Journal of King Saud University – Computer and Information Sciences (2017) **29**, 63–73

King Saud University

Journal of King Saud University –
Computer and Information Sciences

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

A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication

SK Hafizul Islam [a,*], **G.P. Biswas** [b]

[a] *Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333031, India*
[b] *Department of Computer Science and Engineering, Indian School of Mines, Dhanbad 826004, Jharkhand, India*

Received 2 September 2014; revised 26 December 2014; accepted 13 January 2015
Available online 6 November 2015

KEYWORDS

Elliptic curve cryptography;
Identity-based cryptosystem;
Bilinear pairing;
Session key;
BAN logic

Abstract Recently, many identity-based two-party authenticated key agreement (ID-2PAKA) protocols using elliptic curve cryptography (ECC) have been proposed, however, these protocols do not provide adequate security and their computation costs are also relatively high due to bilinear pairing and map-to-point function. Moreover, they require many communication rounds for establishing the session key, and thus results in increased communication latency, which makes them unsuitable for real applications. This paper thus aims to propose a pairing-free ID-2PAKA protocol based on ECC that removes the security flaws of previous protocols. The proposed protocol helps two users to establish a common session key between them through an open network. The formal security analysis using BAN logic and the comparisons with other protocols are given, which demonstrated that our protocol is formally secure and thus, suitable for secure and efficient peer-to-peer communications.

1. Introduction

The flexibility and the mobility of mobile networks help the mobile users to access the network at anytime from anywhere with their personal devices (i.e., laptop, mobile phone). Further, the rapid advancement and deployment of mobile networks, and the portability of hand-held mobile devices attract mobile users to communicate with each other over mobile networks. However, the security and the privacy protection of communicating users in mobile networks are still two important issues, which must be achieved before using the mobile network for various purposes. Recently, the authenticated key agreement protocols are becoming popular with great attention paid for secure and reliable communication in many wireless mobile applications such as IP Multimedia Subsystem (Song et al., 2011), authentication protocol (Wang et al., 2010; Islam and Biswas, 2011; Lee et al., 2011), wireless mobile ad hoc networks (Liaw et al., 2005), mobile

[*] Corresponding author. Tel.: +91 8233348791, +91 8797369160.
E-mail addresses: hafi786@gmail.com, hafizul.ism@gmail.com, hafizul@pilani.bits-pilani.ac.in (S.H. Islam).

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2015.01.004
1319-1578

IP registration (Sadhukhan et al., 2011), etc. In general, two types of authenticated key agreement protocols can be found: authenticated group key agreement protocol (Znaidi and Minier, 2011; Park and Jin, 2010; Kim and Kim, 2011; Islam and Biswas, 2012) and two-party authenticated key agreement (2PAKA) protocol (Smart, 2002; Chen and Kudla, 2002; Shim, 2003; Sun and Hsieh, 2003; Ryu et al., 2004; Boyd and Choo, 2005; Wang et al., 2009, 2008; McCullagh and Barreto, 2005; Xie, 2004; Li et al., 2005; Choie et al., 2005; Zhu et al., 2007; Cao et al., 2008, 2010; Islam and Biswas, 2012; Hölbl et al., 2012). The authenticated group key agreement protocols allow users (more than two) to come up with a common secret session key between them, whereas in the 2PAKA protocol, a common session is established between two communicating users. In both cases, the users can securely exchange the message encrypted by the session key over any hostile network. In the literature, the password-based authenticated key exchange protocol (Sui et al., 2005; Lu et al., 2007; Chang and Chang, 2008; Lo et al., 2010; Pu, 2010; Youn et al., 2011; Guo et al., 2008, 2012) can also be found, which allows two communicating users to generate a session key over any open network. However, the high computation cost and numerous communication rounds of these protocols, where a secret or a password is shared between a pair of users or with a trusted server prior to communication, makes them unsuitable for environments of low-power mobile devices. Therefore, this paper concentrates on the design of a secure and pairing-free ID-2PAKA protocol using elliptic curve cryptography (ECC) Miller et al., 1985; Koblitz, 1987 and identity-based cryptosystem (IBC) Shamir et al., 1981 suitable for low-power mobile devices.

1.1. Discussion about relevant works

In the literature, several ID-2PAKA protocols based on bilinear pairing along with a map-to-point hash function that is used to convert a random string to point on the elliptic curve group, and ECC have been proposed and some of them are discussed now. Based on the identity-based encryption scheme (Boneh and Franklin, 2001), Smart (2002) proposed an ID-2PAKA protocol, but it does not provide the perfect forward secrecy (PFS) of the session key (Chen and Kudla, 2002; Shim, 2003). Shim (2003)) proposed an efficient ID-2PAKA protocol using Weil pairing and claimed that it removes the security flaws of Smart (2002). Sun and Hsieh (2003)) demonstrated that Shim's protocol is not secure against the man-in-the-middle attack (MIMA). Based on the bilinear pairing, Ryu et al. (2004) proposed an ID-2PAKA protocol, which has vulnerability against the key-compromised impersonation (K-CI) attack (Boyd and Choo, 2005). In 2009, Wang et al. (2009) independently showed that Ryu's protocol is not secure against the reflection attack (RA) and then proposed an improved protocol and claimed that known attacks are protected. Xie (2004) showed that the ID-2PAKA protocol proposed by McCullagh and Barreto (2005) is not secure against the K-CI attack and then proposed an enhanced protocol. However, Li et al. (2005) analyzed that Xie's protocol is still insecure against the K-CI attack. In 2008, Wang et al. (2008) proposed an improved protocol over Chen and Kudla's protocol. In 2005, Choie et al. (2005) proposed some efficient pairing-based ID-2PAKA protocols, and claimed that the protocols are designed to provide required security attributes with minimal communication overheads.

In 2005, Sui et al. (2005) proposed an ECC-based password-based authenticated key agreement protocol, which offers PKG's (private key generator) perfect forward security and was included in 3GPP2 (third generation partnership project) specifications to improve the security of the authenticated key distribution protocol useful for wireless communications. However, Lu et al. (2007) shows that the protocol is vulnerable to the off-line password guessing attack, and then proposed an improvement of the protocol in Sui et al. (2005). Unfortunately, Chang and Chang (2008) proved that Lu et al.'s protocol is not secure against the password guessing attack and then proposed a modified protocol to remove the security flaws of Lu et al. (2007). However, Lo et al. (2010) demonstrated that Chang et al.'s protocol lacks to provide the mutual authentication property. Lo et al. also proposed an improved password-based authenticated key agreement protocol using ECC and claimed that the protocol could resist various attacks. In 2010, (Pu, 2010) independently demonstrated that Lu's protocol could not resist the off-line password guessing attack. Recently, Youn et al. (2011) have discovered some security weaknesses of Guo et al.'s protocol (Guo et al., 2008) and proposed an efficient protocol. In 2012, Guo et al. (2012) proposed another efficient and provably secure password-based authenticated key agreement protocol for wireless communications.

1.2. Motivations

Most of the 2PAKA protocols proposed so far can be implemented using two costly operations such as bilinear pairings and map-to-point (MTP) function. In addition, some of these protocols need a number of communication rounds for successful key establishment, which in turn leads to high communication latency. In order to reduce the computation cost, Zhu et al. (2007) and Cao et al. (2008) independently proposed two pairing-free ID-2PAKA protocols, but these protocols require three communication rounds. In 2010, Cao et al. (2010) proposed another two-round pairing-free ID-2PAKA protocol with minimum computation costs. Unfortunately, (Islam and Biswas, 2012) demonstrated that Cao et al.'s protocol (Cao et al., 2010) is vulnerable to known session-specific temporary attack (KSTIA) and key off-set attack (KOA)/key replicating attack (KRA). From these discussions, it can be concluded that the previous protocols are unsuitable for resource-constrained (battery-power, processing, memory or computation) environments for the following reasons: (1) most of the existing authenticated key agreement protocols have high computation costs and communication rounds, and none of them can provide adequate security, (2) in some password-based authenticated key agreement protocols, two users in a group can achieve mutual authentication and session key agreement if they share a password (secret) in advance, which is unsuitable for large scale peer-to-peer communication networks, since each user is required to keep a large number of secrets corresponding to all group members, and (3) in other password-based authenticated key agreement protocols, each user pre-shares a secret with a trusted server and communicates with other users via the server for which many communication rounds are to be performed. As we know, the