Constructing Secure Warrant-Based Proxy Signcryption Schemes

Yuan Zhou, Zhenfu Cao, and Rongxing Lu

Department of Computer Science, Shanghai Jiao Tong University,
1954 Huashan Road, Shanghai 200030, P.R. China
zhouyuan@sjtu.edu.cn, {cao-zf, rxlu}@cs.sjtu.edu.cn

Abstract. Proxy signcryption, proposed by Gamage et al. [1], is a cryptographic primitive, which combines the functionality of a proxy signature scheme with that of an encryption. But to date, no formal definitions of security have been provided. In this paper, we first propose the syntax of warrant-based proxy signcryption scheme, then formalize notions of security for it. After that, we present a warrant-based proxy signcryption scheme based on integer factorization assumption.

Keywords: proxy Signcryption, integer factorization, provable security.

1 Introduction

Signcryption is a cryptographic primitive proposed by Zheng [2] to combine a function of a digital signature scheme with that of a encryption scheme. Signcryption not only provides three services (i.e. authenticity and confidentiality and non-repudiation) but also provides them in a single logical step. So it is more efficient than traditional signature-then-encryption. After Zheng' work, some resarch works has been done. Schemes in [3, 4, 5] have all been designed without a precisely specified secure model and corresponding security proof. A formal model of security for signcryption with non-repudiation is proposed in [6]. In [7], Malone-Lee and Mao provide a formal model of security for signcryption and give the corresponding security proofs of an Signcryption scheme using RSA. In their paper, they claim that their scheme offers non-repudiation in a very simple manner. However, their scheme cannot efficiently provides $\mathcal{NR}$ algorithm defined in [6]. The first formal definition signcryption scheme was issued in[8]. The author of paper defines signcryption as a multi-user primitive which simultaneously satisfies chosen ciphertext security for privacy and existential unforgeability for authenticity.

The notion of proxy signature scheme introduced by Mambo et al in 1996 [9]. A proxy signature scheme allows a entity called original signer to delegate his signing capability to another entity, called proxy signer. In a partial delegation with warrant proxy signature scheme, the original signer uses standard signature algorithm to sign a warrant which includes the type of the information delegated, both the parties identities and the period of delegation, etc. The signature of the

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 172–185, 2005.

warrant is called certificate. With the certificate and his private key, the proxy signer generates a proxy private key. After that, the proxy signer can sign any messages according to the warrant. And a third party would verify the validity of the proxy signature. In [10], some formal security notions for warrant based proxy signature schemes are presented. The proxy signature plays an important role in many applications [11–14] and has received great attention since it was proposed.

Recently, e-commerce environments have been paid great attentions. Let us consider an scenario that an president in a company delegates his capability of signing a message to another entity in case of say, temporal absence or lack of time. As a natural idea, a proxy signature scheme can be taken into account. However, if the message involves some commercial secret, a proxy signature scheme cannot satisfy this requirement. In 1999, Gamage et al. [1] extended the proxy signature and introduced a proxy signcryption scheme by combining proxy signature and encryption technology. It allows an entity to delegate its authority of signcryption to a trusted agent. Gamage' scheme is based on discrete logarithm. However, this scheme is not under an secure model, so the corresponding security proof has not been proposed in it. Further, it is desirable to design a proxy signcryption scheme based on other problems, such as integer factorization assumption.

Being inspired with above ideas, in this paper, we extend the syntax of signcryption proposed in [8] and present the syntax of warrant-based proxy signcryption, which combines the function of a warrant-based proxy signature scheme with that of a encryption scheme. Then, we formalize the notion of security for it. To our best knowledge, no similar works have been done. After that, we propose an efficient proxy signcryption scheme, which is based on integer factorization assumption and can be applied to signcrypt some short message. The scheme is based on Rabin signature scheme [15] and the encryption scheme in [16]. Moreover, our scheme's computation is much lower than Gamage'one.

2 Warrant-Based Proxy Signcryption Schemes

In [8], the syntax of signcryption schemes and some security notions for such schemes have been presented. In this section, we first review the basic works, then extend them to ones for warrant-based proxy signcryption.

2.1 Signcryption Scheme and the Security Notions for It

We recall the components of a signcryption scheme and the notions of security for such schemes [8].

Definition 2.1 (Signcryption scheme). Let signcryption $\mathbf{SC}=(\mathcal{G}, \mathcal{K}, \mathcal{SC}, \mathcal{VD}, \mathcal{NR}, \mathcal{V})$ be defined as follows:

- The parameter generation algorithm $\mathcal{G}$ takes as input 1^k where k is the security parameter, and outputs some global parameters **params**.