The ISC Int'l Journal of Information Security
ISeCure

July 2021, Volume 13, Number 2 (pp. 87–100)
http://www.isecure-journal.org

Privacy Preserving Attribute-Based Encryption with Conjunctive Keyword Search for E-health Records in Cloud

Aniseh Najafi [1], Majid Bayat [2], and Hamid Haj Seyyed Javadi [1,*]

[1] Department of Mathematics and Computer Science, Shahed university, Tehran, Iran.
[2] Department of Computer Engineering, Shahed University, Tehran, Iran.

ARTICLE INFO.

Article history:
Received: April 18, 2020
Revised: October 3, 2020
Accepted: April 8, 2021
Published Online: May 8, 2021

Keywords:
Attribute-Based Searchable Encryption, Hidden Policy, Keyword Guessing Attack, Secure Channel Free, Standard Model

Type: Research Article

doi: 10.22042/isecure.2021.227562.542

dor: 20.1001.1.20082045.2021.13.2.1.6

ABSTRACT

The advent of cloud computing in the healthcare system makes accuracy and speed increased, costs reduced, and health services widely used. However, system users are always seriously concerned about the security of outsourced data. The ciphertext-policy attribute-based encryption (CP-ABE) is a promising way to ensure the security of and facilitate access control over outsourced data. However, conventional CP-ABE schemes have security flaws such as lack of attribute privacy and resistance to the keywords guessing attacks as well as the disability to multi-keyword searches. To meet such shortcomings, we present a scheme supporting multi-keyword search and fine-grained access control, simultaneously. The proposed scheme is resistant to the offline keywords guessing attack. Privacy-preserving in the access structure is another feature of the proposed scheme. The security analysis indicates that our scheme is selectively secure in the standard model. Finally, the performance evaluation of the proposed scheme shows the efficiency is reasonable despite the added functionalities.

1 Introduction

Cloud computing along with the internet of things (IoT) as a kind of fundamental technologies in smart cities are applied in the electronic healthcare industry to develop health systems, health monitoring, and health management[1]. Electronic health systems are developed to realize remote diagnosis, improve treatment accessibility and quality, and share and store patient information [2]. With the rapid development of IoT technologies and cloud computing, the e-health industry is expected to quickly reach the point of the desired service. However, there are still many unresolved problems, especially the simultaneous realization of privacy and accessibility. In the e-health system, electronic health record (EHR) contains patient sensitive information, such as demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, personal statistics like age and weight, and billing information. Suppose a patient decides to submit his EHR to the number of sightly experts. For this purpose, there are two problems: on the one hand, he must use encryption and access control methods to protect privacy; On the other hand, to easy access the desired EHRs among the large volume of datasets, the ability of search over encrypted data is a necessity of e-health systems. Although the most patients expects only authorized professional health caregivers to access his encrypted EHR, most of the available

[*] Corresponding author.

Email addresses: ensiyeh.najafi@shahed.ac.ir, mbayat@shahed.ac.ir, h.s.javadi@shahed.ac.ir

ISSN: 2008-2045 © 2020 ISC. All rights reserved.

access control methods violate the patient's privacy in the fine grained-access control. In addition, encryption methods with hidden access control usually do not allow searching over encrypted datasets.

Attribute-based encryption (ABE) presents a promising solution to privacy-preserving of outsourced electronic health records [3]. ABE schemes are placed into one of KP-ABE (Key Policy-ABE) [4] and CP-ABE (ciphertext policy-ABE) [5] categories depending on the access policy's placement in the ciphertext or secret key. In healthcare systems, the CP-ABE scheme is applicable because the patient needs to exert access policies over his EHR. Access policy is actually an access structure that is built based on patient attributes and is explicitly accessible to anyone who has access to encrypted EHR. Therefore, in most ABE schemes, the privacy of the attributes used in the access structure has not been realized [4–14], however, disclosure of access policies can leak sensitive information to malicious viewers. For example, if the access policy of an EHR consist of statement ("hospital A" AND "expert B"), the malicious viewer can detect the information about the residence area and the disease of the EHR owner, by observing the hospital name and the type of expert, which leads to information leakage and violation of patient privacy. On the other hand, although encrypting and then outsourcing EHRs would preserve data privacy, all data must be downloaded and decrypted to obtain some part of the data. Clearly, the computation and communication costs of this method are not affordable.

Hidden access policies can solve the privacy problem of attribute-based encryption. Hiding the attributes in the access structure can be done in two ways: partial hiding and full hiding. In CP-ABE with partially hidden access policies, the name of the attribute is obvious and its value is hidden, while in CP-ABE with fully hidden access policies, both the name and the value of the attributes are hidden. However, there is a trade-off between privacy and efficiency: the CP-ABE schemes with partially hidden access policies have better efficiency and instead have more privacy leaks, while the CP-ABE schemes with fully hidden access policies provide less efficiency despite the more privacy.

The promising method to solve the secure accessibility problem is searchable encryption as a paradigm that provides search functionality over the encrypted data [15, 16]. Using searchable encryption, the data owner can extract indicator keywords from his dataset and send the encrypted forms along with the encrypted data to the cloud server. Using an encrypted form of query keywords named trapdoor, the data user demands searching over encrypted data from the cloud server. The cloud server sends the search results to the data user after a secure search on the encrypted data. Searchable encryption methods are divided into two categories: symmetric and asymmetric. Symmetric searchable encryption (SSE) schemes provide only coarse-grained access control by sending the owner's private key through a secure channel [17]. Therefore, using these schemes in health systems is not efficient. In the traditional asymmetric searchable encryption (or public-key encryption with keyword search (PEKS)), in particular ABE providing fine-grained access control, the malicious adversary can launch an offline keyword guessing attack (KGA) [18, 19]. To this end, the adversary makes the ciphertext of all keywords in the dictionary. This is possible because of the keyword space polynomial size. The data user sends the cloud server a trapdoor that the adversary grabs through eavesdropping the channel. It then searches over the encrypted keywords and extracts the contents of the trapdoor. For this reason, public-key encryption with keyword search schemes vulnerable to keyword guessing attack requires a secure channel for trapdoor transmission. A designated server technique is applied in some PEKS schemes to prevent this attack so that it is only the server that can execute the search algorithm [13, 20–23]. However, most attribute-based encryptions with keyword search (ABKS) schemes [10, 24–28] do not support other featheres such as hidden access policy, secure multi-keyword search in the standard model, and security against keyword guessing attack, simultaneously.

1.1 Our Contribution

In this paper, based on inner product encryption, we present an attribute-based encryption scheme with keyword search for the healthcare system that is resistant to offline keyword guessing attacks in the standard model. In the proposed scheme, hidden access policy along with multi-keyword search are the features required to outsource large volume sensitive data such as health information, which provides privacy preserving and selective recovery, simultaneously. To the best of our knowledge, there is no secure ABKS scheme with multi-keyword search and fully hidden access policy, in the standard model. The main contribution of this paper is summarized as follows.

- **Attribute privacy**: In our scheme, attributes of access structure are hidden in prime order group so that malicious viewers do not understand sensitive information about the electronic health record and its privileged data users.
- **Search functionality**: The proposed scheme supports searching over encrypted data that lead to efficient and secure storage and selective retrieval of health information. For healthcare system, our scheme is the first proper secure channel free ABKS scheme with a hidden access

policy secured in the standard model in comparison to the previous ones.
- **Multi-keyword search**: we add conjunctive keyword search functionality to our scheme to improve search quality. The data user can receive all results including all query keywords with once sending the trapdoor.
- **Security against keyword guessing attack**: Using the designated cloud server, we design a scheme that is secure against KGA in standard model. In this way, the data user can send the trapdoor securely through the public channel to the cloud server.
- **And gate policies with wildcard**: Access policy is defined by and-gate with positive, negative and wildcard values for attributes, in our scheme. So far, none of the proposed searchable encryption schemes support and-gate with wildcard using only one group element to represent an attribute with three possible values.

1.2 Organization

The paper is organized as follows: Section 2 deals with the related work. Section 3 is entitled preliminaries associated with problem statement and basic definitions required for designing the proposed scheme. Section 4 provides the proposed model. Section 5 presents the security and performance analysis of our scheme. The final Section covers the conclusion.

2 Related Work

Authorization is an essential requirement of many information systems, especially healthcare. Applying attribute-based encryption primitive fulfills this requirement by providing fine-grained access control. However, the security and functionalities of most of the ABE schemes presented so far do not meet the necessities of the real world. Therefore, researchers were encouraged to add features to ABE schemes such as hierarchical access structure, hidden policy, search functionality, and traceability.

Using CP-ABE in healthcare systems, the attributes in the access structure may carry user sensitive information although the content of the data remains unknown, indicating that the attribute privacy is more important than other functionalities of an ABE scheme. Nishide *et al.* [29] proposed the first partially hidden CP-ABE with AND-gate policies. Presenting the fully hidden access policy scheme where the size of the ciphertext grows based on the number of attributes, Lai *et al.* [30] and Phuong *et al.* [31] developed Nishides work. Overcoming the problem of ciphertext size, Jin *et al.* [32] presented a fully secure scheme in the standard model where the access structure is defined using AND-gate with positive, negative and wildcard. In addition, Zhang *et al.* [33] introduce a fully secure privacy-aware smart health access control system with partially hidden access policy in the standard model. Then, some efforts have been made to improve efficiency and functionality, considering the possibility of a hidden access policy [34–39]. However, none of these schemes support keyword searches.

Large volume of sensitive healthcare data requires the privacy of data along with efficiency of their recovery. For the first time, the authors of [40] presented CP-ABKS schemes to realize fine-grained access control and keyword search, at the same time. In [41], the authors design an anonymous attribute based searchable encryption that is secure under the selective ciphertext-policy with chosen plaintext attack and under the selective ciphertext-policy with chosen keyword attack. However, the structure of CP-ABKS schemes is vulnerable against keyword guessing attack [18, 19]. Keyword space polynomial-size leads the attacker to generate all ciphertexts. Then, attacker launches offline keyword guessing attack over all ciphertexts, captures trapdoor, and then obtains the content of the trapdoor. Miao et al, [42] proposed a verifiable KGA secure scheme with keyword search, fine-grained access control and data-owner updating, in standard model. Furthermore, Qiu *et al.* [43] presented the first CP-ABKS scheme supporting keyword search and hidden access structure resistant against KGA. Adding shared multi-owner and traceability functionalities, the proposed scheme in [24] improved the work presented by Qiu *et al.* [43]. Recently, Chaudhari and Das [44] proposed a KGA secure CP-ABKS scheme with hidden access policy that performs the search operation efficiently. This scheme takes constant time complexity for single-index and linear time complexity for multi-index dataset. Nevertheless, the recent reviewed schemes do not support multi-keyword search and security in the standard model.

To search over encrypted personal health records, Miao *et al.* [26] design a secure cryptographic primitive called ciphertext policy attribute based on multi-keyword searchable encryption which is selectively secure against chosen keyword attack. In other work, Miao *et al.* [10] proposed a scheme with a hierarchical data structure and multi-keyword search functionality non resistant against KGA. For big data-based mobile healthcare networks, Chen *et al.* [11] present a verifiable keyword search scheme with fine-grained access control. Recently, Xu *et al.* [13] design an efficient multi-keyword searchable scheme supporting online/offline encryption and outsourcing decryption. Based on inner product encryption, Chen *et al.* [45] enhance an ABKS scheme with conjunctive keyword search functionality and security against KGA. Un-

Table 1. Notations

Notation	Description
U	The set of attribute universe
L	The number of attribute universe
N_1	Maximum number of wildcard attributes in access structure
N_2	Maximum number of positive attributes in access structure
N_3	Maximum number of negative attributes in access structure
l	Maximum number of extracted keyword from a ducument
$b \overset{R}{\leftarrow} B$	Random selection b of set B
$[n]$	$\{1, \ldots n\}$

fortunately, none of the recent schemes supports the attributes privacy in the access structure.

In [46], the secure proposed scheme provide attribute privacy and search functionality using a secure channel. However, compared to access control in our proposal, these schemes do not support and gate policies with wildcard. In addition, Wang *et al.* [47] design a scheme with almost the capabilities of [46], in which, despite being more efficient, it is not secure channel free and secure in the standard model. A secure channel free and policies hiding searchable encryption scheme with conjunctive keyword search proposed in [48] that is secure in the standard model. Unfortunately, the cloud server and the user can collude for searching without access permission. Moreover, these scheme leaks some sensitive information from the index and the trapdoor.

3 Preliminaries

This section presents some required preliminaries in two basic definition and problem statement subsections.

3.1 Basic Definition

Notations: Table 1 presents the notations of the paper.

Bilinear Map: Let G and G_T be cyclic groups of prime order p and $g \in G$ is generator of G. A bilinear pairing is a map $e : G \times G \to G_T$ with the following properties:

- Bilinearity: $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for all $g_1, g_2 \in G$, $a, b \in \mathbf{Z}$,
- Non-degeneracy: $e(g, g) \neq 1$, in which 1 is identity element of G_T,
- Computability: There is an efficient algorithm to compute $e(g_1, g_2)$ for any $g_1, g_2 \in G$.

Decisional Deffi-Hellman (DDH) Assumption: Pick random generator $g \in G$ and random elements $a, b \in \mathbb{Z}_q$. The DDH assumption is defined as: Given (g, g^a, g^b, g^{ab}, Z), distinguish whether $Z = g^{ab}$ or $Z \overset{R}{\leftarrow} \mathbb{Z}_q$ with the non-negligible advantage in the polynomial time.

Viete Formula: Let $J = \{j_1, \ldots, j_n\} \subset \{1, \ldots, L\}$. Based on J, we consider identity polynomial $\prod_{j\in J}(i - j) = \sum_{k=0}^{n} \lambda_k i^k$. The coefficients of this polynomial are constructed according to the viete's formula as follows:

$$\lambda_{n-k} = \sum_{1\le i_1<i_2<\cdots<i_k\le n} j_{i_1} \ldots j_{i_k}, \qquad 0 \le k \le n, \tag{1}$$

where $n = |J|$.

Inner Product Predicate: Functional encryption [49] as a new paradigm allows the data owner to specify a policy describing how data users can decrypt the ciphertext without knowing the information of these users. Predicate encryption is a functional encryption sub-class in which the user gains a plaintext function, decrypting the ciphertext. If user attributes satisfy the ciphertext access policy or, in other words, the evaluation of the predicate is 1, decryption will be fulfilled.

The access policy is public in some of the functionalities proposed for predicate encryption so far such as ID-based encryption [50] and attribute-based encryption [3]. However, in most applications such as healthcare and military, access policy leaks sensitive information. Some suggested predicate encryption systems such as anonymous identity-based encryption [16], hidden vector encryption [5], and inner product predicate [49] have been used to make the access policy hidden. In our scheme, we apply the inner product predicate. Evaluation of inner product predicate will be 1 if a dot product operation is equal to 0 and otherwise is 0.

Access Structure: Let $\{Att_1, \ldots, Att_L\}$ be the ordered set of system attributes. AND-gate with wildcard access policy is represented by $P = \{P_1, \ldots, P_L\}$, where each P_i can have one of $+$, $-$ and $*$ values. The positive and negative values for P_i, respectively, mean requisiteness of the presence and absence of the attribute in the user attribute set. The wildcard $*$ implicates both positive and negative accepted values for attributes. On the other hand, each user in the system is identified by the set $S = \{S_1, \ldots, S_L\}$ where value of any S_i is $+$ or $-$. The user attribute set will satisfy the access policy if the value of attributes corresponding to the positive values in the access policy is positive, and that corresponding to the negative

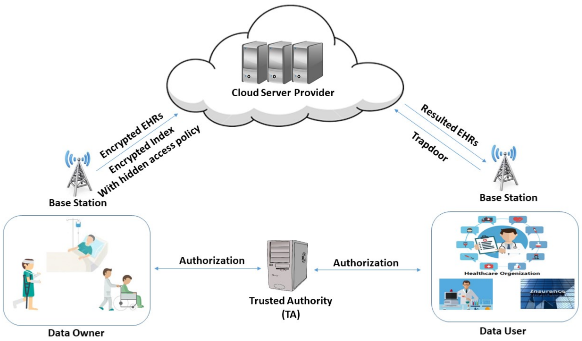


Figure 1. Architecture of the secure outsourcing of EHRs in an e-health system

values in the access policy is negative.

3.2 Problem Statement

System Model: There are four entities in the proposed scheme as follows: the trusted authority (TA), cloud server provider, data owner or patient, and data user - a physician, surgeon, researcher, etc. Figure 1 depicts the overview of the secure outsourcing process to the cloud, the entities, and their relationships to implement the process.

TA is responsible for initializing the system and granting fine-grained access privilege to data users based on their attributes.

The cloud server has abundant storage and computational resources and stores the EHRs and the corresponding indexes. It is also responsible for searching operations on encrypted data.

Using the traditional encryption algorithm such as AES or DES, the patient encrypts his EHRs to preserve privacy. The owner of records defines a different access policy for the keyword set extracted from each EHR and encrypts the extracted keyword set as the index form. Then, she/he sends the encrypted EHRs and indexes to the cloud server.

To get the desired encrypted data, the data user sends her/his attributes to the TA and receives the secret key corresponding to the attributes. The data user then sends the trapdoor corresponding to requested keywords to the cloud server. The cloud server returns the resulted files after searching on the encrypted EHRs. The records selected in the search phase, in addition to including the requested keywords have an access policy satisfied by the user attributes.

Threat Model: In the proposed scheme, the cloud server is an honest-but-curious entity that executing the search algorithm honestly can infer some sensitive information of the patients out of curiosity. On the other hand, outside adversary intends to infer privacy information by eavesdropping and analyzing the indexes and trapdoors transmitted on a public channels. Regarding attribute privacy, the adversary (cloud server or outside attacker) may obtain sensitive information through attributes in the access structure. Patients, TA, and data users are fully trusted. The cloud server is assumed not to collude with the outside attacker.

Design Goal: Our proposed scheme for the e-health cloud aims to achieve the following goals.

- EHR Confidentiality: Due to the high sensitivity of healthcare data, EHRs and the extracted keywords should be protected from unauthorized access.
- Fine-grained Access Control: To eliminate the inherent drawback of public-key cryptography, we aim to apply fine-grained access structure in our scheme to provide one-to-many rather than one-to-one searchable encryption and to lead flexible access control over EHRs.
- Conjunctive Keyword Search: By a single search query, the data user can receive records containing multiple keywords simultaneously. Searching with multiple keywords reduces the computation and communication overhead significantly. In addition, the data user can receive the most relevant documents instead of many documents, which may be unrelated.
- Attribute Privacy Protection: Access policy, which is visible to anyone with access to ciphertext, may reveal sensitive information to attackers in the healthcare cloud system. Protecting the privacy of the access structure to Improve the privacy of patients is one of our goals in the proposed scheme.
- Security against Keyword Guessing Attack: The small size of the keyword space, index generating only using public parameters and keywords and, the public check ability of the index and trapdoor adaptability or non-adaptability make the outside attacker succeed in index generating all the keywords and adaptability checking all of them with the trapdoor to launch the offline keyword guessing attack. For this reason, the PEKS schemes use the secure channel to send the trapdoor for security against KGA. We aim to design a scheme where the use of a public channel does not threaten the security of query keywords.
- Secure Channel Free: In a secure channel free searchable encryption system, a cloud server must be designated as a tester and only the designated server can run the search algorithm. This eliminates the need to transmit trapdoors keywords through a secure channel.

4 Construction

In this section, we first present the framework of our scheme and security model of it. Then, we explain how an attribute-based encryption scheme enhances to a secure channel free scheme with fully hidden access control and search functionality, simultaneously. Finally, we prove that our proposal is policy hiding ABKS scheme and secure resistance selectively keyword guessing attack based on the standard model.

4.1 Overview of Our Scheme

- $Setup(k, U) \rightarrow (PP, MSK)$. The *setup* algorithm takes security parameter k and attribute universe set as input. It outputs public parameters PP and master secret key MSK.
- $KeyGen_U(PP, MSK, S) \rightarrow SK_U$. The $KeyGen_U$ algorithm takes public parameters PP, master secret key MSK and attribute set $S \subset U$ from data user. It outputs secret key SK, related to S.
- $KeyGen_S(k) \rightarrow (PK_S, SK_S)$. The $KeyGen_S$ algorithm takes the security parameter of the system as an input. It output a secret key (PK_S, SK_S) for the cloud server.
- $IndGen(PP, W) \rightarrow CT$. The $BuildInd$ algorithm takes keyword set W and public parameters PP as input. It output index CT as the ciphertext of the keyword set.
- $TrapGen(PP, SK, Q) \rightarrow T$. The $TrapGen$ algorithm takes public parameter PP, secret key SK, and query keyword set Q as input. It generates trapdoor T related to Q.
- $Search(PP, CT, T) \rightarrow \{0, 1\}$. The $Search$ algorithm takes public parameter PP, index CT and trapdoor T as input. If there are all query keywords in the index, It outputs 1, otherwise, 0.

4.1.1 Security Model

The main challenge in the security of our scheme is to investigate the indistinguishability of the indexes and the hidden access policies. To solve this challenge, we apply the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$.

- Init. $\mathcal{A}$ outputs the challenge access policies P_0, P_1 and the extracted keyword sets W_0, W_1.
- Setup. The $\mathcal{B}$ runs the setup algorithm and gives public parameters PP to the $\mathcal{A}$.
- Phase 1. $\mathcal{A}$ submits attribute set L adaptively to generate a secret key with the condition that attribute set L does not satisfy access policies P_0, P_1. Moreover, $\mathcal{A}$ submits the access policy P and keyword set W. $\mathcal{B}$ returns ciphertext $CT_{P,W}$ to $\mathcal{A}$. $\mathcal{A}$ can repeat these queries polynomial time.
- Challenge. Once the adversary $\mathcal{A}$ decides that phase 1 is over, the challenger $\mathcal{B}$ flips a random coin $b \in \{0, 1\}$ and returns CT_{P_b, W_b} to $\mathcal{A}$.
- Phase 2. $\mathcal{A}$ continues to adaptively query the challenger for secret keys and ciphertexts corresponding to sets of attributes and access policies along with keyword sets, respectively. Non of the attribute sets related to the received secret keys matches P_0 or P_1.
- Guess. The adversary $\mathcal{A}$ outputs a guess bit $b' \in \{0, 1\}$ and wins the game if $b' = b$. The advantage of $\mathcal{A}$ is defined $\left|Pr[b' = b] - \frac{1}{2}\right|$ and the proposed scheme with hidden access policy is selectively secure if for any probabilistic polynomial-time adversary $\mathcal{A}$

$$Adv_{\mathcal{A}}(k) = \left| Pr[b, = b] - \frac{1}{2} \right| < \epsilon,$$

where ϵ is negligible.

4.2 Concrete Construction

The proposed scheme is defined with six randomized algorithms as follows:

- $Setup(k, U) \rightarrow (PK, MSK)$. Let G and G_T are the cyclic groups of prime order q and g be a random generator of G. Moreover, let $e : G \times G \rightarrow G_T$ be a bilinear pairing and $n = N_1 + l + 4$. According to the security parameter k and universe attribute set U, for $i \in [n]$, TA randomly selects $u_{1,i}, u_{2,i}, w_{1,i}, w_{2,i}, \gamma, \theta \xleftarrow{R} \mathbb{Z}_q$, so that $\gamma(u_{2,i} - u_{1,i})$ and $\eta(w_{2,i} - w_{1,i})$ is equal to the constant random numbers $\Delta_1, \Delta_2 \in \mathbb{Z}_q$, respectively. In the end, TA obtains the public parameters PP and the master secret key MSK as

$$\begin{aligned} PP =& (g, G, G_T, p, e, H, \{U_{1,i}, U_{2,i}\}_{i=1}^{n}, \\ & \{W_{1,i}, W_{2,i}\}_{i=1}^{n}, V, Y), \end{aligned}$$

$$MSK = \left(\{u_{1,i}, u_{2,i}\}_{i=1}^{n}, \{w_{1,i}, w_{2,i}\}_{i=1}^{n}, \gamma, \theta\right),$$

Where, for $i \in [n]$, $U_{1,i} = g^{u_{1,i}}$, $U_{2,i} = g^{u_{2,i}}$, $W_{1,i} = g^{w_{1,i}}$, $W_{2,i} = g^{w_{2,i}}$, $V = g^{\gamma}$ and $Y = g^{\theta}$.
- $KeyGen_U(PP, MSK, S) \rightarrow SK_U$. Let $V' \subset \{1, \ldots, L\}$ concludes locations of the positive attributes and $Z' \subset \{1, \ldots, L\}$ concludes locations of the negative attribute in S. TA constructs two vectors

$$\overrightarrow{x_V} = (x_{v_i}) = \left(v'_0, \ldots, v'_{N_1}, 1, 0\right),$$
$$\overrightarrow{x_Z} = (x_{z_i}) = \left(z'_0, \ldots, z'_{N_1}, 0, 1\right),$$

in which

$$v'_k = -\sum_{i \in V'} i^k, \quad k = 0, \ldots, N_1,$$
$$z'_k = -\sum_{i \in Z'} i^k, \quad k = 0, \ldots, N_1.$$

using PP and MSK, TA generates user secret key related to the attribute set S as follows

$$\{K_{1,i}, K_{2,i}\}_{i=1}^{N_1+3} = \left\{g^{f_1 u_{2,i} x_{v_i}}, g^{-f_1 u_{1,i} x_{v_i}}\right\}_{i=1}^{N_1+3},$$
$$\{K_{3,i}, K_{4,i}\}_{i=1}^{N_1+3} = \left\{g^{f_2 w_{2,i} x_{z_i}}, g^{-f_2 w_{1,i} x_{z_i}}\right\}_{i=1}^{N_1+3},$$
$$\left\{K'_{1,i}, K'_{2,i}\right\}_{i=N_1+4}^{n} = \left\{g^{f_1 u_{2,i}}, g^{-f_1 u_{1,i}}\right\}_{i=N_1+4}^{n},$$
$$\left\{K'_{3,i}, K'_{4,i}\right\}_{i=N_1+4}^{n} = \left\{g^{f_2 w_{2,i}}, g^{-f_2 w_{1,i}}\right\}_{i=N_1+4}^{n}.$$

Then, the secret key SK_U associated with the attribute set S is set as

$$SK_U = (\{K_{1,i}, K_{2,i}, K_{3,i}, K_{4,i}\}_{i=1}^{N_1+3}, \\ \{K'_{1,i}, K'_{2,i}, K'_{3,i}, K'_{4,i}\}_{i=N_1+4}^{n}).$$

- $KeyGen_S(k, PP) \rightarrow (PK_S, SK_S)$. The cloud server generates the random number $x \in \mathbb{Z}_{||}$ and creates PK_S and SK_S for the cloud server, where $PK_S = g^x$ and $SK_S = x$.
- $IndGen(PK, W) \rightarrow CT$. Let $W = \{w_1, \ldots, w_{l_1}\}$, $l_1 \leq l$, be extracted keywords from EHR, and $f = \sum_{t=0}^{l_1} \eta_t x^t$ be a polynomial such that, $H(w_1), \ldots, H(w_{l_1})$ as the roots of f and $\eta_t = 0$, $l_1 < t \leq l$. Suppose $P = \{P_1, \ldots, P_L\}$ to be the access structure with $n_1 < N_1$ wildcard, $n_2 < N_2$ positive and $n_3 < N_3$ negative positions. Let J, V and Z be the sets of attributes positions with wildcard, positive and negative values, respectively. To construct the index corresponding to the access policy and keyword set W, data owner firstly computes $\Gamma_V = +\sum_{i \in V} \prod_{t_j \in J}(i - t_j)$ and $\Gamma_Z = -\sum_{i \in Z} \prod_{t_j \in J}(i - t_j)$ values and based on viete formula obtains the polynomial coefficients related to the position of wildcards in the access policy, namely $\{a_0, \ldots a_{n_1}\}$. The index vector is

$$v = (a_0, \ldots, a_{n_1}, 0_{n_1+1}, \ldots, 0_{N_1}, \Gamma_V, \Gamma_Z, \\ \eta_0, \ldots, \eta_l). \qquad (2)$$

To encrypt index vector $v = (v_i)$, data owner selects random elements $s, s_1, s_2, \alpha, \beta \in \mathbb{Z}_q$ and, using the public parameters and public key of the cloud server, generates ciphertext as follows:

$$C_1 = X^s V^{s_1}, \quad C_2 = X^s Y^{s_2}, \quad C_3 = g^s,$$
$$\{C_{1,i}, C_{2,i}\}_{i=1}^{n} = \{U_{1,i}^{s_1} V^{v_i \alpha}, U_{2,i}^{s_1} V^{v_i \alpha}\}_{i=1}^{n},$$
$$\{C_{3,i}, C_{4,i}\}_{i=1}^{n} = \{W_{1,i}^{s_2} Y^{v_i \beta}, W_{2,i}^{s_2} Y^{v_i \beta}\}_{i=1}^{n}.$$

The encrypted index vector is as follows

$$CT = (C_1, C_2, C_3, \{C_{1,i}, C_{2,i}\}_{i=1}^{n}, \\ \{C_{3,i}, C_{4,i}\}_{i=1}^{n}).$$

- TrapGen(PK,SK,Q) → T. To generate the trapdoor related to query keywords $\{w_{i_1}, \ldots, w_{i_m}\}$, data user generates the random numburs $r_{1,i}, r_{2,i} \in \mathbb{Z}_q$, $i \in [n]$, computes $q_j = m^{-1} \sum_{t=1}^{m} H(w_{i_t})^j$, for $0 \leq j \leq l$, and, using the public parameters and her/his secret key, creates trapdoor as

$$T_{1,i} = \begin{cases} A_i^{-1} K_{1,i}, & 1 \leq i \leq N_1 + 3 \\ A_i^{-1} \left(K'_{1,i}\right)^{q_{i-N_1-3}}, & N_1 + 3 < i \leq n \end{cases},$$
$$T_{2,i} = \begin{cases} A_i K_{2,i}, & 1 \leq i \leq N_1 + 3 \\ A_i \left(K'_{2,i}\right)^{q_{i-N_1-3}}, & N_1 + 3 < i \leq n \end{cases},$$
$$T_{3,i} = \begin{cases} B_i^{-1} K_{3,i}, & 1 \leq i \leq N_1 + 3 \\ B_i^{-1} \left(K'_{3,i}\right)^{q_{i-N_1-3}}, & N_1 + 3 < i \leq n \end{cases},$$
$$T_{4,i} = \begin{cases} B_i K_{4,i}, & 1 \leq i \leq N_1 + 3 \\ B_i \left(K'_{4,i}\right)^{q_{i-N_1-3}}, & N_1 + 3 < i \leq n \end{cases},$$

$$T'_{1,i} = g^{-u_{2,i} r_{1,i}}, \quad T'_{1,i} = g^{u_{1,i} r_{1,i}},$$
$$T'_{1,i} = g^{-w_{2,i} r_{2,i}}, \quad T'_{1,i} = g^{w_{1,i} r_{2,i}},$$

where $A_i = V^{r_{1,i}}$, $B_i = Y^{r_{2,i}}$ and $t_i = t^i$. The trapdoor related to query keywords $\{w_{i_1}, \ldots, w_{i_m}\}$ is set as

$$T = (\{T_{1,i}, T_{2,i}, T_{3,i}, T_{4,i}\}_{i=1}^{n}, \\ \{T'_{1,i}, T'_{2,i}, T'_{3,i}, T'_{4,i}\}_{i=1}^{n}).$$

- Search(PP,CT,T) → {0,1}. Applying public parameters, each index associated with EHRs and trapdoor, the cloud server checks equation

$$\prod_{j=1}^{2} \prod_{i=1}^{n} e(C_1, T'_{j,i}) e(C_2, T'_{j+2,i}) \qquad (3)$$
$$\prod_{j=1}^{4} \prod_{i=1}^{n} e(C_{j,i}, T_{j,i}) = e(C_3, \prod_{j=1}^{4} \prod_{i=1}^{n} T'_{j,i})^x.$$

If Equation 3 is true, the output of the search algorithm will be 1, otherwise, 0.

4.3 Correctness

We now show the correctness of the test Equation 3: the cloud server check whether the attributes of the trapdoor sender T satisfies the access structure embedded in the given encrypted index CT and CT contains all of the keywords specified by T.

$$e(C_1, T'_{1,i}) = e(X^s V^{s_1}, g^{-u_{2,i} r_{1,i}}) \\ = e(g^{sx}, T'_{1,i}) e(g^{s_1 \gamma}, g^{-u_{2,i} r_{1,i}}),$$

$$e(C_1, T'_{2,i}) = e(X^s V^{s_1}, g^{u_{1,i} r_{1,i}}) \\ = e(g^{sx}, T'_{2,i}) e(g^{s_1 \gamma}, g^{u_{1,i} r_{1,i}}),$$

$$e(C_2, T'_{3,i}) = e(X^s Y^{s_2}, g^{-w_{2,i} r_{2,i}}) \\ = e(g^{sx}, T'_{3,i}) e(g^{s_2 \theta}, g^{-w_{2,i} r_{2,i}}),$$

$$
\begin{aligned}
e(C_2, T'_{4,i}) &= e(X^s Y^{s_2}, g^{w_{1,i} r_{2,i}}) \\
&= e(g^{sx}, T'_{4,i}) e(g^{s_2\theta}, g^{w_{1,i} r_{2,i}}),
\end{aligned}
$$

Then, we have

$$
\begin{aligned}
&\prod_{j=1}^{2}\prod_{i=1}^{n} e(C_1, T'_{j,i}) e(C_2, T'_{j+2,i}) = \\
&\prod_{j=1}^{4}\prod_{i=1}^{n} e(g^{sx}, T'_{j,i}), \\
&\prod_{i=1}^{n} e(g,g)^{s_1\gamma\ r_{1,i}(u_{1,i}-u_{2,i})} e(g,g)^{s_2\theta\ r_{2,i}(w_{1,i}-w_{2,i})} = \\
&e(g,g)^{-s_1\gamma\ \Delta_1 \sum_{i=1}^{n} r_{1,i}}. \\
&e(g,g)^{-s_2\theta\ \Delta_2 \sum_{i=1}^{n} r_{2,i}} e(C_3, \prod_{j=1}^{4}\prod_{i=1}^{n} T'_{j,i}).
\end{aligned}
$$

For $1 \leq i \leq N_1 + 3$,

$$
\begin{aligned}
e(C_{1,i}, T_{1,i}) &= (U_{1,i}^{s_1} V^{v_i \alpha}, V^{-r_{1,i}} g^{f_1 u_{2,i} x_{v_i}}), \\
e(C_{2,i}, T_{2,i}) &= (U_{2,i}^{s_1} V^{v_i \alpha}, V^{r_{1,i}} g^{-f_1 u_{1,i} x_{v_i}}).
\end{aligned}
$$

$$
\begin{aligned}
e(C_{3,i}, T_{1,i}) &= (W_{1,i}^{s_2} Y^{v_i \beta}, Y^{-r_{2,i}} g^{f_2 w_{2,i} x_{z_i}}), \\
e(C_{2,i}, T_{2,i}) &= (W_{2,i}^{s_2} Y^{v_i \beta}, Y^{r_{2,i}} g^{-f_2 w_{1,i} x_{z_i}}).
\end{aligned}
$$

and for $N_1 + 3 < i \leq n$,

$$
\begin{aligned}
e(C_{1,i}, T_{1,i}) &= (U_{1,i}^{s_1} V^{v_i \alpha}, V^{-r_{1,i}} g^{f_1 u_{2,i} q_i}), \\
e(C_{2,i}, T_{2,i}) &= (U_{2,i}^{s_1} V^{v_i \alpha}, V^{r_{1,i}} g^{-f_1 u_{1,i} q_i}).
\end{aligned}
$$

$$
\begin{aligned}
e(C_{3,i}, T_{1,i}) &= (W_{1,i}^{s_2} Y^{v_i \beta}, Y^{-r_{2,i}} g^{f_2 w_{2,i} q_i}), \\
e(C_{2,i}, T_{2,i}) &= (W_{2,i}^{s_2} Y^{v_i \beta}, Y^{r_{2,i}} g^{-f_2 w_{1,i} q_i}).
\end{aligned}
$$

Then,

$$
\begin{aligned}
&\prod_{j=1}^{4}\prod_{i=1}^{n} e(C_{j,i}, T_{j,i}) = \prod_{i=1}^{N_1+3} e(g,g)^{s_1\gamma\ r_{1,i}(u_{2,i}-u_{1,i})}. \\
&\quad e(g,g)^{\gamma\ v_i \alpha f_1 x_{v_i}(u_{2,i}-u_{1,i})} \\
&\quad = \prod_{i=1}^{N_1+3} e(g,g)^{s_2\theta\ r_{2,i}(w_{2,i}-w_{1,i})}. \\
&\quad e(g,g)^{\theta\ v_i \beta f_2 x_{z_i}(w_{2,i}-w_{1,i})} \\
&\quad = \prod_{i=N_1+4}^{n} e(g,g)^{s_1\gamma\ r_{1,i}(u_{2,i}-u_{1,i})} \\
&\quad e(g,g)^{\gamma\ v_i \alpha f_1 q_i(u_{2,i}-u_{1,i})}. \qquad (4) \\
&\quad = \prod_{i=N_1+4}^{n} e(g,g)^{s_2\theta\ r_{2,i}(w_{2,i}-w_{1,i})}. \\
&\quad e(g,g)^{\theta\ v_i \beta f_2 q_i(w_{2,i}-w_{1,i})} \\
&\quad = e(g,g)^{s_1\gamma\ \Delta_1 \sum_{i=1}^{n} r_{1,i}}. \\
&\quad e(g,g)^{s_2\theta\ \Delta_2 \sum_{i=1}^{n} r_{2,i}}. \\
&\quad e(g,g)^{\gamma\ \alpha f_1 \Delta_1 (\sum_{i=0}^{N_1+3} v_i x_{v_i} + \sum_{i=N_1+4}^{n} v_i q_i)}. \\
&\quad e(g,g)^{\theta\ \beta f_2 \Delta_2 (\sum_{i=0}^{N_1+3} v_i x_{z_i} + \sum_{i=N_1+4}^{n} v_i q_i)}
\end{aligned}
$$

So if the attributes satisfy the access policies and query keywords existed in an extracted keyword from the associated EHR or, in other words, the inner product values of $< v, (x_v||q_0||\ldots||q_l) >$ and $< v, (x_z||q_0||\ldots||q_l) >$ will be zero, the left-hand Equation 3 equals to $e(C_3, \prod_{j=1}^{4}\prod_{i=1}^{n} T'_{j,i})$.

5 Security and Performance Analysis

In this section, we analyze the security and performance of the proposed scheme.

5.1 Security Analysis

Theorem 1. *Let the decisional Diffie-Hellman assumption hold in group G, then our proposed scheme with public parameters*

$$
\begin{aligned}
PP = (g, G, G_T, p, e, H, &\{U_{1,i}, U_{2,i}\}_{i=1}^{n}, \\
&\{W_{1,i}, W_{2,i}\}_{i=1}^{n}, V, Y),
\end{aligned}
$$

be policy hiding ABKS scheme and secure resistance selectively keyword guessing attack in the standard model.

Assume adversary $\mathcal{A}$ outputs $v = (P_0, W_0)$ and $x = (P_1, W_1)$ as challenge access policies and keyword sets. To proof the selective security of the proposed scheme, we apply a sequence of games and reduce each game to the next. We can prove the indistinguishability of the encrypted form of v and x as follows:

- *Game*$_0$. The challenge ciphertext in this game is normal as follow:

  $$
  \begin{aligned}
  CT^* = (X^s V^{s_1}, X^s Y^{s_2}, g^s, &\left\{U_{1,i}^{s_1} V^{v_i \alpha}, U_{2,i}^{s_1} V^{v_i \alpha}\right\}_{i=1}^{n}, \\
  &\left\{W_{1,i}^{s_2} Y^{v_i \beta}, W_{2,i}^{s_2} Y^{v_i \beta}\right\}_{i=1}^{n}),
  \end{aligned}
  $$

  in which the access policy and keyword set are $\{v = (P_0, W_0), v = (P_0, W_0)\}$.
- *Game*$_1$. Challenge ciphertext in this game is as follows:

  $$
  \begin{aligned}
  CT^* = (X^s V^{s_1}, X^s Y^{s_2}, g^s, &\left\{U_{1,i}^{s_1} V^{v_i \alpha}, U_{2,i}^{s_1} V^{v_i \alpha}\right\}_{i=1}^{n}, \\
  &\left\{W_{1,i}^{s_2}, W_{2,i}^{s_2}\right\}_{i=1}^{n}),
  \end{aligned}
  $$

  in which the access policy and extracted keyword are $\{v = (P_0, W_0), (0, 0)\}$.
- *Game*$_2$. The challenge ciphertext in this game is as follows:

  $$
  \begin{aligned}
  CT^* = (X^s V^{s_1}, X^s Y^{s_2}, g^s, &\left\{U_{1,i}^{s_1} V^{v_i \alpha}, U_{2,i}^{s_1} V^{v_i \alpha}\right\}_{i=1}^{n}, \\
  &\left\{W_{1,i}^{s_2} Y^{x_i \beta}, W_{2,i}^{s_2} Y^{x_i \beta}\right\}_{i=1}^{n}),
  \end{aligned}
  $$

  in which the access policy and extracted keyword are $\{v = (P_0, W_0), x = (P_1, W_1)\}$.
- *Game*$_3$. The challenge ciphertext in this game is as follows

  $$
  \begin{aligned}
  CT^* = (X^s V^{s_1}, X^s Y^{s_2}, g^s, &\{U_{1,i}^{s_1}, U_{2,i}^{s_1}\}_{i=1}^{n}, \\
  &\left\{W_{1,i}^{s_2} Y^{x_i \beta}, W_{2,i}^{s_2} Y^{x_i \beta}\right\}_{i=1}^{n}),
  \end{aligned}
  $$

in which the access policy and extracted keyword are $\{v = (0, 0), x = (P_1, W_1)\}$.

- $Game_4$. The challenge ciphertext in this game is as follows
$$CT^* = (X^sV^{s_1}, X^sY^{s_2}, g^s, \left\{U_{1,i}^{s_1}V^{x_i\alpha}, U_{2,i}^{s_1}V^{x_i\alpha}\right\}_{i=1}^n, \\ \left\{W_{1,i}^{s_2}Y^{x_i\beta}, W_{2,i}^{s_2}Y^{x_i\beta}\right\}_{i=1}^n),$$
in which the access policy and extracted keyword are $\{v = (P_1, W_1), x = (P_1, W_1)\}$.

Lemma 1. *Let the decisional DDH assumption holds, there is no PPT adversary with non-negligible advantage to distinguish $Game_0$ and $Game_1$.*

Proof. Suppose there exists an adversary $\mathcal{A}$ such that distinguishes between $Game_0$ and $Game_1$ with non-negligible advantage ϵ, we construct a simulator $\mathcal{B}$ with advantage ϵ in breaking Assumption 3.1. On input (g, g^a, g^b, g^{ab}, Z), $\mathcal{B}$ simulates the following game for $\mathcal{A}$.

- Setup. $\mathcal{B}$ selects random elements $\Delta_1, \Delta_2, \gamma, \theta \in \mathbb{Z}_q$ and $u_{1,i}, u_{2,i}, w_{1,i}, w_{2,i} \in \mathbb{Z}_q$ for $i \in [n]$ so that $\Delta_1 = \gamma(u_{2,i} - u_{1,i})$ and $\Delta_2 = \theta(w_{2,i} - w_{1,i})$. Then, for $i \in [n]$, it sets
$$U_{1,i} = g^{u_{1,i}}, U_{2,i} = g^{u_{2,i}}$$
$$W_{1,i} = g^{w_{1,i}}(g^b)^{\theta v_i}, W_{2,i} = g^{w_{2,i}}(g^b)^{\theta v_i}$$
$$V = g^\gamma, Y = g^\theta.$$
In the end, $\mathcal{B}$ sends the public parameters
$$PP = (g, G, G_T, p, e, H, \{U_{1,i}, U_{2,i}\}_{i=1}^n, \\ \{W_{1,i}, W_{2,i}\}_{i=1}^n, V, Y),$$
to $\mathcal{A}$.
- Phase1. $\mathcal{B}$ can generate normal keys in response to requested attributes of $\mathcal{A}$ by using the key generation algorithm and normal trapdoor in response to requested keywords of $\mathcal{A}$ by using the trapdoor generation algorithm.
- Challenge. To generate the challenge ciphertext, $\mathcal{B}$ considers random elements as
$$s_2 = a, \quad \beta = b,$$
and selects $s_1 \in \mathbb{Z}_q$. Then, $\mathcal{B}$ sets
$$C_1 = X^sV^{s_1}, \quad C_2 = X^s(g^b)^{\theta v_i}, \quad C_3 = g^s,$$
$$\{C_{1,i}, C_{2,i}\}_{i=1}^n = \{U_{1,i}^{s_1}V^{v_i\alpha}, U_{2,i}^{s_1}V^{v_i\alpha}\}_{i=1}^n,$$
$$\{C_{3,i}, C_{4,i}\}_{i=1}^n = \left\{(g^a)^{w_{1,i}}Z^{v_i\theta}, (g^a)^{w_{2,i}}Z^{v_i\theta}\right\}_{i=1}^n.$$
- Phase2. $\mathcal{B}$ does as in phase 1.
- Guess. If $Z = g^{ab}$, then $\mathcal{B}$ simulates $Game_1$ as follows
$$\begin{aligned}\{C_{3,i}, C_{4,i}\}_{i=1}^n &= \left\{(g^a)^{w_{1,i}}(g^{ab})^{v_i\theta}, (g^a)^{w_{2,i}}(g^{ab})^{v_i\theta}\right\}_{i=1}^n \\ &= \left\{(g^{w_{1,i}}(g^\theta)^{v_ib})^a, (g^{w_{2,i}}(g^\theta)^{v_ib})^a\right\}_{i=1}^n \\ &= \left\{W_{1,i}^{s_2}, W_{2,i}^{s_2}\right\}_{i=1}^n.\end{aligned}$$

If $Z = g^{ab}g^r$ for r selected randomly in $\mathbb{Z}_q$, then $\mathcal{B}$ simulates $Game_0$ with $\beta = r$ as follows
$$\{C_{3,i}, C_{4,i}\}_{i=1}^n = \\ \left\{(g^a)^{w_{1,i}}(g^{ab}g^r)^{v_i\theta}, (g^a)^{w_{2,i}}(g^{ab}g^r)^{v_i\theta}\right\}_{i=1}^n = \\ \left\{(g^{w_{1,i}}(g^\theta)^{v_ib})^a(g^\theta)^{v_ir}, (g^{w_{2,i}}(g^\theta)^{v_ib})^a(g^\theta)^{v_ir}\right\}_{i=1}^n = \\ \left\{W_{1,i}^{s_2}Y^{v_i\beta}, W_{2,i}^{s_2}Y^{v_i\beta}\right\}_{i=1}^n.$$

Therefore, if $\mathcal{A}$ distinguishes $Game_0$ and $Game_1$, $\mathcal{B}$ can solve the DDH problem.

□

Lemma 2. *Let decisional DDH assumption holds, there is no PPT adversary with non-negligible advantage to distinguish $Game_1$ and $Game_2$.*

Proof. Suppose there is an adversary $\mathcal{A}$ such that distinguishes between $Game_0$ and $Game_1$ with non-negligible advantage ϵ, we construct a simulator $\mathcal{B}$ with advantage ϵ in breaking Assumption 3.1. $\mathcal{B}$ simulates the following game for $\mathcal{A}$ on input (g, g^a, g^b, g^{ab}, Z),.

- Setup. $\mathcal{B}$ selects random elements $\Delta_1, \Delta_2, \gamma, \theta \in \mathbb{Z}_q$ and $u_{1,i}, u_{2,i}, w_{1,i}, w_{2,i} \in \mathbb{Z}_q$ for $i \in [n]$ so that $\Delta_1 = \gamma(u_{2,i} - u_{1,i})$ and $\Delta_2 = \theta(w_{2,i} - w_{1,i})$. Then for $i \in [n]$, it sets
$$U_{1,i} = g^{u_{1,i}}, U_{2,i} = g^{u_{2,i}},$$
$$W_{1,i} = g^{w_{1,i}}(g^b)^{\theta v_i}, W_{2,i} = g^{w_{2,i}}(g^b)^{\theta x_i},$$
$$V = g^\gamma, Y = g^\theta.$$
In the end, $\mathcal{B}$ sends the public parameters
$$PP = (g, G, G_T, p, e, H, \{U_{1,i}, U_{2,i}\}_{i=1}^n, \\ \{W_{1,i}, W_{2,i}\}_{i=1}^n, V, Y),$$
to $\mathcal{A}$.
- Phase1. Using the key and trapdoor generation algorithms, $\mathcal{B}$ generates normal keys and normal trapdoors in response to $\mathcal{A}$s requested attributes and keywords, respectively.
- Challenge. To generate challenge ciphertext, $\mathcal{B}$ considers random elements as
$$s_2 = a, \quad \beta = b,$$
and selects $s_1 \in \mathbb{Z}_q$. Then, $\mathcal{B}$ sets
$$C_1 = X^sV^{s_1}, \quad C_2 = X^s(g^b)^{\theta v_i}, \quad C_3 = g^s,$$
$$\{C_{1,i}, C_{2,i}\}_{i=1}^n = \{U_{1,i}^{s_1}V^{v_i\alpha}, U_{2,i}^{s_1}V^{v_i\alpha}\}_{i=1}^n$$
$$\{C_{3,i}, C_{4,i}\}_{i=1}^n = \left\{(g^a)^{w_{1,i}}Z^{v_i\theta}, (g^a)^{w_{2,i}}Z^{v_i\theta}\right\}_{i=1}^n.$$
- Phase2. $\mathcal{B}$ does as in phase 1.

- Guess. If $Z = g^{ab}$, then $\mathcal{B}$ simulates $Game_1$ as follows

$$\{C_{3,i}, C_{4,i}\}_{i=1}^{n} = \\ \left\{(g^a)^{w_{1,i}}(g^{ab})^{v_i\theta}, (g^a)^{w_{2,i}}(g^{ab})^{x_i\theta}\right\}_{i=1}^{n} = \\ \left\{(g^{w_{1,i}}(g^{\theta})^{v_ib})^a, (g^{w_{2,i}}(g^{\theta})^{x_ib})^a\right\}_{i=1}^{n} = \\ \left\{W_{1,i}^{s_2}, W_{2,i}^{s_2}\right\}_{i=1}^{n}.$$

If $Z = g^{ab}g^r$ for r randomly selected in $\mathbb{Z}_q$, then $\mathcal{B}$ simulates $Game_2$ with $\beta = r$ as follows

$$\{C_{3,i}, C_{4,i}\}_{i=1}^{n} = \\ \left\{(g^a)^{w_{1,i}}(g^{ab}g^r)^{v_i\theta}, (g^a)^{w_{2,i}}(g^{ab}g^r)^{x_i\theta}\right\}_{i=1}^{n} = \\ \left\{(g^{w_{1,i}}(g^{\theta})^{v_ib})^a(g^{\theta})^{v_ir}, (g^{w_{2,i}}(g^{\theta})^{v_ib})^a(g^{\theta})^{x_ir}\right\}_{i=1}^{n} = \\ \left\{W_{1,i}^{s_2}Y^{v_i\beta}, W_{2,i}^{s_2}Y^{x_i\beta}\right\}_{i=1}^{n}.$$

Therefore, if $\mathcal{A}$ can distinguish $Game_1$ and $Game_2$, $\mathcal{B}$ can solve the DDH problem.

□

The rest of distinguishablities are as follows: Distinguishably between $game_2$ to $game_3$ is proved in the same way as Lemma 2. Distinguishably between $game_3$ to $game_4$ is proved in the same way as Lemma 1.

5.2 Performance Analysis

In this section, we compare our scheme firstly in the functionalities and then in the efficiency with the previous related works.

5.2.1 Functionality comparison

Table 2. Comparison of previous ABKS schemes with the proposed schemes in terms of security, efficiency and functionality

Schemes	[43]	[24]	[10, 25, 26, 45]	[48]	[13]	[51]	Ours
Prime Order	✓	✓	✓	✓	✓	✓	✓
Access Structure	AG	LSSS	T	AG	MBF	AG	AG
Hidden Policy	PH	FH	-	PH	-	PH	FH
Wildcard	-	-	-	✓	-	✓	✓
Searchability	✓	✓	✓	✓	✓	✓	✓
Multi-Keyword	-	-	✓	✓	✓	✓	✓
Designated server	-	-	-	-	✓	-	✓
Standard Model	-	-	-	✓	-	✓	✓

Note: AG=AND-Gate, LSSS=Linear Secret Sharing Schemes, T=Tree, MBF=Monotone Boolean Function, FH=Fully Hidden, PH= Partially Hidden.

Table 2 compares the functionalities of the proposed scheme with that of the state-of-the-art schemes [10, 13, 24–26, 43, 45, 48, 51] that support fine-grained access control and search over encrypted data. In[10, 13, 25, 26, 45, 48, 51], we observe that the schemes can provide multi-keyword search in prime order groups. However, the proposed scheme in [10, 13, 25, 26, 45] do not support the security in the standard model and the privacy of the attributes in the access structure. Moreover, the only secure channel free scheme is proposed in [13]. According to the above comparisons indicated in Table 2, none of the previous state-of-the-art schemes has all the features of our scheme at the same time.

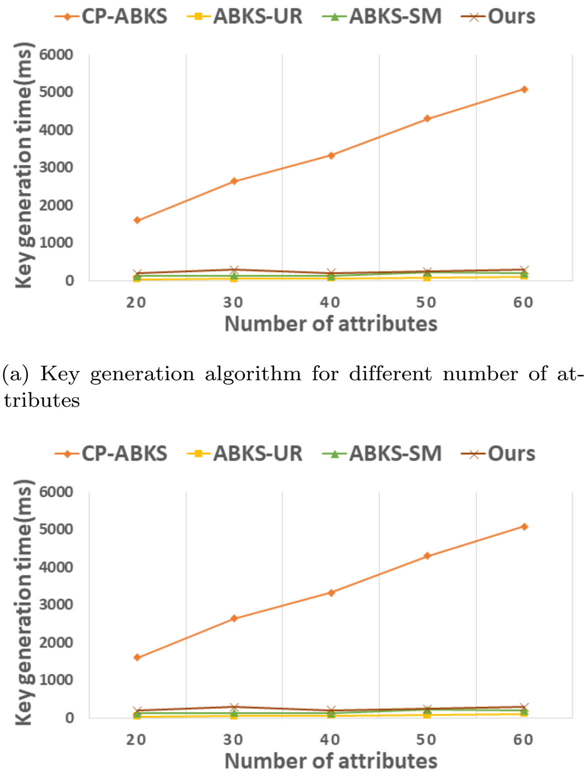
To compare the performance of our scheme with that of the previous related ones, we use python programming in windows 10 operation system. The experimental results are obtained by the processor Intel(R) Core(TM) i7-7500U CPU @ 2.70 GHz 2.90 GHz. We evaluate the performance of our scheme, the CP-ABKS scheme in [26], the ABKS-UR scheme in [25], and ABKS-SM scheme in [24] . For the theoretical analysis, we focus on the computational cost and only on costly operations, i.e., bilinear pairing operation P, hash operation H, exponentiation operation E (resp. E_T) in group G (resp. G_T), in Table 3. In Figure 2 (a) and (b), the diagrams depict the efficiency of the key generation algorithm and the ciphertext generation algorithm for various number of attributes, respectively. We observe that as the number of attributes increases, the running time of both algorithms in the CP-ABKS scheme increases almost linearly, while the running time increasing of these algorithms in the other three schemes is not significant. So, our scheme performance is almost similar to that of the ABKS-UR and ABKS-SM schemes and better than the CP-ABKS scheme. Figure 3 (a) compares the time cost of the trapdoor generation algorithm in the four schemes. As the number of attributes increases, the running time of the CP-ABKS, ABKS-UR, and ABKS-SM schemes increases almost linearly, while increasing the number of attributes has no multiplier effect in the running time of this algorithm in our scheme. Furthermore, if the number of attributes is greater than about 45, our scheme performance is better than the previous three ones.

5.2.2 Experimental evaluation

Figure 3 (b) confirms that increasing the number of attributes has less effect on our scheme than the increasing running time of the search algorithm, compared to the three previous schemes. Despite the functionalities and privacy provided, the efficiency of the proposed scheme is reasonable compared to three previous ones.

6 Conclusion

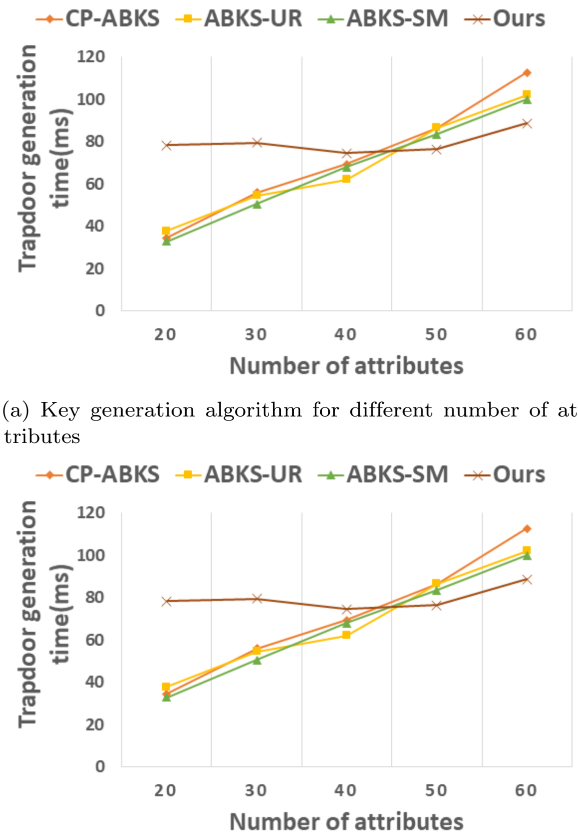
In this paper, we proposed an attribute-based encryption scheme with keyword search and designated server. Supporting hidden access policy and multi-keyword search, our scheme is suitable for secure outsourcing large volume of sensitive data such as electronic health records in the healthcare system. Since the attributes in the access policy may leak information about encrypted data and data users privilege, the hidden access policy can play an important role in protecting sensitive data. To the best of our knowledge, there is no secure channel free ABE scheme with multi-keyword search and hidden access policy, at the same time. Furthermore, in comparison to the previous works, our scheme is the first multi-keyword searchable encryption that is selectively secure against KGA in the standard model. Finally, we demonstrated that despite the added functionalities, performance of our scheme is reasonable.



(a) Key generation algorithm for different number of attributes

(b) Ciphertext generation algorithm for different number of attributes

Figure 2. Time cost of two algorithms



(a) Key generation algorithm for different number of attributes

(b) Ciphertext generation algorithm for different number of attributes

Figure 3. Time cost of two algorithms

References

[1] Parvaneh Asghari, Amir Masoud Rahmani, and Hamid Haj Seyyed Javadi. Internet of things applications: A systematic review. *Computer Networks*, 148:241–261, 2019.

[2] Parvaneh Asghari, Amir Masoud Rahmani, and Hamid Haj Seyyed Javadi. A medical monitoring scheme and health-medical service composition model in cloud-based iot platform. *Transactions on Emerging Telecommunications Technologies*, 30(6):e3637, 2019.

[3] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 457–473. Springer, 2005.

[4] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98. Acm, 2006.

[5] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *2007 IEEE symposium on security and privacy (SP'07)*, pages 321–334. IEEE, 2007.

[6] Zhiguo Wan, Jun'e Liu, and Robert H Deng. Hasbe: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *IEEE transactions on information forensics and security*, 7(2):743–754, 2011.

[7] Majid Bayat and Mohammad Reza Aref. An attribute-based tripartite key agreement protocol. *International Journal of Communication Systems*, 28(8):1419–1431, 2015.

[8] Majid Bayat, Hamid Reza Arkian, and Moham-

Table 3. Computational cost comparison

Schemes	CP-ABKS [26]	ABKS-UR [25]	ABKS-SM [24]	Ours
KeyGen	$(2n+2)E+nH$	$(2n+1)E+E_T$	$(2n+4)E+E_T+H$	$(8n+1)E$
IndGen	$(2n+4)E+nH$	$(n+1)E+E_T$	$(n+5)E+3E_T$	$(4(n+w+l_1)+13)E$
TrapGen	$(2n+4)E$	$(2n+1)E$	$(2n+1)E$	$(4(n-N_1)-5)E$
Search	$(2n+3)P+nE_T$	$(n+1)P+E_T$	$(2n+1)P+E_T$	$(12n+1)P+E$

mad Reza Aref. A revocable attribute based data sharing scheme resilient to dos attacks in smart grid. *Wireless Networks*, 21(3):871–881, 2015.

[9] Zhenhua Liu, Shuhong Duan, Peilin Zhou, and Baocang Wang. Traceable-then-revocable ciphertext-policy attribute-based encryption scheme. *Future Generation Computer Systems*, 2017.

[10] Yinbin Miao, Jianfeng Ma, Ximeng Liu, Xinghua Li, Qi Jiang, and Junwei Zhang. Attribute-based keyword search over hierarchical data in cloud computing. *IEEE Transactions on Services Computing*, pages –, 2017.

[11] Zehong Chen, Fangguo Zhang, Peng Zhang, Joseph K Liu, Jiwu Huang, Hanbang Zhao, and Jian Shen. Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control. *Future Generation Computer Systems*, 87:712–724, 2018.

[12] Saeid Rezaei, M Ali Doostari, and Majid Bayat. A lightweight and efficient data sharing scheme for cloud computing. *International Journal of Electronics and Information Engineering*, 9(2):115–131, 2018.

[13] Qian Xu, Chengxiang Tan, Wenye Zhu, Ya Xiao, Zhijie Fan, and Fujia Cheng. Decentralized attribute-based conjunctive keyword search scheme with online/offline encryption and outsource decryption for cloud computing. *Future Generation Computer Systems*, 97:306–326, 2019.

[14] Kobra Alimohammadi, Majid Bayat, and Hamid HS Javadi. A secure key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage. *Multimedia Tools and Applications*, 79(3):2855–2872, 2020.

[15] Dawn Xiaoding Song, David Wagner, and Adrian Perrig. Practical techniques for searches on encrypted data. In *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, pages 44–55. IEEE, 2000.

[16] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *International conference on the theory and applications of cryptographic techniques*, pages 506–522. Springer, 2004.

[17] Aniseh Najafi, Hamid Haj Seyyed Javadi, and Majid Bayat. Verifiable ranked search over encrypted data with forward and backward privacy. *Future Generation Computer Systems*, 101:410–419, 2019.

[18] Jin Wook Byun, Hyun Suk Rhee, Hyun-A Park, and Dong Hoon Lee. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data. In *Workshop on Secure Data Management*, pages 75–83. Springer, 2006.

[19] Wei-Chuen Yau, Raphael C-W Phan, Swee-Huay Heng, and Bok-Min Goi. Keyword guessing attacks on secure searchable public key encryption schemes with a designated tester. *International Journal of Computer Mathematics*, 90(12):2581–2587, 2013.

[20] Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo. Public key encryption with keyword search revisited. In *International conference on Computational Science and Its Applications*, pages 1249–1259. Springer, 2008.

[21] Hyun Sook Rhee, Jong Hwan Park, Willy Susilo, and Dong Hoon Lee. Trapdoor security in a searchable public-key encryption scheme with a designated tester. *Journal of Systems and Software*, 83(5):763–771, 2010.

[22] Chengyu Hu and Pengtao Liu. An enhanced searchable public key encryption scheme with a designated tester and its extensions. *J. Comput*, 7(3):716–723, 2012.

[23] Yang Yang and Maode Ma. Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds. *IEEE Transactions on Information Forensics and Security*, 11(4):746–759, 2016.

[24] Yinbin Miao, Ximeng Liu, Kim-Kwang Raymond Choo, Robert H Deng, Jiguo Li, Hongwei Li, and Jianfeng Ma. Privacy-preserving attribute-based keyword search in shared multi-owner setting. *IEEE Transactions on Dependable and Secure Computing*, 2019.

[25] Wenhai Sun, Shucheng Yu, Wenjing Lou, Y Thomas Hou, and Hui Li. Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. *IEEE Transactions on Parallel and Distributed Systems*, 27(4):1187–1198, 2014.

[26] Yinbin Miao, Jianfeng Ma, Ximeng Liu, Fushan

Wei, Zhiquan Liu, and Xu An Wang. m2-abks: Attribute-based multi-keyword search over encrypted personal health records in multi-owner setting. *Journal of medical systems*, 40(11):246, 2016.

[27] Yinbin Miao, Jianfeng Ma, Ximeng Liu, Jian Weng, Hongwei Li, and Hui Li. Lightweight fine-grained search over encrypted data in fog computing. *IEEE Transactions on Services Computing*, 2018.

[28] Yinbin Miao, Jianfeng Ma, Ximeng Liu, Xinghua Li, Zhiquan Liu, and Hui Li. Practical attribute-based multi-keyword search scheme in mobile crowdsourcing. *IEEE Internet of Things Journal*, 5(4):3008–3018, 2017.

[29] Takashi Nishide, Kazuki Yoneyama, and Kazuo Ohta. Attribute-based encryption with partially hidden encryptor-specified access structures. In *International conference on applied cryptography and network security*, pages 111–129. Springer, 2008.

[30] Junzuo Lai, Robert H Deng, and Yingjiu Li. Fully secure cipertext-policy hiding cp-abe. In *International conference on information security practice and experience*, pages 24–39. Springer, 2011.

[31] Tran Viet Xuan Phuong, Guomin Yang, and Willy Susilo. Hidden ciphertext policy attribute-based encryption under standard assumptions. *IEEE transactions on information forensics and security*, 11(1):35–45, 2015.

[32] Cancan Jin, Xinyu Feng, and Qingni Shen. Fully secure hidden ciphertext policy attribute-based encryption with short ciphertext size. In *Proceedings of the 6th International Conference on Communication and Network Security*, pages 91–98. ACM, 2016.

[33] Yinghui Zhang, Dong Zheng, and Robert H Deng. Security and privacy in smart health: Efficient policy-hiding attribute-based access control. *IEEE Internet of Things Journal*, 5(3):2130–2145, 2018.

[34] Fawad Khan, Hui Li, Liangxuan Zhang, and Jian Shen. An expressive hidden access policy cp-abe. In *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, pages 178–186. IEEE, 2017.

[35] Hong Zhong, Wenlong Zhu, Yan Xu, and Jie Cui. Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage. *Soft Computing*, 22(1):243–251, 2018.

[36] Hu Xiong, Hao Zhang, and Jianfei Sun. Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing. *IEEE Systems Journal*, 2018.

[37] Sana Belguith, Nesrine Kaaniche, Maryline Laurent, Abderrazak Jemai, and Rabah Attia. Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot. *Computer Networks*, 133:141–156, 2018.

[38] Leyou Zhang, Yilei Cui, and Yi Mu. Improving security and privacy attribute based data sharing in cloud computing. *IEEE Systems Journal*, pages –, 2019.

[39] Hassan Nasiraee and Maede Ashouri-Talouki. Anonymous decentralized attribute-based access control for cloud-assisted iot. *Future Generation Computer Systems*, 2020.

[40] Qingji Zheng, Shouhuai Xu, and Giuseppe Ateniese. Vabks: verifiable attribute-based keyword search over outsourced encrypted data. In *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, pages 522–530. IEEE, 2014.

[41] Payal Chaudhari and Manik Lal Das. A 2 bse: Anonymous attribute based searchable encryption. In *2017 ISEA Asia Security and Privacy (ISEASP)*, pages 1–10. IEEE, 2017.

[42] Yinbin Miao, Jianfeng Ma, Ximeng Liu, Zhiquan Liu, Limin Shen, and Fushan Wei. Vmkdo: Verifiable multi-keyword search over encrypted cloud data for dynamic data-owner. *Peer-to-Peer Networking and Applications*, 11(2):287–297, 2018.

[43] Shuo Qiu, Jiqiang Liu, Yanfeng Shi, and Rui Zhang. Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack. *Science China Information Sciences*, 60(5):052105, 2017.

[44] Payal Chaudhari and Manik Lal Das. Keysea: Keyword-based search with receiver anonymity in attribute-based searchable encryption. *IEEE Transactions on Services Computing*, 2020.

[45] Yang Chen, Wenmin Li, Fei Gao, Kaitai Liang, Hua Zhang, and Qiaoyan Wen. Practical attribute-based conjunctive keyword search scheme. *The Computer Journal*, 2019.

[46] Laicheng Cao, Yifan Kang, Qirui Wu, Rong Wu, Xian Guo, and Tao Feng. Searchable encryption cloud storage with dynamic data update to support efficient policy hiding. *China Communications*, 17(6):153–163, 2020.

[47] Haijiang Wang, Xiaolei Dong, and Zhenfu Cao. Multi-value-independent ciphertext-policy attribute based encryption with fast keyword search. *IEEE Transactions on Services Computing*, 2017.

[48] Lixue Sun and Chunxiang Xu. Hidden policy ciphertext-policy attribute based encryption with conjunctive keyword search. In *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pages 1439–1443. IEEE, 2017.

[49] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions,

polynomial equations, and inner products. In *annual international conference on the theory and applications of cryptographic techniques*, pages 146–162. Springer, 2008.

[50] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques*, pages 47–53. Springer, 1984.

[51] Mukti Padhya and Devesh Jinwala. A novel approach for searchable cp-abe with hidden ciphertext-policy. In *International Conference on Information Systems Security*, pages 167–184. Springer, 2014.

Aniseh Najafi recieved the Ph.D. degree in mathematics and computer Sciences at Shahed University in Tehran, Iran. She received her B.S. and M.S. degrees from the Department of Mathematics and Computer Sciences at Tehran University and Shahed University, respectively. Her interested area is cryptography.

Majid Bayat is an assistant professor of computer engineering of Shahed University, Tehran, Iran. His research interests include IoT, E-health, smart grid, VANET and V2G. He has authored over 30 papers in international journals and conferences in the above areas.

Hamid Haj Seyyed Javadi received the B.S., M.S., and Ph.D. degrees from Amir Kabir University. He is currently a full-time faculty member and a professor of Shahed University. His research interests are algebra, computer algebra, and wireless networks and security.