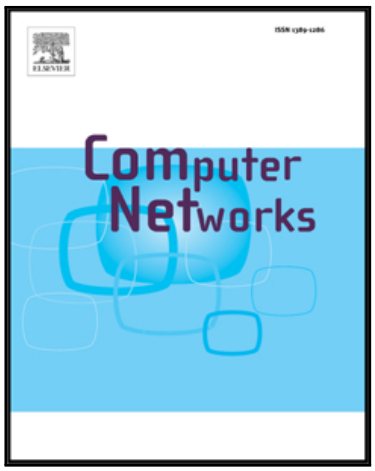

A General Framework to Design Secure Cloud Storage Protocol Using Homomorphic Encryption Scheme

Jian Zhang, Yang Yang, Yanjiao Chen, Jing Chen, Qian Zhang

PII: S1389-1286(17)30332-8
DOI: 10.1016/j.comnet.2017.08.019
Reference: COMPNW 6292

To appear in: *Computer Networks*

Received date: 17 April 2017
Revised date: 20 July 2017
Accepted date: 21 August 2017

Please cite this article as: Jian Zhang, Yang Yang, Yanjiao Chen, Jing Chen, Qian Zhang, A General Framework to Design Secure Cloud Storage Protocol Using Homomorphic Encryption Scheme, *Computer Networks* (2017), doi: 10.1016/j.comnet.2017.08.019

A General Framework to Design Secure Cloud Storage Protocol Using Homomorphic Encryption Scheme

Jian Zhang[a], Yang Yang[a], Yanjiao Chen[b,*], Jing Chen[b], Qian Zhang[c]

[a] *Computer School of Wuhan University, China*
[b] *State Key Lab of Software Engineering, Computer School of Wuhan University, China*
[c] *Department of Computer Science and Engineering*
Hong Kong University of Science and Technology, Hong Kong

Abstract

With the growing popularity of cloud storage, to guarantee the security of outsourced data becomes more and more important. In this paper, we make the first attempt to explore the intrinsic relationship between secure cloud storage and homomorphic encryption scheme, based on which we present a Generic way to design a Secure Cloud Storage protocol, denoted as G-SCS, using any homomorphic encryption scheme (HES). The proposed G-SCS is secure under a definition that satisfy the security requirement of cloud storage. To address various issues in real application scenarios, we further extend the protocol to support deterministic and randomized auditing, data dynamics (i.e., data insertion, deletion and modification), as well as third-party public auditing, while preserving the efficiency and security of the protocol. By instantiating all abstract semantics in G-SCS, we construct three concrete secure cloud storage protocols using RSA-based, Paillier-based and DGHV-based HESs, which are multiplicatively, additively and fully HESs, respectively. We conduct extensive theoretical analysis and experimental evaluations to validate the practicability of the proposed protocol.

Keywords: Secure cloud storage; homomorphic encryption scheme; data dynamics; third-party public auditing.

*Corresponding author. Tel.: +86 (027) 68773612
Email address: chenyanjiao@whu.edu.cn (Yanjiao Chen)