Information Sciences 268 (2014) 447–457

Contents lists available at ScienceDirect

Information Sciences

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

Certificate-free *ad hoc* anonymous authentication

Zhiguang Qin [a], Hu Xiong [a,b,*], Guobin Zhu [a], Zhong Chen [c]

[a] Network and Data Security Key Laboratory of Sichuan Province, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, PR China
[b] Key Lab of Network Security and Cryptology, Fijian Normal University, Fuzhou 350007, PR China
[c] School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, PR China

ARTICLE INFO

Article history:
Received 8 November 2012
Received in revised form 23 October 2013
Accepted 1 November 2013
Available online 18 November 2013

Keywords:
Information security
Anonymous authentication
Certificateless cryptography
Ring signature

ABSTRACT

There is an increasing demand of *ad hoc* anonymous authentication (AHAA) to secure communications between *ad hoc* group members while preserving privacy for the members. The main obstacles in AHAA is that it is difficult to deploy traditional public-key infrastructure (PKI) in this scenario and the end users are usually limited in computation. This paper addresses these obstacles with a pairing-free certificateless ring signature scheme. The scheme does not require a setup procedure and each user can sign on behalf of a group generated in an *ad hoc* way. The signer does not need any certificate but only a legal signer can generate a valid signature to be validated. The signature verification does not leak any information about the signer's identity, even if the attacker is computationally unbound. The scheme exploits only traditional efficient modular exponentiations, without relying on time-consuming bilinear map operations. The scheme is shown to be secure in the random oracle model. Therefore, our proposal is practical for *ad hoc* anonymous authentication.

1. Introduction

As one of the most important cryptographic primitives, digital signature has been widely used for secure software distribution and financial transactions by providing authentication, non-repudiation and integrity. By validating of a conventional signature, anyone can authenticate a particular signer and verify that a signer is who he/she is claiming to be. With the increasing interests of user privacy [35], anonymous authentication is desirable in the field of electronic transactions [21,34,33] and *ad hoc* networks [38,15]. Hence, to achieve anonymous authentication, ordinary signature should be elegantly extended to enable an individual of a group authenticating membership on behalf of the group without revealing his identity.

Ring signature, initially formalized by Rivest et al. [36], is featured with anonymity and spontaneity. The anonymity means that a signer can represent a group of potential signers (called a ring) including himself to sign a message while preserving unconditionally anonymous for the signer; the spontaneity states that the signature generation procedure requires neither group managers to initialize the system nor the cooperation from the other ring members, i.e., the real signer can decide other ring members in an *ad hoc* way. Therefore, ring signatures can be applied in the above scenarios.

Since its introduction [36,37], ring signature has been well-studied along several research lines. Many ring signature schemes have been proposed in various mathematical settings such as pairing-based [10], discrete-log-based [22], mixture-based (trapdoor-permutation-type and discrete-log-type) [1], code-based [19,30], lattice-based [12] and multi-variate-based [41]. According to the adversary's attack power, security models for ring signature schemes fall into three

* Corresponding author at: Network and Data Security Key Laboratory of Sichuan Province, School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, PR China. Tel.: +86 13402802747.
E-mail address: xionghu.uestc@gmail.com (H. Xiong).

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.11.015

categories. The security model where the adversary is only allowed to mount a chosen-message attack was introduced in [36]. Later Abe et al. [1] proposed an improved model achieving unforgeability against chosen sub-ring attacks. Finally, the insider attack resilient model where the adversary can adaptively corrupt honest participants and obtain their secret keys has been introduced in [9]. The former two models were defined in the random oracle model [7], and the latter was defined in the standard model [42]. Furthermore, forking lemma for ring signature has also been given in [22]. To respond to the different scenarios, researchers have extended basic ring signatures with more versatile properties and proposed variations such as proxy ring signature [44], threshold ring signature [11], concurrent signature [14] and linkable ring signature [28].

Observe that the public keys of ring members are usually "random" strings in traditional public key infrastructure (PKI) and cannot be bound with the identities of the owners of the public keys. Thus, a trusted-by-all certificate authority (CA) must issue a digital certificate to link the public key and the corresponding identity. In this way, the user's certificate must be verified before checking the validity of the signature. The management of certificates is usually considered to be expensive and unaffordable for ring signatures, which involves validating a large number of public keys.

To circumvent heavy certificate management in traditional PKI, Identity-based public key cryptography (ID-PKC) was introduced by Shamir [39]. In ID-PKC, the public key of each user can be directly inferred from his identity (such as an email address, social insurance number), while the private key related to that identity is generated by a trusted private key generator (PKG). Thus, the complex management of certificate can be simplified. Based on bilinear pairings, Zhang and Kim proposed the first ID-based ring signature [43]. Subsequently, a more efficient construction has been given by Lin and Wu [27], while Awasthi and Lal [5] showed and fixed some small inconsistencies in [43,27]. Another ID-based ring signature scheme along with the extension for anonymous subsets was presented by Herranz and Sáez [23]. After that, Chow et al. [16] and Nguyen [31]'s constructions achieved a constant number of pairing computations and a constant size signature, respectively. Besides, ID-based ring signature secure in the standard model has been given by Au et al. [3]. To avoid the expensive pairing operation, Herranz [24] and Tsang et al. [40] suggested two pairing-free ID-based ring signature from RSA independently. The motivation and design philosophy of ID-based ring signature have been insightfully surveyed in [17]. Ring signatures in ID-PKC, however, suffer from an inherent key escrow problem, i.e., the PKG has any user's private key. Thus, avoiding key escrow in ID-based ring signatures is significant to make them more applicable in the real world.

To gain the merits of traditional PKI and ID-PKC simultaneously, Al-Riyami and Paterson [2] proposed the notion of certificateless public key cryptography (CL-PKC). Like ID-PKC, CL-PKC does not rely on certificate to authenticate the public key and needs a semi-trusted Key Generation Center (KGC) to generate the partial private key for users [2]. However, the user's full private key is computed by combing the secret value chosen by himself and his partial private key. So, CL-PKC does not subject to the key escrow problem since the KGC cannot access user's full private key. The first certificateless signature (CLS) scheme has been proposed in [2]. Following the Al-Riyami and Paterson's original work, several secure and efficient CLS schemes have been given [25,47]. Recently, Zhang et al. [46] and Chow and Yap [18] introduced ring signature into CL-PKC environment and proposed two concrete certificateless ring signature (CL-RS) schemes independently. After that, Chang et al. [13] suggested a more efficient construction along with the t-out-of-n threshold extension. Similar to CL-RS, ring signature schemes in certificate-based and self-certified setting have also been proposed to solve the certificate management problem in PKI and key escrow problem in ID-PKC in [26,4], respectively. Unfortunately, all of these CL-RS schemes are derived from bilinear pairings, a powerful but computationally expensive primitive. Compared with other problems from number theory such as discrete logarithms, factoring and RSA, bilinear pairings were only investigated recently and did not enjoy the same exposure to cryptanalysis attacks [45]. In addition, many companies or official organizations may have already invested in the development and deployment of traditional cryptosystems and thus new pairing technique may not be re-invested in terms of industry implementation. Thus, it is of great interest to design pairing-free CL-RS scheme.

In this paper, we present a certificateless pairing-free ring signature scheme. Under the standard RSA and discrete-logarithm assumptions, the proposed scheme can be formally proved to be existentially unforgeable[1] against adaptive chosen-message attacks in the random oracle model. The scheme allows a user to sign any documents anonymously on behalf a ring of users including himself. The signer can form the user ring in an *ad hoc* way. That is, the other members in the ring can be chosen on demand, even without letting the chosen users know that they appear in the ring. Our scheme is also very efficient in computation due to the removal of time-consuming bilinear pairing operations in the signing and verifying procedures. This implies that our scheme is very applicable to *ad hoc* anonymous authentication.

The rest of this paper is organized as follows. Some preliminaries required throughout the paper are reviewed in Section 2. We propose a new CL-RS scheme in Section 3 and the security of our scheme is analyzed in Section 4. Finally, the conclusions are given in Section 5.

2. Preliminaries

In this section, we review some fundamental backgrounds required in this paper, namely the definition and security model of CL-RS scheme, and the complexity assumptions.

[1] According to [20], a signature scheme is said to be existentially unforgeable if, given any polynomial number of pairs $((m_1, S(m_1)), (m_2, S(m_2)), \ldots, (m_k, S(m_k)))$ where $S(m)$ denotes the signature on the message m and k denotes the security parameter, it is computationally impractical to generate a pair $(m_{k+1}, S(m_{k+1}))$ regarding any message $m_{k+1} \notin \{m_1, \cdots, m_k\}$.