Accepted Manuscript

Title: Efficient auditing for shared data in the cloud with secure user revocation and computations outsourcing

Author: Yuchuan Luo, Ming Xu, Kai Huang, Dongsheng Wang, Shaojing Fu

Please cite this article as: Yuchuan Luo, Ming Xu, Kai Huang, Dongsheng Wang, Shaojing Fu, Efficient auditing for shared data in the cloud with secure user revocation and computations outsourcing, *Computers & Security* (2017), https://doi.org/10.1016/j.cose.2017.12.004.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Efficient Auditing for Shared Data in the Cloud with Secure User Revocation and Computations Outsourcing

Yuchuan Luo[a], Ming Xu[a,*], Kai Huang[a,b], Dongsheng Wang[a], Shaojing Fu[a,b]

[a]*College of Computer, National University of Defense Technology, Changsha, China*

[b]*State Key Laboratory of Cryptography, Beijing, China*

Biographical sketch

Yuchuan Luo received the B.S. degree and M.S. degree from National University of Defense Technology (NUDT) in 2009, 2015 respectively, both in Computer Science and Technology. He is currently working towards the Ph.D degree in Computer Science and Technology in NUDT. He is currently studying at the City University of Hong Kong for a year. His research interests include Cloud Computing Security, Crowdsensing Security and Privacy.

Ming Xu is currently a professor and director of the Network Engineering Department in the College of Computer, National University of Defense Technology, China. Prof. Xu is a senior member of CCF and member of IEEE and ACM. His major research interests include mobile computing, wireless network, cloud computing and network security.

Kai Huang received the B.S. degree in Network Engineering and the M.S. degree in Cryptography from Naval University of Engineering, China, in 2007 and 2009, respectively. Currently, he is working towards the Ph.D. degree in the College of Computer at National University of Defense Technology. His research interests are in the areas of Cloud Computing security.

Dongsheng Wang received the B.S. degree from Tsinghua University, Beijing, China and the M.S. degree from National University of Defense Technology, Changsha China, in 2009 and 2012, respectively. He is currently a Ph.D. candidate at National University of Defense Technology, Changsha, China. His research interests focus on network and cloud computing security.

Shaojing Fu received his Ph.D. degree in applied cryptography from National University of Defense Technology in 2012 and has studied at University of Tokyo for one year during his Ph.D. He is currently a lecturer in the College of Computer, National University of Defense Technology. His research interests include cryptography theory and application, cloud storage security.

Abstract

With the cloud storage services, users can easily form a group and share data with each other. Considering the cloud is untrusted, public auditing is needed to ensure the integrity of the shared data. Once a user is revoked from the group, signatures from this revoked users need to be re-computed by an existing user, which may incurs heavy communication and computation cost. Proxy re-signatures can be used here to allow the cloud to compute re-signatures on behalf of the group. However, a malicious cloud is able to arbitrarily convert signatures from one user to

*Corresponding author (e-mail: mingxu@nudt.edu.cn)