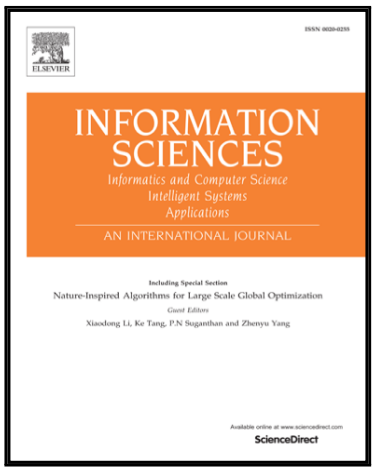

Encrypted Data Processing with Homomorphic Re-Encryption

Wenxiu Ding , Zheng Yan , Robert H. Deng

PII: S0020-0255(16)32256-3
DOI: 10.1016/j.ins.2017.05.004
Reference: INS 12874

To appear in: *Information Sciences*

Received date: 29 December 2016
Revised date: 21 March 2017
Accepted date: 6 May 2017

Please cite this article as: Wenxiu Ding , Zheng Yan , Robert H. Deng , Encrypted Data Processing with Homomorphic Re-Encryption, *Information Sciences* (2017), doi: 10.1016/j.ins.2017.05.004

Encrypted Data Processing with Homomorphic Re-Encryption

Wenxiu Ding
State Key Lab on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China
wenxiuding_1989@126.com

Zheng Yan*
State Key Lab on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China
Department of Communications and Networking, Aalto University, Espoo 02150, Finland
zyan@xidian.edu.cn; zheng.yan@aalto.fi

Robert H. Deng
School of Information Systems, Singapore Management University, Singapore 178902
robertdeng@smu.edu.sg

* Corresponding author: Zheng Yan (email: zyan@xidian.edu.cn)

Abstract
Cloud computing offers various services to users by re-arranging storage and computing resources. In order to preserve data privacy, cloud users may choose to upload encrypted data rather than raw data to the cloud. However, processing and analyzing encrypted data are challenging problems, which have received increasing attention in recent years. Homomorphic Encryption (HE) was proposed to support computation on encrypted data and ensure data confidentiality simultaneously. However, a limitation of HE is it is a single user system, which means it only allows the party that owns a homomorphic decryption key to decrypt processed ciphertexts. Original HE cannot support multiple users to access the processed ciphertexts flexibly. In this paper, we propose a Privacy-Preserving Data Processing (PPDP) system with the support of a Homomorphic Re-Encryption Scheme (HRES). The HRES extends partial HE from a single-user system to a multi-user one by offering ciphertext re-encryption to allow multiple users to access processed ciphertexts. Through the cooperation of a Data Service Provider (DSP) and an Access Control Server (ACS), the PPDP system can support seven basic operations over ciphertexts, which include *Addition*, *Subtraction*, *Multiplication*, *Sign Acquisition*, *Comparison*, *Equivalent Test*, and *Variance*. To enhance the flexibility and security of our system, we further apply multiple ACSs to take in charge of the data from their own users and design computing operations over ciphertexts belonging to multiple ACSs. We then prove the security of PPDP, analyze its performance and advantages by comparing with some latest work, and demonstrate its efficiency and effectiveness through simulations with regard to big data process.

Keywords: Homomorphic Encryption, Privacy Preservation, Data Sharing, Proxy Re-encryption, Access Control, Cloud Computing