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

 ISSN 1349-4198
pp. **2725–2735**

AN INNOVATIVE ONE-SERVER PRIVATE INFORMATION RETRIEVAL SCHEME ALONG WITH MUTUAL AUTHENTICATION BY SCHNORR SIGNATURE ALGORITHM

Chun-Hua Chen and Chao-Hsing Hsu

Department of Computer and Communication Engineering
Chienkuo Technology University
No. 1, Chieh-Shou N. Rd., Changhua 500, Taiwan
godsons@ctu.edu.tw; chaohsinghsu@yahoo.com

Received January 2009; revised June 2009

Abstract. *In the e-commerce environment, the protection of users' privacy from a server was not considered feasible until the private information retrieval (PIR) problem was stated and solved. A PIR scheme allows a user to retrieve a data item from an online database while hiding the identity of the item from the database server. To better improve the quality of exiting PIR schemes, a new PIR scheme is proposed, along with mutual authentication by Schnorr signature algorithm for protecting the privacy of users. The proposed scheme has optimal communication complexity O(1) and optimal computation complexity O(1). Using only one server, with the mutual authentication process in the proposed scheme, the proposed PIR scheme offers a more robust security and a more practical usage in the real e-commerce environment compared to previous PIR solutions. In addition, security analyses of our scheme and comparisons to other PIR schemes are given.*

Keywords: User's privacy, Private information retrieval (PIR), Authentication, Schnorr signature algorithm

1. **Introduction.** With the advancement of information technology and declining hardware price, organizations and companies are able to collect large amount of personal data. Moreover, advanced data analysis and mining techniques have been proposed to derived patterns hidden in data. However, the increasing power in data processing and analysis also raises concerns over the proper usage of personal information. It was found that a sensitive medical record was uniquely linked to a named record in a publicly available list through the shared attributes of Zip, Birth date and Sex. It is not surprising that many organizations are reluctant to disclose their data even when there may be great potential gains from the data exploration. Therefore research in the area of privacy preservation is important for many practical reasons.

1.1. **Motivation.** Nowadays, the knowledge about user preferences is important and valuable. However, this information may lead to negative effects if it is used against the user. One long-held assumption is that the server will not employ user preferences against the user. Nevertheless, this assumption is clearly incorrect. The solutions for the private information retrieval (PIR) problem make it possible for a user to keep his or her preferences private from everybody else, including the server. Here are two examples of the mentioned thought in an e-commerce environment:

(1) Patent Databases:
A lot of problems may result if the patent server knew which patent the user is interested in. Imagine a scientist who just discovered a chemical equation, "$CaCO_3$+2HCl