The Journal of Systems and Software 85 (2012) 209–214

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

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

ID-based proxy signature scheme with message recovery

Harendra Singh, Girraj Kumar Verma*

Department of Mathematics, Hindustan College of Science and Technology, Farah, Mathura, India

ARTICLE INFO

Article history:
Received 8 February 2011
Received in revised form 28 July 2011
Accepted 16 August 2011
Available online 26 August 2011

Keywords:
ID-based signature
Proxy signature
Mobile agent
Bilinear pairing
Signature with message recovery

ABSTRACT

A proxy signature scheme, introduced by Mambo, Usuda and Okamoto, allows an entity to delegate its signing rights to another entity. Identity based public key cryptosystems are a good alternative for a certificate based public key setting, especially when efficient key management and moderate security are required. From inception several ID-based proxy signature schemes have been discussed, but no more attention has been given to proxy signature with message recovery. In this paper, we are proposing provably secure ID-based proxy signature scheme with message recovery and we have proved that our scheme is secure as existential forgery-adaptively chosen message and ID attack. As proposed scheme is efficient in terms of communication overhead and security, it can be a good alternative for certificate based proxy signatures, used in various applications such as wireless e-commerce, mobile agents, mobile communication and distributed shared object systems, etc.

1. Introduction

A digital signature scheme with message recovery is a signature scheme in which the original message of the signature is not required to be transmitted together with the signature since it has been appended to the signature and can be recovered according to the verification/message recovery process. It is different to an authenticated encryption scheme or signcryption scheme, since in this scheme, the embeded message can be recovered by anyone without the secret information. The purpose of this kind of signatures is to minimize the total length of the original message and the appended signature. So, these are useful in any organization where bandwidth is one of the main concern or useful for the application in which small message should be signed.

1.1. Related work

In 1984, Shamir (1985) introduced the idea of identity based public key cryptography to simplify key management procedure of traditional certificate based public key infrastructure. In ID-based public key cryptography, an entity's public key is directly derived from certain aspects of its identity, such as e-mail address, phone number, an IP address belonging to a network, or its social security number. Private keys are generated by a third trusted party called Private Key Generator (PKG). The direct derivation of public keys in these infrastructures eliminates the need for the certificate and some of the problem associated with them.

Mambo et al. (1996) proposed the concept of proxy signature in 1996, which allows a designated person, called proxy signer, to sign on behalf of an original signer. The proxy signature plays an important role in many applications (Boldyreva et al., 2003; Hong and Chen, 2007; Hwang and Chen, 2000; Shao, 2003; Zhang and Kim, 2003) and have been received great attention since inception. In 2003, Zhang and Kim (2003) proposed an ID-based proxy signature scheme using bilinear pairing. The scheme is similar to Kim et al.'s (1993) scheme which is based on certificate based public key infrastructure. Later in 2004, Zhou et al. (2008) proposed a new provable secure ID-based proxy signature scheme using pairing and during the same, Malkin et al. (2004) proposed a generic construction of proxy signature using self delegation. In 2005, Gu and Zhu (2005) proposed a new security model for a provable secure ID-based proxy signature scheme and during the same Zhang et al. (2005) proposed an ID-based digital signature scheme with message recovery for shortening the signature length and Li et al. (2005) proposed a new proxy signature scheme with message recovery. In 2006, Gu and Zhu (2008) proposed an efficient version of Zhang and Kim (2003) scheme using the security model described in Gu and Zhu (2005). During the same, Galindo et al. (2006) proposed a generic construction of some identity based signatures with special properties and mentioned how to construct identity based proxy signatures and during the same Tso et al. (2007) proposed an efficient version of scheme by Zhang et al. (2005) using pairing. In 2007, Wu et al. (2007) proposed a new proxy signature scheme which improves the security aspects of an ID-based proxy signature scheme. Recenrtly, in 2008, Schuldt et al. (2008) has given a

* Corresponding author.
E-mail address: girrajv@gmail.com (G.K. Verma).

0164-1212/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2011.08.018

stronger model and gave a new generic construction from (sequential) aggreegate signatures. During the same, Wang (2008) has given a new identity based proxy signature in random oracle model and secure against proxy key exposure. Recently, Wu et al. (2009) has given a proxy signature scheme with message recovery using self certified public keys. Many ID-based proxy signature schemes were given since 2003, but no more attention has been given to an ID-based proxy signature scheme with message recovery. In this paper, we are introducing an ID-based proxy signature scheme with message recovery and we have proved the security of proposal. Our scheme is based on work done by Zhang et al. (2005) and Tso et al. (2007).

The mobile agent (Hong and Chen, 2007) is an autonomous software entity which can migrate across different execution environments through network. The characteristics of the mobile agent, mobility and autonomy, make it ideal for electronic commerce applications. One of the tasks of a mobile agent is to sign a digital signature on behalf of its owner. For example, we consider a scenario that a mobile agent is ordered to search the price of a flight ticket and book it on behalf of a customer. To make it possible, the mobile agent must act as a proxy signer of the customer. Hence proxy signatures can be used for such booking. Our proposed scheme provides an efficient proxy signature and hence it can be used for mobile agent.

Our real contribution is to design a provably secure signature scheme and to provide the security proof also.

The rest of the paper is organized as follows:

In Section 2 we call some preliminary work. In Section 3 we present an ID-based proxy signature scheme with message recovery. In Section 4 we analyzed our schemes according to the efficiency and security point of view and shown a Table 1 for efficiency comparison with related existing schemes. In Section 5 we have considered an example showing the need of proxy signature scheme. In Section 6 we have concluded our discussion.

2. Preliminaries

2.1. Bilinear pairing

Let G_1 be a cyclic additive group and G_2 be a cyclic multiplicative group of same prime order q. We assume that the discrete logarithm problem in both $G_1$and G_2 is hard. A bilinear pairing e is a map $e: G_1 \times G_1 \to G_2$, which satisfies the following properties:

1. **Bilinear:** For any P, $Q \in G_1$ and $a, b \in Z_q^*$, we have $e(aP, bP) = e(P, P)^{ab}$.
2. **Non-degeneracy:** There exist $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
3. **Computability:** There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$. Basically G_1 is a set of points of elliptic curve and e be the Weil or Tate pairing.

We now describe two mathematically hard problems, namely the Decisional Diffie-Hellmen Problem (DDHP) and Computational Diffie-Hellmen Problem (CDHP) and the GDH Group.

1. Definition (DDHP). For $a, b, c \in Z_q^*$, given $P, aP, bP, cP \in G_1$ and to decide whether $c = ab \ mod \ q$. The DDHP is easy in G_1, since it is easy to compute $e(aP, bP) = e(P, P)^{ab}$ and to decide whetheher $e(P, P)^{ab} = e(P, P)^c$.
2. Definition (CDHP). For $a, b \in Z_q^*$, given $P, aP, bP \in G_1$ to compute $abP \in G_1$. A (τ, ϵ)-CDH adversary in G_1 is a probabilisic machine $\mathcal{A}$ running in time τ such that $Adv_{G_1}^{CDH}(\mathcal{A}) = Pr[A(P, aP, bP) = abP] \geq \epsilon$ where the probability is taken over the random values a and b. The CDH problem is (τ, ϵ)-interactable if there is no (τ, ϵ)adversary in G_1.
3. Definition (GDH Group). In group G_1, the DDHP can be solved in polynomal time and no polynomial time algorithm can solve CDHP with non negligible advantage, we reffered G_1 as a Gap Diffie-Hellmen group.

2.2. Framework of an ID-based proxy signature scheme with message recovery

In this section, we provide a formal framework of an ID-based proxy signature scheme with message recovery (IDPSWM), our model is inspired by Gu and Zhu (2005). There are mainly three entities original signer, proxy signer and verifier in this protocol.

Definition. (IDPSWM) An IDPSWM consists of the following eight polynomial time algorithms: *Setup, Extract, DelGen, DelVerify, PKgen, PSign, SignVerify/Message Recovery, ID.*

1. *Setup:* This algorithm takes as input a security parameter λ and outputs the key generation center KGC's master key, global public key and system parameters *params*.
2. *Extract:* An algorithm, which takes as input an identity $ID_A \in \{0, 1\}^*$, of a user A and master key of KGC and then outputs the public key and private key pair (q_A, d_A).
3. *DelGen:* In this algorithm the original signer A computes the delegation $W_{A \to B}$ from his secret key d_A and warrant m_w and sends to the proxy signer in a secure way.
4. *DelVerify:* The delegation verification algorithm, takes as input ID_A, $W_{A \to B}$ and verifies whether $W_{A \to B}$ is a valid deligation come from A.
5. *PKGen:* The proxy key generation algorithm, takes as input $W_{A \to B}$ and some secret information (for example the secret key of executer) and outputs a signing key d_p for proxy signer.
6. *PSign:* In this probabilistic algorithm, the proxy signer computes the proxy signature δ on a message $m \in \{0, 1\}^l$ using the proxy signing key.
7. *SignVerify/Message Recovery:* In this deterministic algorithm the verifier recieves the signature and takes the identity of original signer and the identity of the proxy signer as input and then recover the message and dispalys accept or reject.
8. *ID:* The proxy identification algorithm, it takes as input a valid proxy signature and outputs the identity of proxy signer.
9. *Correctness:* This algorithm shows the proof of correctness of SignVerify/Message Recovery.

2.3. Security model

We consider the security model described in Gu and Zhu (2005), in which an adversary $\mathcal{A}$ which is assumed to be a probabilistic Turing machine, takes as input the global scheme parameters and a random tape and perform an experiment, as described below.

Definition. For an ID-based proxy signature scheme with message recovery (IDPSWM), we define an experiment $Exp_{\mathcal{A}}^{IDPSWM}(\lambda)$ of adversary $\mathcal{A}$ and security parameter λ as follows:

1. A challenger C runs setup and gives the system parameters *param* to $\mathcal{A}$.
2. Set $C_{list} \leftarrow \phi$, $D_{list} \leftarrow \phi$, $G_{list} \leftarrow \phi$, $S_{list} \leftarrow \phi$.
3. Adversary $\mathcal{A}$ can make the following requests or queries adaptively:
   - Extract(.): This oracle takes as input a user's ID_i, and returns the corresponding private key d_i. If $\mathcal{A}$ gets $d_i \leftarrow Extract(ID_i)$, let $C_{list} \leftarrow C_{list} \cup \{(ID_i, d_i)\}$.
   - Delegate(.): This oracle takes as input the designater's identity ID and a warrant m_w and output a delegation W. If $\mathcal{A}$ gets $W \leftarrow Delegate(ID, m_w)$, let $D_{list} \leftarrow D_{list} \cup \{(ID, m_w, W)\}$.