International Journal of Innovative
Computing, Information and Control
Volume 4, Number 6, June 2008
 ISSN 1349-4198
pp. 1365–1370

LOW-COMPUTATION OBLIVIOUS TRANSFER SCHEME FOR PRIVATE INFORMATION RETRIEVAL

Hui-Feng Huang[1] and Chin-Chen Chang[2]

[1]Department of Information Management
National Taichung Institute of Technology
Taichung 404, Taiwan
phoenix@ntit.edu.tw

[2]Department of Information Engineering and Computer Science
Feng Chia University
Taichung 40724, Taiwan
ccc@cs.ccu.edu.tw

Received March 2007; revised August 2007

Abstract. *The most efficient previous oblivious transfer schemes require 2t rounds of communication to obtain t secret messages. Its computational requirements and bandwidth consumption are quite demanding. Therefore, to guarantee the quality of this growing popular communication service, an efficient t-out-n oblivious transfer scheme is urgently desired. Based on the discrete logarithm, we propose an efficient t-out-n oblivious transfer scheme in this paper. Compared with existing oblivious transfer schemes, our scheme can reduce many computations and communications for both the sender and the receiver. In our scheme, only several modular multiplications and three rounds of communications are needed for a user (receiver) to obtain t messages. Since no modular exponentiation and inverse computations are performed by a user (receiver), our proposed scheme is suitable for the limited computation capacities of receivers such as smart cards or mobile units.*
Keywords: Oblivious transfer, Private information retrieval, Discrete logarithm

1. **Introduction.** Rabin [7] proposed the concept of the two-party oblivious transfer (OT) scheme in the cryptographic scenario. For 1-out-2 OT, Alice (sender) has two secrets m_1 and m_2 and would like to let Bob (receiver) choose one of them. Again, Bob does not want Alice to know which secret he chooses. The 1-out-n OT is a natural extension of 1-out-2 OT, in case of n secrets, in which the sender has n secrets $m_1, m_2, \ldots, m_n$, and is willing to reveal one of them to a receiver at the receiver's choice. Also the receiver cannot obtain other $n-1$ secrets. The oblivious transfer has found many applications in cryptographic studies, such as fair electronic contract signing, oblivious secure computation, private information retrieval (PIR), etc [2-4,12-14].

A general approach for constructing t-out-n OT is more practical than 1-out-n OT for applications. For example, with private information retrieval applications (PIR), a user may want to query some data blocks from a database, but the user does not want the database manager (DBM) to know in which t blocks he is interested [2,12]. In fairness, the DBM does not want the user to obtain other $n-t$ secret blocks. So far, the most efficient previous 1-out-n OT schemes cannot easily construct a t-out-n OT scheme [1,6,8-10]. These previous constructions require $2t$ rounds of communication for 1-out-n OT to obtain t secret messages. Their computation complexity is $O(nt)$ modular exponentiations for Alice (sender) and $O(t)$ modular exponentiations for Bob (receiver). In Tzeng's scheme [9,10] the most efficient previous scheme to the best of our knowledge, the sender