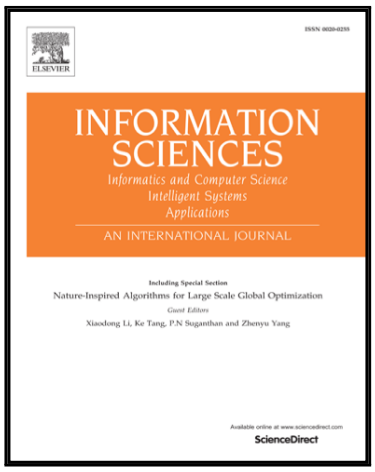

Generic construction of public key encryption, identity-based encryption and signcryption with equality test

Xi-Jun Lin, Lin Sun, Haipeng Qu

PII: S0020-0255(18)30289-5
DOI: 10.1016/j.ins.2018.04.035
Reference: INS 13578

To appear in: *Information Sciences*

Received date: 25 June 2017
Revised date: 4 April 2018
Accepted date: 7 April 2018

Please cite this article as: Xi-Jun Lin, Lin Sun, Haipeng Qu, Generic construction of public key encryption, identity-based encryption and signcryption with equality test, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.04.035

Generic construction of public key encryption, identity-based encryption and signcryption with equality test

Xi-Jun Lin *, Lin Sun †and Haipeng Qu ‡

April 9, 2018

Abstract: Public key encryption with equality test (PKEET) allows the cloud server to test whether two ciphertexts are generated on the same message. Recently, Lee et al. proposed a semi-generic approach for PKEET constructions by using the traditional public key encryption schemes. However, how to design a generic approach is still an open problem. In this paper, we propose a generic approach for PKEET constructions. Our approach can be easily extended to the identity-based setting. Compared with Lee et al.'s approach, ours is (surprisingly) more efficient. Moreover, we propose a new primitive, called signcryption with equality test (SCET). Compared with the traditional PKEET, SCET provides both confidentiality and authentication simultaneously.

Key words: public key encryption with equality test; generic construction; cloud computing; signcryption

1 Introduction

Public key encryption with equality test (PKEET), which was first proposed by Yang et al. [10], allows the cloud server to test whether two ciphertexts are generated on the same message. However, anyone is able to test the ciphertexts without any authorization in Yang et al.'s proposal, which violates the data owners' privacy. Therefore, several schemes with authorization mechanisms [5, 7, 8, 9, 2, 3, 4] were proposed.

1.1 Our contribution

In this paper, we propose a generic approach for PKEET constructions that exploits traditional public key encryption (PKE) schemes. The system model follows that of all-or-nothing PKEET (AoN-PKEET) scheme proposed by Tang [8], where each receiver submits a trapdoor to allow the cloud server to test the equality of all of his ciphertexts.

The motivation of our work is as follows. In [8], Tang attempted to propose a generic PKEET construction. The ciphertext is computed as follows:

$$(C_1, C_2) = (\mathrm{PKE}_1.\mathrm{Enc}(pk_1, m),\ \mathrm{PKE}_2.\mathrm{Enc}(pk_2, H_1(m))),$$

*X.J.Lin is with the Department of Computer Science and Technology, Ocean University of China. Qingdao 266100, P.R.China. email: linxj77@163.com

†L. Sun is with the College of Liberal Arts, Qingdao University. Qingdao 266071, P.R.China.

‡H.Qu is with the Department of Computer Science and Technology, Ocean University of China. Qingdao 266100, P.R.China.