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

Zechao Liu, Zoe L. Jiang, Xuan Wang, S.M. Yiu

PII: S1084-8045(18)30030-4

DOI: 10.1016/j.jnca.2018.01.016

Reference: YJNCA 2058

To appear in: *Journal of Network and Computer Applications*

Received Date: 3 May 2017

Revised Date: 12 January 2018

Accepted Date: 26 January 2018

Please cite this article as: Liu, Z., Jiang, Z.L., Wang, X., Yiu, S.M., Practical attribute-based encryption: Outsourcing decryption, attribute revocation and policy updating, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.01.016.

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, HKSAR, China

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.

Keywords: attribute-based encryption, outsourcing decryption, attribute revocation, policy updating, large universe, multiple authorities

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.

[*] Corresponding author
Email address: zoeljiang@hit.edu.cn (Zoe L. Jiang)