International Journal of Innovative Computing, Information and Control
Volume **7**, Number **3**, March **2011**

ICIC International ©2011 ISSN 1349-4198
pp. **1273–1284**

AN EFFICIENT AND SECURE THREE-PASS AUTHENTICATED KEY AGREEMENT ELLIPTIC CURVE BASED PROTOCOL

Zeyad Mohammad[1], Chien-Lung Hsu[2], Yaw-Chung Chen[3] and Chi-Chun Lo[1]

[1]Institute of Information Management
[3]Department of Computer Science
National Chiao Tung University
No. 1001, University Road, Hsinchu 300, Taiwan
zeyad.cs94g@nctu.edu.tw; cclo@faculty.nctu.edu.tw; ycchen@cs.nctu.edu.tw

[2]Department of Information Management
Chang-Gung University
No. 259, Wen-Hwa 1st Road, Kwei-Shan, Taoyuan 333, Taiwan
clhsu@mail.cgu.edu.tw

Received November 2009; revised March 2010

Abstract. *Key agreement protocols are a fundamental building block of cryptography to establish a common secret key over public network. We propose an efficient and secure three-pass authenticated key agreement protocol based on elliptic curve where three-pass protocols have significant advantages over two-pass in terms of security properties and applications. The three-pass protocols can prevent denial of service attacks in complex and unpredictable communication environments such as wireless networks and Internet. We show the proposed protocol can withstand a stronger adversary under eCK security model by using a trick in its block of hashing a static secret key with an ephemeral secret key. Furthermore, it can provide an assurance of the identity authentication of its partner, thus it can withstand non-repudiation attacks. Therefore, it is suitable for electronic commerce to provide non-repudiation services. By comparing the security and computational complexity of the proposed protocol with other existing protocols in our study, we show that the proposed protocol not only satisfies all security attributes but also obtains computational efficiency with a cost of 3 point multiplications.*
Keywords: Cryptography, Key agreement, Elliptic curve cryptosystem, Extended Canetti-Krawczyk

1. **Introduction.** With the rapid development of Internet-based applications which are using wireless communications, there are diverse communication devices used in daily life to transform the trends and style of traditional environment into a technology based one. Due to the exposure of transmitted data over wireless mediums, several security issues and requirements must be considered in the developments [9,34]. Therefore, a secret key distribution and user authentication become the most important security services for open networks. Nowadays, secure and efficient user authentication and key exchange schemes are important for successful Internet based commerce [10,12,24,28,29,34,35].

A key agreement protocol is a fundamental building block of cryptography over an open network. In two-party authenticated key agreement asymmetric scheme based, the two parties are exchanging static and ephemeral public keys between them, thereafter, they combine their secret keys with public keys to compute a common secret key. The common secret key can provide data privacy, data integrity, non-repudiation and entity authentication over an open communication channel.