Accepted Manuscript

Multi-authority fine-grained access control with accountability and its application in cloud

Jin Li, Xiaofeng Chen, Sherman S.M. Chow, Qiong Huang, Duncan S. Wong, Zheli Liu

PII:	S1084-8045(18)30087-0
DOI:	10.1016/j.jnca.2018.03.006
Reference:	YJNCA 2087
To appear in:	*Journal of Network and Computer Applications*
Received Date:	14 November 2017
Revised Date:	24 February 2018
Accepted Date:	12 March 2018

Please cite this article as: Li, J., Chen, X., Chow, S.S.M., Huang, Q., Wong, D.S., Liu, Z., Multi-authority fine-grained access control with accountability and its application in cloud, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.03.006.

Multi-Authority Fine-grained Access Control with Accountability and Its Application in Cloud

Jin Li[a,*], Xiaofeng Chen[b], Sherman S.M. Chow[c], Qiong Huang[d], Duncan S. Wong[e], Zheli Liu[f]

[a] *Department of Computer Science, Guangzhou University, China.*
[b] *Key Laboratory of Computer Networks and Information Security, Xidian University, China.*
[c] *Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong.*
[d] *College of Informatics, South China Agricultural University, China*
[e] *Security and Data Sciences Technology Division, ASTRI, Hong Kong*
[f] *College of Computer and Control Engineering, Nankai University, China.*

Abstract

Attribute-based encryption (ABE) is one of critical primitives for the application of fine-grained access control. To reduce the trust assumption on the attribute authority and in the meanwhile enhancing the privacy of users and the security of the encryption scheme, the notion of multi-authority ABE with an anonymous key issuing protocol has been proposed. In an ABE scheme, it allows to encrypt data for a set of users satisfying some specified attribute policy and any leakage of a decryption key cannot be associated to a user. As a result, a misbehaving user could abuse the property of access anonymity by sharing its key other unauthorized users. On the other hand, the previous work mainly focus on the key-policy ABE, which cannot support ciphertext-policy access control. In this paper, we propose a privacy-aware multi-authority ciphertext-policy ABE scheme with *accountability*, which hides the attribute information in the ciphertext and allows to trace the dishonest user identity who shares the decryption key. The

[*] Corresponding author.
Email addresses: lijin@gzhu.edu.cn (Jin Li), xfchen@xidian.edu.cn (Xiaofeng Chen), smchow@uwaterloo.ca (Sherman S.M. Chow), csqhuang@alumni.cityu.edu.hk (Qiong Huang), duncan@cityu.edu.hk (Duncan S. Wong), liuzheli@nankai.edu.cn (Zheli Liu)