Journal of King Saud University – Computer and Information Sciences (2014) **26**, 89–97

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings

SK Hafizul Islam *, G.P. Biswas

Department of Computer Science and Engineering, Indian School of Mines, Dhanbad 826004, Jharkhand, India

Received 8 July 2012; revised 27 December 2012; accepted 26 May 2013
Available online 31 May 2013

KEYWORDS

Public key infrastructure;
Identity-based cryptography;
Certificateless cryptography;
Elliptic curve cryptography;
Bilinear pairing;
Short multisignature

Abstract Several certificateless short signature and multisignature schemes based on traditional public key infrastructure (PKI) or identity-based cryptosystem (IBC) have been proposed in the literature; however, no certificateless short sequential (or serial) multisignature (CL-SSMS) or short broadcast (or parallel) multisignature (CL-SBMS) schemes have been proposed. In this paper, we propose two such new CL-SSMS and CL-SBMS schemes based on elliptic curve bilinear pairing. Like any certificateless public key cryptosystem (CL-PKC), the proposed schemes are free from the public key certificate management burden and the private key escrow problem as found in PKI- and IBC-based cryptosystems, respectively. In addition, the requirements of the expected security level and the fixed length signature with constant verification time have been achieved in our schemes. The schemes are communication efficient as the length of the multisignature is equivalent to a single elliptic curve point and thus become the shortest possible multisignature scheme. The proposed schemes are then suitable for communication systems having resource constrained devices such as PDAs, mobile phones, RFID chips, and sensors where the communication bandwidth, battery life, computing power and storage space are limited.

1. Introduction

Digital signatures play a vital role in the security of information and communication networks by providing message integrity, authentication and non-repudiation during transmission over any insecure or hostile network. The property of message integrity guarantees that the receiver detects any alteration of the message during transmission, and the authentication property ensures the message generation by an expected sender. Compared with these two properties, the non-repudiation property is equally important, which assures that after creating a signature, the signer cannot deny the signature generation at a later time. However, in some real-life applications, such as electronic check signing, electronic contracts, decision-making processes, petitions, and workflow systems a message needs to be authenticated or approved by two or more persons concurrently. In this situation, a multisignature approach is more appropriate than any ordinary signature scheme. There are different multisignature schemes (Itakura and Nakamura, 1983; Harn, 1994; Chen and Hwang, 1994; Pon et al., 2002; Chen et al., 2004; Meng et al., 2007; Shim, 2008; Chang et al.,

* Corresponding author. Tel.: +91 8797369160.
E-mail addresses: hafi786@gmail.com, hafizul.ism@gmail.com (S.H. Islam), gpbiswas@gmail.com (G.P. Biswas).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

1319-1578 © 2013 Production and hosting by Elsevier B.V. on behalf of King Saud University.
http://dx.doi.org/10.1016/j.jksuci.2013.05.001

2009; Harn and Ren, 2010) where two or more signers mutually sign on the same message to generate a single and valid multisignature. At a later time, the multisignature can be verified by a public verifier using the public keys of all the signers.

1.1. Literature review

Based on an extended RSA technique, Itakura and Nakamura (1983) first proposed a sequential (or serial) multisignature scheme, and other similar schemes are presented in (Pon et al., 2002; Meng et al., 2007; Gangishetti et al., 2006; Shim, 2008; Chu and Zhao, 2008). The CL-SSMS has many real-life applications such as when an electronic check needs to be signed serially by the various persons in an office based on their designation. On the other hand, the broadcast (or parallel) multisignature schemes can be found in (Harn and Ren, 2010; Chen et al., 2004; Chang et al., 2009; Harn, 1994; Chen and Hwang, 1994; Gangishetti et al., 2006; Chu and Zhao, 2008; Giri and Srivastava, 2007; Yang et al., 2010; Gui and Zhang, 2010). The multisignature schemes (Giri and Srivastava, 2007; Chu and Zhao, 2008; Le and Gabillon, 2009) designed upon traditional public key infrastructure (PKI) (Diffie and Hellman, 1976) have some problems such as the requirement of huge storage space to store the public key certificates, complicated management strategy to distribute the certificates and additional computing power to verify the certificates (Giri and Srivastava 2007; Chu and Zhao, 2008; Le and Gabillon, 2009; Das et al., 2013). The identity-based cryptosystem (IBC), first introduced by Shamir (1984), can solve these drawbacks because IBC abolishes the need for public key certificate management and distribution infrastructure (Gangishetti et al., 2006; Biao et al. 2010; Yang et al., 2010; Islam and Biswas 2013b, 2013c) as required in PKI. A user can derive his public key from a known identity such as an email address, and IP address and the public key can be revoked easily by just binding a time duration to it (Boneh and Franklin, 2001). However, because a trusted third party called the private key generator (PKG) is required to compute the corresponding private key, IBC becomes vulnerable to the private key escrow problem. To remove the key escrow problem of IBC, Al-Riyami and Paterson (2003) proposed the concept of certificateless public key cryptography (CL-PKC), where the PKG generates the identity-based partial private key and a user himself generates the full private key by using the partial private key received from PKG and his own chosen random secret value. The PKG does not have access to the user's full private key and hence, the private key escrow problem and the need for a public key certificate are solved in the CL-PKC system.

1.2. Motivations and contributions

Recently, the certificateless short signature (CL-SS) schemes (Huang et al., 2007; Chen et al., 2008; Du and Wen, 2009; Choi et al., 2011) have been used extensively in many resource constrained wireless devices such as PDAs, mobile phones, RFID chips, and sensors where the communication bandwidth, battery life, computing power and storage space are limited. The short signature designed based on elliptic curve cryptography (ECC) can also offer high levels of security with comparatively short length signatures, and hence, most of the schemes use ECC (Miller, 1985; Koblitz, 1987) for the implementation of public key cryptosystems (PKC). Compared with other PKCs, the ECC-based PKC offers the same level of security with reduced key size, faster computation as well as less memory, energy and bandwidth usage, and thus, it is more suitable for resource-constrained devices. In the literature, several digital multisignature schemes (Itakura and Nakamura, 1983; Harn, 1994; Chen and Hwang, 1994; Pon et al., 2002; Chen et al., 2004; Gangishetti et al., 2006; Meng et al., 2007; Giri and Srivastava, 2007; Chu and Zhao, 2008; Shim, 2008; Chang et al., 2009; Le and Gabillon, 2009; Harn and Ren, 2010; Biao et al., 2010; Yang et al., 2010; Gui and Zhang, 2010) in PKI or IBC and many certificateless short signature schemes have been proposed; however, no certificateless short multisignature scheme has yet been designed. We combined the advantages of short signature and multisignature together with the features of CL-PKC and propose two efficient certificateless short sequential multisignature (CL-SSMS) and certificateless short broadcast multisignature (CL-SBMS) schemes using elliptic curve bilinear pairing (Boneh and Franklin, 2001). It is shown that both the schemes are secure and more computationally efficient than the others. The length of the proposed multisignature in both of the schemes is equal to an elliptic curve point and thus efficient in communication.

1.3. Paper organization

The rest of the paper is organized as follows. Section 2 describes some preliminary ideas about elliptic curve bilinear pairing and the related intractable hard problems. In Section 3, the two proposed certificateless short multisignature schemes CL-SSMS and CL-SBMS are described. The security and efficiency analyses of the schemes are given in Section 4, and Section 5 concludes the paper.

2. Preliminaries

This section briefly describes the basic concepts and properties of bilinear pairing and some computational hard problems, which are incorporated in our proposed signature schemes for achieving the desired security.

2.1. Bilinear pairing

Let G_q be an additive cyclic group of elliptic curve points of prime order q (where $q \geqslant 2^k$ and k is security parameter) and G_m be a multiplicative group of the same order q. Let $\hat{e} : G_q \times G_q \rightarrow G_m$ be an admissible bilinear mapping that satisfies the following properties:

- **Bilinearity**: For any P, Q, $R \in G_q$ then $\hat{e}(P+Q,R) = \hat{e}(P,R)\hat{e}(Q,R)$ and $\hat{e}(P,Q+R) = \hat{e}(P,Q)\hat{e}(P,R)$. Therefore, for any $a, b \in_R Z_q^* : hate(aP,bQ) = \hat{e}(P,Q)^{ab} = \hat{e}(abP,Q) = \hat{e}(P,abQ)$ holds.
- **Non-degeneracy**: There exists P, Q $\in G_q$ such that $\hat{e}$(P, Q) $\neq 1_m$, where 1_m is an identity element of G_m.
- **Computability**: There must be an efficient algorithm, which can compute $\hat{e}(P, Q)$ for all $P, Q \in G_q$.

In general, G_q is a group of points on an elliptic curve and G_m is a multiplicative subgroup of a finite field. The bilinear