Journal of Network and Computer Applications 108 (2018) 112–123

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating

Zechao Liu [a], Zoe L. Jiang [a,*], Xuan Wang [a], S.M. Yiu [b]

[a] Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, 518055, China
[b] The University of Hong Kong, Hong Kong Special Administrative Region

ARTICLE INFO

Keywords:
Attribute-based encryption
Outsourcing decryption
Attribute revocation
Policy updating
Large universe
Multiple authorities

ABSTRACT

Attribute-Based Encryption (ABE) offers fine-grained access control policy over encrypted data, and thus applicable in cloud storage to provide authorized data privacy. However, there are some issues that should be solved before deploying ABE in practice. Firstly, as the heavy decryption cost grows with the complexity of access policy, an ABE with outsourcing decryption is preferred to relieve user's computation cost. Secondly, when user's attributes are altered, it is required for ABE supporting attribute revocation to change user's access privilege timely and effectively. Thirdly, in the case of access control policy changed by data owner, policy updating requirement must be met in designing ABE. Therefore, a practical ABE scheme is proposed which can solve aforementioned issues simultaneously. In order to support flexible number of attributes, our scheme also achieves large universe and multiple attribute authorities. The security and performance of the proposed scheme are discussed, followed by extensive experiments to demonstrate its effectiveness and practicability.

1. Introduction

In this big data era, cloud computing offers the advantage of highly scalable and reliable storage on third-party servers, which results in an almost revolution of data storage way. However, as the data resources are not physically under the full control of data owners and the cloud server cannot be guaranteed fully trusted, the concern about data security and privacy arises. One method for solving this problem is to store data in encrypted form, which can achieve data confidentiality for unauthorized parties. But for authorized users, how to realize efficient and flexible data sharing on ciphertext becomes a new challenge.

To address this issue, the concept of Fuzzy Identity-Based Encryption (FIBE) was put forth by Sahai and Waters (2005) in 2005. Then Goyal et al. (2006) classified it into two complementary forms: Key-Policy ABE (KP-ABE) (Goyal et al., 2006) and Ciphertext-Policy ABE (CP-ABE) (Bethencourt et al., 2007). In KP-ABE, a user's secret key is issued according to an access policy and the ciphertext is annotated by attributes. Conversely, in CP-ABE, secret keys are issued according to users' attributes and the ciphertext is labeled with an access policy. Before uploading data resources to the cloud server, the data owner first defines an access policy and then encrypts data under this policy. Only those users whose attributes satisfy the policy have permissions to decrypt the ciphertext successfully. CP-ABE offers fine-grained and non-interactive access control mechanism over encrypted data, and thus it is more applicable in cloud storage service. Recently, a series of ABE schemes have been proposed in Ostrovsky et al. (2007), Lewko et al. (2010), Wang et al. (2010), Waters (2011), Lyu et al. (2016), Li et al. (2018), aiming at better expressiveness, efficiency or security. In particular, multi-authority and large universe are two significant progresses in ABE, we will discuss following.

To deal with the scenario that users' attributes are distributed by multiple authorities, Chase (2007) gave the first multi-authority ABE (MA-ABE) scheme. In this scheme, there existed one fully trusted central authority (CA) which has the power to decrypt all the ciphertext. Later, Chase and Chow (2009) proposed a privacy-preserving MA-ABE solution which removes the trusted CA. Lewko and Waters (2011a) constructed a fully secure MA-ABE scheme using bilinear groups of composite order, and proved its security in random oracle model. Liu et al. (2011) proposed their scheme and proved it adaptively secure in standard model. The "multi-authority" construction for ABE scheme makes it more usable in practice, while single authority ABE can be regarded as a special case of MA-ABE.

In addition, the "large universe" is a desirable property for ABE scheme that supports flexible number of attributes. In a "large universe"

* Corresponding author.
E-mail address: zoeljiang@hitsz.edu.cn (Z.L. Jiang).

https://doi.org/10.1016/j.jnca.2018.01.016
Received 3 May 2017; Received in revised form 12 January 2018; Accepted 26 January 2018
Available online 17 February 2018

ABE scheme, any string can be used as an attribute, and the attributes are not necessarily enumerated at system setup. Moreover, the public parameters consist of a constant number of group elements. Conversely, in "small universe" construction, the attributes are fixed during setup and the size of public parameters grows linearly with the number of attributes (Ning et al., 2015). This can incur two restrictions. On the one hand, if the attribute universe is too small, the system attributes might exceed the bound set. Then the system will have to be rebuilt and possibly re-encrypt all its data. On the other hand, if the bound chosen is too big, the public parameters will be needlessly large and this will cause unnecessary inefficiency (Liu et al., 2016). The first large-universe constructions in the standard model were proposed in Lewko and Waters (2011b). But this scheme was constructed on composite order groups. In order to improve the efficiency, Rouselakis and Waters (2013) presented a large universe ABE scheme from (Lewko and Waters, 2011b) into the prime order setting. Later, Rouselakis and Waters (2015) proposed another large universe scheme which supports multiple attribute authorities.

From practical point of view, there are some issues that should be solved before deploying ABE in practice. Firstly, the computational cost grows linearly with the complexity of access policy or the number of attributes, which brings pressure for users with limited computing resources. Outsourcing computing is a useful technology to solve this problem, aiming to move the heavy computation workloads to powerful computation resources. Note that outsourcing computing is getting widespread attention in scientific community, such as large-scale systems of linear equations (Chen et al., 2015), verifiable database (Chen et al., 2016), privacy-preserving deep learning (Li et al., 2017a, 2017b), profile matching (Gao et al., 2018), aided revocation in identity-based encryption (Li et al., 2015). We refer interested readers to read them for a comprehensive overview of this topic. To reduce the computational overhead of access control using ABE, several ABE schemes with outsourcing computing have also been proposed in the literature (Green et al., 2011; Lai et al., 2013; Li et al., 2014; Liu et al., 2017). Among them, the most common solution is outsourcing decryption, which delegates bilinear pairing operations on ABE ciphertext to a more powerful device. As a result, the computational cost imposed on resource-constrained devices can be effectively reduced.

Secondly, for any cryptosystem that involves many users, when user's attributes are altered, the corresponding user's access privilege should be changed timely and effectively. However, it is not a trivial matter. In ABE scheme, since multiple users may share the same attribute, the revocation of any user or attribute would affect the other unrevoked users who have the same attribute. For ABE systems, there are two types of revocation issues: user revocation and attribute revocation. User revocation means that a user is removed from the whole system. Attribute revocation means that a user who drops some attributes only loses part access privilege, but still exists in the system. So attribute-level revocation can achieve more fine-grained and flexible access control than user-level revocation does. In the literature, several revocation schemes have been proposed. Pirretti et al. (2010) and Bethencourt et al. (2007) realized attribute revocation using timed re-keying mechanism, which requires setting expiration time on each attribute or key. However, both of them cannot achieve immediate revocation. By introducing SEcurity Mediator (SEM), Chen et al. (2014) constructed a scheme which supports immediate user revocation. By allowing a proxy server to re-encrypt the ciphertext with a set of attribute group keys, Hur and Noh (2011) proposed a scheme which supports attribute revocation. Some other revocation schemes in multi-authority scenarios have been proposed in Yang and Jia (2012), Yang et al. (2013a), Li et al. (2016).

Thirdly, since the number of users and data volume boom quickly, data owners may frequently change their access policies over ciphertext in the cloud. Policy updating allows data owners to flexibly adjust the access control policy over their encrypted data. To solve this problem, a trivial method is to let data owners first retrieve their ciphertext from the cloud, then decrypt them in local, and then re-encrypt the plaintext under a new access policy, and finally send the new ciphertext back to the cloud server. However, this method will incur high communication overhead imposed on network bandwidth and high computation burden imposed on data owners. Thus, an efficient policy updating algorithm with lower computation and communication costs is desired in cloud storage system. Recently, Goyal et al. (2006) first discussed the policy updating issue in key-policy structure, and Sahai et al. (2012) discussed it in ciphertext-policy structure. However, both of them can only delegate key/ciphertext under a more restrictive policy. By using proxy re-encryption technique, Liang et al. (2009) proposed the first attribute-based proxy re-encryption (ABPRE) scheme, but the authors only considered the access structure consisting of AND gates. Later, Liang et al. (2013) proposed a new ABPRE scheme supporting any monotonic access structure. In scheme (Yang et al., 2015), Yang et al. proposed some policy updating methods, which could process different types of access policies.

A motivating story: Consider in an e-Healthy system, a patient may want to share medical data with a user who has the attribute "Surgeon" issued by a hospital and the attribute "Medical Researcher" issued by a clinical research center (Liu et al., 2016). The patient should define an access policy as ("Surgeon" AND "Medical Researcher") before encrypting his data under the policy. In this scenario, two authorities, hospital and clinical research center, are needed. Due to resignation from the hospital, a user who loses attribute "Surgeon" cannot decrypt previously shared data anymore, which is attribute revocation as we discussed before. When the patient needs rehabilitation guidance, he needs update his encrypted medical data to allow Rehabilitation Doctor's access, new policy ("Rehabilitation Doctor" AND "Medical Researcher") must be supported.

Motivated by the aforementioned practical issues, we revisit the existing ABE schemes and find that most of them only concentrate on solving one specific issue. This limits the scope of application for ABE schemes. In this paper, we aim to design a comprehensive and more powerful ABE scheme, which can solve several issues in practice. This makes our scheme more practical and usable. We state that our scheme simultaneously supports (a) multiple authorities, (b) large attribute universe, (c) outsourcing decryption, (d) attribute revocation and (e) policy updating.

Compared with our previous work (Liu et al., 2016), we have the following improvements:

(1) In order to support outsourcing decryption, we present the modified system model in Fig. 1. More concretely, a new entity (named Proxy Server) is introduced, which is responsible for computing the majority of decryption workload. Besides, three algorithms ($\mathsf{GenTK}_{out}, \mathsf{Transform}_{out}, \mathsf{Decrypt}_{out}$) in Section 4 are newly added in our scheme.
(2) In this paper, we propose a more powerful CP-ABE scheme, which supports outsourcing decryption, attribute revocation and policy updating simultaneously. Thus our scheme is more useful and flexible in practice.
(3) We analyze and compare the performance of our scheme with other related works theoretically, in terms of storage overhead and computation efficiency. In order to demonstrate its practicability, we also conduct extensive experiments and show the simulation results. More concretely, the total Section 6 is newly added.

The rest of this paper is organized as follows. The preliminaries are introduced in Section 2. The system model and security model are presented in Section 3. The concrete constructions and the security of our proposed scheme are given in Section 4 and 5. The performance analysis and experimental results are shown in Section 6. Finally, we conclude the paper in Section 7.