International Journal of Innovative
Computing, Information and Control
Volume 4, Number 11, November 2008
 ISSN 1349-4198
pp. 2803–2808

# A NEW EFFICIENT AND COMPLETE REMOTE USER AUTHENTICATION PROTOCOL WITH SMART CARDS

Hui-Feng Huang[1] and Wei-Chen Wei[2]

[1]Graduate School of Computer Science and Information Technology
National Taichung Institute of Technology
Taichung 404, Taiwan
phoenix@ntit.edu.tw

[2]Graduate School of Computer Science and Information Technology
National Taichung Institute of Technology
Taichung 404, Taiwan
s18943111@ntit.edu.tw

Received August 2007; revised December 2007

Abstract. *Recently, the smart card-based authentication scheme is becoming more and more important and functional. In 2006, Liaw et al. proposed an efficient and functional remote user authentication scheme with smart cards. However, with the limited computing capability, their scheme is not suitable for the smart cards. In order to achieve low-computation and communication for both parties, the remote user and the server, we will propose a new user authentication protocol with smart cards. Our authentication scheme is only calculated through the exclusive-or operator and the nonce-based number. It can greatly reduce the computation cost and lower the amount of communication for both the smart card user and the server. Without any modular exponential computation, hash function, and cryptosystems are required for the user to achieve the authentication. It is very suitable for the resource constrained devices such as smart cards. Moreover, our scheme also provides complete functionality for the user with smart cards.*
**Keywords:** Authentication, Smart card

1. **Introduction.** Due to the rising and flourishing of computer network developments, people are getting used to the convenience managing their daily work. Today, the application of smart cards has become even more universal. Hence, a remote user authentication scheme over an insecure channel has become a major interest [14,15]. Since Lamport [1] proposed a remote authentication scheme using a password table to achieve remote user authentication for insecure communication in 1981, many remote user authentication schemes [2-13] have been proposed to improve security, efficiency, and functionality extensively by many scholars in recent years. However, these previous proposed schemes are still unable to achieve lower communication and computation costs which indeed depend on hash functions, exponent operations, and cryptosystems. Recently, the smart card-based authentication scheme is becoming more and more important and functional. With the limited computing capability, these traditional cryptosystems are not suitable for smart cards [1-13]. In 2006, Liaw *etal*. [14] proposed an efficient and complete remote user authentication scheme with smart cards. Their scheme can achieve more functionality which includes: (1) the server does not require a verification table; (2) users can freely choose their own passwords; (3) it supplies mutual authentication between the user and the server; (4) users can update their password after the registration phase; (5) session key agreement is generated by the user and the remote server in every session; and (6) no time synchronization problem occurred between the user and the server [14]. However,