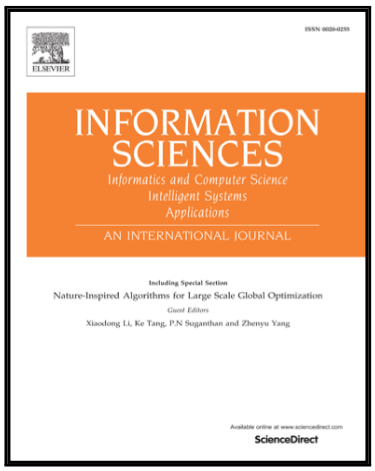

A Generic Scheme of Plaintext-Checkable Database Encryption

Sha Ma, Yi Mu, Willy Susilo

PII: S0020-0255(17)30164-0
DOI: 10.1016/j.ins.2017.11.010
Reference: INS 13238

To appear in: *Information Sciences*

Received date: 17 January 2017
Revised date: 30 October 2017
Accepted date: 1 November 2017

Please cite this article as: Sha Ma, Yi Mu, Willy Susilo, A Generic Scheme of Plaintext-Checkable Database Encryption, *Information Sciences* (2017), doi: 10.1016/j.ins.2017.11.010

A Generic Scheme of Plaintext-Checkable Database Encryption

Sha Ma[a,b,*], Yi Mu[b], Willy Susilo[b]

[a] *College of Mathematics and Informatics, South China Agricultural University, Guangzhou, Guangdong 510640, China*
[b] *School of Computing and Information Technology, University of Wollongong, NSW, Australian*

Abstract

Database encryption is essential for cloud database systems. For a large database, decryption could take a lot of computational time. Therefore, verifying an encryption that contains a correct plaintext without decryption becomes significant for a large database system. Plaintext-checkable encryption (PCE) is a potential tool for such database systems, which is first proposed by Canard et al. in CT-RSA 2012. Although the generic PCE in the random oracle model has been studied intensively, the generic PCE in the standard model and its efficient implementation are still challenging problems. This paper presents the first generic PCE in the standard model using smooth projective hash function (SPHF) and prove its s-priv1-cca security, which is independent of current unlink security. Based on the instantiated SPHF from DDH assumption, we obtain the most efficient PCE in the standard model, without any pairing operation. Finally, we improve two existing generic constructions in the random oracle model so that they are secure under chosen ciphertext attack.

Keywords: database encryption, plaintext-checkable encryption, provable security.

*Corresponding author
Email addresses: martin_deng@163.com (Sha Ma), ymu@uow.edu.au (Yi Mu), wsusilo@uow.edu.au (Willy Susilo)