

Accepted Manuscript

Privacy-Enhanced Attribute-Based Private Information Retrieval

Jianchang Lai, Yi Mu, Fuchun Guo, Peng Jiang, Willy Susilo

PII: S0020-0255(18)30353-0
DOI: [10.1016/j.ins.2018.04.084](https://doi.org/10.1016/j.ins.2018.04.084)
Reference: INS 13627

To appear in: *Information Sciences*

Received date: 8 January 2018
Revised date: 12 March 2018
Accepted date: 30 April 2018

Please cite this article as: Jianchang Lai, Yi Mu, Fuchun Guo, Peng Jiang, Willy Susilo, Privacy-Enhanced Attribute-Based Private Information Retrieval, *Information Sciences* (2018), doi: [10.1016/j.ins.2018.04.084](https://doi.org/10.1016/j.ins.2018.04.084)



This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Privacy-Enhanced Attribute-Based Private Information Retrieval

Jianchang Lai^a, Yi Mu^a, Fuchun Guo^{a,*}, Peng Jiang^{b,*}, Willy Susilo^{a,*}

^a*Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, Australia*

^b*Department of Computing, Hong Kong Polytechnic University, Hong Kong*

Abstract

A private information retrieval protocol allows a user to retrieve w -th data item (or k items) of its choice from a database of N data items without revealing its choice w to the server. The traditional private information retrieval protocols based on the notion of oblivious transfer must publish the description of each data item stored in the database in order for the user to make a choice before users run the protocol (each data item's content is not revealed though). Aiming to eliminate the information leakage of the data item in the private information retrieval system, in this work, we propose a novel attribute-based private information retrieval protocol which can enhance the data privacy. In our proposed protocol, each data item is associated with a set of attributes which is not made public to users who are only given a universal attribute set, which reveals no information about individual data item. For each query, the user can only obtain the data items whose attributes are within its chosen attribute set. We provide a rigorous security analysis of our protocol and demonstrate its efficiency and feasibility.

Keywords: Private information retrieval, Data privacy-enhanced, Attribute-based.

*Corresponding author

Email addresses: j1967@uowmail.edu.au (Jianchang Lai), ymu@uow.edu.au (Yi Mu), fuchun@uow.edu.au (Fuchun Guo), cspjiang@comp.polyu.edu.hk (Peng Jiang), wsusilo@uow.edu.au (Willy Susilo)

Download English Version:

<https://daneshyari.com/en/article/6856386>

Download Persian Version:

<https://daneshyari.com/article/6856386>

[Daneshyari.com](https://daneshyari.com)