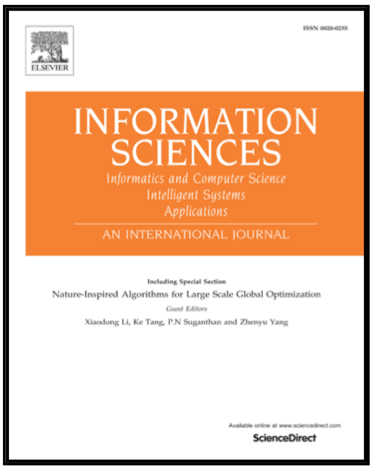

ISSN 0020-0255

ELSEVIER

INFORMATION SCIENCES

Informatics and Computer Science
Intelligent Systems
Applications

AN INTERNATIONAL JOURNAL

Including Special Section
Nature-Inspired Algorithms for Large Scale Global Optimization
Guest Editors
Xiaodong Li, Ke Tang, P.N Suganthan and Zhenyu Yang

Available online at www.sciencedirect.com
ScienceDirect

CCA Secure Encryption Supporting Authorized Equality Test on Ciphertexts in Standard Model and Its Applications

Yujue Wang, HweeHwa Pang, Ngoc Hieu Tran, Robert H. Deng

PII: S0020-0255(17)30227-X
DOI: 10.1016/j.ins.2017.06.008
Reference: INS 12930

To appear in: *Information Sciences*

Received date: 17 January 2017
Revised date: 4 May 2017
Accepted date: 8 June 2017

Please cite this article as: Yujue Wang, HweeHwa Pang, Ngoc Hieu Tran, Robert H. Deng, CCA Secure Encryption Supporting Authorized Equality Test on Ciphertexts in Standard Model and Its Applications, *Information Sciences* (2017), doi: 10.1016/j.ins.2017.06.008

CCA Secure Encryption Supporting Authorized Equality Test on Ciphertexts in Standard Model and Its Applications

Yujue Wang[a,b,*], HweeHwa Pang[b], Ngoc Hieu Tran[b], Robert H. Deng[b]

[a]*School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China*
[b]*School of Information Systems, Singapore Management University, Singapore 188065*

Abstract

We present an *encryption scheme for authorized equality test on ciphertexts* (SEET), which allows the data owner to authorize a tester to compare her ciphertexts without decrypting their values. The security of SEET is formally proved against three types of adversary, two of them for ciphertext confidentiality in the phases before and after authorization respectively, and the third for token privacy. To the best of our knowledge, our SEET construction is the first encryption scheme supporting equality test on ciphertexts that is proven secure against the three types of adversary in the standard model. Our SEET construction outperforms existing schemes in terms of ciphertext size and encryption/decryption/testing costs. To show its application in set operations, we extend it into schemes for *controlled set distance computation*, such that a curious server is able to deduce the similarity/dissimilarity score between two encrypted user sets without knowing their elements.

Keywords: Data encryption, equality test on ciphertexts, data outsourcing, private set intersection, set operation, implicit authentication

[*] Corresponding author
Email address: yjwang@smu.edu.sg (Yujue Wang)