International Journal of Innovative
Computing, Information and Control
Volume **5**, Number **3**, March **2009**

ICIC International ©2009 ISSN 1349-4198
pp. 801–810

A NOVEL PRIVATE INFORMATION RETRIEVAL SCHEME WITH FAIR PRIVACY IN THE USER SIDE AND THE SERVER SIDE

Chun-Hua Chen[1,2], Gwoboa Horng[1] and Chao-Hsing Hsu[2]

[1]Department of Computer Science and Engineering
National Chung-Hsing University
250, Kuo Kuang Rd., Taichung 402, Taiwan
godsons@ctu.edu.tw; gbhorng@cs.nchu.edu.tw

[2]Department of Electronic Engineering
Chienkuo Technology Unversity
No.1, Chieh-Shou N. Rd., Changhua 500, Taiwan
chaohsinghsu@yahoo.com

Received December 2007; revised June 2008

Abstract. *Kushilevitz et al. proposed a private information retrieval (PIR) scheme based on the quadratic-residue assumption and using only one server. It conquers the problem of PIR schemes using k servers: the big overheads for managing these servers. In this paper, we point out that Kushilevitz's PIR scheme will let the user get much more information than he should get in one query of the database. In addition, a novel PIR scheme with fair privacy in the user side and the server side is proposed. It protects not only the privacy of the users like previous PIR schemes, but also protects the privacy of the server to avoid revealing the information more than the user queried. The security analyses of the proposed scheme are included in this paper. The security of the proposed scheme is based on the hard problem of factoring a big number multiplied by two big primes. Finally, we give some comparisons between our scheme and other PIR schemes.*
Keywords: Users' privacy protection, Private information retrieval (PIR), Fair privacy

1. **Introduction.** Because of the popularity of Internet, most of e-commerce and e-service activities are proceeding on Internet instead of private network. For the sake of security, usually those activities are protected under the public key encryption system. No matter what the query of the user or the answer of the database server, the information is encrypted and decrypted between the user and the server. We show this environment as Figure 1. The environment of Figure 1 can protect the security and privacy to other people, but it can not protect the privacy of the user to the server, because the encrypted information is decrypted to the server.

Nowadays, knowledge about user preferences is important and valuable. The assumption, that the server will not employ the user's preferences against the user, has been accepted for a long time. However, this assumption is not reasonable. The solutions for the private information retrieval (PIR) problem would make it possible for a user to keep his preferences private from everybody including the server. The thought mentioned above is very reasonable in the real application environment. We give following two examples.

1) Patent databases. If the patent server knows which patent the user is interested in, this will cause a lot of problems. Imagine that if some scientist discovers a science formula, for example "$2H_2 + O_2 => 2H_2O$". Naturally, he wants to patent it, because it may be valuable in the industry. But first, he checks at an international patent database on the internet to see whether the same or similar patent already exists. If the user's privacy is not secret to the server, the administrator of that server will know the scientist's query. Then the administrator of that server may gain a lot of profits illegally by revealing the