International Journal of Innovative Computing, Information and Control
Volume **4**, Number **4**, April **2008**

ICIC International ©2008 ISSN 1349-4198
pp. **953–960**

A PRACTICAL THREE-PARTY KEY EXCHANGE PROTOCOL WITH ROUND EFFICIENCY

Ya-Fen Chang

Department of Computer Science and Information Engineering
National Taichung Institute of Technology
Taichung 404, Taiwan
cyf@cs.ccu.edu.tw

Received January 2007; revised August 2007

Abstract. *People can only remember simple or meaningful passwords. In three-party key exchange (3PEKE) protocols with password authentication, a client is allowed to share an easy-to-remember password with a trusted server such that two clients can negotiate a session key to communicate with each other secretly. Recently, many 3PEKE protocols have been proposed to improve computation and round efficiencies. However, these protocols cannot provide both efficiencies at the same time, and some violate the original concept of key exchange. In 2006, Lu and Cao proposed an improvement (LC-3PEKE) and claimed that LC-3PEKE could meet all requirements. Unfortunately, LC-3PEKE suffers from undetectable on-line password guessing attacks. This paper will show the security flaw of LC-3PEKE and propose a secure 3PEKE protocol meeting all requirements of key exchange and 3PEKE protocols with only five rounds*
Keywords: Password, Key exchange, 3PEKE, Password guessing attack

1. **Introduction.** To make the communication content secure, a shared secret key is needed for fast encryption and decryption. In 1992, Bellovin and Merritt proposed an encrypted key exchange (EKE) family of key exchange protocols [1]. In these protocols, a user is allowed to use an easy-to-remember password without being threatened by dictionary attacks [9]. For example, a secret password is previously shared by two parties A and B who want to communicate with each other. When A and B obtain a common session key, authentication is achieved.

In 1995, Steiner et al. proposed a 3PEKE protocol (STW-3PEKE) based on EKE protocols [11]. In STW-3PEKE, each user shares an easy-to-remember password with the trusted server S. S acts as a coordinator between two communication parties to complete mutual authentication. Ding and Horster divided password guessing attacks into three classes: (1) detectable on-line password guessing attacks, (2) undetectable on-line password guessing attacks, and (3) off-line password guessing attacks [4]. Ding and Horster also demonstrated that STW-3PEKE suffers from undetectable on-line password guessing attacks [4]. Among the three classes, off-line password guessing attacks are the most critical ones.

Later, Lin et al. showed that STW-3PEKE is vulnerable to undetectable on-line password guessing attacks and off-line password guessing attacks and proposed a 3PEKE protocol (LSH-3PEKE) [6]. In LSH-3PEKE, the trusted server holds a permanent and publicly-known server's public key to resist both the password guessing attacks which STW-3PEKE suffers from. Unfortunately, applying the server's public key places a burden on users because they have to verify the server's public key in advance, and the certificate infrastructure is needed. As a result, Lin et al. proposed a new 3PEKE protocol