Two Proxy Signcryption Schemes from Bilinear Pairings

Qin Wang and Zhenfu Cao

Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200030, P.R. China
{wangqin, cao-zf}@cs.sjtu.edu.cn

Abstract. Proxy signcryption is a cryptographic primitive which combines the functionalities of a proxy signature scheme and a signcryption scheme. In this paper, based on bilinear pairings, we would like to propose two efficient proxy singcryption schemes. One is certificate based and the other is identity based. Also we analyze the two proposed schemes from efficiency point of view. We show that the certificate based scheme achieves great efficiency in terms of communication cost and computation overhead. And the identity based scheme is much more efficient than the scheme proposed by Li and Chen. What's more, we also argument that the two proposed schemes are secure in the random oracle model without a secure channel.

Keywords: proxy signature, signcryption, proxy signcryption, bilinear pairings.

1 Introduction

In the areas of computer communications and electronic transactions, one of the important topics is how to send data in a confidential and authenticated way. Usually, the confidentiality of delivered data is provided by encryption algorithms, and the authentication of messages is guaranteed by digital signatures. In 1997, Zheng proposed a primitive that he called *signcryption* [10]. The idea of a signcryption scheme is to combine the functionality of an encryption scheme with that of a signature scheme. It must provide privacy; must be unforgeable; and there must be a method to settle repudiation disputes. This must be done in a more efficient manner than a composition of an encryption scheme with a signature scheme. After that, some research works on signcryption have been done [5–10].

The *proxy signature* primitive and the first efficient solution were introduced by Mambo, Usuda and Okamoto (MUO) [12]. The scheme allows an entity, called the original signer, to delegate another entity, called a proxy signer, to sign messages on its behalf. Proxy signature has found numerous practical applications, particularly in distributed computing where delegation of rights is quite common, such as e-cash systems, global distribution networks, grid computing, mobile agent applications, and mobile communications. A secure proxy signature scheme should satisfy the following five requirements: verifiability, strong

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 161–171, 2005.

unforgeability, strong identifiability, strong undeniability, prevention of misuse [12, 13].

The *proxy signcryption* primitive and the first scheme were proposed by Gamage, Leiwo, and Zheng (GLZ) in 1999 [11]. The scheme combines the functionality of a proxy signature scheme and a signcryption scheme. It allows an entity to delegate its authority of signcryption to a trusted agent. The proxy signcryption scheme is useful for applications that are based on unreliable datagram style network communication model where messages are individually signed and not serially linked via a session key to provide authenticity and integrity. Along with the concept, Gamage, Leiwo, and Zheng also proposed a proxy signcryption scheme [11]. In 2004, Li and Chen proposed an identity based proxy signcryption scheme [17] from pairings, denoted Li-Chen scheme in this paper.

An *identity based cryptosystem* is a novel type of public cryptographic scheme in which the public keys of the users are their identities or strings derived from their identities. For this to work there is a Key Generation Center (KGC) that generates private keys using some master key related to the global parameters for the system. In [18] Shamir proposed an identity-based signature scheme, but for many years identity-based encryption remained an open problem. Until 2001, Boneh and Franklin [2] presented an ID-based encryption scheme based on properties of bilinear pairings on elliptic curves, which appears to be the first fully functioning, efficient and provably secure identity-based encryption scheme. Since then, many cryptographic protocols using pairings were proposed [1-6, 9, 15, 16].

In this paper, we will give two proxy signcryption schemes from bilinear pairings. One scheme is in certificate based public key setting, and the other scheme is in identity based public key setting. The certificate based scheme achieves great efficiency as the Chen-Lee signcryption scheme [5], and completes signcryption and proxy functionality simultaneously. The identity based scheme is much more efficient than Li-Chen scheme[17] in terms of computation overhead. Both of the two proposed schemes need no secure channel. What's more, we argument that they are both secure in the random oracle model.

The rest of this paper is organized as follows: In section 2, we first review some basic concepts of bilinear pairings. Then we propose a certificate based proxy signcryption scheme and analyze its performance and security in section 3. An identity based proxy signcryption scheme and the analysis of its performance and security are presented in section 4. Finally, the conclusion is given in section 5.

2 Basic Concepts of Bilinear Pairings

In this section, we will briefly review the basic concept and some properties of bilinear pairing.

Let $(\mathbb{G}, +)$ denote a cyclic additive group generated by P, whose order is a large prime q, and $(\mathbb{W}, \cdot)$ denote a cyclic multiplicative group of the same order q. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{W}$ be a pairing which satisfies the following properties: