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

ICIC International ©2010 ISSN 1349-4198
pp. 763–772

ROBUST AND EFFICIENT THREE-PARTY USER AUTHENTICATION AND KEY AGREEMENT USING BILINEAR PAIRINGS

Wen-Shenq Juang[1,*], Chin-Laung Lei[2], Horng-Twu Liaw[3]
and Wei-Ken Nien[3]

[1]Department of Information Management
National Kaohsiung First University of Science and Technology
Kaohsiung, Taiwan
*Corresponding author: wsjuang@ccms.nkfust.edu.tw

[2]Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan
lei@cc.ee.ntu.edu.tw

[3]Department of Information Management
Shih Hsin University
Taipei, Taiwan
htliaw@cc.shu.edu.tw

Received July 2008; revised December 2008

Abstract. *For providing a secure distributed computer environment, flexible and robust user authentication and key agreement is very important. In addition to user authentication and key agreement, identity privacy is very useful for attracting users to share private contents. In three-party environments, both communicating parties can share separately passwords with a trusted third party rather than themselves. This approach can reduce the key management complexity when any two potential users may want to build a secure communication between them. In this paper, we propose a robust and efficient three-party password authenticated key agreement scheme using bilinear pairings. The main merits include: (1) there does not need any password or verification table in the server; (2) a user can choose or change his own password freely; (3) any two users can authenticate each other; (4) it can protect users' privacy; (5) any two users can generate an agreed session key; (6) it does not have a serious synchronization-clock problem; (7) even if the secret information stored in a user's smart card is compromised, it can prevent the offline dictionary attack.*

Keywords: User authentication, Session key agreement, Bilinear pairings, Smart cards, Three-party scheme, Smart card loss problem

1. Introduction.

Since most of the communications in the Internet are in open environments, sensitive data or information must be properly protected [1-17,19,21,22,25-29,31,32]. In order to provide a secure communication in an open network environment, many password-based authenticated key agreement schemes were proposed [1,2,5,6,9-12,15-17,25,27,31]. Among these schemes, Lamport first proposed a password authentication scheme to realize user authentication in an insecure environment [17] in 1981. Later, Shimizu pointed out some weaknesses of Lamport's scheme and proposed an enhanced scheme [27]. Then, many improved remote user authentication schemes were proposed [6,9,11,12,15,19,25,31].