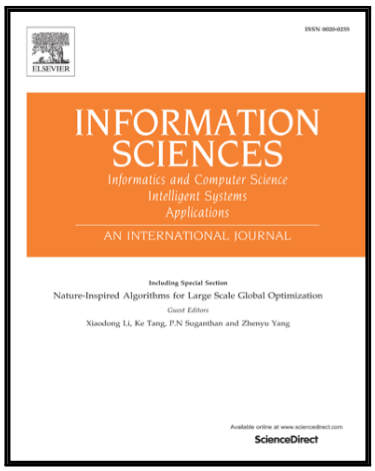
Accepted Manuscript



Insecurity of an identity-based public auditing protocol for the outsourced data in cloud storage

Debiao He, Huaqun Wang, Jianhong Zhang, Lina Wang

PII: S0020-0255(16)30984-7
DOI: 10.1016/j.ins.2016.09.049
Reference: INS 12545

To appear in: *Information Sciences*

Received date: 4 April 2016
Revised date: 4 August 2016
Accepted date: 19 September 2016

Please cite this article as: Debiao He, Huaqun Wang, Jianhong Zhang, Lina Wang, Insecurity of an identity-based public auditing protocol for the outsourced data in cloud storage, *Information Sciences* (2016), doi: 10.1016/j.ins.2016.09.049

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.

ACCEPTED MANUSCRIPT

Insecurity of an identity-based public auditing protocol for the outsourced data in cloud storage

Debiao He [1,2]

[1] *State Key Lab of Software Engineering, Computer School,Wuhan University, Wuhan, China*

[2] *Co-Innovation Center for Information Supply & Assurance Technology, Anhui University, Hefei, China*

Huaqun Wang [3,*]

School of Computer Science & Technology, Nanjing University of Posts and Telecommunications, Nanjing, China

Jianhong Zhang [4]

College of Science, North China University of Technology, Beijing, China

Lina Wang [5]

Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, Computer School,Wuhan University, Wuhan, China

Abstract

Public auditing protocol is very significant for implementing secure cloud storage since it can be used to check the integrity of the data stored in the cloud without downloading them. Recently, Zhang and Dong presented an identity-based public auditing (IBPA) protocol using the bilinear pairing and claimed that their protocol is provably secure in the random oracle model. Through proposing two concrete attacks, we demonstrate that the adversary against Zhang-Dong's protocol can break the data integrity without being found by the auditor. The analysis shows that their protocol is not secure for the cloud storage.

Keywords: public auditing, identity-based cryptography, provable security, bilinear pairing

*Corresponding author
Email address: wanghuaqun@yahoo.com.cn (Huaqun Wang [3,*])

Download English Version:

https://daneshyari.com/en/article/4944951

Download Persian Version:

https://daneshyari.com/article/4944951

Daneshyari.com