Information Sciences xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Information Sciences

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

Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing[☆]

Q1 Yinghui Zhang[a,b], Xiaofeng Chen[c], Jin Li[d], Duncan S. Wong[e], Hui Li[c], Ilsun You[f,*]

[a] *National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, PR China*
[b] *State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, PR China*
[c] *State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an 710071, PR China*
[d] *School of Computer Science and Educational Software, Guangzhou University, Guangzhou, PR China*
[e] *Department of Computer Science, City University of Hong Kong, Hong Kong Special Administrative Region, Hong Kong*
[f] *Department of Information Security Engineering, Soonchunhyang University, Republic of Korea*

ARTICLE INFO

Article history:
Received 14 November 2015
Revised 17 February 2016
Accepted 6 April 2016
Available online xxx

Keywords:
Cloud computing
Attribute-based encryption
Privacy protection
Anonymity
Fast decryption

ABSTRACT

Although many users outsource their various data to clouds, data security and privacy concerns are still the biggest obstacles that hamper the widespread adoption of cloud computing. Anonymous attribute-based encryption (anonymous ABE) enables fine-grained access control over cloud storage and preserves receivers' attribute privacy by hiding attribute information in ciphertexts. However, in existing anonymous ABE work, a user knows whether attributes and a hidden policy match or not only after repeating decryption attempts. And, each decryption usually requires many pairings and the computation overhead grows with the complexity of the access formula. Hence, existing schemes suffer a severe efficiency drawback and are not suitable for mobile cloud computing where users may be resource-constrained.

In this paper, we propose a novel technique called match-then-decrypt, in which a *matching phase* is additionally introduced before the *decryption phase*. This technique works by computing special components in ciphertexts, which are used to perform the test that if the attribute private key matches the hidden access policy in ciphertexts without decryption. For the sake of fast decryption, special attribute secret key components are generated which allow aggregation of pairings during decryption. We propose a basic anonymous ABE construction, and then obtain a security-enhanced extension based on strongly existentially unforgeable one-time signatures. In the proposed constructions, the computation cost of an attribute matching test is less than one decryption operation, which only needs small and constant number of pairings. Formal security analysis and performance comparisons indicate that the proposed solutions simultaneously ensure attribute privacy and improve decryption efficiency for outsourced data storage in mobile cloud computing.

1. Introduction

As a promising computing paradigm, cloud computing integrates various technologies to provide services to an increasing number of organizations and individual users. Mobile cloud computing further combines cloud computing with mobile

[☆] A preliminary abstract of this paper has been presented in ASIACCS 2013.

Q2 [*] Corresponding author. Tel.: +82 29558967.

E-mail addresses: yhzhaang@163.com (Y. Zhang), xfchen@xidian.edu.cn (X. Chen), jinli71@gmail.com (J. Li), duncan@cityu.edu.hk (D.S. Wong), lihui@mail.xidian.edu.cn (H. Li), ilsunu@gmail.com, mail.isyou@gmail.com (I. You).

http://dx.doi.org/10.1016/j.ins.2016.04.015
0020-0255/© 2016 Elsevier Inc. All rights reserved.

devices and ubiquitous wireless infrastructure. With the rapid development of cloud computing technology, more and more people have uploaded their various types of data, including the highly sensitive data, into clouds either for ease of sharing or for cost saving. However, cloud computing security has been a growing concern [1]. Specifically, data security and privacy concerns have been the biggest obstacles that hamper the widespread adoption of cloud computing. In cloud computing, data are outsourced to the cloud service provider, and people would like to make their private data only accessible to authorized users. Differentiated data access is frequently required in the sense that users with different attributes or roles should be granted different levels of access privileges. Thus, it is desirable to put access policy decisions in the hands of data owners in cloud computing. In mobile cloud computing, high efficiency is also important for a successful security solution.

Attribute-based encryption (ABE) is envisioned as a highly promising public key primitive for realizing scalable and fine-grained access control systems [32], where differential yet flexible access rights can be assigned to individual users. Especially, ciphertext-policy attribute-based encryption (CP-ABE) [3] enables data owners to specify an access policy over a universe of attributes and encrypt the data under the access policy with the corresponding public key components. Decryption is enabled if and only if the user's attributes match the corresponding access policy.

Though ABE can be directly applied to design secure access control, there is an increasing need to protect users' privacy in access control systems. In order to address this problem, anonymous ABE was introduced in [19] and further improved by [30]. In anonymous CP-ABE, a user obtains his attribute secret key and if the attribute set associated with the secret key does not satisfy the access policy in the ciphertext, the user cannot decrypt and guess what access policy was specified by the data owner. Anonymous CP-ABE can be applied to military circumstances and commercial fields, where the access policy itself could be sensitive information and needs to be protected.

However, in existing anonymous ABE schemes, the user has to decrypt and decide whether his/her attributes satisfy the hidden access policy in the ciphertext or not. Such a test should be repeated until a successful decryption or all of the possible tests have been considered. The decryption computation overhead in existing work is high as the computational cost grows with the complexity of the access formula, which usually requires many pairings. As a result, this direct decryption method in anonymous ABE will suffer a severe efficiency drawback. Therefore, it is desirable for users to efficiently decide before full decryption whether the hidden policy in a ciphertext matches attributes. Currently, techniques for attribute matching detection in state-of-the-art CP-ABE schemes are implemented through repeated decryption and hence suffer efficiency limitations. In fact, most of the available detection techniques in CP-ABE schemes have to reveal the access policy in the ciphertext, which violates user's attribute privacy. In practice, each user may receive a large number of ciphertexts and such kind of decryption method involves a large computational overhead. Especially, for the case of mobile cloud computing, it is extremely attractive for resource-constrained mobile users to realize fast decryption, in which only small and constant pairings are required. In this paper, for the sake of secure and efficient fine-grained access control in mobile cloud computing, we enable users' attribute privacy protection, anonymous attribute matching and fast decryption, simultaneously.

The contributions of this paper can be summarized as follows.

1. We propose a system architecture of anonymous attribute-based access control in mobile cloud computing and show how to construct an anonymous attribute-based access control system with the anonymous CP-ABE scheme as a main building block. In order to improve decryption efficiency, we introduce a new technique called match-then-decrypt into the decryption of anonymous ABE, in which a *matching phase* is added before the *decryption phase*. This technique works by computing some special components in ciphertexts, which are used to perform the test that if the attribute private key matches the hidden access policy in ciphertexts without decryption. For the sake of fast decryption, special attribute secret key components are generated which allow aggregation of pairings during decryption.
2. Specifically, we propose a basic anonymous CP-ABE construction, and then obtain a security-enhanced extension using the reasonable Canetti–Halevi–Katz technique based on strongly existentially unforgeable one-time signatures. In the proposed schemes, the computation cost of an attribute matching test is less than one decryption operation, which only needs small and constant number of pairings. Performance comparisons indicate that the proposed solutions simultaneously ensure attribute privacy and improve decryption efficiency for outsourced data storage in mobile cloud computing.
3. The basic construction and its extension are proven secure under the presented security models. The basic construction is proved to be selective ciphertext-policy and chosen-plaintext secure (CPA-secure) under the Decisional Bilinear Diffie–Hellman assumption and the Decisional Linear assumption in random oracle models, and the extension is selective ciphertext-policy and chosen-ciphertext secure (CCA2-secure) in random oracle models. In particular, even legitimate decryptors cannot obtain information about the access policy specified for ciphertexts more than the fact that they can recover the corresponding plaintext.

The remainder of this paper is organized as follows. A brief review on the related work is given in Section 2. Some preliminaries are reviewed in Section 3. Section 4 describes the system architecture and the anonymous attribute-based access control system, and presents design goals. Our basic anonymous CP-ABE construction with fast decryption together with its security results are described in Section 5. The security-enhanced construction together with its security results are described in Section 6. Security comparison and performance-related issues are discussed in Section 7. Finally, we draw a conclusion in Section 8.

Please cite this article as: Y. Zhang et al., Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing, Information Sciences (2016), http://dx.doi.org/10.1016/j.ins.2016.04.015