ID-Based Aggregate Signatures from Bilinear Pairings

Jing Xu[1,2], Zhenfeng Zhang[1,3], and Dengguo Feng[1,3]

[1] State Key Laboratory of Information Security, P.R. China
[2] Graduate School of Chinese Academy of Sciences, Beijing 100039, P.R. China
[3] Institute of Software, Chinese Academy of Sciences, Beijing 100080, P.R. China
{xujing, zfzhang, feng}@is.iscas.ac.cn

Abstract. Aggregate signature scheme was recently proposed by Boneh, Gentry, Lynn and Shacham, which presented a method for combining n signatures from n different signers on n different messages into one signature. In this paper, we propose an identity-based aggregate signature scheme based on the bilinear pairings. This enhances the efficiency of communication and signature verification process. We show that the security of our scheme is tightly related to the computational Diffie-Hellman assumption in the random oracle model.

Keywords: ID-based signatures, aggregate signatures, bilinear pairings.

1 Introduction

Authentication constitutes one of the core problems in cryptography. Much modern research focuses on constructing authentication schemes that are: (1) as secure as possible, i.e., provably secure under the most general assumptions; and (2) as efficient as possible, i.e., communication- and computation-efficient. For cryptographic schemes to be adopted in practice, efficiency is crucial. Moreover, communication and storage efficiency—namely, the size of the authentication data, for example the size of a signature—lays an even greater role than computation: while computational power of modern computers has experienced rapid growth over the last several decades, the growth in bandwidth of communication networks seems to have more constraints.

Recently, Boneh et al. [1] introduced and realized aggregate signatures. An aggregate signature scheme is a signature scheme which, in addition to the usual setup, signing, and verification algorithms, admits an efficient algorithm for aggregating n signatures under n different public keys into one signature. Namely, suppose each one of n users has a public-private key pair (PK_i, SK_i) ; each wishes to attest to a message m_i. Each user first signs her message m_i, obtaining a signature σ_i; the n signatures can then be combined by an unrelated party into an aggregate σ. An aggregate signature scheme also includes an extra verification algorithm that verifies such an aggregate signature. An aggregate

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 110–119, 2005.

signature provides non-repudiation simultaneously on message m_1 for User 1, message m_2 for User 2, and so forth. Crucially, such repudiation holds for each user regardless of whether other users are malicious.

In 1984, Shamir proposed a new model for public key cryptography, called identity (ID)- based encryption and signature schemes, to simplify key management procedures of certificate-based public key infrastructures (PKIs) [2]. Since then, several ID-based encryption and signature schemes have been proposed based on integer factorization problem [3][4].

The bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, are important tools for research on algebraic geometry. They have been found various applications in cryptography recently [5][6][7][8][9]. More precisely, they can be used to construct ID-based cryptographic schemes [10].

In spite of several advantages of ID-based signature schemes based on pairings, they suffer some restriction on applications due to efficiency problem: Their signature verifications are ten times or one hundred times slower than that of DSS or RSA [11]. This problem may be critical in some applications such as electronic commerce or banking service in which one server has to verify many signatures simultaneously. In order to enhance the efficiency of verification process and make efficient communication, we consider ID-based aggregate signatures.

Cheon et al.[12] proposed the first ID-based aggregate signature scheme. Their security proofs were obtained through Pointcheval and Stern's forking lemma [13][14]. However, this reduction is inefficient: to break the computational problem with a probability comparable to the success probability of the signature forger, the reduction algorithm needs to execute a full run of the forging algorithm q_H times, where q_H denotes the number of hash function queries made by the forger.

In the area of provable security, the last couple of years saw the rise of a new trend consisting of providing tight security reductions for asymmetric cryptosystems : the security of a cryptographic protocol is said to be tightly related to a hard computational problem if an attacker against the scheme implies an efficient algorithm solving the problem with roughly the same advantage.

In this paper, we begin by giving a formal definition of ID-based aggregate signatures and its security model. We then propose an efficient ID-based aggregate signature scheme whose security can be proved tightly related to computational Diffie-Hellman (CDH) problem in the random oracle model. Unlike [12], we do not rely on the forking lemma in our security reduction,hence the advantage relation can be shown to be linear, which is almost the best possible. Moreover, as pointed out in [12], our scheme seems to be the only known ID-based aggregate signature which has tight security reduction.

The rest of the paper is organized as follows. In Section 2 we give formal definitions of presumed hard computational problems from which our reductions are made and then recall an ID-based signature scheme SOK-IBS [15]. In Section 3, we present an ID-based aggregate signature scheme and formally analyze its security and efficiency. And we end with concluding remarks in Section 4.