Journal of King Saud University – Computer and Information Sciences (2017) **29**, 311–324

King Saud University

Journal of King Saud University – Computer and Information Sciences

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

An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments

S.K. Hafizul Islam [a,*], Ruhul Amin [b], G.P. Biswas [b], Mohammad Sabzinejad Farash [c], Xiong Li [d], Saru Kumari [e]

[a] *Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani Campus, Rajasthan 333031, India*
[b] *Department of Computer Science and Engineering, Indian School of Mines, Dhanbad 826004, Jharkhand, India*
[c] *Department of Mathematical Sciences and Computer, University of Kharazmi, Tehran, Iran*
[d] *School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China*
[e] *Department of Mathematics, Ch. Charan Singh University, Meerut 250004, Uttar Pradesh, India*

Received 12 January 2015; revised 22 April 2015; accepted 27 August 2015
Available online 3 November 2015

KEYWORDS

Elliptic curve cryptography;
Authenticated key exchange protocol;
Man-in-the-middle attack;
Mobile-commerce environments

Abstract In the literature, many three-party authenticated key exchange *(3PAKE)* protocols are put forwarded to established a secure session key between two users with the help of trusted server. The computed session key will ensure secure message exchange between the users over any insecure communication networks. In this paper, we identified some deficiencies in Tan's *3PAKE* protocol and then devised an improved *3PAKE* protocol without symmetric key en/decryption technique for mobile-commerce environments. The proposed protocol is based on the elliptic curve cryptography and one-way cryptographic hash function. In order to prove security validation of the proposed *3PAKE* protocol we have used widely accepted *AVISPA* software whose results confirm that the proposed protocol is secure against active and passive attacks including replay and man-in-the-middle attacks. The proposed protocol is not only secure in the *AVISPA* software, but it also secure

* Corresponding author.
E-mail addresses: hafi786@gmail.com (S.H. Islam), amin_ruhul@live.com (R. Amin), gpbiswas@gmail.com (G.P. Biswas), sabzinejad@khu.ac.ir (M.S. Farash), lixiongzhq@163.com (X. Li), saryusiirohi@gmail.com (S. Kumari).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2015.08.002

against relevant numerous security attacks such as man-in-the-middle attack, impersonation attack, parallel attack, key-compromise impersonation attack, etc. In addition, our protocol is designed with lower computation cost than other relevant protocols. Therefore, the proposed protocol is more efficient and suitable for practical use than other protocols in mobile-commerce environments.

1. Introduction

The authentication of the communicating clients and the confidentiality of the transmitted message are the primary objectives of network security, when the communication media is a public network. Thus, to achieve these two security goals simultaneously, many *3PAKE* protocols have been introduced. *3PAKE* protocol allows two clients to authenticate each other with the assistance of a trusted server and then computes a secret session key via any public network. The session key can subsequently be used to establish a secure channel between the clients. *3PAKE* protocol is divided into following categories: password-based *3PAKE* (Lin et al., 2000, 2001, 2004; Chang and Chang, 2004; Lu and Cao, 2006; Chen et al., 2008b; Yoon and Yoo, 2008; Sun et al., 2005; Lee and Hwang, 2010; Yang et al., 2007; Reddy and Padmavathamma, 2007) and *3PAKE* protocol using server's public key (Chen et al., 2008a; Yang and Chang, 2009; Pu et al., 2009; Tan, 2010a). In password-based *3PAKE* protocol, two clients share an easy-memorable password with the trusted server and then generate the session key securely between them with the help of the server. However, most of these protocols are susceptible to undetectable off-line password guessing attack (Lin et al., 2000, 2001), on-line password guessing attack (Chen et al., 2008b; Yoon and Yoo, 2008; Sun et al., 2005; Nam et al., 2006; Phan et al., 2008), impersonation attack (Chung and Ku, 2008), unknown key-share attack (Phan et al., 2008; Guo et al., 2008), etc. In addition, the computation cost and communication load of these protocols are heavy because they have employed the modular exponentiation (Lin et al., 2001; Lee et al., 2004; Chang and Chang, 2004; Chen et al., 2008b; Sun et al., 2005), public/symmetric key encryption/decryption (Lin et al., 2000, 2001; Chang and Chang, 2004; Yoon and Yoo, 2008; Sun et al., 2005) and the transmitted message size is large in each round (Lin et al., 2000; Lee et al., 2004; Chang and Chang, 2004; Sun et al., 2005). Due to the limitations of bandwidth, computation ability and storage space of the low-power mobile devices, the above mentioned protocols are not suitable for mobile-commerce environments. Another type of *3PAKE* protocol used the server's public key and public/symmetric key cryptosystem. In Fig. 1, we have made a tree structure to show the *3PAKE* protocol division categories and their differences.

1.1. Literature review

In 2008, Chen et al. (2008a) proposed a round and computation-efficient *3PAKE* protocol using smartcard, but the protocol is later shown to be vulnerable to stolen-verifier attack as claimed by Yang and Chang (2009). If the adversary steals the pre-shared secret from the smartcard, then he/she can impersonate the legal client and share the session key with other clients. Moreover, the protocol has the high computation cost and communication loads. Therefore, Chen et al.'s *3PAKE* protocol is not suitable for mobile-commerce environments. To overcome the weaknesses of Chen et al., Yang and Chang (2009) proposed an efficient *3PAKE* protocol using elliptic curve cryptography *(ECC)* and without sharing any pre-shared secrete between client and server in which computation and communication overheads for establishing a session key are significantly reduced. However, Pu et al. (2009) demonstrated that the protocol is potentially vulnerable to unknown key-share attack, man-in-the-middle attack and impersonation attack.

1.2. Motivation and contribution

In 2010, Tan (2010a) independently pointed out that Yang and Chang's protocol is still susceptible to impersonation-of-initiator attack, impersonation-of-responder attack and parallel attack, and further proposed an improved *3PAKE* protocol based on *ECC*. In 2011, Nose et al. (2011) demonstrated that Tan's *3PAKE* protocol still suffers from the impersonation-of-initiator attack, impersonation-of-responder attack and man-in-the-middle attack. Nose et al. also claimed that these three attacks can be mounted on Yang and Chang's protocol (Yang and Chang, 2009), and Pu et al.'s protocol (Pu et al., 2009). Furthermore, this paper shows that Tan's protocol cannot resist the known session-specific temporary attack and the clock synchronization problem. In addition, Tan's protocol has high computation cost due to additional elliptic curve scalar point multiplication and symmetric en/decryption process. In this paper, we proposed an improved *3PAKE* protocol based on *ECC* for mobile-commerce environments. The proposed protocol employs the simple hash function (Message Digest Algorithm, 1992) but no en/decryption (Advanced Encryption Standard, 2001) process is needed. The proposed protocol is secure under known attacks and has lower computation cost, and thus it will be suitable for mobile-commerce environments.

1.3. Outline of the paper

We presented the basic concept of elliptic curve cryptography and the related computational problems in Section 2. Section 3 addressed Tan's *3PAKE* protocol and the security analysis of it is given in Section 4. We then proposed our improved protocol in Section 5. The formal security validation of our protocol in AVISPA software is explained in Section 6. The informal security analysis of our protocol appears in Section 7. Section 8 discussed the performance analysis and the conclusion of this paper in Section 9.