The Journal of Systems and Software 135 (2018) 157–164

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

Large universe attribute based access control with efficient decryption in cloud storage system

Xingbing Fu[a,*], Xuyun Nie[b], Ting Wu[a], Fagen Li[c]

[a] School of Cyberspace, Hangzhou Dianzi University, Hangzhou, 310018, PR China
[b] School of Information and Software Engineering, University of Electronic Science and Technology of China, PR China
[c] School of Computer Science and Engineering, University of Electronic Science and Technology of China, PR China

ARTICLE INFO

Article history:
Received 6 May 2016
Revised 16 September 2017
Accepted 15 October 2017

Keywords:
Attribute based encryption
Decryption outsourcing
Fine grained access control
Large universe construction
Cloud storage

ABSTRACT

Ciphertext Policy Attribute Based Encryption scheme is a promising technique for access control in the cloud storage, since it allows the data owner to define access policy over the outsourced data. However, the existing attribute based access control mechanism in the cloud storage is based on small universe construction, where the attribute set is defined at setup, and the size of the public parameters scales with the number of attributes. A large number of new attributes need to be added to the system over time, small universe attribute based access control is no longer suitable for cloud storage, whereas large universe attribute based encryption where any string can be employed as an attribute and attributes are not required to be enumerated at system setup meets this requirement. Unfortunately, one of the main efficiency drawbacks of existing large universe attribute based encryption is that ciphertext size and decryption time scale with the complexity of the access structure. In this work, we propose large universe attribute based access control scheme with efficient decryption. The user provides the cloud computing server with a transformation key with which the cloud computing server transforms the ciphertext associated with the access structure satisfied by the attributes associated with the private key into a simple and short ciphertext; thus it significantly reduces the time for the user to decrypt the ciphertext without the cloud computing server knowing the underlying plaintext; the user can check whether the transformation done by the cloud computing server is correct to verify transformation correctness. Security analysis and performance evaluation show our scheme is secure and efficient.

1. Introduction

Cloud storage can reduce the data owners' costs. However, when data are stored on the remote cloud storage server, the data owners will lose control on their sensitive data. Existing server mediated access control method uses a trusted server to store the sensitive data and mediate access control. When the trusted server is compromised, the confidentiality of the data will be compromised as well, which makes this method unsuitable for the cloud storage system where the cloud storage server is semi-trusted. A solution to the problem is to employ cryptographically enforced access control method where the sensitive data are stored in the encrypted form, such that even if the cloud storage server is compromised, the sensitive data will still be kept private.

However, most existing public encryption schemes allow one user to share sensitive data with another user. They are not able to efficiently address more expressive access control over the encrypted data. In recent years, Attribute Based Encryption (ABE) schemes due to Sahai and Waters (2005) have been employed to achieve fine grained access control over the encrypted data. Depending on whether access policy is associated with the key or with the ciphertext, attribute based encryption schemes are classified as two types: Key Policy Attribute Based Encryption (KP–ABE) scheme (Goyal et al., 2006) where the ciphertext is labeled with the attribute set and the key is associated with access structure, and Ciphertext Policy Attribute Based Encryption (CP–ABE) scheme (Bethencourt et al., 2007; Lewko and Waters, 2011a; Mller et al., 2008; Cheung and Newport, 2007; Ostrovsky et al., 2007; Goyal et al., 2008; Waters, 2011) where the key is labeled with the attribute set and the ciphertext is associated with access structure. If and only if the attributes satisfy the access policy, the decryptor can decrypt the data. In KP–ABE scheme, the encryptor does not exert any control on who can access data he encrypts, except that he can select the descriptive attributes for the data. In CP–ABE scheme, the data owner can define and enforce access control pol-

* Corresponding author. Tel.: (+86)18981973018.
E-mail addresses: fuxbuestc@126.com, uestcfuxb@126.com (X. Fu).

https://doi.org/10.1016/j.jss.2017.10.020
0164-1212/

icy which can specify who can access the data that he encrypts. Therefore, in cloud storage systems, CP–ABE scheme is more practical than KP–ABE scheme.

Attribute Based Encryption is classified as “small universe” attribute based encryption and “large universe” attribute based encryption in terms of construction. In “small universe” attribute based encryption scheme, the attributes are fixed at setup, and the size of attribute space is polynomially bounded in the security parameter. In “large universe” attribute based encryption scheme, the size of attribute space is exponentially large, any string can be employed as an attribute and the attributes are not be required to be enumerated at system setup.

In the cloud storage system, if small universe CP–ABE scheme is employed to achieve fine grained access control over the encrypted data, once the public parameters are set, the current constructions will not allow complete versatility when the attributes and access structures are chosen. However, the set of attributes and the particular access structures may change over time. Small universe CP–ABE scheme is no longer suitable for the scenario, whereas large universe CP–ABE scheme can meet this requirement. Unfortunately, one of the main efficiency drawbacks of the existing large universe CP–ABE schemes is that the ciphertext size and decryption time scale with the complexity of the access structure. The conventional desktop computers can handle the task for the access structure. However, when the users store and view private data on mobile devices whose processors are one to two orders of magnitude slower than their desktop counterparts and whose battery life is an unsolved problem, this presents a severe challenge. In this work, we will address this problem.

Our contribution. In this work, we propose a large universe attribute based access control scheme with efficient decryption which is employed to achieve fine grained access control over the encrypted data in the cloud storage system. Our scheme is proven selectively secure in the standard model. In contrast with prior schemes, our scheme eliminates one use restriction and has the constant number of public parameters. In our scheme, any string can be employed as an attribute, and attributes are not required to be enumerated at system setup. Outsourcing decryption of ABE ciphertexts to the cloud computing server makes the overheads for the users significantly eliminated, and simultaneously the cloud computing server unable to read any user’s messages. The decryption time for the user and power consumption are significantly reduced as well.

Organization. The remainders of this paper are organized as follows: We discuss related work in Section 2. We introduce preliminaries in Section 3. We present the architecture of the proposed scheme in Section 4. We present the syntax, and security model of the proposed scheme in Section 5. We present the scheme construction in Section 6. We give the security proof of the proposed scheme in Section 7. The performance of the proposed scheme is evaluated in Section 8. We draw the conclusion in Section 9.

2. Related work

Sahai and Waters (2005) introduced attribute based encryption scheme. Goyal et al. (2006) presented two forms of attribute based encryption: **KP–ABE** (Goyal et al., 2006) and **CP–ABE** (Bethencourt et al., 2007; Lewko and Waters, 2011a; Mller et al., 2008; Cheung and Newport, 2007; Ostrovsky et al., 2007; Goyal et al., 2008; Waters, 2011). Lewko and Waters (2011b) proposed the first large universe KP–ABE scheme in the standard model, where their scheme is based on composite order bilinear group, which makes their scheme less efficient than attribute based encryption in prime order bilinear group. To increase efficiency, Lewko (2012) employed dual pairing vector space due to Lewko et al. (2010) to construct the first large universe KP–ABE scheme in prime order bilinear group in the standard model, which improves the efficiency of the original construction. However, there is still significant efficiency overhead in their scheme in that the vector size is larger. Rouselakis and Waters (2013) presented the first large universe CP–ABE scheme in the standard model in prime order bilinear group. Unfortunately, in their scheme, ciphertext size and decryption time scale with the complexity of access structure.

Matthew Green and Waters (2011) presented an ABE scheme with outsourced decryption that significantly eliminates the overheads for users. Junzuo et al. (2013) proposed an ABE scheme with verifiable outsourced decryption. Their scheme not only guarantees the confidentiality of the plaintext message and achieves the improved decryption efficiency, but also achieves verifiability guarantee that a user can efficiently check whether the transformation done by the cloud computing server is performed correctly. However, the public parameters of the both schemes scale with the number of attributes. Furthermore, their schemes have one use restriction that an attribute occurs at most once in the access formula. How to achieve large universe attribute based access control with efficient decryption in the standard model without one use restriction and with constant size public parameters is still an open problem.

3. Preliminaries

In this subsection, we present a brief review of bilinear maps, the formal definition of access structure and linear secret sharing scheme (A., 1996), proxy re-encryption and RCCA security. Our scheme employs them as tools.

3.1. Bilinear map

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic groups of the same prime order p. g, u are a generator of $\mathbb{G}$, respectively. e is a bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ that has the properties as follows:

Bilinearity: for any $a, b \in \mathbb{Z}_p$, $e(g^a, u^b) = e(g, u)^{ab}$.

Nondegenerate: $e(g, g) \neq 1_{\mathbb{G}_T}$, $e(g, g)$ is a generator of $\mathbb{G}_T$.

If the group operation on $\mathbb{G}$ and the bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ are efficiently computable, then $\mathbb{G}$ is a bilinear group. We employ the symmetric bilinear map such that $e(g^a, u^b) = e(g, u)^{ab} = e(g^b, u^a)$.

3.2. Access structure

Let $\mathbb{S}$ denote the attribute universe. An access structure (A., 1996) over $\mathbb{S}$ is a collection $\mathbb{A}$ of non-empty subsets of attributes, i.e., $\mathbb{A} \subseteq 2^{\mathbb{S}} \setminus \{\}$. The sets in $\mathbb{A}$ are called the authorized attribute sets, and the sets not in $\mathbb{A}$ are called the unauthorized attribute sets. Specifically, an access structure is monotone if $\forall B, C$: if $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$. In this scheme, only monotone access structure is handled.

3.3. Linear secret sharing scheme

A secret sharing scheme Π (A., 1996) over the attribute set is called linear over $\mathbb{Z}_p$ if 1. The shares for each attribute of a secret form a vector over $\mathbb{Z}_p$ 2. There is a matrix M with h rows and n columns for Π . For any $j = 1, \ldots, h$, let the function φ defined the attribute that labels the j^{th} row as $\varphi(j)$. Given the column vector $\overrightarrow{v} = (s, x_2, \ldots, x_n)^T$, in which T is the transpose of the vector $\overrightarrow{v}$, s is the secret that will be shared, and $x_2, \ldots, x_n \in \mathbb{Z}_p$ are uniformly at random chosen, then $M\overrightarrow{v}$ is the vector of h shares of the secret s based on Π .The share $(M\overrightarrow{v})_j$ belongs to the attribute $\varphi(j)$.

Let attribute set $S \in \mathbb{A} \bigwedge S \in \mathbb{S}$ be any authorized attribute set, and let $J = \{j | j \in \{1, \ldots, h\} \bigwedge \varphi(j) \in S\}$. Then, there exist constants