International Journal of Innovative Computing, Information and Control
Volume **6**, Number **11**, November **2010**

ICIC International ©2010 ISSN 1349-4198
pp. **5249–5258**

A SECURE AND EFFICIENT ECC-BASED AKA PROTOCOL FOR WIRELESS MOBILE COMMUNICATIONS

Jung-Wen Lo[1,2], Cheng-Chi Lee[3,4], Min-Shiang Hwang[5,*] and Yen-Ping Chu[6]

[1]Department of Computer Science and Engineering
[5]Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Road, Taichung 402, Taiwan
*Corresponding author: mshwang@nchu.edu.tw

[2]Department of Information Management
National Taichung Institute of Technology
129 Sec. 3, San-min Rd., Taichung 413, Taiwan
asalo@ntit.edu.tw

[3]Department of Computer and Communication Engineering
Asia University
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan

[4]Department of Library and Information Science
Fu Jen Catholic University
510 Jhongjheng Rd., Sinjhuang City, Taipei County 24205, Taiwan
cclee@mail.fju.edu.tw

[6]Department of Computer Science and Information Engineering
Tunghai University
181 Sec. 3, Taichung Harbor Rd., Taichung 407, Taiwan
ypchu@thu.edu.tw

Received July 2009; revised December 2009

Abstract. *Considering the performance, encrypting the transmission message by the symmetric cryptosystem is the best choice if the session key generation problem is overcome. Diffie-Hellman key exchange protocol gives a new direction for making session key but is lack of the authentication property. The RSA-based public key cryptography makes the sufficient security for the key agreement but is not suitable for wireless mobile systems. In 2005, Sui et al. proposed an authenticated key agreement (AKA) protocol based on the elliptic curve cryptography (ECC) for wireless mobile communication. Lu et al. pointed out a secure defect in Sui et al.'s protocol and proposed an enhanced protocol. Later, Chang et al. stated that Lu's scheme is insecure and proposed an improved scheme in 2008. We found that Chang et al.'s scheme did not satisfy the mutual authentication, so a securer and more efficient protocol is proposed. The protocol can be applied not only in 3GPP2 specification but also in other wireless environments.*
Keywords: Authentication, Key agreement, Key exchange, Elliptic curve cryptography, Wireless communications

1. **Introduction.** To avoid the leak of transmission messages, using the cryptosystem to encrypt the message is the best solution. As lots of malicious people snoop the network for the valuable data, therefore we should protect the transmission data over networks. Asymmetric cryptography provides a good protection but it is inefficient due to the computations of the exponentiation, especially for the mobile devices. On the contrary, the