Security Model of Proxy-Multi Signature Schemes

Feng Cao and Zhenfu Cao

Department of Computer Science and Engineering, Shanghai Jiao Tong University
800 Dongchuan Road, Shanghai, 200240, P.R. China
cf_1977@163.com, cao-zf@cs.sjtu.edu.cn

Abstract. In a proxy multi-signature scheme, a designated proxy signer can generate the signature on behalf of a group of original signers. Although some work has been done in proxy-multi signature schemes, until now there is no formalized definition and security model for them. In this paper, we will give the formal definition and a security model of proxy-multi signature scheme. We also constructed a proxy-multi signature scheme based on the BLS short signature scheme and proved its security in our security model.

1 Introduction

The concept of a proxy signature was first introduced by Mambo et al. [4] in 1996. In the proxy signature scheme, generally, there are two entities: an original signer and a proxy signer. The original signer can delegate his signing power to a proxy signer. The proxy signer can generate a valid signature on behalf of the original signer. Since then, many proxy signature schemes have been proposed [8,9,10]. Proxy signatures can combine other special signatures to obtain some new types of proxy signatures. Till now, there are various kind of proxy signature schemes have been proposed.

One well-known new type of the proxy signatures is the proxy multi-signature which was first proposed in 2000 by Yi et al. [5]. 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, and program office, etc. The document must by signed jointly by these entities, or signed by a proxy signer who is trusted by all of these entities. One solution to the later case of this problem is to use a proxy multi-signature scheme [5,6].

In 2003, Boldyreva et al. formalized a notion of security for proxy signature schemes [1], and that was the first work on proxy signature in the provable-security direction. In [2], Wang and Cao identified a security weakness in the model of [1]. But till now, no security notion has been proposed for proxy-multi signature schemes. In this paper, based on the work of [1,2,3], we give a formal definition and security model on the proxy-multi signature schemes.

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 144–152, 2006.

The rest of this paper is organized as follows: In section 2, we introduced some related mathematical problems. In section 3, we given a definition of the proxy-multi signature schemes and then defined a security model of the proxy-multi signature schemes. In section 4, we proposed a new proxy-multi signature scheme and proved its security in our security model. And conclusions are presented in the final section.

2 Preliminaries

In this section, we review some concepts about bilinear maps, and some related mathematic problems.

Let G_1 and G_2 be two groups of order q for some large prime q. A bilinear map is a map $e : G_1 \times G_1 \to G_2$ with the following properties:

1. Bilinear: For all $u, v \in G_1$, and all $a, b \in \mathbb{Z}$, $e(u^a, v^b) = e(u, v)^{ab}$.
2. Non-degenerate: There exist $u, v \in G_1$, such that $e(u, v) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(u, v)$ for any $u, v \in G_1$.

Let G be a multiplicative group of the prime order q, We consider the following problems in G.

Discrete Logarithm (DL) Problem: Given $y \in G$, find an integer $x \in Z_q^*$ such that $y = g^x$ whenever such integer x exists.

Computational Diffie-Hellman Problem: Given $g, u, v \in G$, to compute $h = g^{\log_g u \cdot \log_g v}$.

Decision Diffie-Hellman Problem: For $a, b, c \in Z_q^*$, given $g, g^a, g^b, g^c, \in G$, decide whether $c \equiv ab \ mod \ q$.

A group G is a GDH group if there exists an efficient algorithm to solve the DDH problem in G and there is no polynomial-time algorithm to solve the CDH problem.

3 Proxy-Multi Signature Schemes

3.1 Definition of Proxy-Multi Signature Schemes

In a proxy-multi signature scheme, there is a proxy signer and a group of original signers. Let $O_1, \cdots, O_n$ be the original signers and P be the proxy signer designated by $O_1, \cdots, O_n$. For $i \in \{1, \cdots, n\}$, O_i has a public key pk_{o_i} and a secret key sk_{o_i}, P has a public key pk_p and a secret key sk_p.

Definition 1. [Proxy-multi signature scheme] A proxy-multi signature scheme is a tuple $PMS = (KeyGen, Sign, Veri, PMGen, PMsign, PMVeri)$.

KeyGen: On input of a security parameter 1^k, the algorithm produces private/public key pairs as usual. The public and private key pairs for the proxy signer and the original signers are $(pk_p, sk_p), (pk_{o_1}, sk_{o_1}), \cdots, (pk_{o_n}, sk_{o_n})$.

Sign: This is a (possibly) randomized standard signing algorithm. On input of a secret key sk and a message $m \in \{0, 1\}^*$, the algorithm outputs a signature σ.