P3ASC: Privacy-Preserving Pseudonym and Attribute-Based Signcryption Scheme for Cloud-Based Mobile Healthcare System

Changji Wang[1,2](✉), Yuan Yuan[3], and Shengyi Jiang[1,2]

[1] School of Information Science and Technology,
Guangdong University of Foreign Studies, Guangzhou 510006, China
wchangji@gmail.com
[2] Collaborative Innovation Center for 21st-Century Maritime Silk Road Studies,
Guangdong University of Foreign Studies, Guangzhou 510006, China
[3] School of Finance, Guangdong University of Foreign Studies,
Guangzhou 510006, China

Abstract. With the development of wireless body sensor network and mobile cloud computing, cloud-based mobile healthcare, which extends the operation of healthcare provider into a pervasive environment for better health delivery and monitoring, has attracted considerable interest recently. However, how to keep data security and privacy in cloud-based mobile healthcare system is an important and challenging issue since personal health information is quite sensitive. In this paper, we introduce a new cryptographic primitive named privacy-preserving pseudonym and attribute-based signcryption (P3ASC) scheme, which can fulfill the functionality of pseudonym-based signature and key-policy attribute-based encryption in a logical step. We propose a provable secure P3ASC scheme from bilinear pairings and present a novel secure and efficient cloud-based mobile healthcare system by exploiting our proposed P3ASC scheme. The proposed system can ensure data confidentiality, integrity, source authentication and non-repudiation, but also can provide fine-grained access control and user anonymity.

Keywords: Mobile healthcare · Cloud computing
Wireless body area network · Pseudonym-based signature
Key-policy attribute-based encryption · Signcryption

1 Introduction

The promotion of wireless body area network (WBAN) has accelerated the explosive growth of medical and biological data, posing new challenges to data storage and data processing for health care providers [1,2]. A possible way to overcome these challenges is to exploit the benefits of cloud computing [3]. Cloud computing can provide an information technology infrastructure that allows hospitals,

S. Qing et al. (Eds.): ICICS 2017, LNCS 10631, pp. 399–411, 2018.
https://doi.org/10.1007/978-3-319-89500-0_35

insurance companies, research institutions and other government agencies in the healthcare ecosystem to leverage improved computing capabilities with lower cost and complexity, and allows them to access a shared pool of configurable computing resources from anywhere at any time.

Cloud computing has been widely deployed in mobile healthcare systems to improve the quality of healthcare services and potentially reduce healthcare costs in recent years. However, it also brings about a series of challenges, especially how to ensure the security of personal health information (PHI) and user privacy from various attacks [4]. Firstly, the outsourced PHI may be misused or accessed by unauthorized users. Secondly, the outsourced PHI contain personal and sensitive private information. User privacy will be destroyed once exposed to the public. Thus, scalable and strict security mechanisms are mandatory and should provide data confidentiality, integrity, source authentication, access control and user anonymity [5,6].

To solve the problem of fine-grained access control over encrypted data, Sahai and Waters [7] first introduced the concept of attribute-based encryption (ABE). Since then, various ABE schemes have been proposed, such as [8–11], and several cloud-based secure systems using ABE have been developed, such as [12–14]. There are two different and complementary notions of ABE: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE).

In KP-ABE scheme [8], ciphertexts are labeled by the data owner with a set of descriptive attributes, while data users' private keys are issued by a trusted private key generator (PKG) captures an access policy that specifies which type of ciphertexts the key can decrypt. When the access policy defined in the private key matches the attributes labeled with the ciphertext, then it decrypts the ciphertext. In CP-ABE scheme [9], the data owner encrypts a message under an access policy over attributes. A data user who possesses a set of attributes can obtain corresponding secret attribute keys from the PKG. A data user is able to decrypt a ciphertext if his attributes satisfy the access policy associated with the ciphertext.

In recent years, various cloud-based healthcare systems have been proposed by exploiting CP-ABE scheme to simultaneously achieve data confidentiality and access control. Yu et al. [15] and Tan et al. [16] pointed out that KP-ABE scheme is more appropriate than the CP-ABE scheme to be implemented in cloud-based mobile healthcare system. The main reasons are as follows: Firstly, encryption performs by using descriptive attributes has lower encryption complexity and shorter computation time than encryption to be performed by using access policy. Secondly, assignment of descriptive attributes in KP-ABE for encryption purpose is much simpler and less time consuming than assignment of access policy in CP-ABE encryption. This results from the fact that a slight update mistake in the access policy would cause a complication in the entire encryption and decryption system. Furthermore, in terms of access control, KP-ABE allows higher flexibility and efficiency in the modification of access control towards any authorized personnel compared to CP-ABE. This stems from the fact that the updates made on the descriptive attributes are much simpler than updates made on access structure.

Given the importance of PHI and the compliance of health insurance portability and accountability act (HIPPA), it is critical to guarantee source authentication and integrity of PHI in cloud-based mobile healthcare system. Otherwise, anyone can modify or forge someone's PHI, which is undesirable. In addition, user privacy may impede its wide adoption. Digital signature is a very useful tool for providing authenticity, integrity and non-repudiation while it is rarely considered to provide user privacy by its own. Although privacy-preserving signature schemes, such as ring signature, group signature, mesh signature, attribute-based signature [17], have been widely studied in recent years, they are very complicated and time-consuming.

In this paper, we introduce a new cryptographic primitive named privacy preserving pseudonym and attribute-based signcryption (P3ASC) scheme, which can fulfill the functionality of pseudonym-based signature and key-policy attribute-based encryption in a logical step. To achieve user anonymity, privacy preserving technique based on pseudonyms is adopted. Then, we propose a P3ASC scheme and prove it is indistinguishable against adaptive chosen plaintext attacks in the selective-set model under the DBDH assumption, and is existentially unforgeable against adaptive chosen message and pseudonym attacks in the random oracle model under the ECDL assumption. Finally, we provide an architectural model of cloud-based mobile healthcare system by exploiting our proposed P3ASC scheme. It can ensure data confidentiality, integrity, authenticity, and non-repudiation, but also can provide fine-grained access control and user anonymity.

The rest of the paper is organized as follows. We introduce some necessary preliminary work in Sect. 2. We give syntax and security definitions for P3ASC scheme in Sect. 3. We present a P3ASC scheme in Sect. 3. We describe an architecture of cloud-based mobile healthcare system by exploiting the proposed P3ASC scheme in Sect. 4. Finally, we conclude our paper and discuss our future work in Sect. 5.

2 Preliminaries

We denote by κ the system security parameter. When $\mathbf{S}$ is a set, $x \overset{\$}{\leftarrow} \mathbf{S}$ denotes that x is uniformly picked from $\mathbf{S}$. Let $\mathbf{M}$, $\mathbf{ID}$ and $\boldsymbol{\Omega}$ be message universe, identity (pseudonym) universe and attribute universe, respectively.

2.1 Access Structure and Linear Secret Sharing Scheme

Let $\boldsymbol{\Omega} = \{\omega_1, \omega_2, \cdots, \omega_n\}$ be a set of attributes, and denote by $2^{\boldsymbol{\Omega}}$ its power set. A collection $\mathbb{A} \subseteq 2^{\boldsymbol{\Omega}}$ is monotone if for every $\mathbf{B}$ and $\mathbf{C}$, if $\mathbf{B} \in \mathbb{A}$ and $\mathbf{B} \subseteq \mathbf{C}$ then $\mathbf{C} \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of non-empty subsets of $\boldsymbol{\Omega}$, i.e.

$\boldsymbol{\Omega} \setminus \emptyset$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets [9].

We restrict our attention to monotone access structures. If a set of attributes $\boldsymbol{\omega}$ satisfies an access policy (access structure) $\mathbb{A}$, we denote it as $\mathbb{A}(\boldsymbol{\omega}) = 1$. Otherwise, we denote it as $\mathbb{A}(\boldsymbol{\omega}) = 0$.

Let $\mathbf{M}_{\ell\times k}$ be a matrix, and $\rho : \{1, \ldots, \ell\} \rightarrow \boldsymbol{\Omega}$ be a function that maps a row of $\mathbf{M}_{\ell\times k}$ to an attribute for labeling. A secret sharing scheme for access structure $\mathbb{A}$ over a set of attributes $\boldsymbol{\Omega}$ is a linear secret-sharing scheme over $\mathbf{F}_q$ and is represented by $(\mathbf{M}_{\ell\times k}, \rho)$ if it consists of two polynomial-time algorithms:

- Share: The algorithm takes as input $s \in \mathbf{F}_q$ which is to be shared. It chooses $\upsilon_2, \ldots, \upsilon_k \overset{\$}{\leftarrow} \mathbf{F}_q$ and let $\boldsymbol{\upsilon} = (s, \upsilon_2, \ldots, \upsilon_k)$. It outputs $\mathbf{M}_{\ell\times k} \cdot \boldsymbol{\upsilon}^\top$ as the vector of ℓ shares of the secret s. The share $\lambda_i =<\mathbf{M}_i, \boldsymbol{\upsilon}>$ belongs to party $\rho(i)$, where we denote $\mathbf{M}_i$ as the i-th row in $\mathbf{M}_{\ell\times k}$.
- $\mathsf{Reconstruct}$: The algorithm takes as input $\mathbf{S} \subseteq \boldsymbol{\Omega}$ satisfies $\mathbb{A}$. Let $\mathbf{I} = \{i|\rho(i) \in \mathbf{S}\}$. It outputs reconstruction constants $\{(i, \mu_i)\}_{i\in\mathbf{I}}$ which has a linear reconstruction property, i.e., $\sum_{i\in\mathbf{I}} \lambda_i \cdot \mu_i = s$.

2.2 Bilinear Pairing and Complexity Assumptions

Let P be a point with a prime order q in an elliptic curve $\mathrm{E}_p(a, b)$, and $\mathbf{G}$ be a subgroup generated by the base point P, i.e., $\mathbf{G} \overset{\text{def}}{=} \langle P \rangle$.

Definition 1. *Given $Q \in \mathbf{G}$, the elliptic curve discrete logarithm problem (ECDLP) in $\mathbf{G}$ is to find the integer a where $1 \le a \le q$, such that $Q = [a]P$.*

The advantage of an adversary $\mathcal{A}$ in breaking the ECDLP in $\mathbf{G}$ is defined by

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{ECDLP}}(1^\kappa) = \Pr[\mathcal{A}(P, Q = [a]P) = a \mid a \overset{\$}{\leftarrow} \mathbf{Z}_q^*].$$

We say that the ECDL assumption holds for the group $\mathbf{G}$, if for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{ECDLP}}(1^\kappa)$ is a negligible function in the security parameter κ.

A bilinear group parameter generator $\mathcal{G}$ is an algorithm that takes as input a security parameter κ and outputs a bilinear group setting $(q, \mathbf{G}_1, \mathbf{G}_T, \hat{e})$, where $\mathbf{G}_1$ and $\mathbf{G}_T$ are a cyclic additive group and a multiplicative group of prime order q, respectively, and $\hat{e}$: $\mathbf{G}_1 \times \mathbf{G}_1 \rightarrow \mathbf{G}_T$ is a bilinear pairing with the following properties:

- Bilinearity: For $P_1, P_2 \overset{\$}{\leftarrow} \mathbf{G}_1$ and $a, b \overset{\$}{\leftarrow} \mathbf{Z}_q^*$, we have $\hat{e}([a]P_1, [b]P_2) = \hat{e}(P_1, P_2)^{ab}$.
- Non-degeneracy: There exists $P_1, Q_1 \in \mathbf{G}_1$ such that $\hat{e}(P_1, Q_1) \neq 1_{\mathbf{G}_T}$.
- Computability: There is an efficient algorithm to compute $\hat{e}(P_1, Q_1)$ for $P_1, Q_1 \overset{\$}{\leftarrow} \mathbf{G}_1$.

Definition 2. *Given a bilinear group setting $(q, \mathbf{G}_1, \mathbf{G}_T, \hat{e})$ generated by $\mathcal{G}(1^\kappa)$, define two distributions*

$$\mathcal{D}_0(1^\kappa) \overset{\text{def}}{=} \{P_1, [a]P_1, [b]P_1, [c]P_1, \hat{e}(P_1, P_1)^z\}$$
$$\mathcal{D}_1(1^\kappa) \overset{\text{def}}{=} \{P_1, [a]P_1, [b]P_1, [c]P_1, \hat{e}(P_1, P_1)^{abc}\}$$

where $a, b, c, z \overset{\$}{\leftarrow} \mathbf{Z}_q^*$, $P_1 \overset{\$}{\leftarrow} \mathbf{G}_1$, the decisional bilinear Diffie-Hellman problem (DBDHP) in $(q, \mathbf{G}_1, \mathbf{G}_T, \hat{e})$ is to determine whether $\hat{e}(P_1, P_1)^z = \hat{e}(P_1, P_1)^{abc}$.

The advantage of an adversary $\mathcal{A}$ in breaking DBDHP in $(q, \mathbf{G}_1, \mathbf{G}_T, \hat{e})$ is defined by

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{DBDHP}}(1^\kappa) = |\Pr[\mathcal{D}_0(1^\kappa) \to 1] - \Pr[\mathcal{D}_1(1^\kappa) \to 1]|$$

We say that the DBDH assumption holds for $(q, \mathbf{G}_1, \mathbf{G}_T, \hat{e})$, if for any PPT adversary $\mathcal{A}$, the advantage $\mathsf{Adv}_{\mathcal{A}}^{\mathrm{DBDHP}}(1^\kappa)$ is a negligible function in the security parameter κ.

3 Privacy-Preserving Pseudonym and Attribute-based SignCryption Scheme

A P3ASC scheme consists of the following six polynomial-time algorithms:

- Setup: The probabilistic setup algorithm is run by the PKG. It takes as input a security parameter κ and an attribute universe $\mathbf{\Omega}$. It outputs the public system parameters *mpk*, and the master secret key *msk* which is known only to the PKG.
- PIDKeyGen: The probabilistic pseudonym-based private key generation algorithm is run by the PKG. It takes as input *mpk*, *msk*, and a real user identity id. It outputs a pseudonym pid and a private key sk_{pid} corresponding to the pseudonym.
- ABKeyGen: The probabilistic attribute-based private key generation algorithm is run by the PKG. It takes as input *mpk*, *msk*, and an access structure $\mathbb{A}$ assigned to a user. It outputs a private key $dk_{\mathbb{A}}$ corresponding to the access structure $\mathbb{A}$.
- SignCrypt: The probabilistic signcrypt algorithm is run by a sender. It takes as input *mpk*, a message Msg, a sender's pseudonym-based private key sk_{pid}, and a set $\boldsymbol{\omega}$ of descriptive attributes. It outputs a signcrypted ciphertext Sct.
- PubVerify: The deterministic public verifiability algorithm is run by any receivers. It takes as input *mpk*, a signcrypted ciphertext Sct, a sender's pseudonym pid, and a set $\boldsymbol{\omega}$ of descriptive attributes. It outputs a bit b which is 1 if Sct is generated by the sender, or 0 if Sct is not generated by the sender.
- UnSigncrypt: The deterministic unsigncryption algorithm is run by a receiver. It takes as input *mpk*, a signcrypted ciphertext Sct, a sender's pseudonym pid, a set $\boldsymbol{\omega}$ of descriptive attributes, and a receiver's attribute-based private key $dk_{\mathbb{A}}$. It outputs Msg if $\mathbb{A}(\boldsymbol{\omega}) = 1$. Otherwise it outputs $\perp$.

The set of algorithms must satisfy the following consistency requirement:

$$\begin{aligned}
&\mathsf{Setup}(1^{\kappa}, \boldsymbol{\Omega}) \rightarrow (mpk, msk), \mathrm{Msg} \xleftarrow{\$} \mathbf{M}, \mathsf{id} \xleftarrow{\$} \mathbf{ID},\\
&\mathsf{PIDKeyGen}(mpk, msk, \mathsf{id}) \rightarrow (\mathsf{pid}, sk_{\mathsf{pid}}),\\
&\mathsf{ABKeyGen}(mpk, msk, \mathbb{A}) \rightarrow dk_{\mathbb{A}},\\
&\mathsf{SignCrypt}(mpk, sk_{\mathsf{pid}}, \boldsymbol{\omega}, \mathrm{Msg}) \rightarrow \mathrm{Sct},\ \boldsymbol{\omega} \in \boldsymbol{\Omega}\\
&\text{If } \mathbb{A}(\boldsymbol{\omega}) = 1 \Rightarrow \begin{cases} \mathsf{PubVerify}(mpk, \mathsf{pid}, \boldsymbol{\omega}, \mathrm{Sct}) = 1\\ \mathsf{UnSignCrypt}(mpk, dk_{\mathbb{A}}, \mathsf{pid}, \boldsymbol{\omega}, \mathrm{Sct}) = \mathrm{Msg} \end{cases}
\end{aligned}$$

A P3ASC scheme should satisfy confidentiality and unforgeability. For the confidentiality, we consider the following indistinguishability against adaptive chosen plaintext attack (IND-CPA) game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ in the selective-set model [8].

- **Init:** $\mathcal{A}$ declares a set of attributes, $\boldsymbol{\omega}^*$.
- **Setup:** $\mathcal{C}$ runs the Setup algorithm, gives mpk to $\mathcal{A}$, while keeps msk secret.
- **Phase 1:** $\mathcal{A}$ is allowed to issue the following queries adaptively.
  - Singing private key query on an identity id_i. $\mathcal{C}$ runs the $\mathsf{PIDKeyGen}$ algorithm, and sends $(\mathsf{pid}_i, sk_{\mathsf{pid}_i})$ back to $\mathcal{A}$.
  - Decrypting private key query on an access structures $\mathbb{A}_j$. If $\mathbb{A}_j(\boldsymbol{\omega}^*) \neq 1$, then $\mathcal{C}$ runs the $\mathsf{ABKeyGen}$ algorithm, and sends $dk_{\mathbb{A}_j}$ back to $\mathcal{A}$. Otherwise, $\mathcal{C}$ rejects the request.
- **Challenge:** $\mathcal{A}$ submits two equal length messages $(\mathrm{Msg}_0, \mathrm{Msg}_1)$, and an identity id to $\mathcal{C}$. Then, $\mathcal{C}$ flips a random coin b, runs $\mathsf{PIDKeyGen}(mpk, msk, \mathsf{id}) \rightarrow (\mathsf{pid}, sk_{\mathsf{pid}})$ and $\mathsf{Signcrypt}(mpk, sk_{\mathsf{pid}}, \boldsymbol{\omega}^*, \mathrm{Msg}_b) \rightarrow \mathrm{Sct}^*$ in sequence. Finally, $\mathcal{C}$ sends Sct^* to $\mathcal{A}$.
- **Phase 2:** Phase 1 is repeated.
- **Guess:** $\mathcal{A}$ outputs a guess b' of b.

The advantage of $\mathcal{A}$ in the above game is defined as

$$\mathrm{Adv}_{\mathcal{A}}^{\text{IND-CPA}}(1^{\kappa}) = \Pr[b' = b] - \frac{1}{2}.$$

Definition 3. *A P3ASC scheme is said to be IND-CPA secure in the selective-set model if $Adv_{\mathcal{A}}^{IND\text{-}CPA}(1^{\kappa})$ is negligible in the security parameter κ.*

For the unforgeability, we consider the following existential unforgeability against adaptive chosen message and pseudonyms attack (UF-CMPA) game played between a challenger $\mathcal{C}$ and a forger $\mathcal{F}$.

- **Setup:** Same as in the above IND-CPA game.
- **Find:** $\mathcal{F}$ is allowed to issue the following queries adaptively.
  - Singing private key query. Same as in the above IND-CPA game.
  - Decrypting private key query. Upon receiving decryption private key query on an access structure $\mathbb{A}_j$, $\mathcal{C}$ runs $\mathsf{ABKeyGen}(mpk, msk, \mathbb{A}_j) \rightarrow dk_{\mathbb{A}_j}$, and sends $dk_{\mathbb{A}_j}$ back to $\mathcal{F}$.

  - Signcrypt query on $\langle \text{Msg}, sk_{\mathsf{pid}}, \boldsymbol{\omega} \rangle$. $\mathcal{C}$ runs $\mathsf{Signcrypt}(mpk, sk_{\mathsf{pid}}, \boldsymbol{\omega}, \text{Msg}) \rightarrow \text{Sct}$ successively. Finally, $\mathcal{C}$ sends Sct back to $\mathcal{F}$.

- **Forgery:** $\mathcal{F}$ produces a new triple $\langle \text{Sct}^*, \boldsymbol{\omega}^*, \mathsf{pid}^* \rangle$. The only restriction is that $\langle \boldsymbol{\omega}^*, \mathsf{pid}^* \rangle$ does not appear in the set of previous Signcrypt queries during the Find stage and the signing private key of pid^* is never returned by any PIDKeyGen query.

$\mathcal{F}$ wins the game if

$$\mathsf{PubVerify}(mpk, \mathsf{pid}^*, \boldsymbol{\omega}^*, \text{Sct}^*) = 1,$$

and the advantage of $\mathcal{F}$ is defined as the probability that it wins.

Definition 4. *A P3ASC scheme is said to be EUF-CMPA secure if no polynomially bounded adversary $\mathcal{F}$ has non-negligible advantage in the above game.*

3.1 Our Proposed P3ASC Scheme

Our proposed P3ASC scheme is described as follows.

- Setup: The PKG performs as follows.
  1. Generate an elliptic curve group $\mathbf{G} \overset{\text{def}}{=} \langle P \rangle$.
  2. Run $\mathcal{G}(1^\kappa) \rightarrow \langle q, \mathbf{G}_1, \mathbf{G}_T, \hat{e} \rangle$.
  3. Choose $P \overset{\$}{\leftarrow} \mathbf{G}$, $P_1 \overset{\$}{\leftarrow} \mathbf{G}_1$, $x, y \overset{\$}{\leftarrow} \mathbf{Z}_q^*$, $t_i \overset{\$}{\leftarrow} \mathbf{Z}_q^*$ for each attribute $\text{Atr}_i \in \boldsymbol{\Omega}$, four secure hash functions $H_1 : \mathbf{Z}_q^* \times \mathbf{G} \rightarrow \mathbf{ID}$, $H_2 : \mathbf{ID} \times \mathbf{G} \rightarrow \mathbf{Z}_q^*$, $H_3 : \mathbf{G} \times \mathbf{G}_T \times \mathbf{Z}_q^* \rightarrow \mathbf{Z}_q^*$, and $H_4 : \mathbf{G} \times \mathbf{G}_T \times \mathbf{G}_T \rightarrow \mathbf{Z}_q^*$.
  4. Compute $P_{\text{pub}} = [x]P$, $Y = \hat{e}(P_1, P_1)^y$ and $T_i = [t_i]P_1$ for $1 \leq i \leq |\boldsymbol{\Omega}|$.
  5. Set $msk = \{t_1, t_2, \cdots, t_{|\boldsymbol{\Omega}|}, x, y\}$.
  6. Publish $mpk = \{\boldsymbol{\Omega}, T_1, T_2, \cdots, T_{|\boldsymbol{\Omega}|}, P_{\text{pub}}, Y, H_1, H_2, H_3, H_4\}$.
- $\mathsf{PIDKeyGen}$: A user with real identity id_{U} registers to the PKG to get his/her pseudonym pid_{U} and pseudonym-based private key sk_{U} by performing the following pseudonym-based key generation protocol. Figure 1 illustrates the procedure.
  1. The user chooses $\overline{r}_{\text{U}} \overset{\$}{\leftarrow} \mathbb{Z}_q^*$, computes $\overline{R}_{\text{U}} = [\overline{r}_{\text{U}}]P$, and sends a pseudonym-based private key request $(\overline{R}_{\text{U}}, \mathsf{id}_{\text{U}})$ to the PKG.
  2. Upon receiving the private key request, the PKG first verifies id_{U}. If it is valid, then the PKG picks $\widehat{r}_{\text{U}} \overset{\$}{\leftarrow} \mathbb{Z}_q^*$, computes $\widehat{R}_{\text{U}} = [\widehat{r}_{\text{U}}]P$, $R_{\text{U}} = \overline{R}_{\text{U}} + \widehat{R}_{\text{U}}$, $\mathsf{pid}_{\text{U}} = H_1(x, R_{\text{U}}) \oplus \mathsf{pid}_{\text{U}}$, $c_{\text{U}} = H_2(\mathsf{pid}_{\text{U}}, R_{\text{U}})$ and $\widehat{sk}_{\text{U}} = \widehat{r}_{\text{U}} + c_{\text{U}} \cdot x \bmod q$. Finally, the PKG sends $(\mathsf{pid}_{\text{U}}, \widehat{sk}_{\text{U}}, \widehat{R}_{\text{U}})$ to the user via a secure channel.
  3. Upon receiving the response from the PKG, the user computes $R_{\text{U}} = \overline{R}_{\text{U}} + \widehat{R}_{\text{U}}$, $c_{\text{U}} = H_2(\mathsf{pid}_{\text{U}}, R_{\text{U}})$ and $sk_{\text{U}} = \overline{r}_{\text{U}} + \widehat{sk}_{\text{U}} \bmod q$, sets the corresponding public key $Q_{\text{U}} = [sk_{\text{U}}]P$, and checks the following equation:

$$Q_{\text{U}} \overset{?}{=} R_{\text{U}} + [c_{\text{U}}]P_{\text{pub}}$$

     If it holds, the user stores the tuple $(\mathsf{pid}_{\text{U}}, R_{\text{U}})$ and the corresponding private key sk_{U}.

$$\begin{array}{ccc}
\text{MN}_j\ (\mathsf{pid}_{\mathrm{U}}, mpk) & & \text{PKG}\ (msk, mpk) \\
\hline
\mathsf{id}_{\mathrm{U}} \xleftarrow{\$} \mathbf{ID} & & \\
\overline{r}_{\mathrm{U}} \xleftarrow{\$} \mathbb{Z}_q^*,\ \overline{R}_{\mathrm{U}} = [\overline{r}_{\mathrm{U}}]P & & \\
 & \xrightarrow{(\overline{R}_{\mathrm{U}}, \mathsf{id}_{\mathrm{U}})} & \\
 & & \text{Check the validity of } \mathsf{id}_{\mathrm{U}} \\
 & & \widehat{r}_{\mathrm{U}} \xleftarrow{\$} \mathbb{Z}_q^*,\ \widehat{R}_{\mathrm{U}} = [\widehat{r}_{\mathrm{U}}]P \\
 & & R_{\mathrm{U}} = \overline{R}_{\mathrm{U}} + \widehat{R}_{\mathrm{U}} \\
 & & \mathsf{pid}_{\mathrm{U}} = H_1(x, R_{\mathrm{U}}) \oplus \mathsf{id}_{\mathrm{U}} \\
 & & c_{\mathrm{U}} = H_2(\mathsf{pid}_{\mathrm{U}}, R_{\mathrm{U}}) \\
 & & \widehat{sk}_{\mathrm{U}} = \widehat{r}_{\mathrm{U}} + c_{\mathrm{U}} \cdot x \bmod q \\
 & \xleftarrow{(\mathsf{pid}_{\mathrm{U}}, \widehat{sk}_{\mathrm{U}}, \widehat{R}_{\mathrm{U}})} & \\
R_{\mathrm{U}} = \overline{R}_{\mathrm{U}} + \widehat{R}_{\mathrm{U}} & & \\
c_{\mathrm{U}} = H_2(\mathsf{pid}_{\mathrm{U}}, R_{\mathrm{U}}) & & \\
sk_{\mathrm{U}} = \overline{r}_{\mathrm{U}} + \widehat{sk}_{\mathrm{U}} \bmod q & & \\
Q_{\mathrm{U}} = [sk_{\mathrm{U}}]P & & \\
Q_{\mathrm{U}} \overset{?}{=} R_{\mathrm{U}} + [c_{\mathrm{U}}]P_{\mathrm{pub}} & &
\end{array}$$

Fig. 1. Pseudonym-based key generation protocol

- ABKeyGen: A user sends an attribute-based private key request to the PKG, and the PKG performs as follows.
  1. Assign a linear secret sharing scheme for access structure $\mathbb{A}$ described by $(\mathbf{M}_{\ell \times n}, \rho)$ to the user.
  2. Choose $u_i \xleftarrow{\$} \mathbf{Z}_q^*$ for $1 \leq i \leq n$ such that $\sum_{i=1}^{n} u_i = y$, and set $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$.
  3. Compute $\lambda_i =< \mathbf{M}_i, \boldsymbol{u} >$ and $D_i = [\lambda_i / t_{\rho(i)}]P$ for each row vector $\mathbf{M}_i$ of $\mathbf{M}_{\ell \times n}$.
  4. Send the attribute-based decryption key $dk_{\mathbb{A}} = \{D_i\}_{i=1}^{\ell}$ associated with the access structure $\mathbb{A}$ to the user.
- Signcrypt: To signcrypt a message $\mathrm{Msg} \in \mathbf{G}_T$ along with a set $\boldsymbol{\omega}$ of attributes, a sender with pseudonym $\mathsf{pid}_{\mathrm{U}}$ performs as follows.
  1. Compute $c_{\mathrm{U}} = H_2(\mathsf{pid}_{\mathrm{U}}, R_{\mathrm{U}})$.
  2. Choose $s \xleftarrow{\$} \mathbf{Z}_q^*$.
  3. Compute $A = [s]P$, $C' = \mathrm{Msg} \cdot Y^s$, $h_3 = H_3(A, C', c_{\mathrm{U}})$, $\sigma = s + h_3 \cdot sk_{\mathrm{U}}$, $h_4 = H_4(A, \mathrm{Msg}, Y^s)$, and $C_i = [s]T_i$ for $1 \leq i \leq |\boldsymbol{\omega}|$.
  4. Output $\mathrm{Sct} = \{\boldsymbol{\omega}, \mathsf{pid}_{\mathrm{U}}, R_{\mathrm{U}}, C', \{C_i\}_{i=1}^{|\boldsymbol{\omega}|}, A, \sigma, h_4\}$
- PubVerify: Any receiver can check the validity of the signcrypted ciphertext Sct against sender's pseudonym $\mathsf{pid}_{\mathrm{U}}$ as follows.
  1. Compute $c_{\mathrm{U}} = H_2(\mathsf{pid}_{\mathrm{U}}, R_{\mathrm{U}})$ and $h_3 = H_3(A, C', c_{\mathrm{U}})$.
  2. Check $[\sigma]P \overset{?}{=} A + [h_3](R_{\mathrm{U}} + [c_{\mathrm{U}}]P_{\mathrm{pub}})$. It outputs 1 if the equation holds, or 0 if the equation does not hold.

- UnSigncrypt: A receiver uses his decryption private key $dk_{\mathbb{A}}$ associated to the access structure $\mathbb{A}$ described by $(\mathbf{M}_{\ell \times n}, \rho)$ to recover and verify the signcrypted ciphertext $\mathrm{Sct} = \{\boldsymbol{\omega}, \mathsf{pid}_{\mathrm{U}}, R_{\mathrm{U}}, C', \{C_i\}_{i=1}^{|\boldsymbol{\omega}|}, A, \sigma, h_4\}$ as follows.
  1. Determine $\mathbb{A}(\boldsymbol{\omega}) \overset{?}{=} 1$. If not, the receiver rejects the signcrypted ciphertext Sct.
  2. Validate the signcrypted ciphertext Sct as any receiver performs in the PubVerify algorithm.
  3. Define $\mathbf{I} = \{i | \rho(i) \in \boldsymbol{\omega}\} \subset \{1, 2, \ldots, \ell\}$, and let $\{\mu_i\}$ be a set of constants such that if $\{\lambda_i\}$ are valid shares of y according to $(\mathbf{M}_{\ell \times n}, \rho)$, then $\sum_{i \in \mathbf{I}} \lambda_i \cdot \mu_i = y$.
  4. Compute $V = \prod_{\rho(i) \in \boldsymbol{\omega}} \hat{e}(D_i, C_{\rho(i)})^{\mu_i}$ and $\mathrm{Msg}' = C'/V$.
  5. Check $H_4(A, \mathrm{Msg}', V) \overset{?}{=} h_4$. If it holds, the receiver accepts and outputs the message Msg. Otherwise, rejects and outputs $\perp$.

Theorem 1. *Our P3ASC scheme satisfies consistency requirement.*

Proof. Consistency requirement can be verified as follows.

$$\begin{aligned}
[\sigma]P &= [s + h_3 \cdot sk_{\mathrm{U}}]P = [s]P + [h_3][sk_{\mathrm{U}}]P \\
&= A + [h_3](R_{\mathrm{U}} + [c_{\mathrm{U}}]P_{\mathrm{pub}}) \\
V &= \prod_{\rho(i) \in \boldsymbol{\omega}} \hat{e}(D_i, C_{\rho(i)})^{\mu_i} = \prod_{\rho(i) \in \boldsymbol{\omega}} \hat{e}([\lambda_i / t_{\rho(i)}]P, [s \cdot t_{\rho(i)}]P)^{\mu_i} \\
&= \prod_{\rho(i) \in \boldsymbol{\omega}} \hat{e}(P, P)^{s \cdot \lambda_i \cdot \mu_i} = \hat{e}(P, P)^{s \sum_{\rho(i) \in \omega} \lambda_i \cdot \mu_i} \\
&= \hat{e}(P, P)^{sy} \\
\mathrm{Msg}' &= C'/V = \mathrm{Msg} \cdot Y^s / \hat{e}(P, P)^{sy} \\
&= \mathrm{Msg}.
\end{aligned}$$

Theorem 2. *Our P3ASC scheme satisfies the conditional anonymity for the sender.*

Proof. In the PIDKeyGen, sender can choose a family of pseudonyms and obtain associated private keys by running a Schnorr-like lightweight identity-based blind signature scheme with the PKG ([18–20]). Although the signcrypted message Sct must include a pseudonym of the sender and R_{U}. However, anyone, except the PKG, cannot extract sender's real identity id_{U} because they have no idea of the master secret key x. Furthermore, there is no linkage between these pseudonyms, anyone, except the PKG, cannot link two sessions initiated by the same sender. Of course, the PKG can extract the sender's real identity by computing $\mathsf{id}_{\mathrm{U}} = \mathsf{pid}_{\mathrm{U}} \oplus H_1(x, R_{\mathrm{U}})$. Thus, our P3ASC scheme achieves the conditional anonymity for the sender.

Theorem 3. *Our P3ASC scheme is IND-CPA secure in the selective-set model under the DBDH assumption.*

Proof. We will give detailed security proof in the full version due to the space limitation.

Theorem 4. *Our P3ASC scheme is EUF-CMA secure in the adaptive model under the ECDL assumption.*

Proof. We will give detailed security proof in the full version due to the space limitation.

4 Privacy Preserving Cloud-Based Mobile Healthcare System

The general architecture and message sequence of our privacy-preserving cloud-based mobile healthcare system is shown in Fig. 2. Three types of users are supported by our proposed system:

- PHI owner who generates personal health data collected from wireless body sensor network, creates signcrypted ciphertexts and forward them to the medical cloud service provider (CSP).
- PHI reader who can only read a PHI owner's PHI.
- PHI writer who can access a PHI owner's PHI, but also can modify a PHI owner's PHI, e.g., an authorized doctor can generate medical data for a PHI owner.

There are five essential participants in our cloud-based mobile healthcare system: hospital authority (HA), PHI Owners, medical CSP, PHI readers, and PHI writers. We assume that all communications between participants are secured by transport layer security (TLS) protocol.

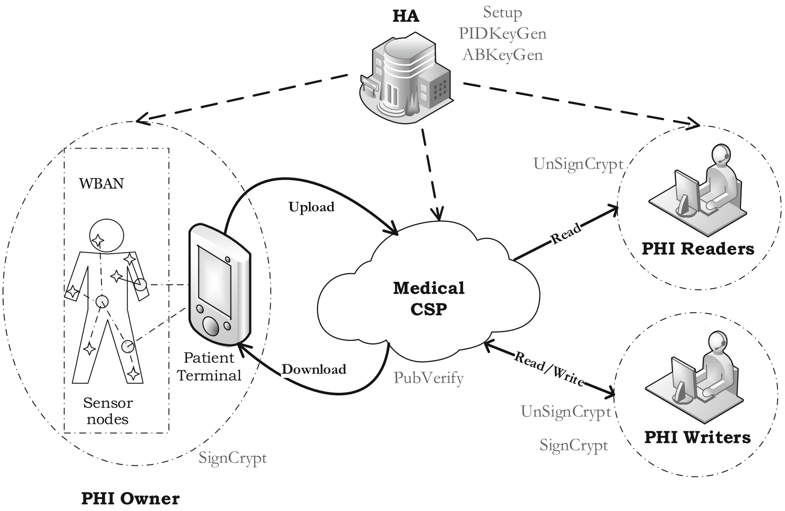

Fig. 2. Architecture of proposed cloud-based mobile healthcare system

- HA, who acts as the PKG. HA is responsible for generating system public parameters, issuing pseudonym-based private keys for PHI owners and PHI writers, and attribute-based private keys for PHI writers and PHI readers.
- PHI Owners, who carry multiple wearable or implanted sensors and a patient terminal. Those sensors can sense and process vital signs or environmental parameters, and transfer the relevant data to the patient terminal. Typically, patient terminal is equipped with mobile health application and database collection and storage functions with the ability for mobile communication. PHI owners register themselves to the HA by sending their real identity, and the HA allocates pseudo-identity to the PHI owner, which is to be used for all the communications in the network. Thus, the actual identity of the PHI owner is concealed.
- Medical CSP, who keeps patient related data of registered users and provides various services to the registered users. We assume that the medical CSP is honest-but-curious, which means that the medical CSP will perfectly execute the protocol specifications, but intend to extract the patient's private personal health information.
- PHI readers, who are allowed to view a PHI owner's PHI. It can be doctors, nurses, researchers, insurance company employees, etc.
- PHI writers, who are allowed to view and update a PHI owner's PHI. It can be doctors who may access the patients' medical information and provide medical services.

5 Conclusions

To achieve medical data security (confidentiality, integrity, authenticity and access control) and user privacy in mobile health cloud, we introduce a new cryptographic primitive named privacy-preserving pseudonym and attribute-based signcryption scheme, propose a provable secure construction and present a novel secure and efficient cloud-based mobile healthcare system by exploiting our proposed construction. For future work, we plan to further investigate and implement the proposed system in a suitable cloud platform. We will also evaluate the security and performance of the proposed system after being implemented and compare them with the most related work in the area.

Acknowledgments. This research is jointly funded by Science and Technology Program of Guangzhou (Grant No. 201707010358), and the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (Grant No. AGK201707).

References

1. Negra, R., Jemili, I., Belghith, A.: Wireless body area networks: applications and technologies. Procedia Comput. Sci. **83**, 1274–1281 (2016)
2. Kang, J., Adibi, S.: A review of security protocols in mHealth Wireless Body Area Networks (WBAN). In: Doss, R., Piramuthu, S., Zhou, W. (eds.) FNSS 2015. CCIS, vol. 523, pp. 61–83. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-19210-9_5
3. Sadiku, M.N.O., Musa, S.M., Momoh, O.D.: Cloud computing: opportunities and challenges. IEEE Potentials **33**(1), 34–36 (2014)
4. Buchade, A.R., Ingle, R.: Key management for cloud data storage: methods and comparisons. In: Fourth International Conference on Advanced Computing Communication Technologies, pp. 263–270. IEEE Press (2014)
5. Patil, H.K., Seshadri, R.: Big data security and privacy issues in healthcare. In: IEEE International Congress on Big Data, pp. 762–765. IEEE (2014)
6. Samaher, A.J., Ibrahim, A.S., Mohammad, S., Shahaboddin, S.: Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egypt. Inform. J. **18**(2), 113–122 (2017)
7. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_27
8. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute based encryption for fine-grained access conrol of encrypted data. In ACM conference on Computer and Communications Security, pp. 89–98 (2006)
9. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Press (2007)
10. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_4
11. Attrapadung, N., Libert, B., de Panafieu, E.: Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 90–108. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_6
12. Pirretti, M., Traynor, P., McDaniel, P., Waters, B.: Secure attribute-based systems. J. Comput. Secur. **18**(5), 799–837 (2010)
13. Li, M., Yu, S.C., Zheng, Y., Ren, K., Lou, W.J.: Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst. **24**(1), 131–143 (2013)
14. Wang, C.J., Xu, X.L., Shi, D.Y., Fang, J.: Privacy-preserving cloud-based personal health record system using attribute-based encryption and anonymous multi-receiver identity-based encryption. Informatica **39**(4), 375–382 (2015)
15. Yu, S., Wang, C., Ren, K., Lou, W.: Achieving secure, scalable, and fine-grained data access control in cloud computing. In: Proceedings IEEE INFOCOM, pp. 1–9 (2010)
16. Tan, Y.L., Goi, B.M., Komiya, R., Phan, R.: Design and implementation of key-policy attribute-based encryption in body sensor network. Int. J. Cryptol. Res. **4**(1), 84–101 (2013)

17. Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-based signatures. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 376–392. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19074-2_24
18. Pointcheval, D., Stern, J.: Provably secure blind signature schemes. In: Kim, K., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 252–265. Springer, Heidelberg (1996). https://doi.org/10.1007/BFb0034852
19. Galindo, D., Garcia, F.D.: A Schnorr-like lightweight identity-based signature scheme. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 135–148. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02384-2_9
20. Chatterjee, S., Kamath, C., Kumar, V.: Galindo-Garcia identity-based signature revisited. In: Kwon, T., Lee, M.-K., Kwon, D. (eds.) ICISC 2012. LNCS, vol. 7839, pp. 456–471. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-37682-5_32