Information Sciences 318 (2015) 111–122

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Obtain confidentiality or/and authenticity in Big Data by ID-based generalized signcryption

Guiyi Wei [a], Jun Shao [a,*], Yang Xiang [b], Pingping Zhu [a], Rongxing Lu [c]

[a] School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou, Zhejiang 310018, PR China
[b] School of Information Technology, Deakin University, VIC 3125, Australia
[c] School of Electrical and Electronics Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798, Singapore

ARTICLE INFO

Article history:
Received 18 January 2014
Received in revised form 12 May 2014
Accepted 20 May 2014
Available online 11 June 2014

Keywords:
Big Data
Confidentiality
Authenticity
Generalized signcryption
Provable security
Standard model

ABSTRACT

Recently, the Big Data paradigm has received considerable attention since it gives a great opportunity to mine knowledge from massive amounts of data. However, the new mined knowledge will be useless if data is fake, or sometimes the massive amounts of data cannot be collected due to the worry on the abuse of data. This situation asks for new security solutions. On the other hand, the biggest feature of Big Data is "massive", which requires that any security solution for Big Data should be "efficient". In this paper, we propose a new identity-based generalized signcryption scheme to solve the above problems. In particular, it has the following two properties to fit the efficiency requirement. (1) It can work as an encryption scheme, a signature scheme or a signcryption scheme as per need. (2) It does not have the heavy burden on the complicated certificate management as the traditional cryptographic schemes. Furthermore, our proposed scheme can be proven-secure in the standard model.

1. Introduction

The Big Data paradigm recently has received considerable attention since it gives a great opportunity to mine knowledge from massive amounts of data. However, the Big Data paradigm also brings some security challenges [12,10,20,16,22,1,8,19]. For instance, the value of new mined knowledge is decided by the authenticity of the collected massive amounts of data. Furthermore, the massive amounts of data cannot be collected successfully if people are not willing to share their data due to the worry of the abuse of data. It demands that the data could be access only by the authorized people. The above problem is summarized in Fig. 1. In general, to achieve the authenticity and confidentiality alone, the basic tools are signature and encryption, respectively. While to achieve the both properties together, the traditional approach of either "signature-then-encryption" or "encryption-then-signature" will be applied. However, this kind of traditional approach incurs high computational cost and communication overhead. As it is known to us, the efficiency is one of main requirements for any security solution in Big Data. Signcryption [27] is a promising tool to obtain both confidentiality and authenticity efficiently. In particular, it can be realized in a logic step, and has a lower computational cost and communication overhead than the traditional approach. Due to its efficiency, many signcryption schemes have been proposed [2,28,17,4,15].

* Corresponding author. Tel.: +86 571 28008286.
E-mail addresses: weigy@zjgsu.edu.cn (G. Wei), chn.junshao@gmail.com (J. Shao), yang@deakin.edu.au (Y. Xiang), zhupingping717@163.com (P. Zhu), rxlu@ntu.edu.sg (R. Lu).

http://dx.doi.org/10.1016/j.ins.2014.05.034
0020-0255/

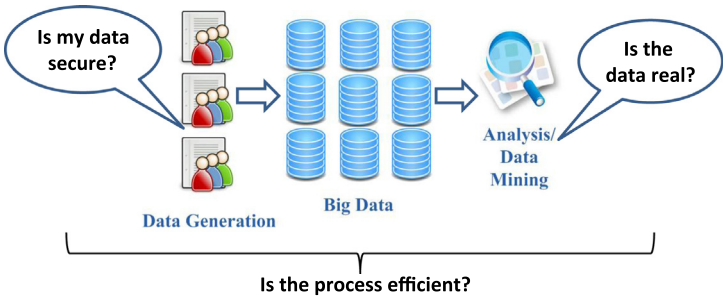

Fig. 1. The security challenges in Big Data diagram.

Nonetheless, the original signcryption has a heavy burden on the certificate management. For example, Alice must check the validity of Bob's public key certificate before signcrypting messages by using Bob's public key. It makes that signcryption is not very suitable for Big Data. One possible solution to reduce the burden is to use the idea of identity-based cryptography firstly introduced by Shamir [23]. The distinguishing property of identity-based cryptography is that user's public key is his/her identity such as email address, name or telephone number and the user's private key is generated from the public key by a trusted third party called private key generator (PKG). Hence, the problem of certificate management can be mitigated. In 2002, Chen and Malone-Lee [21] proposed the first identity-based signcryption scheme along with a security model. Since then, many identity-based signcryption schemes have been proposed [9,5,18].

However, in some cases of Big Data, we sometimes need the confidentiality and authenticity separately, but sometimes need both simultaneously. For example, we only care about the authenticity of statistic data from government, but the confidentiality and authenticity of sales data from companies. To achieve this special requirement, we can naively use three different schemes: an encryption scheme, a signature scheme, and a signcryption scheme. Nevertheless, the naive approach is costly in terms of implementation complexities, which makes it not suitable for Big Data. In this paper, we would like to use a new cryptographic primitive called generalized signcryption to solve the problem.

The concept of generalized signcryption due to Han et al. [11] can work as an encryption scheme, a signature scheme or a signcryption scheme as per need. Han et al. [11] presented the first concrete scheme based on ECDSA yet without a formal security proof. Later, Wang et al. [24] presented the formal security model for generalized signcryption and a proven-secure scheme that is regarded as an improvement of Han et al.'s scheme [11]. In 2008, Lal and Kushwah [14] proposed the first identity-based generalized signcryption along with the security model. However, Yu et al. [26] showed that Lal and Kushwah's security model is not complete, then they modified the security model and proposed their own scheme. Recently, Kushwah and Lal [13] simplified Yu et al.'s security model and proposed an efficient identity-based generalized signcryption scheme.

Nevertheless, all existing identity-based generalized signcryption schemes were proved only in the random oracle model. It has been shown that security in the random oracle model does not guarantee the security in the real world [3,6]. Thus, it is desired to obtain an identity-based generalized signcryption scheme which is proved secure in the standard model. In this paper, we try to take this challenge by using the techniques of Waters [25] and the CHK [7].

The rest of this paper is organized as follows. Section 2 presents some preliminaries related to this paper. Section 3 reviews our scheme. Section 4 analyzes the security of our scheme. Finally, conclusions are present in Section 5.

2. Preliminaries

In this section, we briefly introduce some involved parties of this scheme. Note that the definitions related to the identity-based generalized signcryption follow that proposed by Kushwah and Lal in [13].

2.1. Notations

For easier reading, we give the description of some basic notations in Table 1.

Table 1
Some basic notations.

Notations	Meaning
$\mathbb{G}$, $\mathbb{G}_T$	Bilinear groups with order q
g, g_1, g_2	Elements from $\mathbb{G}$
q	Large prime number
$e : \mathbb{G} \times \mathbb{G} \Rightarrow \mathbb{G}_T$	Bilinear pairing
$\boldsymbol{U}$, $\boldsymbol{M}$, $\boldsymbol{V}$	Vectors with elements from $\mathbb{G}$
u_a, u_b	Identities of the sender and receiver
u_φ	Empty identity
d_u	Private key corresponding to identity u