Improved and Formal Proposal for Device Independent Quantum Private Query (Extended Abstract)

Jyotirmoy Basak[1], Kaushik Chakraborty[2], Arpita Maitra[3], and Subhamoy Maitra[1]

[1]*Applied Statistics Unit, Indian Statistical Institute, Kolkata 700108, India*
[2]*QuTech Academy, Delft, Netherlands*
[3]*TCG Centre for Research and Education in Science and Technology, Kolkata-700091, India*

1 Extended Abstract

Quantum Private Query (QPQ) is a distrustful quantum cryptographic scheme where the client issues queries to a database and obtains the value of data bits corresponding to some particular indices without knowing anything else about the database (known as database security), whereas the server should not gain any information about the query indices of the client (known as user privacy). Although Quantum Private Query (QPQ), Symmetric Private Information Retrieval (SPIR) and Oblivious Transfer (OT) are closely related to each other, they have some differences. In 1 out of N OT, the server has a database with N entries and the client wants to know one of the entries with the intension that her choice would not be known by the server. On the other hand, the server doesn't want the client to retrieve more information than the intended one. SPIR is conceptually same as OT and it is impossible to design an information theoretic secure OT both in quantum as well as classical setting. However, information theoretic secure SPIR can be designed in a distributed database setting [5]. On the other hand, QPQ is much like 1 out of N OT or SPIR with a weaker security requirement. Here the user can gain more information about the database, but it should be upper bounded and must not depend on the size of the database. Moreover, if the server tries to gain more information about client's query then the client can find it out. Due to this weaker security requirement, information theoretic secure QPQ can be designed in a single database setting [6, 1].

Very recently, Maitra et al [1] first identified that the security of the existing QPQ protocols are based on the trustful assumptions over the involved devices. The authors also introduced a testing phase for the involved devices on the server side and proposed a semi-device independent version over the Yang et al [2] protocol. Here we overcome their limitations and propose a fully device independent QPQ protocol. The main contributions of our work can be summarised as follows-

(1) We remove the trustworthiness from the devices (source as well as measurement devices for both server and client) using the self-testing of projective measurements (following the idea proposed in [3]) and self-testing of POVM elements. In the proposal by Maitra et al. [1], the server Bob performs local CHSH test which certifies the shared non maximally entangled states (of some particular form) provided by the source device and his own measurement device. However, this local CHSH test doesn't provide any certification about the functionality of client Alice's measurement device which is used in private query scheme. So, this test doesn't imply device independence in its truest sense. Keeping this in mind, we propose here a device independent QPQ scheme using EPR pairs and a proper self testing mechanism which guarantees full DI security of our protocol.

(2) We replace the usual projective measurement at Alice's side with optimal POVM measurement so that Alice can obtain maximum $(1-\cos\theta)$ fraction conclusive raw key bits of the entire raw key at Bob's side for the parameter θ chosen by Bob in his projective measurements (one can refer to [4] for the optimality proof of $[1-\cos\theta]$ in distinguishing two non orthogonal states).

(3) Contrary to all the existing QPQ protocols, in the present effort, we try to propose a general security analysis by providing an upper bound on the cheating probabilities and a lower bound on the amount of information leakage in terms of min-entropy for both the parties (server as well as the client). Our results show that dishonest Alice can conclusively retrieve atmost $(1-\cos\theta)$ fraction of bits of the entire raw key at Bob's side and dishonest Bob can successfully guess whether a particular database index is queried by Alice with probability atmost $(1-\cos\theta)^k$ where k denotes the number of raw key bits that are XORed to get a bit of the final key.

In summary, we propose a novel DI-QPQ scheme which provides optimal number of raw key bits to the client and certifies the functionality of all the involved devices. As most of the recent QPQ schemes incorporate the idea of Quantum Key Distribution (QKD), QPQ will soon become a crucial near-term application of Quantum Internet. For other applications of QPQ, one may refer to [7].

The full paper version of this extended abstract is available at [8].

References

[1] A. Maitra, G. Paul, S. Roy, Device-independent quantum private query. *Phys. Rev. A*, 95, 4, 042344, 2017.

[2] Y. G. Yang, S. J. Sun, P. Xu, J. Tiang, Flexible protocol for quantum private query based on B92 protocol. *Quant. Info. Proc.*, 13, 805, 2014.

[3] J. Kaniewski, Self-testing of binary observables based on commutation. *Phys. Rev. A*, 95, 6, 062323, 2017.

[4] I. D. Ivanovic How to differentiate between non-orthogonal states *Physics Lett. A*, 123, 6, 257-259, 1987.

[5] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, Protecting data privacy in private information retrieval schemes, *Journal of Computer and System Sciences*, 60, 3, 592–629, 2000.

[6] V. Giovannetti, S. Lloyd, L. Maccone, Quantum private queries, *Physical review letters*, 100, 23, 230502, 2008.

[7] W. Y. Kon, C. C. W. Lim. Provably-secure symmetric private information retrieval with quantum cryptography. *https://arxiv.org/abs/2004.13921*.

[8] J. Basak, K. Chakraborty, A. Maitra, and S. Maitra, Improved and formal proposal for device independent quantum private query, *https://arxiv.org/abs/1901.03042*.