Available online at www.sciencedirect.com
SCIENCE DIRECT®
Applied Mathematics and Computation 168 (2005) 954–961
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

A new deniable authentication protocol from bilinear pairings

Rongxing Lu *, Zhenfu Cao

Department of Computer Science, Shanghai Jiao Tong University, 1954 Huashang Road, Shanghai 200030, Peoples Republic of China

Abstract

Deniable authentication protocol is a new technique of modern cryptography, and several such schemes have been proposed. However, to our knowledge, most of these schemes are interactive and less efficient, and only Shao proposed an efficient non-interactive deniable authentication protocol based on generalized ElGamal signature scheme. Therefore, there is a desire to design other secure and efficient non-interactive deniable authentication protocol. In this paper, based on the bilinear pairings, we would like to propose such a new non-interactive deniable authentication protocol. What's more, we also prove the proposed protocol is secure in the random oracle model.

Keywords: Cryptography; Deniable authentication; Bilinear pairings

1. Introduction

Deniable authentication protocol is a special cryptographic authentication protocol. Compared with the traditional authentication protocols, the deniable authentication protocol has two basic characteristics:

* Corresponding author.
E-mail addresses: rxlu@cs.sjtu.edu.cn (R. Lu), zfcao@cs.sjtu.edu.cn (Z. Cao).

0096-3003/$ - see front matter
doi:10.1016/j.amc.2004.09.030

(1) It enables a specified receiver to identify the source of a given message.
(2) The specified receiver can not prove to a third party the identity of the sender.

Just as the above two characteristics, the deniable authentication protocol can provide freedom from coercion in electronic voting systems and provide security of negotiation over the Internet [2]. Therefore, it has received great interests in practice.

In the past years, some researchers have done a lot of work in this field. Dwork et al. [1] developed a notable deniable authentication protocol based on concurrent zero-knowledge proof, yet the protocol requires a timing constraint and the proof of knowledge is subject to a time delay in the authentication process. In [2,3], Aumann and Rabin proposed another scheme based on the factoring problem, but it should need a pubic directory trusted by the sender and the receiver. Lately, Deng et. al [4] proposed two deniable authentication protocols based on the factoring and the discrete logarithm problem respectively, however, it also requires a trusted public directory. To overcome this weakness, Fan et al. [5] proposed a new deniable authentication protocol based on the Diffie-Hellman key distribution protocol. However, there still exists a common weakness in these scheme: all of them are interactive and less efficient. Therefore, there is a desire to design secure and efficient non-interactive deniable authentication protocol. To our knowledge, till now, only Shao [6] has proposed such an efficient non-interactive deniable authentication protocol based on generalized ElGamal signature scheme.

Motivated by the above mentioned, in this paper, we would like to propose a new deniable authentication protocol from the bilinear pairings. Like Shao's scheme [6], our scheme is also non-interactive and satisfies the basic security requirements of deniable authentication protocol.

The remainder of the paper is organized as follows. In section 2, we first review some basic concepts of bilinear pairings. Then we propose our new deniable authentication protocol in section 3 and analyze its security in Section 4. Finally, concluding remarks are made in Section 5.

2. Basic concepts of bilinear pairings

In this section, we will briefly review the basic concept and some properties of the bilinear pairings.

Let $\mathbb{G}_1$ be a cyclic additive group and $\mathbb{G}_2$ be a cyclic multiplicative group of the same prime order q. A bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, which satisfies the following properties: