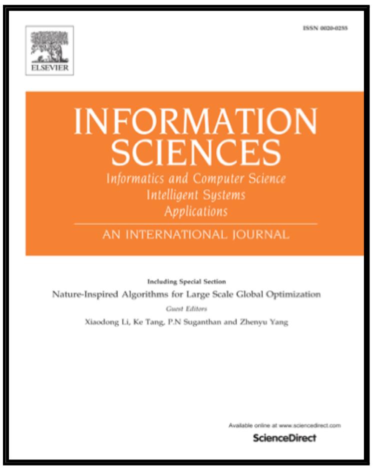
ISSN 0020-0255
ELSEVIER
INFORMATION SCIENCES
Informatics and Computer Science
Intelligent Systems
Applications
AN INTERNATIONAL JOURNAL
Including Special Section
Nature-Inspired Algorithms for Large Scale Global Optimization
Guest Editors
Xiaodong Li, Ke Tang, P.N Suganthan and Zhenyu Yang
Available online at www.sciencedirect.com
ScienceDirect

Attribute-based signcryption scheme based on linear codes

Yun Song, Zhihui Li, Yongming Li, Jing Li

PII: S0020-0255(17)30803-4
DOI: 10.1016/j.ins.2017.06.033
Reference: INS 12955

To appear in: *Information Sciences*

Received date: 30 July 2015
Revised date: 23 June 2017
Accepted date: 24 June 2017

Attribute-based signcryption scheme based on linear codes

Yun Song[1] , Zhihui Li[2] ⋆ , Yongming Li[1] , Jing Li[3]

[1]School of Computer Science, Shaanxi Normal University, Xi'an 710062, China;
[2] School of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062, China;
[3] School of computer science and education software, Guangzhou University, Guangzhou 510006, China

Abstract. Compared with traditional schemes in which encryption follows a signature, the attribute-based signcryption (ABSC) scheme not only costs less both in terms of both computation and communication but also provides message confidentiality, ensures the authenticity of a message, and attests to the attributes of the sender. In this paper, we first formalize a selective-attribute security model of the attribute-based signcryption based on linear codes. Then, we construct a flexible and efficient ABSC scheme based on a secret sharing method called Linear Codes Secret Sharing Scheme. This ABSC scheme breaks the threshold limit and employs diverse attribute sets by constructing the access structures on linear codes. In addition, our scheme achieves confidentiality against chosen-ciphertext attacks and unforgeability against chosen-message attacks in the selective-attribute model. Finally, we compare the proposed scheme with existing schemes in terms of their properties and efficiency.

Keywords: Signcryption; Attribute-based cryptosystem; Bilinear pairing; Linear codes; Selective-attribute model

1 Introduction

Attribute-based cryptography has enormous potential for providing data security in distributed environments. Attribute-based systems allow security functionalities to be provided based on users' attributes instead of their individual identities. Attribute-based encryption (ABE) [11,13,14, 18,20] is a public key encryption scheme in which users with specific attributes are able to decrypt the ciphertext associated with those attributes. In ABE schemes, an encryptor can specify many decryptors by assigning common attributes of the decryptors such as gender, age, affiliation and so on. Nevertheless, the above works can ensure only data confidentiality; they cannot provide authenticity and unforgeability. The concept of an attribute-based signature (ABS) was first introduced by Maji et al. in [9]. In their scheme, a signer can use a private key and a particular signing predicate satisfied by the signer's attributes to compute the signature on any message. Then, a verifier can ensure that a signer has endorsed the message with the attributes satisfying the signing predicate but cannot reveal any information about the attributes of the signer. After the scheme was initially proposed, attribute-based signature methods have been studied by several researchers [2,12,15,21].

In cloud technology, users can outsource their data to the cloud providers to share their data efficiently with other selected users and can also access their data from anywhere through the

[⋆] Corresponding author. Email: lizhihui@snnu.edu.cn