Efficient Identity-Based Signatures and Blind Signatures*

Zhenjie Huang[1,2,3], Kefei Chen[1], and Yumin Wang[3]

[1] Department of Computer Science and Engineering,
Shanghai Jiaotong University, Shanghai 200030, P.R. China
zhj_huang@hotmail.com, chen-kf@cs.sjtu.edu.cn
[2] Department of Mathematics and Information Science,
Zhangzhou Normal University, Fujian, 363000, P.R. China
[3] State Key Laboratory of Integrated Service Networks,
Xidian University, Xi'an, Shaanxi, 710071, P.R. China
ymwang@xidian.edu.cn

Abstract. In this paper, we first propose an efficient provably secure identity-based signature (IBS) scheme based on bilinear pairings, then propose an efficient identity-based blind signature (IBBS) scheme based on our IBS scheme. Assuming the intractability of the Computational Diffie-Hellman Problem, our IBS scheme is unforgeable under adaptive chosen-message and ID attack. Efficiency analyses show that our schemes can offer advantages in runtime over the schemes available. Furthermore, we show that, contrary to the authors claimed, Zhang and Kim's scheme in ACISP 2003 is one-more forgeable, if the ROS-problem is solvable.

Keywords: Identity-based, Signature, Blind signature, Bilinear pairings, Gap Diffie-Hellman group.

1 Introduction

The key generation procedure in the usual sense of public-key cryptography renders all public keys random. Consequently, it is necessary to associate a public key with the identity information of its owner. Such an association can be realized by a public-key authentication framework: a tree-like hierarchical public-key certification infrastructure (e.g., X.509 certification framework). In a certificate-based public key system, before using the public key of a user, the participants must verify the certificate of the user at first. As a consequence, this system requires a large storage and computing time to store and verify each user's public key and the corresponding certificate. In 1984 Shamir [16] introduced the concept of identity-based (simply ID-based) public key cryptosystem to simplify key management procedures in certificate-based public key setting. Since then, many ID-based encryption and signature schemes have been proposed.

* This work is supported by the National Natural Science Foundation of China under Grant No.60273049.

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 120–133, 2005.

ID-based cryptosystems have a property that a user's public key can be easily calculated from his identity by a publicly available function, while his private key can be calculated for him by a trusted authority, called Key Generation Center (KGC). They enable any pair of users to communicate securely without exchanging public key certificates, without keeping a public key directory, and without using online service of a third party, as long as a trusted key generation center issues a private key to each user when he first joins the network, so they can be a good alternative for certificate-based public key infrastructure, especially when efficient key management and moderate security are required.

Early, the bilinear pairings, namely Weil pairing and Tate pairing of algebraic curves, were used in cryptography for the Menezes-Okamoto-Vanstone (MOV) attack [11] (using Weil pairing) and Frey-Rück (FR) attack [7] (using Tate pairing) to reduce the discrete logarithm problem on some elliptic curves or hyperelliptic curves to the discrete logarithm problem in a finite field. Recently, the bilinear pairings have been found positive applications in cryptography to construct new ID-based cryptographic primitives. In 2000, Joux [10] used the Weil pairing to construct a tripartite one round Diffie-Hellman key agreement protocol. After Joux's breakthrough, many ID-based cryptographic schemes have been proposed using the bilinear pairings [5]. In Crypto 2001, Boneh and Franklin [2] presented an ID-based encryption scheme based on bilinear pairings which to be the first fully functioning, efficient and provably secure ID-based encryption scheme. In Asiacrypt 2001, Boneh, Lynn and Shacham [3] proposed a basic signature scheme using pairings which has the shortest length among signature schemes in classical cryptography.

There are five ID-based signature (IBS) schemes based on bilinear pairings have been proposed. Sakai, Ohgishi and Kashara proposed a first IBS Scheme using Weil pairing in 2000.Then, in 2002, Paterson proposed a new IBS scheme using bilinear pairing. But, these two schemes without any formal proof of security. In 2003, there are three provably secure IBS scheme have been proposed. Yi proposed a provably secure IBS scheme using Weil pairing in [18], Cha and Cheon [4] proposed a provably secure IBS scheme from Gap Diffie-Hellman group in PKC2003, and Hess proposed a efficient scheme [9] in SAC 2002.

Blind signature, first introduced by Chaum [6] at Crypto'82, is a variant of digital signatures, which allows the user to get a signature without giving the signer any information about the actual message or the resulting signature. Formally, blindness means that the signer's view and the resulting signature are statistically independent, where the signer's view is the set of all values that can be gotten by the signer during the execution of the signature issuing protocol. This blindness property plays a central role in applications such as electronic voting and electronic cash systems. Up to now, two ID-based blind signature (IBBS) schemes based on bilinear pairings have been proposed. The first scheme was proposed by Zhang and Kim [19] in Asiacrypt 2002. Later, in ACISP 2003, Zhang and Kim [20] proposed a new ID-based blind signature scheme based on bilinear pairings. They claim that the security against generic parallel attack to their new scheme doesn't depend on the difficulty of ROS-problem.