Scientific Research Publishing

Journal of Information Security, 2017, 8, 75-90
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Authenticated Privacy Preserving Pairing-Based Scheme for Remote Health Monitoring Systems

Kambombo Mtonga[1], Eun Jun Yoon[2], Hyun Sung Kim[2]

[1]Mathematical Sciences Department, University of Malawi-Chancellor College, Zomba, Malawi
[2]Department of Cyber Security, Kyungil University, Daegu, South Korea
Email: kmtonga@cc.ac.mw, Name2@xyz.org

How to cite this paper: Mtonga, K., Yoon, E.J. and Kim, H.S. (2017) Authenticated Privacy Preserving Pairing-Based Scheme for Remote Health Monitoring Systems. *Journal of Information Security*, **8**, 75-90.
http://dx.doi.org/10.4236/jis.2017.81006

Received: November 21, 2016
Accepted: January 14, 2017
Published: January 17, 2017

Abstract

The digitization of patient health information has brought many benefits and challenges for both the patients and physicians. However, security and privacy preservation have remained important challenges for remote health monitoring systems. Since a patient's health information is sensitive and the communication channel (*i.e.* the Internet) is insecure, it is important to protect them against unauthorized entities. Otherwise, failure to do so will not only lead to compromise of a patient's privacy, but will also put his/her life at risk. How to provide for confidentiality, patient anonymity and un-traceability, access control to a patient's health information and even key exchange between a patient and her physician are critical issues that need to be addressed if a wider adoption of remote health monitoring systems is to be realized. This paper proposes an authenticated privacy preserving pairing-based scheme for remote health monitoring systems. The scheme is based on the concepts of bilinear paring, identity-based cryptography and non-interactive identity-based key agreement protocol. The scheme also incorporates an efficient batch signature verification scheme to reduce computation cost during multiple simultaneous signature verifications.

Keywords

Remote Healthcare, Bilinear Pairing, Privacy Preservation, Mutual Authentication, ID-Based Cryptography

1. Introduction

The traditional healthcare systems are plagued by many problems and challenges. These problems and challenges include: diagnoses being written illegibly on paper,

physicians not being able to easily access patient health information (PHI), and limitations on time, space, and personnel for monitoring patients. Similarly, the current health care systems—structured and optimized for reacting to crisis and managing illness—are facing new challenges: a rapidly growing population of elderly and rising healthcare spending [1] [2]. As more and more people enter an elder age, the risk of developing certain chronic and debilitating diseases is significantly higher [3] [4]. Furthermore, if aged populations prefer to live alone they do require long-term monitoring for better independent life [5]. Clearly, innovative strategies are needed to tackle the existing problems and to cater to the healthcare needs of an aging population in addition to sustaining the trend towards an independent lifestyle focusing on personalized non-hospital based care [6]. With recent advancements in telecommunication technology however, opportunities exist to improve the current state of the healthcare systems to minimize some of these problems and provide more personalized service [7] [8].

The recent technological advances in sensors, low-power integrated circuits, and wireless communications have enabled the design of low-cost, miniature, lightweight, and intelligent physiological sensor nodes. These sensors capable of sensing, processing, and communicating one or more vital signs, can be seamlessly integrated into wireless personal or body area networks (WPANs or WBANs) for health monitoring [9]. A WBAN contains a number of portable, miniaturized, and autonomous sensor nodes (in-body or/and on-body nodes) that monitors patients under natural physiological states without constraining their normal activities. The gateway (e.g. PC or mobile phone) of the WBAN is responsible for data collection, processing and overall WBAN management. These networks promise to revolutionize healthcare by allowing inexpensive, non-invasive continuous health monitoring with almost real-time updates of medical records via the Internet. Remote health monitoring systems typically collect patient readings and then transmit them to a remote server for storage and later examination by the healthcare professionals. However, the different usage scenarios of remote health monitoring systems ranging from pre-hospital, in-hospital, ambulatory and in-home monitoring have resulted in diverse security and privacy concerns [10] [11]. Also, due to the sensitive nature of some of the remotely electronically collected PHI combined with the insecure nature of the communication channels, there is need to prevent unauthorized access to and use of the PHI by both active and passive adversaries. Otherwise, failure to do so will not only put a patient's privacy in jeopardy, but also her life will be at risk. Hence there is need for new schemes to protect against privacy violation in remote health monitoring environments.

Many security protocols to enhance privacy and security in remote health monitoring systems have been put forward by researchers. Huang *et al.* [12] proposed an identity-based authentication and context privacy preservation scheme in wireless health monitoring system. They adopted identity-based encryption to protect the confidentiality of PHI. However, Huang *et al.*'s scheme does not achieve patient identity privacy and is also prone to password guessing

attacks on the physician's side [13]. Layouni *et al.* [14] proposed a privacy protection protocol for remote monitoring of medical care. They applied symmetric encryption and RSA algorithm to complete the encryption and authentication for PHI. Hasque *et al.* [15] proposed a secure u-healthcare sensor networks using public key based scheme. In their scheme, they adopted asymmetric encryption for confidentiality protection. Yang *et al.* [16] presented a password-based authentication scheme for healthcare delivery systems. The rationale behind their scheme is to allow patients to authenticate to healthcare providers using long-term short passwords. Sadly, password-based authentication systems are vulnerable to dictionary attacks. The U.S. government has also established stringent regulations to ensure that the security and privacy of PHI is properly protected [17]. Clearly, the issues of patient identity and data privacy have not been fully explored in the existing literature.

In this paper an authenticated privacy preserving paring-based scheme for wireless health monitoring systems is proposed. The proposed scheme consists of three parties (see **Figure 1** below), namely; the gateway of patient WBAN, the Electronic Health Record (EHR) database in Health Monitoring Server (HMS) and the physician. In the proposed scheme, all communications between the gateway and EHR, EHR and physician and physician with gateway are carried out over an insecure channel (*i.e.* the Internet). The HMS plays the role of the registration server and system parameter generator (or trusted authority) while the EHR acts as the authentication server. Identity-based cryptography (IBC) encryption is adopted to ensure the secure transmission, receiving, storing and access of PHI. This ensures integrity of PHI which in turn is crucial for accurate diagnoses of a patient by her respective physician. The scheme allows the patient and her physician to establish a secure communication channel via an established session key shared only between the two parties. This is possible because of the concept of non-interactive identity-based key agreement adopted. The analysis will show that the scheme provides confidentiality of a patient's health information, explicit mutual authentication between the patient and her physician, patient anonymity and un-traceability, patient revocation, session key secrecy and resistance against replay attacks.

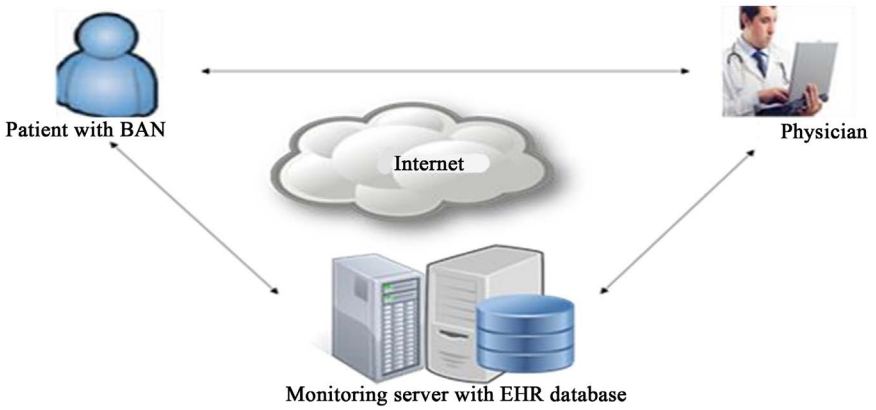

Figure 1. System environment.

The rest of the paper is organized as follows: in Section 2, we describe some of the preliminary work and notations that are used throughout this paper. In Section 3, a discussion of the proposed scheme including system initialization, Registration of parties and health information transfer is presented. Section 4, presents an analysis that proves that our scheme is efficient and that it achieves many desirable security and privacy preserving properties. Section 5 shows that the proposed scheme has a better performance than Huang *et al.* and Layouni *et al.*'s schemes by providing a comparison among the three. Finally, a conclusion is presented in Section 6.

2. Preliminaries

This section briefly reviews bilinear pairings, the Bilinear Diffie-Hellman problem and the original non-interactive identity-based key agreement protocol. Further, the threat model and notations used throughout the remainder of the paper are introduced.

2.1. Notations

Table 1 below presents the notations used throughout the remainder of the paper.

Table 1. Notations.

Notation	Meaning
PT_i	Patient i
D_l	Physician l *i.e.* doctor or nurse
s	Master secret key for TA
P_{pub}	System public key
d_x	Private key for entity x
Q_x	Public key for entity x
id_x	Identity for entity x
$PIDPT_i$	Set of pseudo-IDs for PT_i
pid_j	j^{th} pseudo-ID for PT_i
$PUBPT_i$	Set of public keys for PT_i
$PRIPT_i$	Set of private keys for PT_i
$SKi\text{-}l$	Session key shared between PT_i and D_l
$H_1(\cdot)$	Hash function; $H_1 : \{0,1\}^* \to G_1$
$H_2(\cdot)$	Hash function; $H_2 : \{0,1\}^* \to Z_q^*$
T_x	Time stamp generated by entity x
$\hat{e}$	Bilinear map; $\hat{e} : G_1 * G_1 \to G_2$
$\|\|$	Concatenation

2.2. Bilinearity

Let G_1 be an additive group of prime order q and G_2 be a multiplicative cyclic group of the same order. In reality, G_1 is a subgroup of points on an elliptic curve over Z_q^* and G_2 is a subgroup of the multiplicative group of a finite field Z_{qk}^* for some $k \in Z_q^*$. Let P denote a generator of G_1. Then, there exists an efficient computable bilinear map $\hat{e}: G_1 * G_1 \to G_2$ which has the following properties [18]:

- *Bilinearity*: Given P and Q in G_1 and $a, b \in_R Z_q^*$, we have $\hat{e}(aP, bQ) = (P, Q)^{ab}$.
- *Non-degeneracy*: $\hat{e}(P, P) \neq 1_{G2}$.
- *Computability*: There exists an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$.

2.3. The Bilinear Diffie-Hellman Assumption

The Bilinear Diffie-Hellman (BDH) problem is to compute $\hat{e}(P, P)^{abc} \in G_2$ given $P \in G_1$ and elements $aP, bP, cP \in G_1$ for $a, b, c \in_R Z_q^*$. Computing such a problem is assumed to be hard on $\{G_1, G_2, \hat{e}\}$.

2.4. Computational Diffie-Hellman Problem

The CDH problem is given (P, aP, bP) for any $a, b \in Z_q^*$ and $P \in G_1$, computing abP is assumed hard.

2.5. Non-Interactive Identity-Based Key Agreement

For non-interactive identity-based key agreement protocol, central authority first generates two cyclic groups G_1 and G_2 and the bilinear map $\hat{e}: G_1 * G_1 \to G_2$ to setup the parameters for an identity-based public key system. The central authority also chooses a cryptographic collision free hash function $(\cdot)$: $\{0, 1\}^* \to G_1$. It then chooses a secret key $s \in_R Z_q^*$ and computes corresponding public key $P_{pub} = sP$, where P is a generator of G_1. Lastly it publishes public parameters $\{G_1, G_2, \hat{e}, P, P_{pub}, (\cdot)\}$. For registered party i, the central authority computes a private key $d_i = (id_i)$ and sends it via a secure channel [19] [20].

With such a setup, any two clients of the same central authority can compute shared key using only the identity of the other participant and their own private key. For two clients with identities, id_1 and id_2, the shared key is given by $SK = \hat{e}(H(id_1), H(id_2))^s$ which party id_1 computes as $SK_{1-2} = \hat{e}(d_1, H(id_2))$ and id_2 computes $SK_{2-1} = \hat{e}(d_2, H(id_1))$.

Clearly, $SK_{1-2} = SK_{2-1} = SK$.

3. Proposed Authenticated Privacy Preserving Scheme

In this section the proposed authenticated privacy preserving paring-based scheme for remote health monitoring systems is presented. The existence of a properly setup and functioning patient WBAN with the gateway of the WBAN responsible for collecting data from the biosensors and analyzing it is *presumed*. Based on the analysis, the gateway (equipped with a wireless Ethernet adapter so

as to communicate with standard wireless router/switch) sends a summary report about the patient's condition to the health monitoring server periodically. However, in case the analysis indicates a sudden health deterioration, or a condition that requires immediate attention, it is required that the gateway automatically trigger an emergency signal and send an immediate notification to the health monitoring server so that immediate necessary action can be taken to help the patient. The scheme consists of three parties, namely; the gateway of a patient's WBAN, EHR database in HMS and the physician. Note: from here forth, we refer to a gateway of a patient's WBAN simply as patient for convenience. In the proposed scheme, the HMS plays the role of the registration server and system parameter generator (or trusted authority) while the EHR acts as the authentication server. IBC-encryption is adopted to ensure the secure transmission, receiving, storing and access of PHI. This ensures integrity of PHI which in turn is crucial for accurate diagnoses of a patient by her respective physician. To achieve patient anonymity and un-traceability, privacy preserving technique based on pseudonyms is adopted. These pseudonyms are issued to the patient via a smartcard by trusted authority upon successful registration.

To aid authentication of patients and physicians by EHR, both patients and physicians are required to attach a signature to the message sent to EHR which can be successfully validated by EHR. To reduce computation overhead for EHR during signature validation process, an efficient batch signature verification scheme in which the EHR can simultaneously verify multiple received signatures is adopted [21]. The proposed scheme allows the patient and her physician to establish a secure communication channel via an established session key shared only between the two parties. This is possible because of the concept of non-interactive identity-based key agreement which has been adopted. The scheme also allows revocation of patients. This means that in cases of death, service subscription expiration period or upon request by the patient, the trusted authority can easily terminate service provision to the particular patient. The scheme consists of three main phases: system initialization, registration and health information exchange among patient, EHR and physician. First, a discussion of the threat model followed by a summary of notations and then we discuss the phases of our scheme.

3.1. Privacy Preserving Properties of the Scheme

There are many threats to a patient's privacy and security in remote health monitoring systems. Some of these threats include: data breach by insiders (*i.e.* authorized EHR users or staff of the EHR organization), insider curiosity, accidental disclosure and unauthorized intrusion of network system by outsiders (*i.e.* third parties who act without authorization e.g. hackers) [22]. The aim of the proposed scheme is to enhance patient data and identity privacy against both insiders and outsiders. Below is a brief discussion of some of the security and privacy properties of the scheme and why they are important to a patient's data security and identity privacy in remote health monitoring systems.

3.1.1. Confidentiality

In remote health monitoring systems, the disclosure of PHI to unauthorized persons is a serious security and privacy threat. This is because some of PHI can be sensitive. Hence once accessed, such data can be subjected to different misdemeanors such as fraudulent insurance claims by adversaries. In recent past there have been incidents where PHI was disclosed to external parties [23] [24].

3.1.2. Anonymity and Untraceability

Among common privacy requirements, identity and location privacy, *i.e.* preventing unauthorized parties from learning one's identity and current or past locations, are of paramount importance [25] [26] [27]. The recent expansion of electronic and mobile healthcare systems has resulted in an increased demand for patient anonymity. This is because adversaries are now more capable of breaching network systems and achieve unauthorized access to PHI. For example, hackers may intrude into a hospital's network to access PHI or render the system inoperable. Hence patient anonymity and un-traceability would prove vital in such scenarios.

3.2. System Initialization

Similar to other identity-based schemes, the proposed one also requires a private key generator (PKG). In the proposed scheme HMS acts as PKG. To initialize the system, HMS runs the following steps. Let G_1 be an additive cyclic group of prime order q, and G_2 be multiplicative cyclic group of same order. Let $\hat{e}: G_1 * G_1 \to G_2$ be a bilinear map and P be an arbitrary generator of G_1. HMS then chooses a random number $s \in_R Z_q^*$ as the master secret key and computes the public key $P_{\text{pub}} = sP$. It also chooses two secure collision free cryptographic hash functions $H_1(\cdot): \{0,1\}^* \to G_1$ and $H_2(\cdot): \{0,1\}^* \to Z_q^*$. It further computes the public key $Q_{\text{EHR}} = H_1(id_{\text{EHR}})$ and corresponding private key $d_{\text{EHR}} = sH_1(id_{\text{EHR}})$ for EHR. The key pair $\{Q_{\text{EHR}}, d_{\text{EHR}}\}$ is then sent to EHR via a secure channel (e.g. Transport Layer Security Protocol). HMS then publishes the public system parameters as $\{G_1, G_2, \hat{e}, q, P, P_{\text{pub}}, H_1(\cdot), H_2(\cdot)\}$ and keeps the master secret key s, secret.

3.3. Registration

In this section, the registration process of involved parties in the system is discussed. All registrations are carried out by the HMS via a secure channel (see **Figure 2**).

3.3.1. Physician Registration

To register, D_l (doctor/nurse) submits her identity id_{DL} (e.g. an email address or social security number) to HMS. HMS first validates the submitted identity and if validation is successful it then computes the public key $Q_{Dl} = H_1(id_{Dl})$ and corresponding private key $d_{Dl} = sH_1(id_{Dl})$ for D_l. The HMS then sends $\{Q_{Dl}, d_{Dl}\}$ to D_l via a secure channel.

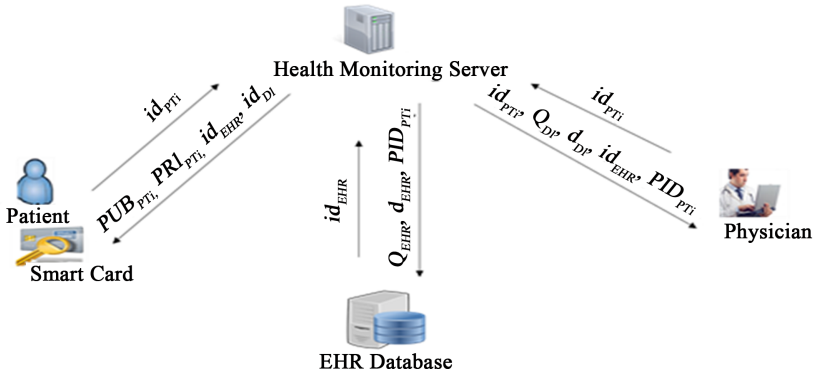

Figure 2. Registration process.

3.3.2. Patient Registration

Let PT_i be a patient seeking medical help from D_l. To register, PT_i submits her real-ID id_{PTi} to HMS. HMS first validates submitted identity. If the validation is successful, HMS then chooses a family of n un-linkable pseudo-IDs for PT_i given by:

$$PID_{PTi} = \left\{ pid_0, \cdots, pid_j, pid_{j+1}, \cdots, pid_{n-1} \right\}. \quad (1)$$

For each pseudo-ID pid_j in PID_{PTi}, HMS computes the public key $Q_j = H_1\left(pid_j\right)$ and the corresponding private key $d_j = sH_1\left(pid_j\right)$, such that the families of public and private keys are:

$$PUB_{PTi} = \left\{ Q_0, \cdots, Q_{j-1}, Q_j, Q_{j+1}, \cdots, Q_{n-1} \right\}. \quad (2)$$

$$PRI_{PTi} = \left\{ d_0, \cdots, d_{j-1}, d_j, d_{j-1}, \cdots, d_{n-1} \right\}. \quad (3)$$

Once PT_i completes registration procedures, the HMS issues her with a smartcard. The smartcard is personalized with parameters (*i.e.* PID_{PTi}, PUB_{PTi}, PRI_{PTi}, id_{DL}, id_{EHR}) which P can later use to register her gateway to the HMS. Upon arrival at home, PT_i passes over the information in the smartcard to the gateway. Since some of the information is sensitive, an assumption is made that, once the gateway gets the parameters, it should erase the information from the memory of the smartcard to avoid security implications that may result in case the smartcard ends up in the hands of an adversary.

With these pseudo-IDs, PT_i can constantly change her pseudo-IDs to achieve anonymity and un-traceability during communication process over the remote health monitoring system. The HMS also sends PID_{PTi} to appropriate D_l and EHR respectively.

To allow for revocation, the HMS adds an ExpiryDate into pid_j for $0 \le j \le n-1$, such that each of the public keys $Q_j = H_1\left(pid_j\right)$ is valid only before the specified expiry time t_j. After the specified time, the corresponding private key $d_j = sH_1\left(pid_j\right)$ is revoked automatically. Let $\left\{ t_0, t_1, \cdots, t_{j-1}, t_j, t_{j+1}, \cdots, t_{n-1} \right\}$ be the set of life spans for each of the pid_j for $0 \le j \le n-1$, such that $t_j = t_{j-1} + \Delta t$, where Δt is a constant value for all pseudo-IDs, meaning that the length of the life span for each of the private keys is the same. Further, suppose that PT_i can only use the pseudo-ID sd_j, $0 \le j \le n-1$ sequentially (*i.e.* that pid_{j+1} can only be used after pid_j has expired). This allows D_l to request for specific patient health

data from EHR. This is possible because D_l is also issued with PT_i's pseudo-IDs, hence making it easy for him/her to know which of the pseudo-IDs has expired or which one is the current pid_j in the sequence of PT_i's pseudo IDs.

Note: according to [14], a system is said to preserve pseudonimity if data records sent by the patient to the health monitoring server are linkable to each other but not to the patient's real-ID. In the proposed scheme a patient's pseudo IDs are assumed to be un-linkable. In this case an assumption is that the system uses other mechanisms for achieving pseudonimity and not a patient's pseudo-IDs. But since there may be need to reveal a patient's real-ID in cases of apparent abuse of conditions of service via judicial procedure, the proposed scheme assumes that only HMS (trusted authority) should know the relationship between the pseudo-IDs and the real-ID of the patient. As such the scheme can provide conditional privacy for the patient.

3.4. Health Information Transfer

Below the following are discussed: 1) patient health information transfer to EHR, 2) patient authentication, health information receiving and storing by the EHR and 3) patient health information request and recovery by the physician (see Figure 3).

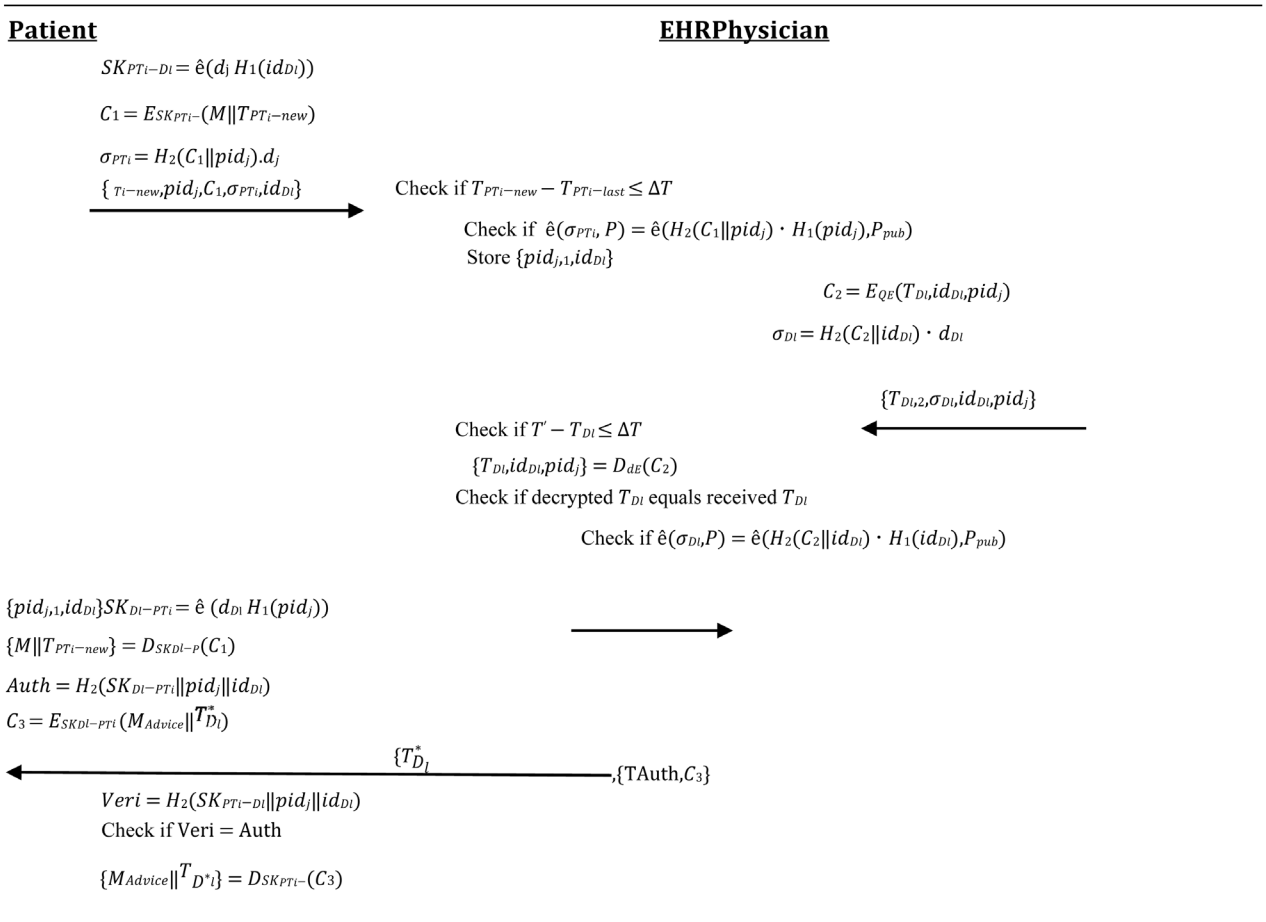

Figure 3. Message exchange among patient, EHR and physician.

3.4.1. Patient Health Information Transfer to HER

To send health information to EHR, PT_i carries out the following steps:

- Picks an unused valid pseudo-ID pid_j and the corresponding private key d_j.
- Using this private key, PT_i computes a session key $SK_{PTi-Dl} = \hat{e}\left(d_j, H_1\left(id_{Dl}\right)\right) = \hat{e}\left(Q_j, Q_{Dl}\right)^s$. This key will be used to encrypt the health information and establish a secure channel with D_l.
- Using SK_{PTi-Dl}, the PT_i performs IBC-encryption on the health data as $C_1 = E_{SKPTi} - \left(M \| T_{PTi-\text{new}}\right)$, where M is the PHI and $T_{PTi-\text{new}}$ is current timestamp. $T_{PTi-\text{new}}$ is added to counter replay attacks. PT_i then computes the signature $\sigma_{PTi} = H_2\left(C_1 \| pid_j\right) d_j$ on C_1.
- Finally PT_i sends the message $\left\{T_{PTi-\text{new}}, pid_j, C_1, \sigma_{PTi}, id_{Dl}\right\}$ to EHR.

3.4.2. Patient Authentication, Health Information Receiving and Storage by HER

When EHR receives the message $\left\{T_{PTi-\text{new}}, pid_j, C_1, \sigma_{PTi}, id_{Dl}\right\}$ from PT_i, it carries out the following authentication steps:

- Checks if the timestamp $T_{PTi-\text{new}}$ satisfies the inequality $T_{PTi-\text{last}} - T_{PTi-\text{new}} \le \Delta T$, where $T_{PTi-\text{last}}$ is last time of message receipt by EHR and ΔT is fixed time interval between successive health information collections. This could help to counter replay attack attempts. If successful, it proceeds to examine *piryDate* included in pid_j to verify the service expiration time.
- Using public parameters and received values, EHR checks the validity of the signature by computing $\hat{e}\left(\sigma_{PTi}, P\right) = \hat{e}\left(H_2\left(C_1 \| pid_j\right) \cdot H_1\left(pid_j\right), P_{pub}\right)$. The equation is valid because:

$$\begin{aligned}\hat{e}\left(\sigma_{PTi}, P\right) &= \hat{e}\left(H_2\left(C_1 \| pid_j\right) \cdot d_j, P\right) \\ &= \hat{e}\left(H_2\left(C_1 \| pid_j\right) \cdot sH_1\left(pid_j\right), P\right) \\ &= \hat{e}\left(H_2\left(C_1 \| pid_j\right) \cdot H_1\left(pid_j\right), sP\right) \\ &= \hat{e}\left(H_2\left(C_1 \| pid_j\right) \cdot H_1\left(pid_j\right), P_{pub}\right).\end{aligned}$$

Once the above steps are satisfied, EHR accepts the message as authentic and stores the necessary message components (see Table 2). EHR can then either notify the respective D_l of the received PHI or may wait for a message request from D_l.

3.4.3. Health Information Access by Physician

To access a patient's health information, D_l first gets herself authenticated to EHR by carrying out the following steps:

Table 2. Patient health information storing by EHR.

Patient ID	*PHI*	*Physician ID*
pid_j	C_1	*idDl*
:	:	:

- Using HER's public key, D_l carries out IBC-encryption as, $C_2 = E_{QEHR}\left(T_{Dl}, id_{Dl}, pid_j\right)$ and computes the signature $\sigma_{Dl} = H_2\left(C_2 \| id_{Dl}\right) \cdot d_{Dl}$. Since D_l is aware that each of the patient's pseudo-IDs has an expiry date and that they are used sequentially, when choosing pid_j, D_l chooses the one that is valid and current. Hence D_l can request for specific patient health information from *EHR* depending on the specified pid_j.
- The D_l then sends $\left\{T_{Dl}, C_2, \sigma_{Dl}, id_{Dl}, pid_j\right\}$ as request for a patient's health information.
- Once EHR receives the message $\left\{T_{Dl}, C_2, \sigma_{Dl}, id_{Dl}, pid_j\right\}$ from D_l, it carries out the following steps to authenticate the request before responding.
- Checks if the timestamp T_{Dl} satisfies the inequality $T' - T_{Dl} \le \Delta T$, where T' is the time of arrival of the request and ΔT is fixed tolerated transmission delay. This can also help in countering replay attacks.
- Applies IBC-decryption as, $\left\{T_{Dl}, id_{HPl}, pid_j\right\} = D_{dE}\left(C_2\right)$. Using id_{DL} and public parameters, *EHR* validates the received signature by computing $\hat{e}\left(\sigma_{Dl}, P\right) = \hat{e}\left(H_2\left(C_2 \| id_{Dl}\right) \cdot H_1\left(id_{Dl}\right), P_{pub}\right)$. Here;

$$\begin{aligned}\hat{e}\left(\sigma_{Dl}, P\right) &= \hat{e}\left(H_2\left(C_2 \| id_{Dl}\right) \cdot d_{Dl}, P\right)\\ &= \hat{e}\left(H_2\left(C_2 \| id_{Dl}\right) \cdot sH_1\left(id_{Dl}\right), P\right)\\ &= \hat{e}\left(H_2\left(C_2 \| id_{Dl}\right) \cdot H_1\left(id_{Dl}\right), sP\right)\\ &= \hat{e}\left(H_2\left(C_2 \| id_{Dl}\right) \cdot H_1\left(id_{Dl}\right), P_{pub}\right).\end{aligned}$$

- Once the above steps are satisfied, *EHR* believes that the request is authentic and forwards the message $\left\{pid_j, C_1, id_{Dl}\right\}$ to.

To recover, D_l first computes $SK_{Dl-PTi} = \hat{e}\left(d_{Dl}, H_1\left(pid_j\right)\right) = \hat{e}\left(Q_{Dl}, Q_j\right)^s$ and uses it to perform IBC-decryption

On C_1 as,

$$\left\{M \| T_{PTi-\text{new}}\right\} = D_{SKDl-PTi}\left(C_1\right).$$

Note: $SK_{Dl-PTi} = SK_{PTi-Dl}$. This is because:

$$\begin{aligned}SK_{HPl-PTi} &= \hat{e}\left(d_{Dl}, H_1\left(pid_j\right)\right)\\ &= \hat{e}\left(sH_1\left(id_{Dl}\right), H_1\left(pid_j\right)\right)\\ &= \hat{e}\left(H_1\left(id_{Dl}\right), H_1\left(pid_j\right)\right)\\ &= \hat{e}\left(H_1\left(id_{Dl}\right), sH_1\left(pid_j\right)\right)\\ &= \hat{e}\left(H_1\left(id_{Dl}\right), d_j\right)\\ &= SK_{PTi-Dl}.\end{aligned}$$

Hence D_l can now analyze M and give necessary and timely medical advice. By checking $T_{PTi-\text{new}}$, D_l is able to tell when the information was sent by the PT_i. This can help her to estimate a patient's health condition since the time the data was collected by biomedical devices. To send medical advice M_{Advice} to the PT_i

in response to the received health information M, D_l computes $\text{Auth} = H_2\left(SK_{Dl-PTi} \| pid_j \| id_{Dl}\right)$ and encrypts M_{Advice} using SK_{Dl-PTi} as, $C_3 = E_{SKDl-PTi}\left(M_{\text{Advice}} \| T_{D^*l}\right)$. D_l then sends $\left\{T_{D^*l}, \text{Auth}, C_3\right\}$ to PT_i.

Upon receiving l, $\left\{T^*_{Dl}, \text{Auth}, C_3\right\}$, PT_i first validate timestamp to overcome replay attacks. If validation is successful, PT_i proceeds to compute verification code $\text{Veri} = H_2\left(SK_{Dl-PTi} \| pid_j \| id_{Dl}\right)$ and checks if $Veri = ? \; Auth$. If the equation holds PT_i believes that the message is from legitimate D_l and that he/she has established a secure channel. This protects the patient from bogus medical advice which could be life threatening for him/her. PT_i can now decrypt C_3 using $_{PTi-Dl}$ as, $\left\{M_{\text{Advice}} \| T_{D^*l}\right\} = D_{SKPTi-Dl}\left(C_3\right)$ and act upon the medical advice.

The protocol above achieves explicit mutual authentication between PT_i and D_l. It also allows anonymous authentication for the PT_i. Furthermore, PT_i and D_l successfully establish a shared symmetric key SK_{PTi-Dl} that is used for the subsequent communication session.

4. Analysis

This section analyses desirable properties of the proposed scheme including security and privacy preserving properties. Note that other properties including patient revocation and replay attack have been analyzed in Section 4.

4.1. Batch Authentication

In the proposed scheme, the EHR verifies an appended signature to a message to ensure the authenticity of PT_i and D_l.

This means that for n distinct patients, $PT_1, PT_2, \cdots, PT_n$, the EHR receives $\sigma_{PT1}, \sigma_{PT2}, \cdots, \sigma_{PTn}$ signatures. All the signatures are valid if:

$$\hat{e}\left(\sum_{i=1}^{n} \sigma PTi, P\right) = \hat{e}\left(\sum_{i=1}^{n} H_2\left(Ci \| pidi\right) \cdot H_1\left(pidi\right), P_{pub}\right),$$

where pid_i is just j^{th} pseudo-ID for patient i. This batch verification equation holds since,

$$\begin{aligned}
\hat{e}\left(\sum_{i=1}^{n} \sigma PTi, P\right) &= \hat{e}\left(\sum_{i=1}^{n} H_2\left(Ci \| pidi\right) \cdot d_j, P\right) \\
&= \hat{e}\left(\sum_{i=1}^{n} H_2\left(Ci \| pidi\right) \cdot sH_1\left(pidi\right), P\right) \\
&= \hat{e}\left(\sum_{i=1}^{n} H_2\left(Ci \| pidi\right) \cdot H_1\left(pidi\right), sP\right) \\
&= \hat{e}\left(\sum_{i=1}^{n} H_2\left(Ci \| pidi\right) \cdot H_1\left(pidi\right), P_{pub}\right).
\end{aligned}$$

Note: the same batch verification method applies in situations where EHR receives $\sigma_{D1}, \sigma_{D2}, \cdots, \sigma_{Dn}$ signatures from n distinct physicians. In this case, all the signatures are valid if;

$$\hat{e}\left(\sum_{l=1}^{n} \sigma Dl, P\right) = \hat{e}\left(\sum_{l=1}^{n} H_2\left(Ci \| id_l\right) \cdot H_1\left(id_l\right), P_{pub}\right),$$

where id_l is the identity for physician l.

4.2. Patient Service Subscription Validation

To check service subscription validation for PT_i, the EHR checks signature $\sigma_{PTi} = H_2\left(C_i \| pid_i\right) \cdot d_j$ appended to the message. The signature $\sigma_{PTi} = H_2\left(C_i \| pid_i\right) \cdot d_j$ is a pseudo-ID-based signature. Without the private key $d_j = sH_1\left(pid_j\right)$, it is infeasible for third parties to forge a valid signature. This is because based on the hardness of the CDH problem in G_1, it is difficult for someone to derive the private key $sH_1(pid_j)$ given pid_j, P and P_{pub}. Hence the pseudo-ID-based signature is unforgeable and a patient's service subscription validation can be achieved.

4.3. Mutual Authentication

The patient and her physician achieves explicit mutual authentication. This is so because, when sending medical advice M_{Advice}, the physician D_l computes $\text{th} = H_2\left(SK_{Dl-PTi} \| pid_j \| id_{Dl}\right)$ and send it to PT_i together with encrypted medical advice C_3 and timestamp T_{D^*l} as part of the message $\left\{T^*_{Dl}, \text{Auth}, C_3\right\}$. The security of th depends on $SK_{Dl-PTi} = \hat{e}\left(d_{Dl}, H_1\left(pid_j\right)\right)$. Based on the BDH problem on $\{G_1, G_2, \hat{e}\}$, it is infeasible for an adversary to derive SK_{Dl-PTi} given id_{Dl}, pid_j, P and P_{pub}. Furthermore, based on the non-interactive identity-based key agreement, only whose private key is d_{Dl} and PT_i who has the private key corresponding to $H_1(pid_j)$ can share this key. Once PT_i receive $Auth$ he/she can then check whether $\text{Veri} = H_2\left(SK_{PTi-Dl} \| pid_j \| id_{Dl}\right) = \text{Auth}$ holds. Note: $Veri = Auth$ since $SK_{Dl-PTi} = SK_{PTi-Dl}$. If the equation holds, then the patient can authenticate the message and trust that it is from the right source otherwise he/she rejects the message.

4.4. Confidentiality

Confidentiality of a PHI entails ensuring that patient health information is not made available or disclosed to unauthorized parties including EHR itself. The proposed scheme achieves confidentiality against both insider and outsider adversaries. This is because the M is stored encrypted in EHR with SK_{PTi-Dl} as, $C_1 = E_{SKPTi} - \left(M \| T_{PTi-\text{new}}\right)$ and based on the BDH problem on $\{G_1, G_2, \hat{e}\}$, it is impossible for anyone else except the legit D_l to derive SK_{PTi-Dl}. The BDH problem on $\{G_1, G_2, \hat{e}\}$ is: compute $\hat{e}\left(P, P\right)^{abc} \in G_2$ with known aP, bP, cP for $a, b, c \in_R Z_q^*$, where P is generator of G_1 and $\hat{e}$ is the bilinear map. In our scheme if an adversary is to succeed in decrypting C_1, he/she must compute

$$SK_{PTi-Dl} = \hat{e}\left(d_j, H_1\left(id_{Dl}\right)\right) = \hat{e}\left(sH_1\left(pid_j\right), H_1\left(id_{Dl}\right)\right)$$

Given id_{Dl}, pid_j, P and P_{pub}. This is the same as solving the BDH. Hence our scheme satisfies the confidentiality property of PHI.

4.5. Patient Anonymity and Untraceability

In the proposed scheme, each PT_i upon successful registration receives a family of n un-linkable pseudo-IDs given by,

$$PID_{PTi} = \left\{ pid_0, pid_1, \cdots, pid_{j-1}, pid_j, pid_{j+1}, \cdots, pid_{n-1} \right\}$$

and corresponding private keys $PRI_{PTi} = \left\{ d_0, d_1, \cdots, d_{j-1}, d_j, d_{j+1}, \cdots, d_{n-1} \right\}$. Instead of using her real-ID for authentication and message transfer, the patient uses these issued pseudo-IDs. This ensures patient identity privacy protection since the pseudo-IDs reveals nothing about the patient's real-ID to other parties. Since there is no linkage between the pseudo-IDs, our scheme can also achieve untraceability.

4.6. Session Key Secrecy

As shown above, computing the session key $SK_{PTi-HPl}$ by adversary means solving the BDH problem in $\{G_1, G_2, \hat{e}\}$. But under the random oracle model, solving BDH is infeasible in $\{G_1, G_2, \hat{e}\}$. Hence the session key between $_i$ and D_l is secure and incomputable by third parties.

5. Comparison

Table 3 below presents a comparison between proposed scheme against Huang *et al.*'s identity-based authentication and context privacy preservation scheme and Layouni *et al.*'s privacy-preserving telemonitoring for ehealth scheme.

6. Conclusion

This paper has proposed a privacy preserving paring based authentication and key established scheme for wireless health monitoring systems. The proposed scheme is based on bilinear paring, IBC and non-interactive key agreement scheme using bilinearity. In the scheme, patients are only pseudonymously identified hence protecting the patients from negative effects of identity theft such as fraudulent insurance claims by adversaries. However, the scheme achieves conditional privacy, this is so because central authority—health monitoring server—knows the patients' real identity hence in case of apparent abuse via judicial procedure, this real identity can be revealed. The security and privacy preservation analysis has shown that the scheme also achieves confidentiality of PHI, and session key secrecy. While the performance comparison has shown that our

Table 3. Performance comparison between proposed scheme against schemes in [13] and [15].

Schemes	Number of Parties	User Anonymity and Untraceability	Conditional Privacy Preservation	Patient Data Privacy against Insiders	Session Key Establishment between Patient & Doctor	Patient Revocation
Huang *et al.*'s [13]	3	No	No	No	No	No
Layouni *et al.*'s [15]	2	Yes	Yes	Yes	No	No
Proposed	3	Yes	Yes	Yes	Yes	Yes

scheme achieves more privacy preserving properties than Huang *et al.* and Layouni *et al.*'s schemes.

References

[1] An Aging World, 2013. http://www.census.gov/prod/2009pubs/p95-09-1.pdf

[2] Borger, C., Smith, S., Truffer, C., Keehan, S., Sisko, A., Posal, J. and Clement, M.K. (2006) Health Spending Projections through 2015: Changes on the Horizon. *Health Affairs Web Exclusive*, **25**, W61-W73.

[3] Kumar, P. and Lee, H.J. (2012) Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. *Sensors*, **12**, 55-91. https://doi.org/10.3390/s120100055

[4] Aging Heart and Arteries (2013) A Scientific Quest. http://www.nia.nih.gov/health/publication/aging-hearts-and-arteries-scientific-quest

[5] Gaddam, A., Mukhopadhyay, S.C. and Gupta, G.S. (2011) Elder Care Based on Cognitive Sensor Network. *IEEE Sensors Journal*, **11**, 574-581. https://doi.org/10.1109/JSEN.2010.2051425

[6] Tablado, A., Illarramendi, A., Bermudez, J. and Goni, A. (2003) Intelligent Monitoring of Elderly People. In: *Proceedings of the 4th Annual IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine*, 24-26 April 2003. https://doi.org/10.1109/itab.2003.1222447

[7] Mtonga, K., Paul, A. and Rho, S. (2014) Time-and-Id-Based Proxy Re-Encryption Scheme. *Journal of Applied Mathematics*, **2014**, Article ID: 329198. https://doi.org/10.1155/2014/329198

[8] Mtonga, K., Yoon, E.J. and Kim, H. (2014) A Pairing Based Authentication and Key establishment Scheme for Remote Monitoring Systems. *e-Infrastructure and eServices for Developing Countries*, *Lecture Notes of the Institute for Computer Sciences*, *Social Informatics and Telecommunications Engineering*, **135**, 79-89. https://doi.org/10.1007/978-3-319-08368-1_9

[9] Ko, J., Lu, C., Srivaslava, M.B., Terzis, A. and Welsh, M. (2009) Wireless Sensor Networks for Healthcare. *Proceedings of the IEEE*, **98**, 1947-1960. https://doi.org/10.1109/JPROC.2010.2065210

[10] Varshney, U. (2003) Pervasive Healthcare. *IEEE Computer*, **36**, 138-140. https://doi.org/10.1109/mc.2003.1250897

[11] Ng, H.S., Sim, M.L. and Tan, C.M. (2006) Security Issues of Wireless Sensor Networks in Healthcare Applications. *BT Technology Journal*, **24**, 138-144. https://doi.org/10.1007/s10550-006-0051-8

[12] Huang, Q., Yang, X. and Li, S. (2011) Identity Authentication and Context Privacy Preservation in Wireless Health Monitoring System. *International Journal of Computer Network and Information Security*, **3**, 53-60. https://doi.org/10.5815/ijcnis.2011.04.08

[13] Gong, L., Lomas, T.M.A., Needham, R.M. and Saltzer, J.H. (1993) Protecting Poorly Chosen Secrets from Guessing Attacks. *IEEE Journal on Selected Areas in Communications*, **11**, 648-656. https://doi.org/10.1109/49.223865

[14] Layouni, M., Verslype, K. and Sandikkaya, M.T. (2009) Privacy-Preserving Telemonitoring for eHealth. Data and Applications Security. *IFIP Annual Conference on Data and Applications Security and Privacy*, Montreal, 12-15 July 2009, 95-110.

[15] Hasque, M.M., Pathan, A.K. and Hong, C.S. (2008) Securing U-Healthcare Sensor Networks Using Public Key Based Scheme. *10th International Conference on Advanced Communication Technology*, Gangwon-Do, 17-20 February 2008, 1108-1111.

[16] Yang, Y., Deng, R.H. and Bao, F. (2006) Fortifying Password Authentication in Integrated Healthcare Delivery Systems. *Proceedings of the ACM Symposium on Information, Computer and Communications Security*, Taipei, 21-24 March 2006, 255-265.

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

[18] Boneh, D. and Franklin, M. (2001) Identity-Based Encryption from the Weil Pairing. *Proceedings of Crypto* 2001, *Santa Barbara*, 19-23 August 2001, 213-229.

[19] Sakai, R. and Kasahara, M. (2000) Cryptosystems Based on Pairings. *Proceedings of the* 2000 *Symposium on Cryptography and Information Security*, Okinawa, January 2000.

[20] Dupont, R. and Enge, A. (2006) Provably Secure Non-Interactive Key Distribution Based on Pairings. *Discrete Applied Mathematics*, **154**, 270-276. https://doi.org/10.1016/j.dam.2005.03.024

[21] He, D., Chen, C., Chan, S. and Bu, J. (2002) Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions. *IEEE Transactions on Wireless Communications*, **11**, 48-53. https://doi.org/10.1109/TWC.2011.110811.111240

[22] National Research Council (NRC) for the Record (1997) Protecting Electric Health Information. National Academy Press, Washington DC.

[23] Dixon, P. (2006) Medical Identity Theft: The Information Crime That Can Kill You. The World Privacy Forum.

[24] Alan, W.M. (2006) Buying Prescription Drugs on the Internet: Promises and Pitfalls. *Cleveland Clinic Journal of Medicine*, **73**, 282-288. https://doi.org/10.3949/ccjm.73.3.282

[25] Liang, X., Chan, L., Lu, R., Lin, X. and Shen, X. (2011) PEC: A Privacypreserving Emergency Call Scheme for Mobile Healthcare Social Networks. *IEEE/KICS Journal Communications and Networks*, **13**, 102-112. https://doi.org/10.1109/JCN.2011.6157409

[26] Freudiger, J., Manshaei, M., Hubaux, J.P. and Parkes, D. (2009) On Noncooperative Location Privacy: A Game-Theoretic Analysis. *Proceedings of the* 16*th ACM Conference on Computer and Communications Security*, Chicago, 9-13 November 2009, 324-337.

[27] Lu, R., Lin, X., Luan, H., Liang, X. and Shen, X. (2012) Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets. *IEEE Transactions on Vehicular Technology*, **61**, 86-96. https://doi.org/10.1109/TVT.2011.2162864