International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **2**, February **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 755–762

EFFICIENT VERIFIER-BASED AUTHENTICATED KEY AGREEMENT PROTOCOL FOR THREE PARTIES

Tzong-Sun Wu[1], Han-Yu Lin[2], Chien-Lung Hsu[3,*] and Kuo-Yi Chang[4]

[1]Department of Computer Science and Engineering
National Taiwan Ocean University
Taiwan
ilan543@gmail.com

[2]Department of Computer Science
National Chiao Tung University
Taiwan
hanyu.cs94g@nctu.edu.tw

[3]Department of Information Management
Chang Gung University
259, Wen-Hwa 1st Road, Kwei-Shan, Tao-Yuan 333, Taiwan
*Corresponding author: clhsu@mail.cgu.edu.tw

[4]Department of Informatics
Fo Guang University
Taiwan
almarten@gmail.com

Received July 2008; revised December 2008

Abstract. *Authenticated key agreement protocols for three parties enable two clients to establish a secure communication channel through an authentication server. Generally speaking, there are two approaches to achieve this purpose. One is to issue a common session key for both clients by the key distribution center (KDC). The other is to use public key cryptosystems and the encrypted key exchange (EKE) protocol to encrypt the transmitted messages and then further derive a common session key. Recently, lots of researches on authenticated key agreement protocol for three parties use the server's public key to ensure the security of transmitted messages. Yet, the approach obviously has some drawbacks, such as increasing the cost of key management for each client. Hence, the demand for secure protocols without the server's public key comes out. In this paper, we propose an efficient verifier-based authenticated key agreement for three parties. The proposed protocol can resist the password guessing attack and other existential attacks. Moreover, compared with previous works, the proposed one also has lower computational costs.*

Keywords: Authenticated, Verifier-based, Key agreement, Encrypted key exchange (EKE), Public key cryptosystem

1. **Introduction.** In a digitalized world, information is usually exchanged via the communication channel such as the Internet. To prevent any malicious adversary from learning the communication content of exchanged messages, we need a private and secure communication channel. To achieve the purpose, we can use a shared session key known to the communication parties only to encrypt the transmitted messages. Consequently, how to protect the security and the privacy of communication content over the Internet can be reduced to the problem of establishing a shared session key. Traditionally, we can apply public key cryptosystems [4,6,7,15,16] to solve the problem of key agreement for