Practical Searchable CP-ABE in Cloud Storage

Hang Su, Zhiqiang Zhu, Lei Sun, Ning Pan
Zhengzhou Information Science and Technology Institute
Zhengzhou, China
e-mail: Suhang_039@163.com

***Abstract*—More and more organizations and individuals outsource their data storage into cloud and using cloud-based services provide data management, then lead to the combination of database and cloud environment, which prompted changes in the information industry and information service, while there exits any security issues. Query providing user capabilities of accessing cloud data and obtaining information. Thus, how to protect both privacy of user queries and data privacy, and how to reduce overhead in the case of rapid query becomes a hot issue.The database protection mechanisms proposed in this paper are based on attribute decomposition and encrypted cloud environment, which not only the server to minimize the number of encryption and decryption of the attribute field, but reduce the amount of computation and effectively encrypt the data of database as well.**

Keywords-hidden access structure, constant cipertext-size, recipient anonymity, asymmetric pairing.

I. INTRODUCTION

Nowadays, more and more enterprises stores their data in the cloud, while the data security is an urgent problem to tackle in cloud storage. Attribute Based Encryption (ABE), which Sahai and Waters first propose in [1], is a preferable settle scheme to the problem, which binds attributes set and ciphertext (user's private keys) together. Only when the attributes sets of ciphertext match that of user's private key, decryption is enabled. ABE scheme is a technique of access control. Based on different position placed access policies, ABE can be categorized as Key Policy Attribute Based Encryption (KP-ABE)[3] and Ciphertext Policy Attribute Based Encryption (CP-ABE) [4].

Search over encrypted data is an important problem in ABE. Downloading all the data from the cloud and decrypting them before search is a straightforward manner, which is inefficient and infeasible. A better solution is to introduce searchable encryption. Attribute Based Searchable Encryption (ABSE), which matches ciphertext and user's attributes set in the search process to enhance search efficiency, is first constructed by Dalia Khader[2].

In recent years, more and more ABSE schemes are proposed. Wenham Sun etc. [6] proposed a Verifiable ABSE scheme, which achieves keywords search and user revocation. In [7], a searchable CP-ABE is presented by Mukti Padhya, which achieves ciphertext policy hidding. In the scheme proposed by Payal Chaudhari[8], recipient anonymous is achieved, but so many pairing computation is required. However, all of these schemes[6-8] have some distance from being practically put into use, and the problem is as follows. (1) These primitives are based on pairing computations, but there isn't an efficient way to perform pairing computing. However, massive pairing computation should be carried out when performs keywords search, and there are too much ciphertexts to be searched in the cloud. (2) Data is encrypted in asymmetric cryptosystem directly in these schemes. And the operating rate of asymmetric encryption is slower than that of symmetric encryption, besides the data to be encrypted usually has large data size. (3)The length of ciphertexts and user's private keys are long, which requires larger storing space.

Our Contributions A practical searchable ciphertext policy attribute based encryption scheme is proposed, which is practical and can be applied in cloud storage. AND-gate with multi-valued attributes, a kind of expressive and flexible access structure, is adopted in the proposed primitive, asymmetric bilinear map is also adopted to achieve practical and efficient encryption and keywords search from an implementation point of view[10]. In the proposed searchable CP-ABE, the access policy that Data owner formulated for Data User is hidden, and the length of ciphertext is constant and short.

The proposed scheme is efficient. In decryption and search process pairing computation is only twice each, the encryption process is also efficient that data is encrypted in symmetric cryptosystem and the symmetric key, which is used to protect the data, is encrypted in the asymmetric cryptosystem.

The proposed scheme employs the way that operate keywords search and judge whether user satisfies access policy inside data simultaneously, which makes keywords search more efficient. Besides conjunctive keywords search can be achieved, which enhances the practicability of the scheme.

The proposed scheme achieves recipient anonymity, which provides better protection to users' privacy. The primitive is proven to be IND-CPA and INA-CKA selectively secure under asymmetric DBDH and DDH1v1 assumption in the standard model.

Organization of the Paper The remaining of this paper is organized as follows. In Section 2, we review some related knowledge associated with our proposed scheme, such as difficulty assumptions. Then we present system model, threat model, and design goals in Section 3. The definition of the proposed scheme and the detailed construction of it is shown

978-1-4673-9026-2/16/$31.00 ©2016 IEEE

in Section 4. In Section 5 the security game and proof is given, and followed by Section 6 the performance analysis is introduced. Finally, the concluding remark of this whole paper is given in Section 7.

II. PRELIMINARIES

A. Asymmetric Bilinear Maps

There are three cyclic groups G_1, G_2 and G_T, and the order of them is prime p. If $e: G_1 \times G_2 \to G_T$ satisfies the following rules, it is an effective bilinear map.

- *Bilinearity* $\forall g_1 \in G_1, \forall g_2 \in G_2, \forall a,b \in_R \mathbb{Z}_p^*$, $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.
- *Non-degeneracy* $\exists g_1 \in G_1, g_2 \in G_2, e(g_1, g_2) \neq 1$.
- *Computability* $\forall g_1 \in G_1, \forall g_2 \in G_2$, there is a polynomial time method to compute $e(g_1, g_2)$.

If $G_1 \neq G_2$, the bilinear map is asymmetric.

B. Hardness Assumption

*Definition*1. *Asymmetric DDH assumption*

Let G_1, G_2, G_T donate groups, $e: G_1 \times G_2 \to G_T$ is an effective bilinear map. $g_1 \in G_1, g_2 \in G_2$ are generators. $(g_1, g_2, g_1^a, g_1^b, g_1^z)$ is an asymmetric DDH tuple. The DDH problem is to decide whether $g_1^z = g_1^{ab}$ or g_1^z is randomly chosen from G_1.

For the convenience of proof, we change the DDH1 asymmetric tuple $(g_1, g_2, g_1^{\bullet}, g_1^b, g_1^z)$ into $(g_1, g_2, g_1^{\bullet}, g_1^b, g_2^z)$, and it's obvious that difficulty of these assumption is the same. Based on the above analysis, we define Asymmetric DDH1v1 assumption as follows.

Definition2. Asymmetric DDH1v1 assumption

Let G_1, G_2, G_T donate groups, $e: G_1 \times G_2 \to G_T$ is an effective bilinear map. $g_1 \in G_1, g_2 \in G_2$ are generators. $(g_1, g_2, g_1^a, g_1^b, g_2^z)$ is an asymmetric DDH tuple. The DDH problem is to decide whether $g_2^z = g_2^{ab}$ or g_2^z is randomly chosen from...

*Definition*3. *Asymmetric DBDH assumption*

Let G_1, G_2, G_T donate groups, $g_1 \in G_1, g_2 \in G_2$ are generators. $(g_1, g_2, g_1^{\bullet}, g_1^b, g_2^b, g_2^c, e(g_1, g_2)^z)$ is an asymmetric DBDH tuple. The DBDH problem is to decide whether $e(g_1, g_2)^z = e(g_1, g_2)^{\bullet abc}$ or $e(g_1, g_2)^z$ is randomly chosen from G_T.

C. Access Structure

AND-gate with multi-valued attributes, where different attributes are connected by AND-gate, and different values of an attribute are connected by OR-gate, is defined as follows:

Let $U = \{1, 2, \cdots, n\}$ donate the attributes set. Each $i \in U$ has multiple values, and $S_i = \{v_{i,1}, v_{i,2} \cdots, v_{i,n}\}$ donates the possible values of it. Attributes set of user is donated as $L = \{L_1, L_2, \cdots, L_n\}, L_i \in S_i$ and access structure is donated as $W = \{W_1, W_2, \cdots, W_n\}, W_i \in S_i$. If $L_i = W_i (i = 1, 2, \cdots, n)$, attributes set L satisfies access structure W.

III. PROBLEM FORMULATION

A. System Model

In our proposed scheme, the framework of system is described in Fig. 1, and there are three entities in the system:

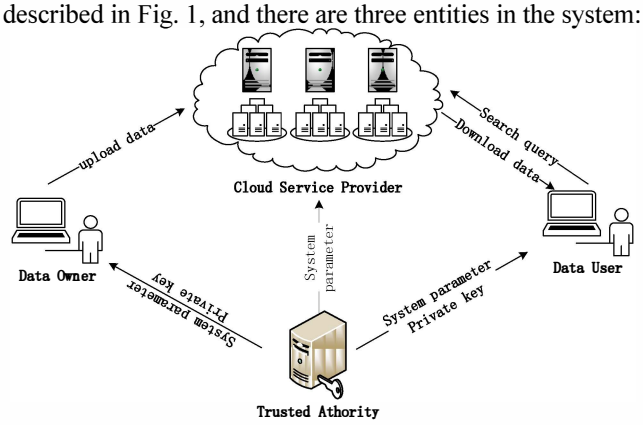

Figure 1. System framework

- *Trusted Authority* As the only trusted third party in the system, the trusted authority (TA) provides system parameters generating and users' private key issuing service.
- *Data Owner and Data User* Data Owner is the enterprise or individual who stores his data on the cloud, and Data User is the one who issues the search query to the cloud or downloads data from the cloud. A user in the cloud usually plays dual roles of Data Owner and Data User.
- *Cloud Service Provider* The data storage and keywords search service are provided by the Cloud Service Provider (CSP). Data Owner uploads encrypted data and keywords index to CSP, and data user sends the search query, receives the search result via CSP and downloads data from CSP.

Detailed system operating process is designed as follows:

Encryption and decryption process is divided into two parts: data/ keywords encryption and decryption. To enhance the efficiency of the system and save calculating expenditure, data is encrypted by a symmetric algorithm. Thus the encryption process includes two steps. At first, the symmetric key used to encrypt data is protected by the CP-ABE scheme, such as AES (Advanced Encryption Standard). Then, data is encrypted by the above-mentioned symmetric key. Accordingly, the decryption process is operating in two steps. Firstly, after downloading encrypted data, intended data users decrypt the CP-ABE ciphertext and obtain the symmetric key, then the data decryption algorithm is performed. Based on the fact that symmetric algorithm is more efficient than the asymmetric algorithm, the encryption and decryption process in the proposed system has more steps than that in most CP-ABE schemes, though the

efficiency is higher. The keywords encryption and decryption is operating by data owner and CSP separately. Keywords are extracted from data by data owner and protected by CP-ABE scheme. The decryption process is to be introduced in the next part.

Keywords search process is executed after Data user generating a trapdoor, and issuing keywords search query, the CSP operates keywords search algorithm. The trapdoor generating and keywords search algorithm are based on CP-ABE scheme. During the keywords search process, whether the data user matches the access policy inside the data is judged at first, and only the matched data is the search target.

B. Threat Model

In this paper, TA is considered to be fully trusted. During the process of public parameters generating, user enrollment and user revocation, TA behaves honestly as we expect. And the CSP is "honest-but-curious" [9], which performs honestly as the proposed scheme designated, but it is curious about the data/keywords stored or queried by users, and it may collude with any malicious or revoked users using their revoked key to getting secret information from these data. Analogue to [10], this threat model is same as the practical cloud storage situation.

C. Security Goals

In this paper, we lay importance mainly on the following items.

- *Plaintext semantic security* In the proposed scheme, the ciphertext should be fully secure against chosen plaintext attack in the standard model.
- *Keywords semantic security* In the proposed scheme, the keywords should be fully secure against chosen keywords attack in the standard model.
- *Recipient anonymity* Without the user's private key, whether the user is the intended receiver cannot be judged. No information on access policy should be leaking from the ciphertext.

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

IV. Proposed Scheme

An anonymous and efficient scheme is proposed in [11]. Though it claimed that its scheme was fully security under standard model, it is selectively secure. We study and improve this CP-ABE scheme, and based on it we construct a practical searchable CP-ABE scheme.

A. Definition of Searchable CP-ABE

Seven algorithms is contained in our proposed searchable CP-ABE scheme. Description of the seven algorithms is as follows.

Setup (1^λ) Setup algorithm is run by TA. The security parameters are the input, public parameters (*PP*) and master secret key (*MSK*) are the output.

KeyGen (PP, MSK, L) KeyGen algorithm is run by TA. It takes the *PP*, *MSK*, and the new user's attributes set L as input and outputs the user's secret key (*USK*).

Encryption (PP, M, W)Data Owner runs the Encryption algorithm. Input of the algorithm are *PP*, data and access policy that Data Owner formulates for the data, and the output are the encrypted data and the encrypted random symmetric key used for encrypting data CT.

KW_Encryption (PP, KW, W) Data Owner runs the KW_Encryption algorithm. Input of the algorithm are *PP*, keywords that Data Owner extracts, and output is the encrypted keywords CT_W.

Trapdoor (USK, SKW) Data User runs the trapdoor algorithm. It inputs the user's secret key and keywords Data User want to search, and outputs the trapdoor.

Search ($CT_W, Trapdoor$) CSP runs the Search algorithm. It inputs the encrypted keywords CT_W, Trapdoor, and outputs the search result.

Decryption (CT, USK) Data User runs the Decryption algorithm. It inputs the KW_ Encryption, user's secret key, and outputs the decryption result.

B. Detailed Construction of Searchable CP-ABE

Let $\mathbb{N} = \{1, 2, \cdots, n\}$ donate the universe attribute set, and each attribute $i \in \mathbb{N}$ has n_i values that can be donate as value set $S_i = \{v_{i,1}, v_{i,2}, \cdots, v_{i,n_i}\}, n_i = |S_i|$ and the attribute i could have one or many values in set *V*. The access policy that Data Owner formulates for the very data is donated by $W = \{W_1, W_2, \cdots W_n\}$, $W_i \in S_i$, and the attribute set that the Data User has is represented by $L = \{L_1, L_2, \cdots, L_n\}$.

Setup The universe attribute set $\mathbb{N}$, and other security parameters are input. TA run the Setup algorithm.

1) TA picks two multiplication cyclic groups G_1 and G_2, both the order of G_1 and G_2 are a prime p, and the bilinear mapping is defined as $e: (G_1 \times G_2) \to G_T$.
2) TA randomly choose generator $g_1 \in G_1$ and $g_2 \in G_2$, and $\alpha, \beta, \lambda \in_R \mathbb{Z}_P^*$. TA calculates $h_2 = g_2^\alpha$, $u_1 = g_1^\beta$, $u_2 = g_2^\beta$, $v_1 = g_1^\gamma$, $v_2 = g_2^\gamma$, and $Y = e(u_1, h_2)$.
3) For the attribute $i, (1 \le i \le n)$, TA selects $a_{i,j} \in_R \mathbb{Z}_P^*$ $(1 \le i \le n, 1 \le j \le n_i)$ at random and calculates $A_{i,j} = g_1^{a_{i,j}}$ $(1 \le i \le n, 1 \le j \le n_i)$. It's assumed that $\forall L, L' (L \ne L')$ $\sum_{v_{i,j} \in L} a_{i,j} \ne \sum_{v_{i,j} \in L'} a_{i,j}$ and as it's proved in [3], the assumption holds with probability larger than $1 - \frac{N^2}{p}$, where $N := \prod_{i=1}^{n} n_i$. If $a_{i,j}$ is randomly chosen from $\mathbb{Z}_p^*$, this assume is natural.

4) TA defines a hash function $H:\{0,1\}^* \to \mathbb{Z}_p$.

5) TA publishes the public parameters as $PP=\left\langle g_1,g_2,h_2,u_1,u_2,v_1,Y,\{\{A_{i,j}\}_{1\le j\le n_i}\}_{1\le i\le n}\right\rangle$ and keeps the master secret key $MSK=\left\langle f,v_2,\{\{a_{i,j}\}_{1\le j\le n_i}\}_{1\le i\le n}\right\rangle$ secretly.

KeyGen In the process of user registry, the new Data User provide his attribute set $L=\{L_1,L_2\cdots,L_n\}$ to TA. TA generate key for decryption and key for search for Data User.

1) Key for decryption: TA selects value $r\in_R \mathbb{Z}_p^*$ at random, then computes $D_0=g_2^r$, $D_1=u_2^{\alpha}\left(v_2 g_2^{\sum_{v_{i,j}\in L_i} a_{i,j}}\right)^r$, and sends the user's secret key (USK) $USK_L=\{D_0,D_1\}$ to Data User securely.

2) key for search: TA select a random key $r_1\in_R \mathbb{Z}_p^*$, then compute $\hat{D}_0=g_2^{r_1}$, $\hat{D}_1=\left(v_2 g_2^{\sum_{v_{i,j}\in L_i} a_{i,j}}\right)^{r_1}$.

Encryption Let M donate the data that Data Owner wants to encrypt.

1) Data Owner generates a symmetric key K_M and use it to encrypt data, the symmetric ciphertext is CT_{M_1}.

2) Data Owner picks random $s\in_R \mathbb{Z}_p^*$ and computes $C=K_M Y^s$ $C_0=g_1^s$, $C_1=\left(v_1\prod_{v_{i,j}\in W_i} A_{i,j}\right)^s$. The encrypted ciphertext is $CT_{M_2}=\{C,C_0,C_1\}$.

KW_ Encryption Let $KW=\{kw_1,kw_2,\cdots,kw_m\}$ donate the keywords Data Owner picks for M.

1) Data Owner picks random $u\in_R \mathbb{Z}_p^*$ and computes $\hat{C}_0=g_1^{\frac{u}{H(kw_1\|kw_2\|\cdots\|kw_m)}}$, $\hat{C}_1=\left(v_1\prod_{v_{i,j}\in W} A_{i,j}\right)^u$, $CT_{KW}=\left\{\hat{C}_0,\hat{C}_1\right\}$.

2) Data Owner uploads the encrypted data $CT_M=\{CT_{M1},CT_{M2},CT_{KW}\}$.

Trapdoor Let $SKW=\{skw_1,skw_2,\cdots,skw_{m_1}\}$ donate the keywords Data User chooses to search. Data User picks random $x\in_R \mathbb{Z}_p^*$, and computes $T_0=\hat{D}_0^{\frac{x}{H(skw_1\|skw_2\|\cdots\|skw_{m_1})}}$, $T_1=\hat{D}_1^{x}$.

Search Once receiving the trapdoor, CSP runs the Search algorithm and computes $e\left(\hat{C}_0,T_1\right)\overset{?}{=}e\left(\hat{C}_1,T_0\right)$, if the equation holds, the data is what the Data User wants, And CSP sends the encrypted data to Data User.

Decryption (CT, USK) Once receiving the encrypted data, Data User decrypt CT_{M2}, and computes $C\frac{e(C_1,D_0)}{e(C_0,D_1)}$. Then using the result to decrypt CT_{M1}, and if the attributes set $L=\{L_1,L_2,\cdots,L_n\}$ matches the access policy $W=\{W_1,W_2,\cdots W_n\}$, $W_i\in S_i$, Data User gets M.

3) 4.3 Correctness

In the decryption process, if attributes set $L=\{L_1,L_2,\cdots,L_n\}$ matches access policy $W=\{W_1,W_2,\cdots W_n\}$, $W_i\in S_i$ then,

$$C\frac{e(C_1,D_0)}{e(C_0,D_1)}=K_M Y^s\times\frac{e\left(\left(g_1^{\gamma}g_1^{\sum_{v_{i,j}\in W_i} a_{i,j}}\right)^s,g_2^r\right)}{e\left(g_1^s,g_2^{\alpha\beta}\left(g_2^{\gamma}g_2^{\sum_{v_{i,j}\in L_i} a_{i,j}}\right)^r\right)}$$

$$=K_M Y^s\frac{e(g_1,g_2)^{s\gamma r}e(g_1,g_2)^{sr\sum_{v_{i,j}\in W_i} a_{i,j}}}{e(g_1,g_2)^{\alpha\beta s}e(g_1,g_2)^{s\gamma r}e(g_1,g_2)^{sr\sum_{v_{i,j}\in L_i} a_{i,j}}}.$$

$$=\frac{K_M Y^s}{e(g_1,g_2)^{\alpha\beta s}}=K_M$$

In the search process, if the attributes set $L=\{L_1,L_2,\cdots,L_n\}$ matches the access policy $W=\{W_1,W_2,\cdots W_n\}$, $W_n\in S_i$, then,

$$e\left(\hat{C}_0,T_1\right)=e\left(g_1^{\frac{u}{H(kw_1\|kw_2\|\cdots\|kw_m)}},\left(g_2^{\gamma}g_2^{\sum_{v_{i,j}\in L_i} a_{i,j}}\right)^{r_1 x}\right),$$

$$=e(g_1,g_2)^{\frac{u\gamma r_1 x}{H(kw_1\|kw_2\|\cdots\|kw_m)}}e(g_1,g_2)^{\frac{ur_1 x\sum_{v_{i,j}\in L_i} a_{i,j}}{H(kw_1\|kw_2\|\cdots\|kw_m)}}$$

$$e\left(\hat{C}_1,T_0\right)=e\left(\left(g_1^{\gamma}\prod_{v_{i,j}\in W_i} g_1^{a_{i,j}}\right)^u,g_2^{\frac{xr_1}{H(skw_1\|skw_2\|\cdots\|skw_{m_1})}}\right).$$

$$=e(g_1,g_2)^{\frac{u\gamma r_1 x}{H(kw_1\|kw_2\|\cdots\|kw_m)}}e(g_1,g_2)^{\frac{ur_1 x\sum_{v_{i,j}\in W_i} a_{i,j}}{H(kw_1\|kw_2\|\cdots\|kw_m)}}$$

If $e\left(\hat{C}_0,T_1\right)=e\left(\hat{C}_1,T_0\right)$, $KW=SKW$, the searching data is right what the Data User searches.

V. SECURITY PROOF

A. Recipient anonymity

Via asymmetric pairing, the proposed scheme achieves recipient anonymity. And the formal proof is as follows:

$W'=\{W_1',W_2',\cdots,W_n'\},W_i'\in S_i$ donates the access policy and $CT_{M_2}=\{C,C_0,C_1\}$ donates the ciphertext encrypted under $W=\{W_1,W_2,\cdots,W_n\},W_i\in S_i$. Given W' and CT_{M_2} to the adversary $\mathcal{A}$. And $\mathcal{A}$ performs DDH test [7].

$$C\frac{e(C_1,g_2)}{e\left(C_0,g_1^{\sum_{v_{i,j}\in W_i'} a_{i,j}}\right)}=K_M Y^s\times\frac{e\left(\left(v_1\prod_{v_{i,j}\in W_i} A_{i,j}\right)^s,g_2\right)}{e\left(g_1^s,g_2^{\sum_{v_{i,j}\in W_i'} a_{i,j}}\right)}$$

$$=\frac{K_M e(g_1,g_2)^{\alpha\beta s}e(g_1,g_2)^{sr\sum_{v_{i,j}\in W_i} a_{i,j}}}{e(g_1,g_2)^{sr\sum_{v_{i,j}\in W_i'} a_{i,j}}}$$

To make classified discussion, there are two cases.

Case 1: Suppose $W'=W$, then $\sum_{v_{i,j}\in W_i'} a_{i,j} = \sum_{v_{i,j}\in W_i} a_{i,j}, 1\le i\le n$.

Hence,

$$C\frac{e(C_1,g_2)}{e\left(C_0,g_1^{\sum_{v_{i,j}\in W_i'} a_{i,j}}\right)} = \frac{K_M e(g_1,g_2)^{\alpha\beta s} e(g_1,g_2)^{sr\sum_{v_{i,j}\in W_i} a_{i,j}}}{e(g_1,g_2)^{sr\sum_{v_{i,j}\in W_i'} a_{i,j}}} = K_M e(g_1,g_2)^{\alpha\beta s}$$

Via performing DDH test, the $\mathcal{A}$ can know nothing whether W equals to W' or not.

Case 2: If $\exists i, W_i' \neq W_i$, suppose $\forall k, W_k' \neq W_k$, $\sum_{v_{k,j}\in W_i} a_{i,j} = x_1$, $\sum_{v_{k,j}\in W_i'} a_{i,j} = x_2$, It's obvious $x_1 \neq x_2$. Hence,

$$C\frac{e(C_1,g_2)}{e\left(C_0,g_1^{\sum_{v_{i,j}\in W_i'} a_{i,j}}\right)} = \frac{K_M e(g_1,g_2)^{\alpha\beta s} e(g_1,g_2)^{sr\sum_{v_{i,j}\in W_i} a_{i,j}}}{e(g_1,g_2)^{sr\sum_{v_{i,j}\in W_i'} a_{i,j}}}$$

$$= K_M e(g_1,g_2)^{\alpha\beta s} e(g_1,g_2)^{sr(x_1-x_2)}$$

And it is the same as Case1, $\mathcal{A}$ can't know whether W equals to W' or not through DDH test.

Thus, the proposed scheme achieves recipient anonymity as we claim.

B. Chosen Plaintext Attack (CPA) Security

Formal proof of CPA security can be given under symmetric DBDH assumption. But we don't give the formal security proof due to the limitation of paper length here.

C. Chosen Keywords Attack (CKA) Security

Security Game: The selective CKA security game between the $\mathcal{A}$ and challenger is defined as follows:

Init: $\mathcal{A}$ submits the challenge access structure $W^*=\{W_1^*, W_2^*, \cdots, W_n^*\}$ to the challenger.

Setup: Challenger provides the security parameters and runs Setup algorithm to generate public parameters and master secret key. Challenger sends the public parameters to $\mathcal{A}$.

Phase1: $\mathcal{A}$ commits the attributes set L to challenger to get the corresponding private key. $\mathcal{A}$ can do key query for polynomial times. Note that if the queried attributes set L satisfies the submitted challenge access structure W^*, challenger won't respond the query.

Challenge: $\mathcal{A}$ submits two keywords sets KW_0 and KW_1. Challenger flips a coin at random. If the result is $b=0$, he runs the Encrypt algorithm to encrypt KW_0, otherwise he encrypts KW_1. Challenger sends $\mathcal{A}$ the challenge ciphertext $CT_{KW_b}{}^*$.

Phase2: Same as in Phase 1, the $\mathcal{A}$ issues key query with the same restriction that $L \neq W^*$.

Guess: $\mathcal{A}$ outputs a guess b' of b. And the advantage of $\mathcal{A}$ in this game is defined as $Adv := |Pr(b'=b) - \frac{1}{2}|$.

Theorem 2. Under the asymmetric DDH1v1 assumption, the proposed scheme is IND-CPA secure. If the polynomial time $\mathcal{A}$ has a non-negligible advantage of ε to win the selective CPA game. Challenger constructs an algorithm Simulator $\mathcal{B}$, and $\mathcal{B}$ can break the DBDH game with the advantage of $\frac{\varepsilon}{2}\left(1-\frac{N^2}{p}\right)$, $N := \prod_{i=1}^{n} n_i$.

Proof: $\mathcal{B}$ is given an asymmetric DDH1v1 tuple $\left(g_1, g_2, g_2^{\,a}, g_2^{\frac{b}{a}}, Z\right)$.

Init: $\mathcal{A}$ submits the challenge access structure $W^*=\{W_1^*, W_2^*, \cdots, W_n^*\}$ to the $\mathcal{B}$.

Setup: $\mathcal{B}$ provides the security parameters and runs Setup algorithm to generate public parameters. $\mathcal{B}$ picks $a_{i,j}' \in_R \mathbb{Z}_p^*$ for $1\le j\le n_i, 1\le i\le n$, computes $A_{i,j} = g^{a_{i,j}} = \begin{cases} g_1^{a_{i,j}'}, & v_{i,j}\in W^* \\ (g_1^b)^{a_{i,j}'}, & v_{i,j}\notin W^* \end{cases}$.

Then $\mathcal{B}$ sends the public parameters $PP = \langle g_1, g_2, h_2, u_1, u_2, v_1, Y, \{\{A_{i,j}\}_{1\le j\le n_i}\}_{1\le i\le n}\rangle$ to $\mathcal{A}$.

Phase1: $\mathcal{A}$ commits the attributes set $L=\{L_1, L_2\cdots, L_n\}$ to $\mathcal{B}$. And $\mathcal{B}$ computes $\sum_{v_{i,j}\in L} a_{i,j} = \sum_{v_{i,j}\in W^*} a_{i,j} + \sum_{v_{i,j}\in W^*} a_{i,j} = \sum_{v_{i,j}\in W^*} a_{i,j}' + b\sum_{v_{i,j}\in W^*} a_{i,j}'$ $= A_1 + bA_2$, picks $r_1 \in_R \mathbb{Z}_p^*$ at random, and computes $\hat{D}_1 = \left(v_2 g_2^{\sum_{v_{i,j}\in L} a_{i,j}}\right)^{r_1} = \left(g_2^{\gamma} g_2^{A_1}\left(g_2^b\right)^{A_2}\right)^{r_1}$, then $\mathcal{B}$ sends $\langle \hat{D}_\bullet, \hat{D}_1\rangle$ to $\mathcal{A}$. Using these keys, $\mathcal{A}$ can generate trapdoor on the searched keywords set SKW.

Challenge: $\mathcal{A}$ submits two keywords sets $KW_\bullet$ and KW_1. $\mathcal{B}$ flips a coin at random, and encrypts KW_b. $\mathcal{B}$ sets $u=ab$, computes $\hat{C}_0 = Z^{\frac{1}{H(kw_1\|kw_2\|\cdots\|kw_m)}}$ and $\hat{C}_1 = \left(v_1\prod_{v_{i,j}\in W^*} A_{i,j}\right)^u = Z^{\gamma+\sum_{v_{i,j}\in W^*} a_{i,j}'}$, then sends $\mathcal{A}$ the challenge ciphertext $CT_{KW_b}{}^* = \left\{\hat{C}_0, \hat{C}_1\right\}$.

Phase2: Same as Phase 1.

Guess: $\mathcal{A}$ outputs a guess b' of b. And $\mathcal{B}$ answers the DDH game according to the guess of $\mathcal{A}$. In the DBDH game, if $b'=b$, $\mathcal{B}$ answers "DDH", otherwise answers "random".

If $Z=g_1^{ab}$, $CT_{KW_b}^*$ is a valid ciphertext, and the advantage of $\mathcal{A}$ is ε. Hence,

$$Adv[B\rightarrow \text{"}DDH\text{"} \mid Z=g_1^{ab}] = Adv[b=b' \mid Z=g_1^{ab}] = \frac{1}{2}+\varepsilon.$$

If $Z = g_1^z$, $CT^*_{KW_b}$ is a valid ciphertext, and the advantage of $\mathcal{A}$ is 0. Hence,

$$Adv[B \to \text{“}random\text{”} \mid Z = g_1^z] = Adv[b = b' \mid Z = g_1^z] = \frac{1}{2}.$$

It follows that in the DBDH game, the advantage of $\mathcal{B}$ is $\frac{\varepsilon}{2}\left(1-\frac{N^2}{p}\right)$.

VI. COMPARISON

The performance of our proposed scheme will be evaluated by properties and computation complexity in the algorithm. Table I and Table II shows some properties of several ABSE schemes. In Table II, pairing computation cost is donated by p, that of exponentiation in G_1,G_2 is donated by e_1, and the computation cost of an exponentiation in G_T is donated by e_2, Via the comparison, our scheme is practical and efficient.

TABLE I. PROPERTIES OF ABSE SCHEMES

	Access structure	**Recipient anonymity**	**assumption**	**pairing**
CW [12]	LSSS	No	q-DBDH	Symmetric
QS [13]	Tree	No	D-Linear	Symmetric
Our scheme	AND	Yes	Asymmetric DBDH,DDH1v1	Asymmetric

TABLE II. PERFORMANCE OF ABSE SCHEMES

	Ciphertxt Length	**Token**	**Search computation**
QS [13]	$O(\lvert S\rvert)\lvert G\rvert$	$O(\lvert TL\rvert)\lvert G\rvert$	$O(\lvert S\rvert)p+O(\lvert S\rvert)e_2$
KW [14]	$O(\lvert S\rvert)\lvert G\rvert+O(1)\lvert\lambda\rvert$	$O(\lvert I^2\rvert)\lvert G\rvert$	$O(\lvert S\rvert)e_1+O(1)p$
Our Scheme	$O(1)\lvert G\rvert$	$O(1)\lvert G\rvert$	$O(1)e_1+O(1)p$

VII. CONCLUSION

In this paper, we have proposed a novel practical searchable CP-ABE scheme with constant-size ciphertext and it has proved that the proposed scheme is IND-CPA and IND-CKA secure. The proposed primitive is practical and efficient.

REFERENCE

[1] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Advances in Cryptology – EUROCRYPT 2005. vol. 3494, R. Cramer, Ed., ed: Springer Berlin Heidelberg, 2005, pp. 457-473.

[2] Khader, Dalia. " Introduction to Attribute Based Searchable Encryption." *Communications and Multimedia Security*. vol.8735, Springer Berlin Heidelberg, 2014, pp.131-135.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," presented at the Proceedings of the 13th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2006, pp. 89-98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy AttributeBased Encryption," in Security and Privacy, 2007. SP '07. IEEE Symposium on, 2007, pp. 321-334.

[5] Ramanna, Somindu C., and P. Sarkar. "Anonymous Constant-Size Ciphertext HIBE from Asymmetric Pairings." *Cryptography and Coding*. vol.8308, Springer Berlin Heidelberg, 2013, pp.344-363.

[6] Sun, W.; Yu, S.; Lou, W.; Hou, Y.T.; Li, H. "Protecting Your Right: Verifiable Attribute-Based Keyword Search with Fine-Grained Owner-Enforced Search Authorization in the Cloud", *Parallel and Distributed Systems, IEEE Transactions on,* On page(s): 1187 - 1198 Volume: 27, Issue: 4, April 1 2016

[7] Mukti Padhya, and Devesh Jinwala. "A Novel Approach for Searchable CP-ABE with Hidden Ciphertext-Policy." *Information Systems Security*. vol.8880, Springer International Publishing, 2014, pp.167-184.

[8] Chaudhari, Payal, and Maniklal Das. "Privacy-preserving Attribute Based Searchable Encryption.",International Association for Cryptologic Research. vol.2015. 2015, PP.899-919.

[9] Q. Liu, C. C. Tan, J. Wu and G. Wang, "Reliable Re-Encryption in Unreliable Clouds," *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, Houston, TX, USA, 2011, pp. 1-5.

[10] Q. Wang, Y. Zhu and X. Luo, "Multi-user Searchable Encryption with Fine-Grained Access Control without Key Sharing," *Advanced Computer Science Applications and Technologies (ACSAT), 2014 3rd International Conference on*, Amman, 2014, pp. 145-150.

[11] J. Li, R. Yanli. "An Efficient Attribute Based Encryption Scheme for Hiding Access Structures." *Journal of Xidian University* , 2015, pp. 97-102.

[12] Wang, Changji, et al. "A Ciphertext-Policy Attribute-Based Encryption Scheme Supporting Keyword Search Function." *Cyberspace Safety and Security*. vol.3800, Springer International Publishing, 2013, pp.377-386.

[13] Q. Zheng, S. Xu and G. Ateniese, "VABKS: Verifiable attribute-based keyword search over outsourced encrypted data," *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, Toronto, ON, 2014, pp. 522-530.

[14] K. Liang and W. Susilo, "Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1981-1992, Sept. 2015.