电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2011, Vol. 33 » Issue (9) :2199-2204 DOI: 10.3724/SP.J.1146.2011.00001

一种基于同态Hash的数据持有性证明方法

陈兰香*

(福建师范大学数学与计算机科学学院 福州 350108) (福建师范大学网络安全与密码技术重点实验室 福州 350108)

A Homomorphic Hashing Based Provable Data Possession

Chen Lan-xiang*

(School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350108, China)
(Key Lab of Network Security and Cryptology, Fuzhou 350108, China)

摘要 在云存储服务中，为了让用户可以验证存储服务提供者正确地持有(保存)用户的数据，该文提出一种基于同态hash (homomorphic hashing)的数据持有性证明方法。因为同态hash算法的同态性，两数据块之和的hash值与它们hash值的乘积相等，初始化时存放所有数据块及其hash值，验证时存储服务器返回若干数据块的和及其hash值的乘积，用户计算这些数据块之和的hash值，然后验证是否与其hash值的乘积相等，从而达到持有性证明的目的。在数据生存周期内，用户可以无限次地验证数据是否被正确持有。该方法在提供数据持有性证明的同时，还可以对数据进行完整性保护。用户只需要保存密钥*K*，约520 byte，验证过程中需要传递的信息少，约18 bit，并且持有性验证时只需要进行一次同态hash运算。文中提供该方法的安全性分析，性能测试表明该方法是可行的。

关键词： 云存储 数据持有性证明 同态hash 存储安全 数据完整性

Abstract： In cloud storage, in order to allow users to verify that the storage service providers store the user's data intactly. A homomorphic hashing based Provable Data Possession (PDP) method is proposed. Because of the homomorphism of hash algorithm, the hash value of the sum of two blocks is equal to the product of the two hash values. It stores all data blocks and their hash values in setup stage. When the user challenges the storage server, the server returns the sum of the requested data blocks and their hash values. The user computes the hash value of the sum of these data blocks and verifies whether they are equal. In the data lifecycle, the user can perform unlimited number of verification. The method provides provable data possession at the same time it provides integrity protection. Users only need to save a key *K*, about 520 byte, the information transferred for verification only need about 18 bit, and verification only needs one time hash computation. The security and performance analysis show that the method is feasible.

Keywords： Cloud storage Provable Data Possession (PDP) Homomorphic hashing Storage security Data integrity

Received 2011-01-04;

本文基金:

福建省教育厅科技项目(JA10079, JB10041)和福建省高校产学合作科技重大项目(2010H6007)资助课题

通讯作者: 陈兰香 Email: lxiangchen@gmail.com

引用本文:

陈兰香.一种基于同态Hash的数据持有性证明方法[J] 电子与信息学报, 2011,V33(9): 2199-2204

Chen Lan-Xiang.A Homomorphic Hashing Based Provable Data Possession[J] , 2011,V33(9): 2199-2204

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2011.00001 或 http://jeit.ie.ac.cn/CN/Y2011/V33/I9/2199