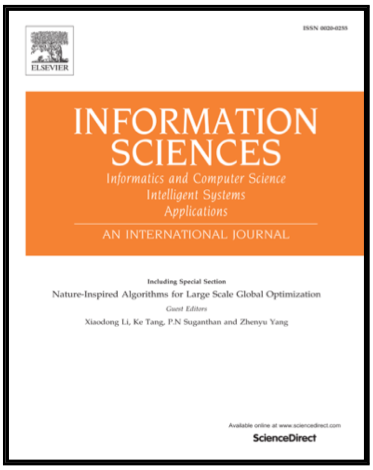

ISSN 0020-0255

ELSEVIER

INFORMATION SCIENCES

Informatics and Computer Science
Intelligent Systems
Applications

AN INTERNATIONAL JOURNAL

Including Special Section

Nature-Inspired Algorithms for Large Scale Global Optimization

Guest Editors

Xiaodong Li, Ke Tang, P.N Suganthan and Zhenyu Yang

Available online at www.sciencedirect.com

ScienceDirect

Quantum Private Set Intersection Cardinality and its Application to Anonymous Authentication

Run-hua Shi , Yi Mu , Hong Zhong , Shun Zhang , Jie Cui

PII: S0020-0255(16)30556-4
DOI: 10.1016/j.ins.2016.07.071
Reference: INS 12397

To appear in: *Information Sciences*

Received date: 9 July 2015
Revised date: 23 March 2016

Please cite this article as: Run-hua Shi , Yi Mu , Hong Zhong , Shun Zhang , Jie Cui , Quantum Private Set Intersection Cardinality and its Application to Anonymous Authentication, *Information Sciences* (2016), doi: 10.1016/j.ins.2016.07.071

Highlights:

- We proposed an unconditionally secure quantum Private Set Intersection Cardinality (PSI-CA) protocol. Compared with the classical PSI-CA protocols, the proposed protocol can dramatically reduce the communication complexity, because it only requires O(1) communication cost, which is fully independent of the size of the sets.
- Based on the proposed quantum PSI-CA protocol, we presented a novel anonymous authentication scheme, which can not only achieve two basic secure goals: secure authentication and anonymity, but can also easily and dynamically update the authorized clients, where the main computation costs of updating are several set operations. However, in most existing anonymous authentication schemes, revoking an authorized client is a very complex task. Before each authentication it usually needs to add an extra revocation test to check whether the client is in the revocation list.