Computer Communications 34 (2011) 257–263

Contents lists available at ScienceDirect

Computer Communications

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

Improvement of a proxy multi-signature scheme without random oracles ☆

Ying Sun [a,*], Chunxiang Xu [a], Yong Yu [a], Bo Yang [b]

[a] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
[b] College of Information, South China Agricultural University, Guangzhou 510642, China

ARTICLE INFO

Article history:
Available online 10 February 2010

Keywords:
Digital signature
Proxy signature
Bilinear pairing
Security proof

ABSTRACT

A proxy multi-signature scheme permits two or more original singers to delegate their signing powers to the same proxy signer. Recently, Liu et al. proposed the first proxy multi-signature that be proven secure in the standard model [Liu et al. (2008) [20]], which can be viewed as a two-level hierarchical signature due to Waters. However, because of the direct employment of Waters' signature, their scheme needs a relatively large number of public parameters and is not tightly reduced to the security assumption. In this paper, inspired by Boneh, Boyen's technique and Waters' technique, we propose a new proxy multi-signature scheme without random oracles, whose unforgeability can be tightly reduced to the CDH assumption in bilinear groups. The new scheme can be regarded as an improvement to overcome the weaknesses of Liu et al.'s scheme. Compared with Liu et al.'s scheme, the improvement has three merits, tighter security reduction, shorter system parameters and higher efficiency.

1. Introduction

In the last two decades, the science of cryptography has focused on the construction of provably secure digital signature schemes. A security proof of a digital signature scheme generally proceeds by a reduction showing how an adversary who can break the digital signature scheme in polynomial time can be used to solve some hard mathematical problems, such as discrete logarithm problem, RSA problem, and Computational Diffie–Hellman (CDH) problem. The "quality" of the reduction is given by the success probability of the adversary to break the underlying intractable problem. A reduction in which the difficulty of forging and the difficulty of solving the underlying hard problem are close is called *tight*; otherwise, it is called *loose*. Naturally, "close", "tight" and "loose" are imprecise terms and make more sense when used in comparison. Today, how to construct a digital signature scheme that can be tightly reduced to a weak security assumption is a hot topic in cryptography [1–4].

In 1996, Mambo et al. [5] introduced the concept of a proxy signature for signature delegation, which allows an original signer to delegate his signing capability to a proxy signer and then the proxy signer can create valid signatures on behalf of the original signer. Proxy signatures have been shown to be useful in a number of applications, including distributed shared object systems, grid computing and mobile agent environment. Moreover, proxy signatures have many variations, such as proxy blind signature [6,7], threshold proxy signature [9,8], multi-proxy signature [10–12], proxy ring signature [7,13], designated verifier proxy signature [14] and so on. Among of them, the concept of proxy multi-signature was first introduced by Yi et al. [15]. In this kind of primitive, a proxy signer can generate a signature for a message on behalf of two or more original signers. It can be used to solve the problem of signing a document for a corporation. For instance, a company releases a document that may involve the financial department, engineering department and program office, etc. The document must be signed jointly by these entities, or signed by a proxy signer authorized by these entities [15]. Followed by Yi et al.'s work, several proxy multi-signature schemes have been proposed [16–21].

To offer strong security guarantee, provable security is very essential for proxy multi-signature schemes. However, the early schemes did not provide formal security proofs, and therefore, most of them do not fully meet the desired security requirement and many schemes were found security flaws [16–19,21]. In 2006, Wang and Cao proposed a new proxy multi-signature scheme [21] and provided security proof in the random oracle model proposed by Bellare and Rogaway [22]. This model replaces hash functions by truly random functions. Although the model is efficient and useful, it has received many criticisms that the proofs in the random oracle model are not perfect. Canetti et al. [23] showed that security in the random oracle model does not imply the security in the real world. Fortunately, by employing Waters' signature scheme [24], Liu et al. [20] proposed such a new scheme that can be proven secure without using the random oracle model in 2008. However, there are two drawbacks of this scheme. Firstly, it needs a relatively large number

☆ This work was supported by the National 863 High-Tech Program of China (No. 2009AA01Z415), National Natural Science Foundation of China under Grants 60773175, 60803133, 60873233, the National Research Foundation for the Doctoral Program of Higher Education of China under Grant No. 200806140010 and the open fund of Youth Science and Technology Foundation of UESTC.

* Corresponding author.
E-mail address: yingsun@uestc.edu.cn (Y. Sun).

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2010.02.002

of public parameters and secondly, its security reduction is loose. Therefore, to find a new proxy multi-signature scheme secure in the standard model with a tighter security reduction and shorter public parameters is an interesting research problem.

1.1. Our contribution

In this paper, we would like to propose a new construction of proxy multi-signature scheme, whose security relies on the hardness of the CDH problem in the standard model. In fact, the new scheme can be viewed as an improved version of Liu et al.'s scheme [20]. We divide the potential adversaries into three kinds according to their attack power, and in Huang et al.'s security model [27,28], prove that the improved scheme is unforgeable against all kinds of adversaries in the standard model. Compared with Liu et al.'s scheme [20], the new scheme has three advantages. Firstly, it achieves a tighter security reduction than Liu et al.'s scheme. Secondly, the size of public parameters is only about one half of that of Liu et al.'s scheme, and finally, the new scheme is more efficient in computation.

1.2. Roadmap

The remainder of this paper is organized as follows. Some preliminary works are given in Section 2. The formal models of proxy multi-signature scheme is described in Section 3. Our proxy multi-signature scheme and the comparison between our scheme and Liu et al.'s scheme is presented in Section 4. We give a formal security proofs in the standard model in Section 5. Finally, conclusions are given in Section 6.

2. Preliminaries

In this section, we will review some fundamental backgrounds used in this paper, including bilinear pairings, complexity assumptions and Waters signature.

2.1. Bilinear pairings

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic multiplicative groups of prime order p and g be a generator of $\mathbb{G}$. The map $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ is said to be an admissible bilinear pairing if the following conditions hold true [29].

(1) e is bilinear, i.e. $e(g^a,g^b)=e(g,g)^{ab}$ for all $a,b\in\mathscr{Z}_p$.
(2) e is non-degenerate, i.e. $e(g,g)\neq 1_{\mathbb{G}_T}$.
(3) e is efficiently computable.

2.2. Complexity assumption

Definition 1 (*Computational Diffie–Hellman (CDH) Problem in* $\mathbb{G}$). Given $g,g^a,g^b\in\mathbb{G}$ for some unknown $a,b\in\mathscr{Z}_p$, compute $g^{ab}\in\mathbb{G}$.

The success probability of a polynomial algorithm $\mathscr{A}$ in solving the CDH problem in $\mathbb{G}$ is denoted as

$$\mathrm{Succ}_{\mathscr{A}}^{CDH}=Pr\left[\mathscr{A}(g,g^a,g^b)=g^{ab}:a,b\in_R\mathscr{Z}_p\right]$$

Definition 2 (*Computational Diffie–Hellman (CDH) Assumption in* $\mathbb{G}$). Given $g,g^a,g^b\in\mathbb{G}$ for some unknown $a,b\in\mathscr{Z}_p$, $\mathrm{Succ}_{\mathscr{A}}^{CDH}$ is negligible.

2.3. Waters signature

In Eurocrypt 2005, Waters [24] presented an efficient identity based encryption scheme secure in the standard model and he also showed how to derive a signature scheme from his encryption scheme. Let us review Waters signature scheme firstly.

Let $\mathbb{G}$ be a group of prime order p. $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ is a bilinear pairing and g is the corresponding generator.

Setup. A secret $\alpha\in Z_p$ is chosen at random. Compute $g_1=g^\alpha$ and choose g_2 randomly in $\mathbb{G}$. Additionally, choose a random value $u'\in\mathbb{G}$ and a random vector $U=(u_1,u_2,\cdots,u_n)$, whose elements are chosen at random from G. The public key is (g,g_1,g_2,u',U) and the secret key is g_2^α.
Signing. Let M be an n-bit message to be signed and M_i denote the ith bit of M, and $\mathscr{M}\subseteq\{1,\cdots,n\}$ be the set of all i for which $M_i=1$. A signature is generated as follows. First, a random $r\in Z_p$ is chosen and then a signature is constructed as

$$\sigma_M=\left(g_2^\alpha\left(u'\prod_{i\in\mathscr{M}}u_i\right)^r,g^r\right).$$

Verification. $\sigma=(\sigma_1,\sigma_2)$ is a valid signature on a message M if

$$e(g,\sigma_1)=e(g_1,g_2)e\left(\sigma_2,u'\prod_{i\in\mathscr{M}}u_i\right).$$

Waters [24] showed that his signature scheme is existentially unforgeable, however, the reduction is not tight with long public key size. Moreover, just as Tan [25] claimed, Waters signature is malleable. It means that an adversary is able to produce a different valid signature on the same message without knowing the private key. In Waters signature, given a signature $\sigma=(\sigma_1,\sigma_2)$ on a message M, anyone can construct another signature on the same message as follows. First. choose a random $r'\in Z_p^*$ and compute $\overline{\sigma_1}=\sigma_1\left(u'\prod_{i\in\mathscr{M}}u_i\right)^{r'}$, $\overline{\sigma_2}=\sigma_2 g^{r'}$. It can be checked that $(\overline{\sigma_1},\overline{\sigma_2})$ is a valid signature on M. The malleability of Waters signature implies that it is not strongly unforgeable [26]. Liu et al.'s proxy multi-signature [20] is a 2-level hierarchical Waters signature, therefore, it is also malleable and is not strongly unforgeable.

3. Definitions and attack model

In this section, we will give the outline of a proxy multi-signature scheme and its security model.

3.1. Outline of proxy multi-signature schemes

There exists three parties in a proxy multi-signature scheme, a set of original signers $\mathscr{L}=\{U_1,U_2,\cdots,U_l\}$, a proxy signer U_p designated by all original signers and a verifier. A proxy multi-signature scheme consists of the following algorithms.

- Setup: Given a security parameter k, this algorithm outputs the system parameters.
- KeyGen: It takes as input the security parameter k and outputs the secret–public key pair (sk_i,pk_i) for each party.
- DelegationGen: Given the system's parameters, the original signer's private key and a warrant W to be signed, this algorithm outputs the delegation σ_W. In a warrant-based proxy multi-signature, the delegation is the original signers' standard signature on the warrant which contains the original signers' identities, the proxy signer's identity, a period of validity, the restrictions on the class of messages for which the warrant is valid and so on.
- DelegationVerify: This is a deterministic verification algorithm to verify the delegation signing by all the original signers on the warrant W. It takes as input the delegation of the original signer