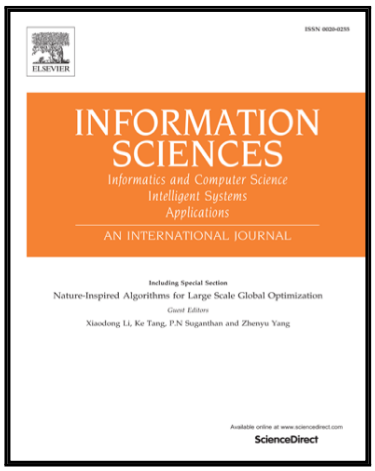

Access Control Encryption with Efficient Verifiable Sanitized Decryption

Huige Wang, Kefei Chen, Joseph K. Liu, Ziyuan Hu, Yu Long

PII: S0020-0255(18)30516-4
DOI: 10.1016/j.ins.2018.06.068
Reference: INS 13761

To appear in: *Information Sciences*

Received date: 18 December 2017
Revised date: 29 June 2018
Accepted date: 30 June 2018

Please cite this article as: Huige Wang, Kefei Chen, Joseph K. Liu, Ziyuan Hu, Yu Long, Access Control Encryption with Efficient Verifiable Sanitized Decryption, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.06.068

Access Control Encryption with Efficient Verifiable Sanitized Decryption

Huige Wang[a], Kefei Chen[b,e,*], Joseph K. Liu[d], Ziyuan Hu[c], Yu Long[c],

[a] *Department of Computer, Anhui Science and Technology University, Fengyang 233100, China*
[b] *School of Science, Hangzhou Normal University, Hangzhou 310036, China*
[c] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*
[d] *Faculty of Information Technology, Monash University, Melbourne, 3800, Australia*
[e] *Westone Cryptologic Research Center, Beijing 100070, China*

Abstract

Access control encryption (ACE), as a new cryptographic framework was proposed by Damgard et al. (at TCC 2016), enables controlling both the writing users and the reading users. Recently, a number of access control encryptions are proposed, but none of them are able to implement the verifiability of the sanitized ciphertexts which may lead to incorrect decryption. To solve this problem, by adapting Kim and Wu's techniques (at TCC 2017) and combining with the strong randomness extractor, we put forward a generic framework of access control encryption with verifiable sanitized decryption for arbitrary policy. The instantiabilities of the used building blocks from standard assumptions illustrates that our new construction works well. Moreover, we prove that our scheme not only satisfies the standard security definitions of access control encryption but also achieves the verifiability security for the sanitized ciphertexts.

Keywords: access control encryption, no-read rule, no-write rule, verifiable sanitized decryption

1. Introduction

ACE, as a new cryptographic primitive for encryption, was proposed by Damgard et al., in [DHO16]. Compared with other public key encryption systems (e.g., attribute-based encryption (ABE) [SW05], identity-based encryption (IBE) [BWY11, BW06, Gen06], and functional encryption (FE) [BSW11]) which only implements access control on receivers (namely it only enables controlling what users are allowed to decrypt), ACE also implements access control on senders (namely it enables controlling what users are allowed to encrypt).

Roughly speaking, ACE is defined associated with not only a set of senders $\mathcal{S}$ and a set of receiver users $\mathcal{R}$, also an access control policy $P : \mathcal{S} \times \mathcal{R} \to \{0, 1\}$ which maps a sender-receiver pair to a boolean output. Specifically, the policy $P(i, j) = 1$ is used to indicate that

*Corresponding author
Email addresses: whgexf@163.com (Huige Wang), kfchen@hznu.edu.cn (Kefei Chen), Joseph.liu@monash.edu (Joseph K. Liu), huziyuan@sina.com (Ziyuan Hu), longyu@sjtu.edu.cn (Yu Long)