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

 ISSN 1349-4198
pp. **2407–2415**

A NOVEL DYNAMIC ID-BASED REMOTE MUTUAL AUTHENTICATION SCHEME

Han-Cheng Hsiang

Department of Information Management
Vanung University
Chungli 32061, Taiwan
shc@vnu.edu.tw

Received September 2008; revised February 2009

Abstract. *Most of remote mutual authentication and key agreement schemes are based on static ID; the static ID may leak partial information about the user's login message so that the adversary may trace a particular user according to the transmitted ID and start some attack actions. It is unsatisfactory for its use in real life applications, such as e-commerce. This paper presents a secure dynamic ID-based remote user authentication scheme to achieve user's anonymity. The proposed scheme not only satisfies all requirements for mutual authentication and key agreement but also achieves efficient computation.*
Keywords: Authentication, Dynamic ID, Session key, Smart card, ID anonymity

1. **Introduction.** In distributed network environment, secure communication in insecure communication channels is a very important issue. Thus, authentication and secret key distribution become the most important security service for distributed environments. However, remote mutual authentication scheme is a main procedure, which allows two communicating parties to mutually authenticate each other through an insecure communication network. In 1981, Lamport proposed a remote user authentication scheme [7] based on verifier table, but this scheme is vulnerable to stolen verifier attack and it also needs additional load of maintaining verifier table on remote system. Since then, several mutual authentication schemes without storing verifiers in the server have been proposed [1,10,15,17]. In 2002, Chien et al. proposed an efficient remote mutual authentication scheme using smart card allowing server and user to authenticate each other [1]. The merits in the scheme include freely chosen passwords, no verification tables, low communication and computation costs. Later, several schemes have been proposed to improve security, cost or efficiency [4,6,8,9,11,12,16]. These schemes share a common weakness, that is, once the user has successfully logged into the server, an attacker might eavesdrop on the line to intercept subsequent transmitted messages. In 2006, Shieh and Wang pointed out the weakness of Juang's scheme [5] and then proposed another similar scheme to improve their weakness [13]. But Shieh-Wang's scheme is vulnerable to a privileged insider's attack and does not provide perfect forward secrecy. In their scheme, once the attacker obtains the secret key x and user ID, he will derive the previous shared session key and can get all previous communication messages. In addition, we find both Juang's scheme and Shieh-Wang's scheme have the problem of slow wrong password detection [18], and users cannot change their password freely. For most of the existing authentication schemes employ a static login ID, when a user wants to login remote server, the user's ID is transmitted in plaintext form at each time. The static ID may leak partial information about the user's login message so that the adversary may trace a particular user according