Cryptology ePrint Archive: Report 2011/674

Extended Combinatorial Constructions for Peer-to-peer User-Private Information Retrieval

Colleen M. Swanson and Douglas R. Stinson

Abstract: We consider user-private information retrieval (UPIR), an interesting alternative to private information retrieval (PIR) introduced by Domingo-Ferrer et al. In UPIR, the database knows which records have been retrieved, but does not know the identity of the person making the query. The goal of UPIR, then, is to disguise user profiles from the point of view of the database. Domingo-Ferrer et al.\ focus on using a peer-to-peer community to construct a UPIR scheme, which we term P2P UPIR. In this paper, we establish a strengthened model for P2P UPIR and clarify the privacy goals of such schemes using standard terminology from the field of privacy research. In particular, we argue that any solution providing privacy against the database should attempt to minimize any corresponding loss of privacy against other users. We consider the problem of user-privacy against other users in detail and consider a stronger adversarial model than previous work. We give an analysis of existing P2P UPIR schemes, which includes a new attack by the database. Finally, we introduce two new P2P UPIR protocols and give an analysis of the privacy properties provided by these protocols. Our P2P UPIR schemes, like those from existing work, draw from the field of combinatorial designs. Unlike previous work, however, which focuses on a special type of design known as a configuration, our protocols make use of more general designs. This allows for more flexibility in protocol set-up, allowing for a choice between having a dynamic scheme (in which users are permitted to enter and leave the system), or providing increased privacy against other users.

Category / Keywords: applications /

Publication Info: Accepted for publication by Advances in Mathematics of Communications

Date: received 12 Dec 2011, last revised 3 Jul 2012

Contact author: c2swanso at uwaterloo ca