7-2020

Lightweight and privacy-aware fine-grained access control for IoT-oriented smart health

Jianfei SUN

Hu XIONG

Ximeng LIU
Singapore Management University, xmliu@smu.edu.sg

Yinghui ZHANG

Xuyun NIE

See next page for additional authors

Published in IEEE Internet of Things Journal, 2020, Volume: 7, Issue: 7, pp. 6566 - 6575.
DOI: 10.1109/JIOT.2020.2974257

Lightweight and Privacy-Aware Fine-Grained Access Control for IoT-oriented Smart Health

Jianfei Sun, Hu Xiong*, Ximeng Liu, Yinghui Zhang, Xuyun Nie, Robert H. Deng, *Fellow, IEEE*

***Abstract*—With the booming of Internet of Things (IoT), smart health (s-health) is becoming an emerging and attractive paradigm. It can provide accurate prediction of various diseases, improve the quality of healthcare. Nevertheless, data security and user privacy concerns still remain as issues to be addressed. As a highly potential and prospective solution to secure IoT-oriented s-health applications, ciphertext policy attribute based encryption (CP-ABE) schemes raise challenges such as heavy overhead and attribute privacy of the end users. To resolve these drawbacks, an optimized vector transformation approach is first proposed to efficiently transform the access policy and user attribute set into respective vectors of shorter length while other approaches result in redundant and longer vectors. Our transformation approach can greatly relieve the costly overheard of key generation, encryption and decryption phases. Then, based on the transformation approach and the offline/online computation technology, we propose a lightweight policy-hiding CP-ABE scheme for the IoT-oriented s-health application. With our proposed scheme, data users in s-health system can perform lightweight encryption and decryption without leaking any sensitive privacy about attributes of the user. Finally, the formal security analysis, the theoretic performance evaluation and experiment results indicate that the solution is secure and efficient.**

***Index Terms*—Internet of Things, smart health, privacy-aware, policy-hiding, feasible.**

I. Introduction

NOWADAYS, Internet of Things (IoT) has gained broad acceptance and increased adoption in many aspects of our daily life, ranging from healthcare, transportation, smart home, smart city to smart environmental monitoring [1], [2]. IoT technologies render a competent and structured approach to promote wellbeing of mankind especially in the healthcare field [3], [4]. It is estimated that the healthcare sector will be remodeled by IoT-based system. In modern healthcare environment, IoT devices generally include wearable or embedded smart devices and conventional sensors. These smart IoT devices implanted inside or worn on the wearer's body are leveraged in gathering the health data, such as pulse rate, blood pressure, lung volume, temperature etc. In such way, smart health records (SHRs) of the wearer can be created by the collected data. For medical practitioners and healthcare providers, SHRs are indispensable in providing accurate diagnosis and timely medical treatment. Commonly, this setting is also known as IoT-oriented smart health (s-health) system [5], [6] in literature.

In a typical s-health system, health data are universally gathered from the wearable or embedded healthcare IoT devices and then delivered to healthcare cloud server for remotely sharing with medical practitioners and healthcare providers. Due to the privacy-sensitive nature of the health data, many concerns such as data privacy and security remain to be addressed to facilitate this practical application [7], [8]. For instance, patients expect that their SHRs can only be accessed by the authorized medical doctors or healthcare providers. Considering the semi-trusted nature of cloud (i.e., it honestly performs the tasks for delegated data users but also attempts to peek at the information privacy), encryption on privacy-aware data prior to outsourcing is commonly regarded as a straightforward approach to preserve data privacy. Whereas, how to enforce fine-grained access privileges over the SHRs remains a persistent challenge. Ciphertext policy attribute based encryption (CP-ABE) [9], [10] is deemed to be a highly promising solution to realize one-to-many encryption and fine-grained access control over encrypted data. In the CP-ABE scheme, access policy is attached to a ciphertext while secret key is associated with the user attribute set. The data can be accessed by data users in case the set of the user attributes embedded in the secret key matches the access policy related to the ciphertext.

Aside from empowering data providers (e.g., patients) to designate the fine-grained access control over the encrypted SHRs, protecting the attribute privacy of access policy is also crucial in s-health system. By considering the fact that the access policy in the standard CP-ABE is attached to a ciphertext in the plaintext form, it is trivial for the adversary to deduce some private information about the data provider from the access policy. For example, in an s-health system, a patient Alice encrypts her SHR data employing CP-ABE under an access policy pol=("City hospital") AND ("Psychology doctor" OR "Psychiatry doctor"). In this case, the SHR data can only be accessed by a psychology doctor or a psychiatry doctor in City hospital. Despite the SHR data is not accessed by non-authorized users, the sensitive information of Alice can be inferred by these users from the SHR ciphertext. Thus, the

J. Sun, H. Xiong and X. Nie are with the School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China; J. Sun is also with the School of Information and Systems, Singapore Management University, Singapore. (E-mail: sjf215.uestc@gmail.com, xionghu.uestc@gmail.com, xynie@uestc.edu.cn).

X. Liu is with the College of Mathematics and Computer Science, Fuzhou University, Fuzhou, China (E-mail: snbnix@gmail.com).

Y. Zhang is with the National Engineering Laboratory for Wireless Security, Xi'an University of Post and Telecommunications, Xi'an, China (E-mail:yhzhaang@163.com).

R. H. Deng is with the school of information and systems, Singapore Management University, Singapore. (E-mail: robertdeng@smu.edu.sg).

H. Xiong is the corresponding author.

privacy of Alice is violated.

Hence, preventing illegal data users from snooping the attribute privacy from access control raises another challenge. Currently, variants of policy-hidden ABE schemes, i.e., partial policy-hiding [11], [12], [13], [14], [15] and full policy-hiding [18], [19], [16], [17], [20], [21], are used to impede the privacy leakage from the access policy. In the partial policy hiding CP-ABE scheme, only partial attribute values of access policy are anonymized, whereas the access policy itself is still in the plaintext form. For privacy-sensitive s-health system, any leakages of attribute information of access policy may seriously disgrace the privacy of data providers. Consequently, it is significant to design a fully hidden policy CP-ABE scheme that supports the whole attribute-hiding. This ensures that private and sensitive attributes of the data providers in s-health system are completely protected. With the goal of achieving fully hidden policy that reveals nothing about user attributes in access policy, based on hidden vector encryption [20], [21] or inner product encryption [18], [19], [16], Phuong *et al.* [17] put forward a CP-ABE scheme with fully hidden policy by transforming the user attribute set and access policy into respective vector sets. Only when the inner product of two vector sets equals to zero, the attribute set can be used to match the corresponding access policy. In this way, the private information about the access policy is elegantly hidden in the vector set.

However, there are some efficiency defects in their scheme, such as the cumbersome computational tasks for the encryption/decryption and prohibitive ciphertext size. To date, protecting the privacy of the whole attributes, supporting fine-grained and high-efficient access control as well as offering lightweight encryption and decryption overhead still have not been well-solved in literature.

Aiming to resolve these limitations afore-mentioned, a novel approach to transform the access policy and user attribute set into respective vector sets has been proposed to achieve lightweight and privacy-aware fine-grained access control based (LPAC-based) CP-ABE construction. Taking the IoT-oriented s-health system as a use case, we simultaneously tackle the issues of fine-gained and lightweight access policy, online/offline encryption, whole attribute privacy protections. The contributions of this paper are mainly concluded below:

- *Fine-grained and optimized access policy*. In LPAC-based CP-ABE scheme, an optimized vector transformation approach is proposed, which can transform the user attributes and access policy into simpler attribute vector and access vector, respectively. These attribute and access vectors that will be used for key generation and ciphertext generation contribute to lower computation and storage cost in encryption and decryption phases. Thus, the smart healthcare IoT devices can greatly relieve the bandwidth and computation time in both ciphertext generation and data recovery phases.
- *Online/offline encryption*. In LPAC-based CP-ABE scheme, ciphertext generation is split into online and offline phases. That is to say, most of computation-intensive work to encrypt records before gaining the records and access policy is completed in the offline phase while only marginal operations are left to the online phase [32]. To be more specific, the smart healthcare IoT devices complete the offline phase when they have adequate power sources and perform the online phase without ongoing battery consumption. This can lower the risks of the service availability.
- *Stronger attribute privacy protection.* Unlike prior conventional CP-ABE schemes, LPAC-based CP-ABE scheme can render data users with whole attribute privacy protection by hiding the access policy. This can avoid leaking privacy-sensitive attribute information.
- *Lightweight decryption overhead*. In the decryption phase, LPAC-based CP-ABE has constant bilinear pairing operations, which does not increase linearly with the complexity of the specified access policy.

The detailed security proofs are also formally presented to indicate that our LPAC-based CP-ABE scheme is selectively secure under the asymmetric decisional bilinear Diffie-Hellman (DBDH) problem and the $\mathcal{P}$-asymmetric decisional bilinear Diffie-Hellman ($\mathcal{P}$-DBDH) problem in the standard model. In addition, the experimental results from the comprehensive performance comparisons reveal that our LPAC-based CP-ABE scheme is more practical and feasible for IoT-oriented s-health systems. In next subsection, the related literature is introduced.

A. Related Works

Many cryptographic primitives including identity based encryption (IBE) only support a coarse-level access control that severely limits the user's ability to selectively share the encrypted data at a fine-grained level. As a feasible solution, attribute based encryption (ABE) [9], [10] was proposed to enforce the expressive and fine-grained access control over the data, such that only authorized users whose attributes match the access policy can access the encrypted data. ABE takes two various forms: Key policy ABE (KP-ABE) [9] and Ciphertext policy ABE (CP-ABE)[10]. In a KP-ABE scheme, each private key is labeled with an access structure and ciphertexts are bound with a set of attributes. Contrarily, in a CP-ABE scheme, each private key is associated with a sets of attributes and an access policy is attached to the ciphertexts. In many real-world scenarios, CP-ABE scheme is more desirable than KP-ABE scheme since it empowers data owners to autonomously select the access policy over the data. In most existing ABE schemes, many CP-ABE schemes have been suggested, mainly focusing on hierarchical structure [25], efficient construction [15], [27] and security [26]. However, the violations of attribute privacy are not considered in these schemess. So, these traditional CP-ABE schemes are inappropriate for privacy-sensitive applications, like smart healthcare record systems (SHRs) [29], [30] and electronic health record systems (EHRs) [28], [22], since the access policy usually contains sensitive information.

To preserve the attribute privacy of users, many policy-hiding CP-ABE schemes have been studied [11], [12], [17], [13], [14], [15], [24], [23], [31], [29]. A CP-ABE scheme supporting the property of hidden access structures is put

forward by Nishide *et al.* [11]. In which, only partial attribute values are anonymized, however anyone can learn the attribute names. Soon after, several similar CP-ABE schemes with hidden policies were proposed in [14], [13], [15]. Specifically, the schemes in [13], [14] are all proven secure under the composite order groups and the scheme in [15] doesn't support wildcard-based AND gate access structure. Furthermore, these three schemes have the similar privacy leakage issues as that in [11]. Li *et al.* [12] suggested a privacy-aware CP-ABE system that can realize the policy hiding and wildcard-based AND gate, whereas this scheme just can hide partial attributes of users and be proven secure in the random oracle model. A policy-hiding CP-ABE scheme was raised by Lai *et al.* [23], whereas this scheme only supports partial policy-hiding under composite order groups. Moreover, the decryption is inefficient since the number of involved bilinear pairings increases linearly with the complexity of access policy. Built from the scheme [23], a novel partially policy-hiding CP-ABE scheme [29] is recently suggested. Although it can render users with privacy preserving of user attributes, the computation overheard of decryption is still the same as that in [23]. Besides, it is also constructed under composite order groups. The scheme in [24] is constructed to support partially hidden policy under prime order groups, whereas the scheme is also demonstrated to be secure in the random oracle model. In addition, the scheme in [24] cannot support wildcard-based AND gate and its storage and computation cost is linear increasingly with the complexity of access policy. Although privacy protections of user attributes are provided in the above policy-hiding CP-ABE schemes, these schemes just can support partial attribute-hiding property instead of full attribute-hiding property. Thus, it's inappropriate for more privacy-sensitive s-health systems.

To resolve the issue of full attribute hiding, Yang *et al.* [31] put forward a novel fully privacy-preserving CP-ABE scheme based on Bloom Filter. However, the security proof is not provided to formalize the attribute-hiding property. In addition, Phuong *et al.* [17] also proposed a fully hidden policy CP-ABE based on wildcard-based AND access control with the technique of inner product encryption [18], [19], [16], [26], however, the computation and storage overhead in encryption and decryption phase increase linearly with complexity of access policy. Further, the approach to generate the attribute and access vectors used for key generation and ciphertext generation is inefficient, which further results in high computation and storage overhead. Motivated by considerations of full attribute privacy protection, fine-grained and efficient access policy as well as lightweight encryption and decryption simultaneously in the IoT-oriented s-health system, a novel LPAC-based CP-ABE that solves all limitations above urgently requires to be proposed, which motivates this research.

II. Preliminaries

In this section, some cryptographic basic knowledge used in LPAC-based CP-ABE is reviewed. Specifically, the definitions of Viete formulas, AND and wildcard access control are concluded below.

A. Viete Formulas

Let $\vec{v} = (v_1, v_2, \ldots, v_\ell)$ and $\vec{u} = (u_1, u_2, \ldots, u_\ell)$ stand for two vectors, where the former vector contains both alphabets ("$+$", or "$-$") and wildcards ("$*$") while the latter vector only contains alphabets. A position set $I = \{i_1, \ldots, i_n\} \subset \{1, \ldots, \ell\}$ indicates the wildcards positions of $\vec{v}$. Refer to the above descriptions, the statement $((v_i = u_i) \vee (v_i = *)$ for $i \in [1, \ell])$ can be easily derived. Thus, it is not intractable to achieve

$$\sum_{i=1, i\notin I}^{\ell} v_i \prod_{k_w \in I} (i - k_w) = \sum_{i=1}^{L} u_i \prod_{k_w \in I} (i - k_w) \tag{1}$$

If expanding $\prod_{k_w \in I} (i - k_w) = \sum_{j=1}^{n} a_j i^j$, then the coefficients a_j can be easily created relied on set I. Thus, the equation (2) below can be derived from (1):

$$\sum_{i=1, i\notin I}^{\ell} v_i \prod_{k_w \in I} (i - k_w) = \sum_{j=0}^{n} a_j \sum_{i=1}^{L} u_i i^j \tag{2}$$

To hide the equations in (2), a group element B_i is selected at random. When viewing v_i, u_i as B_i's exponents, the equation (3) below can be further obtained from (2)

$$\prod_{i=1, i\notin I}^{L} B_i^{v_i \prod_{k\in I}(i-k)} = \prod_{j=0}^{n} (\prod_{i=1}^{\ell} B_i^{u_i i^j})^{a_j} \tag{3}$$

According to the derivation process of the Viete's formulas, it's simple to see that those coefficients a_j in (2) can be rebuilt by

$$a_{n-j} = (-1)^j \sum_{1\le i_1 < i_2 < \ldots < i_j \le n} k_{i_1} k_{i_2} \ldots k_{i_j}, 0 \le j \le n = |I|. \tag{4}$$

If taking set $I = \{i_1, i_2, i_3, i_4\}$ as an instance, the polynomial is then created as $(i - i_1)(i - i_2)(i - i_3)(i - i_4)$, therefore, we can derive the coefficient values as $a_4 = 1, a_3 = -(i_1+i_2+i_3+i_4)$, $a_2 = (i_1i_2+i_1i_3+i_1i_4+i_2i_3+i_2i_4+i_3i_4)$, $a_1 = -(i_1i_2i_3 + i_1i_2i_4 + i_1i_3i_4 + i_2i_3i_4)$, $a_0 = i_1i_2i_3i_4$.

B. AND-Gate and Wildcard Access Structure

Denote the universe of system attributes as $\mathsf{A} = \{\mathsf{A}_1, \mathsf{A}_2, \ldots, \mathsf{A}_\mathsf{L}\}$, where each A_k, for $k \in \{1, \ldots, \mathsf{L}\}$, owns two possible values, i.e., negative value "$-$" and positive value "$+$". Each user in the system is bound with a set of attributes $\mathsf{U} = \{\mathsf{U}_1, \ldots, \mathsf{U}_\mathsf{L}\}$, where each attribute $\mathsf{U}_k \in \{\text{"}+\text{"}, \text{"}-\text{"}\}$ for $i \in \{1, \ldots, \mathsf{L}\}$. Also, let $\mathbb{W} = \{\mathcal{W}'_1, \ldots, \mathcal{W}'_\mathsf{L}\}$ be an access policy, where each $\mathcal{W}'_k \in \{\text{"}+\text{"}, \text{"}-\text{"}, \text{"}*\text{"}\}$. The wildcard "$*$" signifies that it does not make sense for the corresponding attribute value irrespective of "$+$" or "$-$".

For instance, assume $\mathsf{A} = \{\mathsf{A}_1 = \text{"}\mathsf{CS}\text{"}, \mathsf{A}_2 = \text{"}\mathsf{SE}\text{"}, \mathsf{A}_3 = \text{"}\mathsf{Faculty}\text{"}, \mathsf{A}_4 = \text{"}\mathsf{Student}\text{"}\}$, where "CS" and "SE" stand for computer science and software engineering, respectively. Alice is a faculty who works in CS department. A student Bob studies in SE department. Carol acts as a faculty who works in both CS and SE departments. An access policy $\mathbb{W}_1$ could be matched by all SE faculties without working in the

CS. Another access policy $\mathbb{W}_2$ could be contented by all CS faculties and students excluding those in the SE. The above user attributes and access policies are described in TABLE I.

TABLE I: User Attributes and Access Policies

Attribute	A_1	A_2	A_3	A_4
Description	CS	SE	Faculty	Student
Alice	+	−	+	−
Bob	−	+	−	+
Carol	+	+	+	−
$\mathbb{W}_1$	−	+	+	−
$\mathbb{W}_2$	+	−	*	*

III. Problem Formulation

For ease of following the concrete construction and security of LPAC-based CP-ABE, the system model is first shown. The threat & security models are then presented as the basis of security analysis.

A. System Model

In the system model of LPAC-based CP-ABE, a IoT-oriented smart health scenario is taken as an instance, which involves four types of different entities: Trusted Authority, Data Owner, Healthcare Server Cloud and Data Users in Fig. 1. Specifically, the trusted authority takes charge of the generation of public parameters for the entire system (step ①) and the distribution of secret keys to data users (step ③). The data owner (e.g. patient), who wears tiny wireless sensors or other smart, gathers his/her related SHR information such as pulse rate, blood pressure and lung volume via wireless protocols. After that, the SHRs are encrypted and then transmitted via the base station (step ②) to the cloud server for remotely sharing with multiple authorized data users. When the data user (like medical doctor or researcher) desires to know his/her health condition, he/she requires to deliver his/her attributes to trusted authority for secret key generation. After downloading the SHR ciphertext, the data user then deciphers the SHR ciphertext (step ④).

B. Threat & Security Model

In the threat model, the data owner and the authority are assumed to be fully trusted. The healthcare cloud server is considered as a semi-honest entity that can offer infinite storage computing resources on demand to data users. That is, the healthcare cloud server could render infinite amount of storage, computing power and honestly perform the tasks for data users but also attempts to snoop some sensitive information about the stored data. Prior to introducing the formalized security model, the formal definition of LPAC-based CP-ABE scheme is defined in **Supplemental Material A-A**. Suppose that the adversary $\mathcal{A}$ has a specified ability to launch attacks, the security model is given to analyze the security of the LPAC-based CP-ABE. Besides, the indistinguishability against the selective chosen plaintext attack in LPAC-based CP-ABE is introduced in **Supplemental Material A-B**

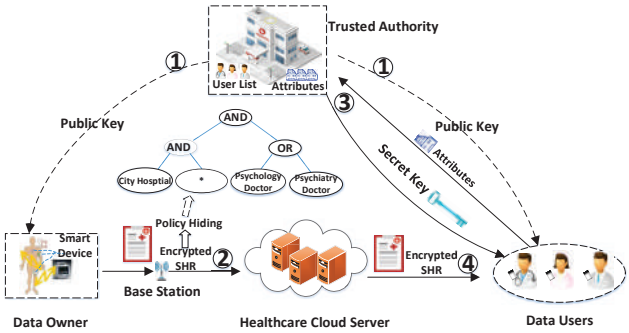


Fig. 1: An architecture of LPAC-based CP-ABE.

Algorithm 1 Previous Attribute and Access Vector Generation Approach

Input: Given an access structure that contains at most ℓ wildcards ("*"), ℓ_+ positive attributes ("+") and ℓ_- negative attributes ("-"); Given a set of user attributes $\mathsf{U} = \{\mathsf{U}_1, \ldots, \mathsf{U}_\mathsf{L}\}$, where each attribute $\mathsf{U}_i \in \{\text{"}+\text{"}, \text{"}-\text{"}\}$ for $i \in \{1, \ldots, \mathsf{L}\}$.

Output: An access vector and two attribute vectors.

1: Positive, negative and wildcard symbols in an access structure are first separated into three position sets J, K and I;
2: **while** $k_w \in I$ **do**
3: Expand $\prod_{k_w \in I} (i - k_w) = \sum_{j=0}^{n} a_j i^j$ to derive coefficients a_j;
4: **end while**
5: **for** $k_w \in I$ and $i \in J$ **do**
6: Compute $\prod_J = + \sum_{i \in J} \prod_{k_w \in I} (i - k_w)$;
7: **end for**
8: **for** $k_w \in I$ and $i \in K$ **do**
9: Compute $\prod_K = - \sum_{i \in K} \prod_{k_w \in I} (i - k_w)$;
10: **end for**
11: Positive and negative symbols in a user attribute set are also separated into two position sets J' and K';
12: **for** $i = 1$ to ℓ and $i \in J'$ **do**
13: Compute $\{u_j = - \sum_{i \in J'} i^j\}$;
14: **end for**
15: **for** $i = 1$ to ℓ and $i \in K'$ **do**
16: Compute $\{u'_j = + \sum_{i \in K'} i^j\}$;
17: **end for**
18: Return access vector $\vec{v} = (a_0, a_1, \ldots, a_n, 0_{n+1}, \ldots, 0_\ell, \prod_J, \prod_K)$, attribute vectors $\vec{u}_{J'} = (u_0, u_1, \ldots, u_\ell, 1, 0)$ and $\vec{u}_{K'} = (u'_0, u'_1, \ldots, u'_\ell, 0, 1)$.

$\underline{\mathsf{Setup}}(1^\lambda)$: This algorithm is performed by trusted authority. Based on a security parameter 1^λ, it randomly chooses an asymmetric bilinear map group $(\mathbb{G}_0, \mathbb{G}_1, \mathbb{G}_2, p, g, h, e)$ such that $e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_2$, where g, h are corresponding generators of groups $\mathbb{G}_0, \mathbb{G}_1$ of the same prime order p. Also, it randomly picks $\alpha, \theta, \sigma, \rho, \tau_1 \ldots, \tau_n \in \mathbb{Z}_p$, computes $g_0 = g^\rho, g_1 = g^\alpha, g_{1,1} = g^{\tau_1}, \ldots, g_{1,n} = g^{\tau_n} \in \mathbb{G}_0$ and $h_0 = h^\sigma, h_1 = h^\alpha, h_{1,1} = h^{\tau_1}, \ldots, h_{1,n} = h^{\tau_n} \in \mathbb{G}_1$. Finally, it outputs the public parameter $\mathsf{PP} = (g, g_0, g_1, g_{1,1} \ldots, g_{1,n}, U = e(g, h^\sigma)) \in \mathbb{G}_0^{n+3} \times \mathbb{G}_2$ and holds the master secret key $\mathsf{MSK} = (h, h_0, h_1, h_{1,1} \ldots, h_{1,n}) \in \mathbb{G}_1^{n+3}$ securely.

$\underline{\mathsf{KeyGen}(\mathsf{PP}, \mathsf{MSK}, \vec{u})}$: It is also executed by trusted authority. According to PP, MSK and an attribute vector $\vec{u} = (u_1, \ldots, u_n)$, it picks $r_1, s_1 \in \mathbb{Z}_p$ at random and generates the secret key $\mathsf{SK} = (sk_1, sk_2, sk_3, u_1, \ldots, u_n)$ as $sk_1 = h^\sigma \prod_{i=1}^{n} (h_{1,i})^{u_i r_1} h_1^{s_1}, sk_2 = h^{r_1}, sk_3 = h^{s_1}$.

$\underline{\mathsf{Offline.Encrypt}\ (\mathsf{PP}, \mathbb{W})}$: This algorithm is pre-performed by data owner. Relied on PP and access policy $\mathbb{W}$, it randomly picks $t, \rho_1, \ldots, \rho_n \in \mathbb{Z}_p$ and creates the offline ciphertext $\mathsf{Off.CT}$ and the access vector $\vec{v} = (v_1, \ldots, v_n)$ as

$$\begin{aligned}\mathsf{Off.CT} &= (U^t, g^t, g_{1,1}^t g_0^{-\rho_1}, \ldots, g_{1,n}^t g_0^{-\rho_n}, g_1^t) \\ &= (C_0', C_1, \{C_{1,i}\}_{i\in[1,n]}, C_2).\end{aligned}$$

It finally stores intermediate result $(\mathsf{Off.CT}, t, \rho_1, \ldots, \rho_n)$ and $\vec{v} = (v_1, \ldots, v_n)$ for the online.encryption algorithm.

$\underline{\mathsf{Online.Encrypt}\ (\mathsf{PP}, \mathsf{Off.CT}, M, \vec{v})}$: This algorithm is also completed by data owner. Depended on PP, the plaintext message M, the pre-stored offline parameter $(\mathsf{Off.CT}, t, \rho_1, \ldots, \rho_n)$ and the access vector $\vec{v} = (v_1, \ldots, v_n)$, it first computes $C_0 = M \cdot U^t$, $e_i = \rho_i + t v_i \mod p$ and then generates the ciphertext $\mathsf{CT} = (C_0, C_1, C_{1,i}, C_2, e_1, \ldots, e_n)$.

$\underline{\mathsf{Decrypt}\ (\mathsf{PP}, \mathsf{CT}, \mathsf{SK})}$: This algorithm is conducted by data user. Based on PP and $\mathsf{SK} = (sk_1, sk_2, sk_3)$, it recovers the plaintext message $M = C_0/(E_1 {E_0}^{-1})$ if the attributes content the access policy, where $E_0 = e(g_0^{\sum_{i=1}^{n} e_i u_i} \prod_{i=1}^{n} (C_{1,i})^{u_i}, sk_2)$ and $E_1 = e(sk_3, C_2)^{-1} e(sk_1, C_1)$.

Fig. 2: The concrete construction of LPAC-based CP-ABE

IV. Our LPAC-based CP-ABE in s-health System

A. High Level of Attribute and Access Vector Generation

In this section, we discover an optimized vector transformation technique shown in **Algorithm 2**, which can efficiently make a conversion from user attribute set and access policy to attribute vector and access vector. Compared to the previous vector transformation technique in **Algorithm 1** introduced in [17], our approach can generate a smaller number of attribute vectors and access vector with shorter length, which will be efficiently used for key generation and encryption. In [17], the scheme is inefficient in terms of both computation and communication cost. The basic reason of the defeats originates from the fact that redundant information is embedded in the vectors corresponding to the access policy and attribute sets, and thus this kind of vectors will result in considerable computation and communication overhead in key generation, encryption and decryption phases.

Specifically, by observation of the process of attribute and access vector generation in **Algorithm 1**, it is easy to observe that since the sets J' and K' are mutually exclusive sets, only one of them actually needs to be used for producing the attribute vector. In other words, there is no need simultaneously to produce two vectors $\vec{u}_{J'}$ and $\vec{u}_{K'}$ for key generation. As shown in **Algorithm 2**, an optimized vector transformation method is presented.

B. Our Concrete Construction of LPAC-based CP-ABE

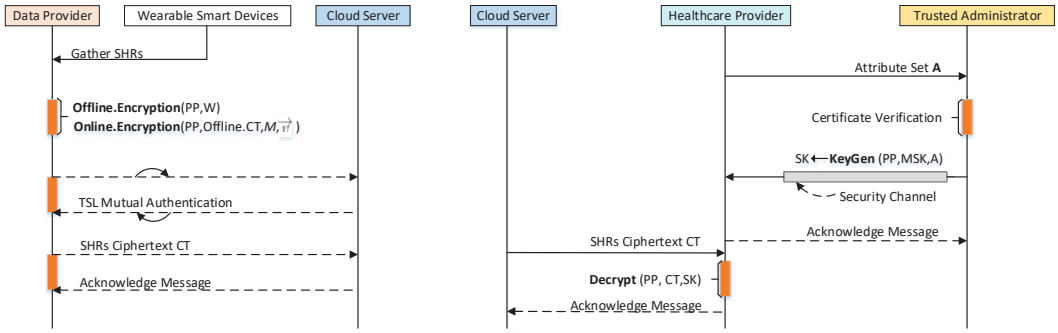
With the goal of realizing LPAC-based attribute based encryption, our main thought is to transform user attribute set and access control into attribute vector and access vector. These

Algorithm 2 Optimized Attribute and Access Vector Generation Approach

Input: Given an access structure that contains at most ℓ wildcards ("*"), ℓ_+ positive attributes ("+") and ℓ_- negative attributes ("-"); Given a set of user attributes $\mathsf{U} = \{\mathsf{U}_1, \ldots, \mathsf{U}_\mathsf{L}\}$, where each attribute $\mathsf{U}_i \in \{\text{"}+\text{"}, \text{"}-\text{"}\}$ for $i \in \{1, \ldots, \mathsf{L}\}$.

Output: An access vector and an attribute vector.

1: Positive and wildcard symbols in an access structure only need to be separated into two position sets J and I;
2: **while** $k_w \in I$ **do**
3: Expand $\prod_{k_w \in I} (i - k_w) = \sum_{j=0}^{n} a_j i^j$ to derive coefficients a_j;
4: **end while**
5: **for** $k_w \in I$ and $i \in J$ **do**
6: Compute $\prod = + \sum_{i \in J} \prod_{k_w \in I} (i - k_w)$;
7: **end for**
8: Only positive symbols in a user attribute set are separated into one position set J';
9: **for** $i = 1$ to ℓ and $i \in J'$ **do**
10: Compute $\{u_j = + \sum_{i \in J'} i^j\}$;
11: **end for**
12: Return the access vector $\vec{v} = (a_0, a_1, \ldots, a_n, 0_{n+1}, \ldots, 0_\ell, \prod)$ and the attribute vector $\vec{u}_{J'} = (u_0, u_1, \ldots, u_\ell, -1)$.



(a) SHRs uploading

(b) Key distribution & SHRs accessing

Fig. 3: Protocol modules in s-health system.

vectors that will be correspondingly used for key generation and ciphertext generation are more lightweight. Additionally, to speed up the ciphertext generation, time-consuming encryption preprocessing is performed, which leaves smart devices with lightweight computation cost. In other words, most of computation-intensive operations are completed in the encryption preprocessing under offline mode. Our LPAC-based CP-ABE consists of five algorithms: Setup, KeyGen, Offline.Encrypt, Online.Encrypt and Decrypt. The concrete construction of LPAC-based CP-ABE is presented in Fig. 2.

Remark: Our LPAC-based CP-ABE can largely offload the computation-intensive burden on smart devices in s-health scenario. Before key generation and ciphertext generation, the attribute set and access policy are simplified into the simpler attribute vector and access vector, respectively. Commonly, simpler attribute vector and access vector that are used for key generation and ciphertext generation mean lower computation and storage cost. In addition, to further ease the computation cost of ciphertext generation, in offline.Encrypt, most of burdensome tasks are pre-completed when smart devices have sufficient capacity and power. In Decrypt, data users can quickly recover the plaintext message. Due to the lightweight encryption and decryption, we will present how to extend the LPAC-based CP-ABE in the s-health system in following subsection.

C. Deployment of LPAC-based CP-ABE in IoT-oriented S-Health System

In this section, LPAC-based CP-ABE is exploited as the main building block to build an s-health system for smart healthcare IoT devices. In detail, the s-health system also comprises four types of entities: trusted system administrator, patient, medical doctor/research, healthcare cloud server, which is almost the same to Fig. 1. The trusted system administrator works as the authority to take charge of the generation of public parameters for the entire s-health system and the distribution of secret keys to patients, doctors or researches. The patient acts as the data provider who wears tiny wireless sensors or other smart healthcare IoT devices, which can continuously monitor and generate related SHR information, such as pulse rate, blood pressure and lung volume. After that, the SHRs are encrypted and transmitted to the healthcare cloud server for remotely sharing with multiple authorized data users. The medical doctor or researcher acts as the healthcare provider decrypts the encrypted SHRs. Subsequently, we present the protocol of LPAC-based CP-ABE in IoT-oriented s-health scenario, which mainly involves three protocol modules in Fig. 3: SHRs uploading, key distribution and SHRs accessing.

In the SHRs uploading module (see Fig. 3(a)), the SHRs are gathered from distinct smart devices via base station by the data provider (refer to the patient), subsequently, the collected SHRs are encrypted by performing Offline.Encrypt $(\mathsf{PP}, \mathbb{W})$ and Online.Encrypt $(\mathsf{PP}, \mathsf{Off.CT}, M, \vec{v})$ in LPAC-based CP-ABE. Finally, the SHRs encryptions are delivered to healthcare cloud server for remotely sharing with healthcare provider. Practically, to verify the fact that the delivered SHRs ciphertext has been indeed received, the healthcare cloud server responds an acknowledge message to data provider. Note that with the patient's TLS (Transport Layer Security) handshake, the mutual authentication can be gained, which ensures that the SHRs are sent by the patient and have been stored on target healthcare cloud server.

In the key distribution module (see the right part of Fig. 3(b)), the healthcare provider (refer to medical doctor/researcher) sends his/her attribute set to the trusted administrator, then the trusted administrator performs certificate verification to ensure the healthcare provider's legitimacy, afterwards uses the vector transformation technique to convert the attribute set into simpler attribute vector and finally call $\mathsf{KeyGen}(\mathsf{PP}, \mathsf{MSK}, \vec{u})$ to create the secret key SK, which is then transmitted to the healthcare provider via the security channel (e.g. SSL, Secure Sockets Layer).

In the SHRs accessing module (see the left part of Fig. 3(b)), with the secret key SK, after downloading the SHRs ciphertext $\mathsf{CT} = (C_0, C_1, C_{1,i}, C_2, e_1, \ldots, e_n)$, the healthcare provider calls Decrypt $(\mathsf{PP}, \mathsf{CT}, \mathsf{SK})$ to recover the SHRs.

V. Security and Performance Analysis

Now, the security and performance of LPAC-based CP-ABE are analyzed (Sections V-A and V-A, respectively). Due to the

TABLE II: Attack-resistance ability comparisons of listed CP-ABE schemes

Scheme	Replay attack	User impersonation attack	Denial-of-service attack	User anonymity	Collusion attack	Man-in-the-middle attack
[11], [12]	×	✓	×	×	✓	×
[13], [14]	×	✓	×	×	✓	×
[15]	×	✓	×	×	✓	×
[24]	×	✓	×	×	✓	×
[23]	×	✓	×	×	✓	×
[29]	×	✓	×	×	✓	×
[31]	×	✓	×	✓	✓	×
[17]	×	✓	×	✓	✓	×
Ours	✓	✓	✓	✓	✓	✓

TABLE III: Comparisons of hidden policy CP-ABE schemes

Scheme	Order Group	Access Structure	Hardness Assumption	Asymmetric Pairing	Wildcard	Online/Offline encryption	Full Privacy Awareness	Standard Model
[11], [12]	Prime	AND-gates on multi-valued attributes	DBDH+DLIN	×	✓	×	×	×
[13], [14]	Composite	AND-gates on multi-valued attributes	Subgroup Assumption	✓	✓	×	×	✓
[15]	Prime	LSSS	Decisional (q-1) assumption+DLIN	×	×	×	×	✓
[24]	Prime	AND-gates on multi-valued attributes	n-BDHE	×	×	×	×	×
[23]	Composite	LSSS	DBDH+DLIN	✓	×	×	×	✓
[29]	Composite	LSSS	DBDH+DLIN	✓	×	×	×	✓
[31]	Prime	LSSS	q-BDHE Assumption	×	×	×	✓	×
[17]	Prime	AND-gates on +/-	DBDH+DLIN	×	✓	×	✓	✓
Our scheme	Prime	AND-gates on +/-	DBDH+$\mathcal{P}$-DBDH	✓	✓	✓	✓	✓

TABLE IV: Performance comparisons of hidden policy CP-ABE schemes under prime order groups in the standard model

Scheme	Public Parameter Size	Secret Key Size	Ciphertext Size	Setup Cost	KeyGen Cost	Offline/Online Encryption Cost	Decryption Cost
[17]	$(8n+28)\lvert\mathbb{G}_0\rvert+\lvert\mathbb{G}_2\rvert$	$(4n+14)\lvert\mathbb{G}_0\rvert$	$(4n+14)\lvert\mathbb{G}_0\rvert+\lvert\mathbb{G}_2\rvert$	$(8n+27)\mathsf{Exp}_0+\mathsf{Exp}_2$	$13(n+3)\mathsf{Exp}_0$	$-/(12n+38)\mathsf{Exp}_0+\mathsf{Exp}_2$	$(4n+14)\mathsf{Pair}$
Ours	$(n+5)\lvert\mathbb{G}_0\rvert+\lvert\mathbb{G}_2\rvert$	$3\lvert\mathbb{G}_1\rvert+(n+2)\lvert\mathbb{Z}_p\rvert$	$(n+4)\lvert\mathbb{G}_0\rvert+\lvert\mathbb{G}_2\rvert+(n+2)\lvert\mathbb{Z}_p\rvert$	$(n+5)\mathsf{Exp}_0+\mathsf{Pair}$	$(n+6)\mathsf{Exp}_0$	$(2n+6)\mathsf{Exp}_0+\mathsf{Exp}_2/0$	$3\mathsf{Pair}+(n+3)\mathsf{Exp}_1$

space limitation, the correctness of LPAC-based CP-ABE is omitted here.

A. Security Analysis

Provided that the selective security game similar to the security game in [33] could not be breached by the adversary $\mathcal{A}$, then our LPAC-based CP-ABE can achieve the selective-security against chosen plaintext attacks (CPA). The security of LPAC-based CP-ABE can be ensured by the following theorem.

Theorem 1: The LPAC-based CP-ABE scheme is said to achieve the policy-hiding property and be selectively CPA-secure in the standard model under the DBDH & $\mathcal{P}$-DBDH problems [33] shown in **Supplemental Material A-C**.

Proof: The detailed security proofs are shown in **Supplemental Material B**.

We also consider very few attacks in this section to show the security strength of our scheme in IoT-oriented s-health system against existing relevant attacks such as replay attack, user impersonation attack, denial-of-service attack, user anonymity, collusion attack, man-in-the-middle attack, etc.

As shown in TABLE II, we can observe that the works [11], [12], [13], [14], [15], [24], [23], [29] neither resist replay attack, denial-of-service attack and man-in-the-middle attack, nor support user anonymity, while they are capable of blocking both user impersonation attack and collusion attack. The works [31], [17] are prone to suffering from replay attack, denial-of-service attack, man-in-the-middle attack and replay attack but support user anonymity, collusion-resistance attack and user impersonation-resistance attack. Compared to the above mentioned works, only our work has the ability to defend replay attack, user impersonation attack, denial-of-service attack, collusion attack, man-in-the-middle attack, and considers the user anonymity. Specifically, in our IoT-oriented s-health application, the certification verification and TSL mutual authentication are correspondingly used for checking whether the attributes of a healthcare provider are authenticated by trusted authority and testing whether a data provider is permitted within the specified timestamp to deliver the raw data to cloud, which ensures that illegal users do not have any ability to prove as a valid user to successfully send previously used authentication messages during the authentication and verification phases. As a consequence, our work can resist replay and man-in-the middle attacks. Since the cloud server only works as storing the data of data providers and any non-authorization entity has no legal secret key, any non-authorization entity cannot forge and send a valid decryption request to derive the target data. So, user impersonation attack is blocked in ours. Besides, the hiding-policy technique is used to hide the specified attributes of access policy, which makes

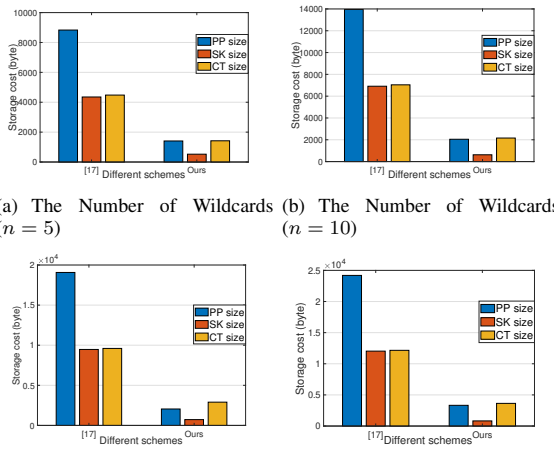
that any users cannot derive any user attribute information from access policy. Consequently, the user anonymity can also be realized. As one of the principal security challenges in all ABE works is to resist collusion attack, our work can ensure that colluding attackers cannot decrypt the ciphertext unless their own attribute sets satisfy the access policy of the ciphertext. In addition, during the message transmission, the acknowledge message as the authentication is used for mutual successful authentication. If an attacker blocks the messages from reaching a user and the cloud, the uses and cloud will know about malicious dropping of such control messages. Hence, the denial-of-service attack is prevented in our work.

B. Performance Analysis

In this section, previous related works supporting privacy protection of user attributes [11], [12], [17], [13], [14], [15], [24], [23], [29] are compared with our scheme in terms of security model, access structure, hardness assumption and other performance features. In table III, the comprehensive comparisons are given according to important features containing group type, wildcard, online/offline encryption, pairing type, full privacy awareness, standard model. We denote linear secret share scheme, decisional linear assumption and q-bilinear Diffie-Hellman exponent problem as LSSS, DLIN assumption and q-BDHE problem, respectively. As presented in table III, we can find that our scheme and the schemes [13], [14], [23], [29] support asymmetric pairing operations whereas the rest of other schemes [11], [12], [17], [15], [24], [31] only support symmetric pair operations. Further, in these schemes supporting asymmetric pairing operations, only our scheme is online/offline construction based on prime group. As well, we can also see that only our scheme and the scheme [17] can render users with full privacy protection while the remainder schemes can just support partial privacy protection. In addition, we can conclude that only our scheme and the schemes [13], [14], [17] are wildcard constructions and secure in the standard model. In summary, according to the above analyzing, only our LPAC-based CP-ABE scheme is both wildcard construction and under prime group construction while simultaneously achieving asymmetric pairing operation, online/offline encryption, full privacy protection in the standard model.

Further, we exclude [11], [12], [13], [14], [15], [24], [23], [29] from comparisons because they cannot provide full privacy awareness and some of them are under composite order constructions. In this way, we just make a quantitative analysis for performance comparisons between the scheme [17] and our scheme in table IV, where we represent public parameters, secret key and ciphertext as PP, SK and CT, respectively. In our experimental simulations, type A elliptic curve, as the fastest pairing among all types of elliptic curves, is chosen to implement the experiments. The curve expression E of type-A curve is $y^2 = x^3 + x$ over $\mathbb{F}_q$ finite field. Thus, the length of one element in each group $\mathbb{G}_0$, $\mathbb{G}_1$ and target group $\mathbb{G}_2$ is set to 1024 bits and the length of one element in $\mathbb{Z}_p$ is set to 160 bits. Exp_0, Exp_1, Exp_2 and Pair are exploited to denote an exponentiation computation in $\mathbb{G}_0$, an exponentiation computation in $\mathbb{G}_1$, an exponentiation computation in $\mathbb{G}_2$ and a bilinear pairing computation, respectively. Let n denote the number of wildcards in the access policy. It can be seen in table IV that the public key size, secret key size and ciphertext size in our scheme are much smaller than those in [17] although these sizes in [17] and ours increase linearly with the number of wildcards. Additionally, from table IV, we can also find that our scheme completely outperforms the scheme [17] respecting the size of the setup cost, the key generation cost, the encryption cost and the decryption cost. To sum up, our scheme has an excellent performance compared to the scheme [17] with respect to the storage and computation cost. For clarity, the comparisons of related sizes are presented in Fig. 4(a), Fig. 4(b), Fig. 4(c) and Fig. 4(d), where we assume that n is set to 5, 10, 15, 20, respectively for the convenience of comparison.

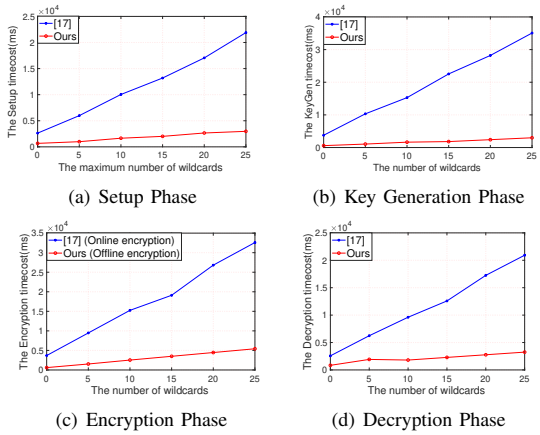
To clearly present the performance comparisons, we conduct experiments to evaluate the performance of ours and Phuong *et. al*'s work [17] based on the latest JPBC library [34] for underlying cryptographic operations. The configuration is as



(a) The Number of Wildcards ($n = 5$) (b) The Number of Wildcards ($n = 10$)

(c) The Number of Wildcards ($n = 15$) (d) The Number of Wildcards ($n = 20$)

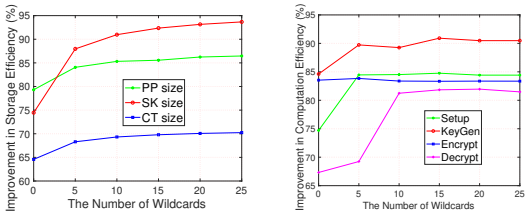
Fig. 4: Storage Cost Comparison of PP, SK and CT.



(a) Setup Phase (b) Key Generation Phase

(c) Encryption Phase (d) Decryption Phase

Fig. 5: Computation Cost Comparison of Different Phases.



(a) Improvement in Storage Cost (b) Improvement in Computation Cost

Fig. 6: Improvement in Storage and Computation Efficiency.

follows: All the experiments are compiled in the JAVA 8 language with the version of Intellij IDEA-2018.2.5, where each user is replaced by a Huawei Android 6.0.1 phone equipped with 3GB RAM, two-core 2.36GHz Cortex A73 processor and two-core Cortex A53 1.8 GHz processor. The " Cloud " is simulated with a Lenovo server which has Inter(R) Core(TM) i7-7700 CPU @3.60 GHz @3.60 GHz and 8GB RAM, 512SSD, 1TB mechanical hard disk and runs on the Windows 10 64 bits operating system.

In Fig. 5, we compare [17] with our scheme with regard to the setup time, key generation time, the encryption time and the decryption time. Specifically, the setup time, key generation time, the encryption time and the decryption time with the number of wildcard change in access policy are correspondingly depicted in Fig. 5(a), Fig. 5(b), Fig. 5(c) and Fig. 5(d). From Fig. 5, we can easily see that the computation cost of each phase in our proposed scheme is much lower than that in [17]. In Fig. 6, we present our improvement in storage and computation efficiency compared to [17]. As shown in Fig. 6, compared with [17], the saved storage cost ranges are $79.31\% \sim 86.46\%$, $74.46\% \sim 93.67\%$, $64.58\% \sim 70.24\%$ respectively in terms of PP size, SK size and CT size. The saved computation cost ranges are $74.71\% \sim 84.42\%$, $84.62\% \sim 90.48\%$, $83.34\% \sim 83.84\%$, $67.33\% \sim 81.48\%$, respectively with respect to the Setup, KeyGen, Encrypt and Decrypt phases.

In conclusion, our LPAC-based CP-ABE scheme outperforms the existing schemes. Particularly, our scheme supports more lightweight storage and computation cost while it enjoys versatile properties presented in table III. Therefore, our proposed scheme is more applicable for the s-health system.

VI. Conclusion

In this paper, an optimized vector transformation approach was suggested to efficiently transform the user attributes and access policy into more succinct attribute vector and access vector. Then, with this approach and the online/offline computation technology, we proposed a novel LPAC-based CP-ABE scheme that was designed for IoT-oriented s-health system. More specifically, our LPAC-based CP-ABE scheme supports stronger attribute privacy protection, lightweight and fine-grained access policy, online/offline encryption and efficient decryption. The elaborated security proofs and performance evaluation were presented to prove that LPAC-based CP-ABE scheme gained selectively CPA security in the standard model and was practical and efficient. One of our future researches would be to build a fully policy-hiding CP-ABE with fully CPA-security under prime order groups. On the other hand, seeking attribute revocation, traceability and CCA-based mechanisms based on our scheme are also considered in our future work.

Acknowledgment

This work was supported in part by the 13th Five-Year Plan of National Cryptography Development Fund for Cryptographic Theory of China under Grant MMJJ20170204, in part by the Guangxi Colleges and Universities Key Laboratory of Cloud Computing and Complex Systems, in part by the Sichuan Science and Technology Project under Grant 2018KZ0007, in part by Open Foundation of State Key Laboratory of Networking and Switching Technology under Grant SKLNST-2019-2-13 (Beijing University of Posts and Telecommunications), in part by the Major International (Regional) Joint Research Project of China National Science Foundation under grant No.61520106007.

References

[1] A. Bassi, G. Horn., "Internet of Things in 2020: A Roadmap for the Future", *European Commission: Information Society and Media*, vol. 22, pp. 97-114, 2008.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, et al., "Internet of things: A survey on enabling technologies, protocols, and applications", *IEEE Communications Surveys & Tutorials,* vol. 17, no. 4, pp. 2347-2376, 2015.

[3] J. Sun, S. Hu, X. Nie X, et al., "Efficient ranked multi-keyword retrieval with privacy protection for multiple data owners in cloud computing", *IEEE Systems Journal,* DOI: 10.1109/JSYST.2019.2933346, 2019.

[4] D. Chen, N. Zhang, Z. Qin, et al., "S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol", *IEEE Internet of Things Journal,* vol. 4, no. 1, pp. 88-100, 2017.

[5] A. Solanas, C. Patsakis, M. Conti, et al., "Smart health: a context-aware health paradigm within smart cities", *IEEE Communications Magazine,* vol. 52, no. 8, pp. 74-81, 2014.

[6] G. Muhammad, S. Rahman, A. Alelaiwi, et al., "Smart health solution integrating IoT and cloud: a case study of voice pathology monitoring", *IEEE Communications Magazine,* vol. 55, no. 1, pp. 69-73, 2017.

[7] Y. Yang, L. Wu, G. Yin, et al., "A survey on security and privacy issues in internet-of-things", *IEEE Internet of Things Journal,* vol. 4, no. 5, pp. 1250-1258, 2017.

[8] X. Liu, B. Qin, R. Deng, et al., "An efficient privacy-preserving outsourced computation over public data," IEEE Transactions on Services Computing, vol. 10, no. 5, pp. 756-770, 2017.

[9] V. Goyal, O. Pandey, A. Sahai, et al., "Attribute-based encryption for fine-grained access control of encrypted data", *ACM CCS 2006,* pp. 89-98, 2006.

[10] R. Ostrovsky, A. Sahai, B. Waters, "Attribute-based encryption with non-monotonic access structures", *ACM CCS 2007,* pp. 195-203, 2007.

[11] T. Nishide, K. Yoneyama, K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures", *International Conference on Applied Cryptography and Network Security,* Springer, pp. 111-129, 2008.

[12] J. Li, K. Ren, B. Zhu, et al., "Privacy-Aware Attribute-Based Encryption with User Accountability", *International Conference on Information Security,* Springer, pp. 347-362, 2009.

[13] J. Lai, R. Deng, Y. Li, "Fully secure cipertext-policy hiding CP-ABE", *International Conference on Information Security Practice and Experience,* Springer, pp. 24-39, 2011.

[14] C. Jin, X. Feng, Q. Shen, "Fully Secure Hidden Ciphertext Policy Attribute-Based Encryption with Short Ciphertext Size", *International Conference on Communication and Network Security,* ACM, pp. 91-98, 2016.

[15] H. Cui, R. Deng, G. Wu, et al., "An Efficient and Expressive Ciphertext-Policy Attribute-Based Encryption Scheme with Partially Hidden Access Structures", *Provable Security,* Springer, pp. 19-38, 2016.

[16] T. Phuong, G. Yang, W. Susilo, "Poster: Efficient ciphertext policy attribute based encryption under decisional linear assumption," *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS 2014)*, pp. 1490-1492, 2014.
[17] T. Phuong, G. Yang, W. Susilo, "Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions", *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 35-45, IEEE, 2014.
[18] T. Okamoto, K. Takashima, "Fully secure unbounded inner-product and attribute-based encryption", *ASIACRYPT 2012*, Springer, Berlin, Heidelberg, LNCS 7658, pp. 349-366, 2012.
[19] P. Datta, T. Okamoto, J. Tomida, "Full-Hiding (Unbounded) Multi-input Inner Product Functional Encryption from the k-Linear Assumption", *IACR International Workshop on Public Key Cryptography (PKC 2018)*, Springer, Cham, LNCS 10770, 245-277, 2018.
[20] V. Iovino, G. Persiano, "Hidden-vector encryption with groups of prime order", *International Conference on Pairing-Based Cryptography,* Springer, Berlin, Heidelberg, LNCS 5209, pp. 75-88, 2008.
[21] T. Phuong, G. Yang, W. Susilo, "Efficient hidden vector encryption with constant-size ciphertext", *European Symposium on Research in Computer Security,* Springer, Cham, LNCS 8712, pp. 472-487, 2014.
[22] H. Yuan, X. Chen, J. Li, et al., "Secure Cloud Data Deduplication with Efficient Re-encryption", *IEEE Transactions on Services Computing,* DOI: 10.1109/TSC.2019.2948007, 2019.
[23] J. Lai, R. Deng, Y. Li, "Expressive CP-ABE with partially hidden access structures", *ACM Symposium on Information, Compuer and Communications Security (ASIACCS'12)*, ACM, pp. 18-19, 2012.
[24] Y. Zhang, X. Chen, J. Li, et al., "Anonymous attribute-based encryption supporting efficient decryption test", *ACM Symposium on Information, Computer and Communications Security (ASIACCS'12)*, ACM, pp. 511-516, 2013.
[25] S. Wang, J. Zhou, J. Liu, et al., "An efficient file hierarchy attribute-based encryption scheme in cloud computing", *IEEE Transactions on Information Forensics and Security,* vol. 11, no. 6, pp. 1265-1277, 2016.
[26] J. Park, "Inner-product encryption under standard assumptions", *Designs, Codes and Cryptography,* vol. 58, no. 3, pp. 235-257, 2011.
[27] J. Sun, H. Xiong, H. Zhang, L. Peng, "Mobile access and flexible search over encrypted cloud data in heterogeneous systems", *Information Sciences,* vol. 507, no. 1-15, 2020.
[28] J. Sun, H. Xiong, R. H. Deng, et al., "Lightweight Attribute-Based Keyword Search with Policy Protection for Cloud-Assisted IoT", *IEEE Conference on Dependable and Secure Computing (DSC)*, pp, 1-8, IEEE, 2019.
[29] Y. Zhang, D. Zheng, R. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control", *IEEE Internet of Things Journal*, IEEE, vol. 5, no. 3, pp. 2130-2145, 2018.
[30] G. Xu, H. Li, Y. Dai, et al., "Enabling efficient and geometric range query with access control over encrypted spatial data", *IEEE Transactions on Information Forensics and Security,* vol. 14, no. 4, pp. 870-885, 2018.
[31] K. Yang, Q. Han, H. Li, et al., "An efficient and fine-grained big data access control scheme with privacy-preserving policy", *IEEE Internet of Things Journal,* vol. 4, no. 2, pp. 563-571, 2017.
[32] S. Hohenberger, B. Waters, "Online/offline attribute-based encryption", *International Workshop on Public Key Cryptography,* Springer, Berlin, Heidelberg, LNCS 8383, pp. 293-310, 2014.
[33] I. Kim, S. Hwang, J. Park, et al., "An Efficient Predicate Encryption with Constant Pairing Computations and Minimum Costs", *IEEE Transactions on Computers,* vol. 65, no. 10, pp. 2947-2958, 2016.
[34] B. Lynn, JPbc library, accessed: Jan. 2020, Available: http://crypto.stanford.edu/jpbc/.

Jianfei Sun is currently pursuing the Ph.D. degree with the School of Information and Software Engineering, University of Electronic Science and Technology of China. His research interests include public key cryptography and network security.

Hu Xiong received the Ph.D. degree from the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC) in 2009. He is currently a full professor with the School of Information and Software Engineering, UESTC. His research interests include applied cryptography and cypberspace security. He is a member of IEEE.

Ximeng Liu received Ph.D. degrees from Xidian University, China, in 2015. Now, he is a full professor at College of Math- ematics and Computer Science, Fuzhou Univer- sity, China. He has published over 100 research articles include IEEE TIFS, TDSC, TC, TII, TSC and TCC. His research interests include cloud security, applied cryptography and big data security.

Yinghui Zhang received his Ph.D degree in Cryptography from Xidian University, China, in 2013. He is a professor at School of Cyberspace Security, National Engineering Laboratory for Wireless Security (NELWS), Xi'an University of Posts & Telecommunications. He has published over 80 research articles in ACM ASIACCS, IEEE TDSC, IEEE TSC, IEEE TCC, IEEE IoTJ, IEEE TII, etc. His research interests include public key cryptography, cloud security and wireless network security.

Xuyun Nie received the Ph.D. degree in information security from the Graduate University of Chinese Academy of Sciences, Beijing, China, in 2007. He is currently an Associate Professor with the University of Electronic Science and Technology of China. His research interests include cryptography and information security.

Robert H. Deng is AXA Chair Professor of Cybersecurity and Professor of Information Systems in the School of Information Systems, Singapore Management University since 2004. His research interests include data security and privacy, multimedia security, network and system security. He has received the Distinguished Paper Award (NDSS 2012), Best Paper Award (CMS 2012), Best Journal Paper Award (IEEE Communications Society 2017). He is a fellow of the IEEE.