International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **10**, October **2011**

 ISSN 1349-4198
pp. 5619–5630

PROVABLY SECURE HIGH ENTROPY THREE-PARTY AUTHENTICATED KEY EXCHANGE SCHEME FOR NETWORK ENVIRONMENTS

Chin-Chen Chang[1,2], Hao-Chuan Tsai[2] and Ya-Chieh Huang[1]

[1]Department of Computer Science and Information Engineering
Feng Chia University
No. 100, Wen-Hwa Road, Taichung 40724, Taiwan
ccc@cs.ccu.edu.tw

[2]Department of Computer Science and Information Engineering
National Chung Cheng University
No. 168, University Road, Min-Hsiung, Chiayi 621, Taiwan
tsaihc@cs.ccu.edu.tw

Received April 2010; revised August 2010

Abstract. *In 2008, Chen et al. proposed a round, efficient, three-party authenticated, key-exchange (3PAKE) scheme. Although the authors claimed that their scheme is superior to the previous schemes in terms of security and efficiency, later Yang and Chang pointed out that Chen et al.'s scheme can suffer from a stolen-verifier attack. Also, it fails to achieve some security requirements, such as the computational costs, and its communication loads are high. For use in mobile communication environments, Yang and Chang proposed a more efficient scheme by employing elliptical curve cryptosystems. Unfortunately, it is still a fact that Yang and Chang's scheme cannot withstand an impersonation-response attack. Therefore, we propose an improved version with better security, and, also, we have proven that our proposed scheme is secure in a three-party setting.*

Keywords: Three-party, Authenticated key exchange, Password, Elliptic curve, Mobile commerce

1. **Introduction.** Secure party communications are one of the most desirable classes of service to be included in network environments. Over the past decades, many mechanisms [1,4,12,22,23,25,27] have been aimed at achieving the goal of improved security and performance. Among them, the password-based mechanism is regarded as the most useful mechanism for user authentication, since passwords have memorable characters and are simple to use. In addition, after successful authentication of the password, it is essential to establish a common session key to encrypt messages for later secure communications.

In 1992, Bellovin and Merritt [2] proposed the first well-known, password-based, authenticated, two party key-exchange scheme (2PAKE). The 2PAKE scheme enables two communication entities to authenticate each other and establish a shared session key for later secure transmissions with a shared, low-entropy password. Since Bellovin and Merritt's work in 1992, many 2PAKE protocols [9,10,13,15,20,26] have been proposed for improving security and performance. Although 2PAKE is quite suitable for either a client-to-server or a small-scale client-to-client architecture, a common problem exists; in order to communicate simultaneously with many other clients over a period of time, the number of shared passwords that a client must memorize would increase linearly with the number of communicating parties. In other words, if N entities want to communicate with each other individually, each entity must maintain at least passwords to establish a