International Journal of Innovative Computing, Information and Control
Volume **8**, Number **4**, April **2012**

ICIC International ©2012 ISSN 1349-4198
pp. **2637–2653**

A SECURE AND EFFICIENCY ID-BASED AUTHENTICATED KEY AGREEMENT SCHEME BASED ON ELLIPTIC CURVE CRYPTOSYSTEM FOR MOBILE DEVICES

Eun-Jun Yoon[1], Sung-Bae Choi[2] and Kee-Young Yoo[3,*]

[1]School of Computer Engineering
Kyungil University
33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea
ejyoon@kiu.ac.kr

[2]Korea Institute of Science and Technology Information
335 Gwahangno, Yuseong-Gu, Daejeon 305-806, Republic of Korea
sbchoi@kisti.re.kr

[3]Department of Computer Engineering
Kyungpook National University
1370 Sankyuk-dong, Buk-gu Daegu 702-701, Republic of Korea
*Corresponding author: yook@knu.ac.kr

Received September 2010; revised August 2011

Abstract. *In 2009, Yang and Chang proposed an ID-based remote mutual authentication with key agreement scheme on elliptic curve cryptosystem (ECC). Based upon ID-based concept, Yang and Chang scheme (YC scheme) does not require additional computations for certificate and is not constructed by bilinear-pairings, which is an expensive operation on elliptic curve. In addition, YC scheme not only provides mutual authentication but also supports a session key agreement between the user and the server. Therefore, YC scheme is more efficient and practical than the related works. However, we find that YC scheme not only is vulnerable to an impersonation attack but also does not provide perfect forward secrecy in spite of efforts to perform mutual authentication and session key agreement between the user and the remote server and reduce the computational costs than the related works. Therefore, this paper proposes an improved ID-based remote mutual authentication with key agreement scheme for mobile devices based on ECC. Compared with YC scheme, the proposed scheme is more secure, efficient and practical for mobile devices because the proposed scheme not only eliminates the security flaws of YC scheme but also reduces the computational costs between the user and the server.*

Keywords: Security, Cryptography, ID-based, Mutual authentication, Key agreement, Mobile devices, Elliptic curve cryptosystem, One-way hash function

1. **Introduction.** Mobile devices (e.g., cell phone, PDA and notebook PC) have gained increasingly popularity due to their portability nature [1]. People use these small mobile devices to accomplish the electronic transactions anytime and anywhere. Accordingly, it makes human life more convenient. Various electronic transaction applications, such as on-line shopping, Internet banking and pay-TV, are accomplished on Internet or wireless networks. Therefore, secure remote user authentication over insecure communication channels is an important issue for the fair transaction [2-28].

Recently, various authentication schemes based on elliptic curve cryptosystem (ECC) [29-34] are proposed to resolve the time-consuming computation problem such as modular exponentiation of traditional public-key cryptosystems (PKC) [35, 36] and the limited problem of computation ability and battery capacity of mobile devices. Generally, the