Information Sciences 179 (2009) 292–302

Contents lists available at ScienceDirect

Information Sciences

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

A secure identity-based proxy multi-signature scheme

Feng Cao, Zhenfu Cao *

Department of Computer Science and Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, China

ARTICLE INFO

Article history:
Received 24 November 2006
Received in revised form 21 April 2008
Accepted 10 May 2008

Keywords:
Digital signature
Identity-based
Proxy multi-signature
Provable security
Security model

ABSTRACT

In a proxy multi-signature scheme, a designated proxy signer can generate the signature on behalf of a group of original signers. To our best knowledge, most of existing proxy multi-signature schemes are proposed in public key infrastructure setting, which may be the bottleneck due to its complexity. To deduce the complexity, several proxy multi-signature schemes are proposed in the ID-based setting. However, no formal definitions on ID-based proxy are proposed until now. To fill the gap, this paper proposes the formal definition. Furthermore, we present a proven secure ID-based proxy multi-signature scheme, which is more efficient than existing schemes in term of computational cost.

1. Introduction

In 1984, Shamir [14] introduced the concept of identity-based cryptography to simplify key management and remove the necessity of public key certificates. Although many identity-based encryption schemes have been proposed since 1984, the problem of designing an efficient and secure identity-based encryption scheme remained open until 2001, when the work of Boneh and Franklin appeared [2].

In identity-based cryptography, a user's public is the user's identity information, such as his email address. The user's private key is obtained from a private key generator (PKG) who holds a secret called master-key. As a result, the complexity of public key's certificate management can be reduced largely.

The concept of proxy signature was first introduced by Mambo et al. [13] in 1996. In a proxy signature scheme, generally, there are two entities: an original signer and a proxy signer. The original signer can delegate his signing right to a proxy signer. The proxy signer can generate a valid signature on behalf of the original signer. Since the proxy signature primitive was introduced, various extensions of the basic proxy signature primitive have been considered, such as threshold proxy signature [6], proxy blind signature [1], and proxy multi-signature [5,7–11,18,19].

The proxy multi-signature primitive and the first efficient solution were introduced by Yi et al. [18]. In a proxy multi-signature scheme, a designated proxy signer can generate the signature on behalf of a group of original signers. It plays an important role in the following scenario: A company releases a document that may involve the financial department, engineering department, program office, etc. The document must be signed jointly by these entities, or signed by a proxy signer who is trusted by all of these entities. One solution to the latter case of this problem is to use a proxy multi-signature scheme.

* Corresponding author. Tel./fax: +86 21 34205345.
E-mail address: zfcao@cs.sjtu.edu.cn (Z. Cao).

0020-0255/$ - see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2008.05.039

Although many proxy multi-signature schemes have been proposed or improved in the last few years, there was no provably secure proxy multi-signature scheme. All previous known proxy multi-signature schemes [5,7–11,18,19] did not give a formal definition and security model, and their securities were only heuristically analyzed.

Our contribution. In this paper, based on the work of Boldyreva et al. [4], Wang and Cao [15], Wang et al. [16], and Xu et al. [17], we give a formal definition and security model for identity-based proxy multi-signature scheme, then we propose an identity-based proxy multi-signature scheme from bilinear pairings which is provably secure in the random oracle model. The security of our proxy multi-signature scheme is based on the hardness of computational Diffie–Hellman problem. Moreover, our scheme is more efficient than that given in [10].

Organization. The rest of this paper is organized as follows: In Section 2, we introduce the complexity assumption. In Section 3, we give a definition of identity-based proxy multi-signature scheme and then define a security model for it. In Section 4, we propose a new identity-based proxy multi-signature scheme, and we prove its security using the model in Section 5. In Section 6, we compare the efficiency of our scheme with that in [10]. Finally, Section 7 concludes the paper.

2. Preliminaries

In this section, we review some concepts about bilinear pairings and computational Diffie–Hellman assumption.

2.1. Bilinear pairings

Let G_1 be a cyclic additive group generated by P, whose order is a prime q (q is a large prime), and G_2 be a cyclic multiplicative group of the same order. A bilinear pairing is a map $e : G_1 \times G_1 \to G_2$ with the following properties:

(1) Bilinear: For any $P, Q, R \in G_1$, we have $e(P+Q,R) = e(P,R)e(Q,R)$ and $e(P,Q+R) = e(P,Q)e(P,R)$. In particular, for any $a, b \in \mathbb{Z}_q$,

$$e(aP,bP) = e(P,P)^{ab} = e(P,abP) = e(abP,P).$$

(2) Non-degenerate: There exists $P, Q \in G_1$, such that $e(P,Q) \neq 1$.
(3) Computable: There is an efficient algorithm to compute $e(P,Q)$ for any $P, Q \in G_1$.

The typical way of obtaining such pairings is by deriving them from the modified Weil-pairing or the Tate-pairing on an elliptic curve over a finite field [2].

2.2. Complexity assumption

Now, we briefly review the definitions of the computational Diffie–Hellman (CDH) problem and the CDH assumption.

Definition 1. Given a group G_1 of prime order q with generator P and elements $aP, bP \in G_1$ where a, b are selected at random from $\mathbb{Z}_q^*$, the CDH problem in G_1 is to compute abP.

Definition 2. We say that the $(t,\varepsilon)-$CDH assumption holds in a group G_1 if no algorithm running in time at most t can solve the CDH problem in G_1 with probability at least ε.

3. Identity-based proxy multi-signature schemes

Based on the work of Boldyreva et al. [4], Wang and Cao [15], and Wang et al. [16], we give a formal definition and security model for identity-based proxy multi-signature schemes.

3.1. Definition of identity-based proxy multi-signature schemes

In an identity-based proxy multi-signature scheme, there is a proxy signer and a group of original signers. Let $\mathcal{O}_1, \ldots, \mathcal{O}_n$ be the original signers and $\mathcal{P}$ be the proxy signer designated by $\mathcal{O}_1, \ldots, \mathcal{O}_n$. For $i \in \{1, \ldots, n\}$, $\mathcal{O}_i$ has an identity ID_i, $\mathcal{P}$ has an identity ID_p.

Definition 3. An identity-based proxy multi-signature scheme is a tuple $\mathsf{IBPMS} = (\mathsf{Setup}, \mathsf{Extract}, \mathsf{Sign}, \mathsf{Veri}, \mathsf{PMGen}, \mathsf{PMSign}, \mathsf{PMVeri})$.

- Setup: This algorithm is run by the master entity *PKG* on input a security parameter 1^k ($k \in N$), and generates the public parameters `params` of the scheme and a master secret key s. The master entity publishes `params` and keeps the master secret to itself.