Efficient ID-Based One-Time Proxy Signature and Its Application in E-Cheque

Rongxing Lu, Zhenfu Cao, and Xiaolei Dong

Department of Computer Science and Engineer, Shanghai Jiao Tong University
800 Dongchuan Road, Shanghai 200240, P.R. China
rxlu.cn@gmail.com, {cao-zf, dong-xl}@cs.sjtu.edu.cn
http://tdt.sjtu.edu.cn

Abstract. To put restrictions on signing capability of the proxy signer, the notion of one-time proxy signature was put forth by Kim et al. in 2001. Today, to our best knowledge, although plenty of one-time proxy signature schemes have been proposed, no ID-based one-time proxy signature (IBOTPS) has yet been presented. Therefore, in this paper, to fill this void, we first formalize the security notions for IBOTPS, and propose the first efficient IBOTPS scheme based on the bilinear pairings and provide the formal security proofs in the random oracle model. Also, we consider an application of the proposed scheme in E-cheque scenarios.

1 Introduction

Background and Related Work. With the explosion of electronic business over the Internet in recent years, the proxy signature has been of increasing practical importance, mainly due to its special proxy function. In a proxy signature scheme, an original signer is allowed to delegate his signing capability to a proxy signer, then the proxy signer can sign messages on behalf of the former within a given context. After receiving a proxy signature, any verifier not only can validate its correctness by a given verification procedure, but also be convinced of the original signer's agreement on the signed message. Based on the delegation type [14,15], the proxy signatures can be classified into full delegation, partial delegation, and delegation by warrant schemes. In a full delegation scheme, the original signer's private key is given the proxy signer directly so the latter has the same signing capability as the former. For most of real world settings, such schemes are obviously impractical and insecure. In a partial delegation scheme, the proxy signer holds a proxy secret key which is different from the original signer's private key. So, the proxy signatures are also distinguishable from the original signer's normal signatures. However, in such schemes the range of messages that a proxy signer can sign is not limited. In a delegation by warrant scheme, the above weakness is eliminated by adding a proxy warrant that specifies the identities of the original signer and the proxy signer, the types of message to be delegated, and the delegation period, etc.

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 153–167, 2006.
© Springer-Verlag Berlin Heidelberg 2006

Following Mambo et al.'s first work in 1996 [14,15], many new constructions and extensions of proxy signature have been proposed, such as threshold proxy signatures [18,20], multi-proxy signature [10], proxy multi-signature [24], proxy blind signatures [21] and so on. In 2001, to put restrictions on signing capability of the proxy signer, Kim et al. [11] introduced the concept of one-time proxy signature. In this paradigm, each proxy key pair can be used to sign only one message. If the proxy signer uses the same proxy key to sign more than once, then his private key will be disclosed. In recent years, several one-time proxy signature schemes have been put forth [8,1,22,13]. Choi et al. [8] proposed a one-time proxy signature to resolve key exposure problem. Al-Ibrahim and Cerny [1] proposed a threshold proxy one-time signature scheme for group-based applications. In Asiacrypt 2003, Wang and Pieprzyk [22] also proposed an efficient one-time proxy signature scheme. More recently, Mehta and Harn [13] have proposed another two efficient one-time proxy signature schemes.

As is known to us, ID-based system introduced by Shamir [17] can simplify key management procedures in certificate-based public key infrastructure, and after the bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, have been found various positive applications in cryptography, many ID-based cryptographic schemes have been proposed [2,7,4,25,23]. However, we observe that no researchers have yet to propose an ID-based one-time proxy signature (IBOTPS) using pairing techniques. Therefore, in this paper, to fill this void, we would like to present the first efficient IBOTPS scheme based on the bilinear pairing.

Our Contributions. We regard the main contributions of this paper to be of two-fold significance:

- We formalize the definition and security notions for IBOTPS at first. Then, we present the *first* efficient IBOTPS scheme based on the bilinear pairings and provide the proofs of security of the scheme in the random oracle model.
- We also discuss the application scenarios of electronic cheque (E-cheque), and show that our proposed IBOTPS scheme will be suitable for such scenarios.

Organization. In the next section, we set up the definition and security notion for IBOTPS. In section 3, we review the bilinear pairings and underlying problems on which we build. Then, we propose our new IBOTPS scheme and provide the proofs of the security in section 4. In section 5, we present an application of the proposed IBOTPS scheme in E-cheque scenarios. Finally, we draw our conclusions in section 6.

2 Definition and Security Model for IBOTPS

2.1 Notations

Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ denote the set of natural numbers. If $k \in \mathbb{N}$, then 1^k is the string of k 1s. If x, y are two strings, then $|x|$ is the length of x and $x \| y$ is