.3/\text{sec, with pairing precomputation.} \end{cases} \quad (26)$$

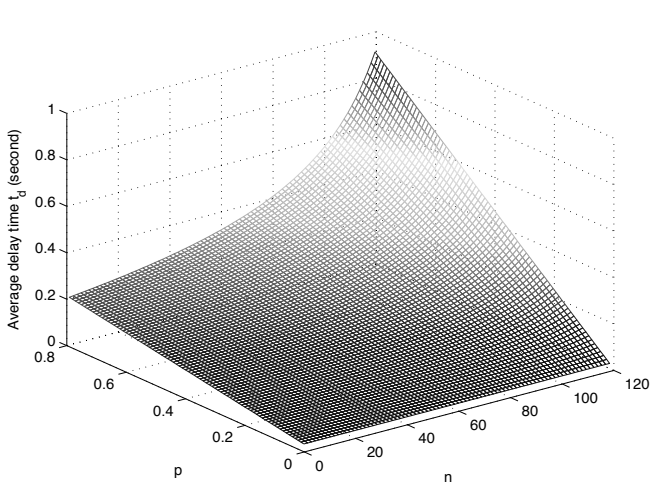
Based on the M/D/1 process [46], the average delay time (wait time + authentication time) of PHI before being put into the PRI buffer is

$$\frac{2-\rho}{2\mu(1-\rho)}, \text{ where } \rho = \frac{\lambda}{\mu} < 1 \quad (27)$$

By broadcasting PIR, the number for PHIs' broadcasting, signing and verification can be reduced. However, this mech-



(a) T v.s. n and p with $\lambda = 120$ w/o pairing precomput.



(b) T v.s. n and p with $\lambda = 120$ with pairing precomput.

Fig. 10. Average transmission delay t_d varies with p and n, where $1\% \leq p \leq 80\%$ and $1 \leq n \leq 120$

anism will incur the transmission delay. In addition, both the replaying attack and the forging attack will also cause the transmission delay. Let the invalid probability of a PHI arriving at DP be p due to the replaying and forging attacks. We study the average delay time in PIR buffer as follows.

We first consider how long it takes the i-th PHI in PRI to wait for the arrival of the next $i+1$-th PHI. Since the invalid probability of a PHI is p, when a valid PHI is put into the PRI buffer, the number of PHI authentications at DP is a geometrically distributed random variable:

$$P(\text{number of authentication} = k) = p^{k-1}(1-p) \qquad (28)$$

where $k = 1, 2, \cdots$. We define $t_{i(i+1)}$ to be average waiting time,

$$t_{i(i+1)} = \sum_{k=1}^{\infty} \frac{k}{\mu} \cdot p^{k-1}(1-p) = \frac{1}{\mu(1-p)} \qquad (29)$$

for $i = 1, 2, \cdots, n-1$. Also, for the trivial case $i = n$, $t_{ii} = t_{nn} = 0$. Thus, before a PRI is sent, the waiting time for each PHI in the PRI buffer is

$$T_i = \begin{cases} \dfrac{n-i}{\mu(1-p)}, & i = 1, 2, \cdots, n-1; \\ 0, & i = n. \end{cases} \qquad (30)$$

and the average waiting time is

$$\begin{aligned} \sum_{i=1}^{n} \frac{1}{n} T_i &= \frac{1}{n} \cdot \frac{1}{\mu(1-p)} \cdot (1 + 2 + \cdots + (n-1)) \\ &= \frac{1}{n} \cdot \frac{1}{\mu(1-p)} \cdot \frac{n(n-1)}{2} \\ &= \frac{n-1}{2\mu(1-p)} \end{aligned} \qquad (31)$$

Subsequently, we can calculate the transmission delay t_d of SAGE at eHealth center is

$$t_d = \frac{2-\rho}{2\mu(1-\rho)} + \frac{n-1}{2\mu(1-p)} + t_s + t_v, \qquad \rho = \frac{\lambda}{\mu} < 1 \quad (32)$$

Fixing the parameters n and p, Fig. 9 shows the transmission delay t_d varies with the average arrival rate λ, where $1 \leq \lambda \leq 120$. As seen in Fig. 9, the transmission delay t_d rises with the increase of λ on the whole. For the same λ, the transmission delay t_d with pairing precomputation is less than that without pairing precomputation. This result indicates that the transmission delay could be reduced when the performance of DP is improved. In addition, from Fig. 9, we can also roughly observe the relation between t_d and p, n, i.e., with the increase of p and n, the transmission delay t_d will also increase.

TABLE II
TIME COSTS OF REQUIRED OPERATIONS

Operation	Rough Estimated Time	
PHI authentication	6.7 ms *	3.0 ms **
PIR signing (t_s)	5.8 ms	
PIR verification (t_v)	16.3 ms *	8.9 ms **

* w/o pairing precomput., ** with pairing precomput.

To further discuss the relation subtly, we plot t_d varies with p and n in Fig. 10, where λ is fixed as 120. It can be seen that for small p, the transmission delay increases very slow with n. However, for large p, the transmission delay increases quickly. This indicates that the parameter p due to the replaying attack and forging attack is the dominant factor for the transmission delay. Therefore, for small p, the proposed scheme can gain a good performance in terms of transmission delay. In addition, the difference between Fig. 10(a) and Fig. 10(b) also demonstrates that the precomputation can reduce the transmission delay.

VII. CONCLUSIONS

Patient privacy is crucial to the success and full flourish of the eHealth systems. In this paper, we have studied the capabilities of different adversaries, and proposed a strong privacy-preserving Scheme Against Global Eavesdropping for eHealth systems. Formal security proofs show the SAGE can achieve not only the content oriented privacy but also the contextual privacy under the strong global adversary model. In addition, through the extensive performance evaluation, the

SAGE has been demonstrated efficient in terms of transmission delay. Our future work will focus on investigating the relation between patient mobility and privacy under the strong global eavesdropping.

REFERENCES

[1] U. Varshney, "Pervasive healthcare and wireless health monitoring", *Mobile Networks and Applications*, Vol. 12, No. 2-3, pp. 113-127, 2007.

[2] L. Gatzoulis and I. Iakovidis, "Wearable and portable eHealth systems", *IEEE Eng. Med. Biol. Mag.*, Vol. 26, No. 5, pp. 51-56, 2007.

[3] I. Iakovidis, "Towards personal health record: Current situation, obstacles and trends in implementation of electronic healthcare records in Europe", *International Journal of Medical Informatics*, Vol. 52, No. 1, pp. 105-115, 1998.

[4] Y. Xiao, X. Shen, B. Sun, and L. Cai, "Security and privacy in rfid and applications in telemedicine", *IEEE Commun. Mag.*, Vol. 44, No. 4, pp. 64-72, 2006.

[5] C. Dong and N. Dulay, "Privacy preserving trust negotiation for pervasive healthcare", in *Proc. 1st International Conference on Pervasive Computing Technologies for Healthcare - PervasiveHealth 2006*, Inssbruck, Austria, Nov.-Dec. 2006.

[6] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology", in *Proc. 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society* , pp. 5053-5058, New York, US, Aug. 2006.

[7] K.K. Venkatasubramanian and S.K.S. Gupta, "Security for pervasive health monitoring sensor applications", in *Proc. 4th International Conference on Intelligent Sensing and Information Processing 2006 - ICISIP 2006*, pp. 197-202, Bangalore, India, Dec. 2006.

[8] K.K. Venkatasubramanian and S.K.S. Gupta, "Security Solutions for Pervasive Healthcare", in *Security in distributed, grid, mobile, and pervasive computing, eds Yang Xiao*, pp. 443-464, Auerbach Publications, CRC Press, 2007.

[9] D. Halperin, T.S. Heydt-Benjamin, K. Fu, T. Kohno, and W.H. Maisel, "Security and privacy for implantable medical devices", *Pervasive Computing*, Vol. 7, No. 1, pp. 30-39, 2008.

[10] R.G. Lee, K.C. Chen, C.C. Hsiao, and C.L. Tseng, "A mobile care system with alert mechanism", *IEEE Trans. Inform. Technol. Biomed.*, Vol. 11, No. 5, pp. 507-517, 2007.

[11] Health Insurance Portability Accountability Act (HIPAA).

[12] E. Villalba, M.T. Arredondo, S. Guillen, and E. Hoyo-Barbolla, "A new solution for a heart failure monitoring system based on wearable and information technologies", in *Proc. International Workshop on Wearable and Implantable Body Sensor Networks 2006 - BSN 2006*, Cambridge, Massachusetts, US, Apr. 2006.

[13] O. Aziz, B. Lo, R. King, A. Darzi, and G.Z. Yang, "Pervasive body sensor network: an approach to monitoring the post-operative surgical patient", in *Proc. International Workshop on Wearable and Implantable Body Sensor Networks 2006 - BSN 2006*, Cambridge, Massachusetts, US, Apr. 2006.

[14] C. Linti, H. Horter, P. Osterreicher, H. Planck, "Sensory baby vest for the monitoring of infants", in *Proc. International Workshop on Wearable and Implantable Body Sensor Networks 2006 - BSN 2006*, Cambridge, Massachusetts, US, Apr. 2006.

[15] J. Espina, T. Falck, J. Muehlsteff, and X. Aubert, "Wireless body sensor network for continuous cuff-less blood pressure monitoring", in *Proc. 3rd IEEE-EMBS Internation Summer School and Symposium on Medical Devices and Biosensors*, MIT, Boston, US, Sept. 2006.

[16] S.D. Bao and Y.T. Zhang, "A new symmetric cryptosystem of body area sensor networks for telemedicine", in *Proc. 6th Asian-Pacific Conference on Medical and Biological Engineering*, Japan, Apr. 2005.

[17] S.D. Bao, Y.T. Zhang, and L.F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems", in *Proc. 27th IEEE Conference on Engineering in Medicine and Biology*, pp. 2455-2458, Shanghai, China, Sept. 2005.

[18] K. Tan, F. Jiang, Q. Zhang, and X. Shen, "Congestion control in multihop wireless networks", *IEEE Trans. Veh. Technol.*, Vol. 56, No. 2, pp. 863-873, July 2007.

[19] C. Zhang, R. Lu, X. Lin, P.H. Ho and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks", in *Proc. IEEE INFOCOM'08*, Phoenix, AZ, USA, April 14-18, 2008.

[20] R. Lu and Z. Cao, "Efficient remote user authentication scheme using smart card", *Computer Networks*, Vol. 49, No. 4, pp. 535-540, 2005.

[21] A. Serjantov and S.J. Murdoch, "Message splitting against the partial adversary", in *5th International Workshop on Privacy Enhancing Technologies - PET 2005*, LNCS 3856, pp. 26-39, Springer-Verlag, 2006.

[22] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing", in *Proc. 25th IEEE International Conference on Distributed Computing Systems - ICDCS 2005*, Columbus, Ohio, USA, June 2005, pp. 599-608.

[23] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper", in *Proc. IEEE International Conference on Network Protocols, 2007 - ICNP 2007*, Beijing, China, 2007, pp. 314-323.

[24] W. Mao, *Modern Cryptography: Theory and Practice*, Prentice Hall PTR, 2003.

[25] D. Chaum, "Untraceable electronic mail, return addresses and digital pseudonyms", *Communications of the A.C.M.*, Vol. 24, No. 2, pp. 84-88, February 1981.

[26] D. Chaum, "The dining cryptographers problem: unconditional sender and recipient untraceability", *J. Cryptology*, Vol. 1, No. 1, pp. 65-75, 1988.

[27] A. Pfitzmann and M. Waidner, "Networks without user observability, design options", *Computers & Security*, Vol. 6, No. 2, pp. 158-166, 1987.

[28] A. Jerichow, J. Müller, A. Pfitzmann, B. Pfitzmann, and M. Waidner, "Real-time mixes: a bandwidth-efficient anonymity protocol", *IEEE J. Sel. Areas Commun.*, Vol. 16, No. 4, pp. 495-509, 1998.

[29] D. Kesdogan, J. Egner, and R. Büschkes, "Stop-and-go mixes providing probabilistic security in an open system", in *Prof. of Second International Workshop on Information Hiding*, LNCS 1525, pp. 213-229, Springer-Verlag, 1998.

[30] O. Berthold, H. Federrath, and S. Köpsell, "Web mixes: a system for anonymous and unobservable internet access", in *Proc. International Workshop on Design Issues in Anonymity and Unobservability*, LNCS 2009, pp. 115-129, Springer-Verlag, 2001.

[31] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping adversaries for source protection in sensor networks", in *Proc. International Symposium on on Word of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 23 -24, June 2006.

[32] C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smit, "Parametric probabilistic sensor network routing," in *Proc. 2nd ACM international conference on Wireless sensor networks and applications*, San Diego, CA, USA, 2003, pp. 122 - 131.

[33] Z. Cheng and W. Heinzelman, "Flooding strategy for target discovery in wireless networks," in *Proc. 6th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems (MSWiM 2003)*, San Diego, CA, USA, 2003, pp. 33 - 41.

[34] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proc. Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networks (MobiCOM)*, Boston, MA, USA, August 2000, pp. 56 - 67.

[35] H. Lim and C. Kim, "Flooding in wireless ad-hoc networks", *Computer Communications*, Vol. 24, No. 3. pp. 353-363, February 2001.

[36] B. Karp and H.T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proc. Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networks (MobiCOM)*, Boston, MA, USA, August 2000, pp. 243-254.

[37] D. Niculescu and B. Nath, "Trajectory based forwarding and its applications," in *Proc. Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networks (MobiCOM)*, San Diego, CA, USA, September 2003, pp. 260-272.

[38] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks", *Proc. IEEE INFOCOM 2007*, Anchorage, Alaska, USA, May 2007.

[39] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", in *Advances in Cryptology - CRYPTO 2001*, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[40] R. Lu, Z. Cao, and R. Su, "A self-encryption remote user anonymous authentication scheme using smart cards", *J. Shanghai Jiaotong University (Science)*, Vol. E-11, No. 2, pp. 210-214, 2006.

[41] J. Cha and J. Cheon, "An identity-based signature from gap diffie-hellman groups", in *Prof. Practice and Theory in Public Key Cryptography – PKC'2003*, LNCS 21392567 pp. 18-30, Springer-Verlag, 2003.

[42] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols", in *Proc. 1st ACM conference on Computer and Communications Security (CCS) 1993*, Fairfax, Virginia, USA, November 1993, pp. 62-73.

[43] V. Shoup, "OAEP reconsidered", *J.Cryptology*, Vol. 15, No. 4, pp. 223-249, 2002.

[44] J. Coron, "On the exact security of full domain hash", in *Advances in Cryptology - CRYPTO 2000*, LNCS 1880, pp. 229 - 235, Springer-Verlag, 2000.

[45] M. Scott, "Efficient implementation of crytographic pairings," [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/ Slides/Thursday/mscott-samos07.pdf
[46] D. Gross and C.M. Harris, *Fundamentals of Queueing Theory*, Wiley, 1998.

Xiaodong Lin (S'07-M'09) received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently an Assistant Professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada. His research interests include wireless network security, applied cryptography, computer forensics, and anomaly-based intrusion detection. Dr. Lin was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Award of the IEEE International Conference on Communications (ICC'07) - Computer and Communications Security Symposium.

Rongxing Lu is currently working toward the Ph.D degree with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada. He is currently a Research Assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

Xuemin (Sherman) Shen (M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a University Research Chair Professor, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on mobility and resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks. He is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen serves as the Tutorial Chair for IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for IEEE Transactions on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; KICS/IEEE Journal of Communications and Networks, Computer Networks; ACM/Wireless Networks; and Wireless Communications and Mobile Computing (Wiley), etc. He has also served as Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada.

Yoshiaki Nemoto (SM'05) received his B.E., M.E., and Ph.D. degrees from Tohoku University in1968, 1970, and 1973, respectively. He was a full professor with the Graduate School of Information Sciences until 2008. Currently he is serving as the senior vice president of Tohoku University. He has been engaged in research work on micro wave networks, communication systems, computer network systems, image processing, and handwritten character recognition. He is a co-recipient of the 1982 Microwave Prize from the IEEE MTT society, the 2005 Distinguished Contributions to Satellite Communications award from IEEE ComSoc society, FUNAI information Science Award 2007 and several prestigious awards from Japanese Ministries. He is a senior member of IEEE, and a fellow member of IEICE and IPSJ.

Nei Kato (SM'05) received his M.S. and Ph.D. Degrees from Tohoku University, Japan, in 1988 and 1991, respectively. He has been working with Tohoku University since then and is currently a full professor at the Graduate School of Information Sciences. He has been engaged in research on computer networking, wireless mobile communications, image processing and neural networks. He has published more than 130 papers in journals and peer-reviewed conference proceedings. Nei Kato has served as a symposium co-chair for GLOBECOM'07 and ChinaCom'08, and TPC member for a large number of IEEE international conferences, including ICC, GLOBECOM, WCNC and HPSR. He is a technical editor of IEEE Wireless Communications from 2006, an editor of IEEE Transactions on Wireless Communications from 2008, a co-guest-editor for IEEE Wireless Communications Magazine SI on "Wireless Communications for E-healthcare". He is a co-recipient of the 2005 Distinguished Contributions to Satellite Communications Award from the IEEE Communications Society, Satellite and Space Communications Technical Committee, the co-recipient of FUNAI information Science Award, 2007, and the co-recipient of 2008 TELCOM System Technology Award from Foundation for Electrical Communications diffusion. He is serving as an expert member of Telecommunications Council, Ministry of Internal Affairs and Communications, Japan. Nei Kato is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and a senior member of IEEE.