Specious Adversaries and Quantum Private Information Retrieval
Abstract for QCRYPT 2013 contributed talk

Ämin Baumeler[1, *] and Anne Broadbent[2, †]
[1]*Faculty of Informatics, Università della Svizzera italiana, Lugano, Switzerland*
[2]*Department of Combinatorics and Optimization & Institute for Quantum Computing*
University of Waterloo, Waterloo, Canada
(Dated: June 19, 2013)

Our contribution [2] is twofold. On the one hand, we show that information-theoretic single-server Quantum Private Information Retrieval requires a linear amount of communication to be secure against specious adversaries, which are the quantum analog of honest-but-curious adversaries. On the other hand, we stress the importance of adequate comparison between classical and quantum adversaries—unfair comparisons might lead to an unjustified advantage for the quantum case.

I. INTRODUCTION

Private Information Retrieval (PIR) is a cryptographic scheme that allows a client to secretly query a database. Here, we consider information-theoretic single-server PIR, which we describe more formally as follows. Let a server hold an n-bit database. After the query, the client knows the i-th bit of the database, whereas the server knows nothing about i (there are no restrictions on what the client learns from the server beyond the i-th bit).

In the trivial PIR protocol, the server sends the whole database to the client. This protocol has a communication complexity of n bits. The study of PIR is mostly concerned with minimizing the communication complexity. In particular, one asks for the communication complexity lower bound for any PIR protocol. In 1998, Chor, Kushilevitz, Goldreich, and Sudan proved that n is the tight lower bound for single-server and information-theoretic PIR [4].

The fact that the quantum model, in contrast to the classical model, helped to improve solutions to cryptographic tasks [3, 8], raised hope to minimize the lower bound beyond n by using quantum information. A PIR scheme where quantum information is used is called Quantum Private Information Retrieval (QPIR). In 1999, Nayak proved the communication complexity lower bound for QPIR protocols to be n, as in the classical case [7]. His proof however, applies only to an unrestricted adversarial quantum server.

A recent QPIR protocol from 2012 by Le Gall however achieves a communication complexity in the order of $\sqrt{n}$ [6]. This improvement could only be achieved because the power of the adversarial quantum server is restricted to precisely follow the protocol, even to the extent of discarding information. Our work was mainly motivated by his result. We asked ourselves: What is the communication lower bound for QPIR protocols that are secure against only the *weakest reasonable quantum adversary*? To answer this question, one first needs to know how to model the weakest reasonable quantum adversary. In classical cryptography this adversary is called *honest-but-curious* and is well defined. The quantum analog to this adversary was defined in 2010 by Dupuis, Nielsen, and Salvail [5]. The authors named it *specious*. Our main contribution is that a QPIR protocol that is secure against specious adversaries needs at least n bits of communication. This concludes that the improvement in this recent protocol [6] is only due to an unfair comparison between the classical and quantum adversary.

This introduction continues with a description of our contributions and their importance to quantum cryptography. After this, we describe the adversarial model in more detail and compare it to the classical honest-but-curious model. Then we present the ideas for the lower bound proof.

A. Contributions and importance to quantum cryptography

In our work [2] we prove that, even by relaxing the power of a quantum adversary as much as as possible, QPIR protocols need at least the same amount of communication as the database size. Hence, the trivial QPIR protocol, in which the whole database is sent to the server, is optimal. Furthermore, we stress the importance of adequate comparison between classical and quantum adversaries. An unfair comparison, as we think has been done in a recent work [6], might lead to an unjustified quantum advantage. Such results leave hopes for further improvements, which would be illusory only.

In Theorem 1, we formally state our main result, where the following notions are used. Let $H_{\text{bin}}(p)$ be the binary entropy defined as $H_{\text{bin}}(p) := -p\log(p) - (1-p)\log(1-p)$. We call a protocol $(1-\delta)$-correct if the output of the protocol does not deviate more than δ from the intended behavior, with respect to the trace distance. Furthermore, we call a protocol $(1-\varepsilon)$-private against specious servers if at every step of the protocol, any specious adversary

[*] Electronic address: amin.baumeler@usi.ch
[†] Electronic address: albroadb@iqc.ca

does not know more than an ε-portion of the index, with respect to the trace distance (see full version [2] for details).

Theorem 1. *Let Π be an s-round, n-bit, single-server QPIR protocol, that is $(1-\delta)$-correct and $(1-\varepsilon)$-private against specious servers. Then Π has communication complexity of at least*

$$\left(1 - H_{bin}\left(1 - \delta - 2\sqrt{\varepsilon(1-\varepsilon)}\right)\right) n\,.$$

This result closes the open questions of information-theoretic single-server QPIR protocols. Another impact is that this result makes an example of the importance on dealing correctly with quantum adversaries. Furthermore, it reminds us that improvements are not guaranteed, if we use quantum information instead of classical information.

II. WEAKEST REASONABLE CLASSICAL AND QUANTUM ADVERSARIES

In this section, we describe the honest-but-curious adversaries, which are the weakest reasonable classical adversaries. Based on this, we give a first try to formulate the quantum analog of the honest-but-curious adversaries and point out the difficulties that arise. After that, we describe the specious adversaries, which are the weakest reasonable quantum adversaries. The specious adversaries are then related to the well known purified adversary. Finally, we analyze Le Gall's adversarial model.

A. Classical honest-but-curious adversary

In classical cryptography, the weakest reasonable adversary is called honest-but-curious. Its name precisely describes how such an adversary acts. It is honest, which means it follows the protocol at every step, but then it is also curious and remembers every transaction with the clients. This adversary can be justified as the weakest reasonable classical adversary. The reason for this is that, if one tries to restrict a classical adversary as much as possible, one can say that all transactions are invalid except the honest one. The honest transaction cannot be forbidden, because this would impact the correctness of the protocol. On the other hand, we cannot restrict the actions of the adversary in his laboratory. Hence, copying is allowed.

Stated in other words, an adversary is honest-but-curious, if it passes an imaginary audit at the end of the protocol. The adversary passes the audit if it can reproduce a state that, when joined with the client's state, is indistinguishable from the joint honest state.

B. Quantum specious adversary

A one-to-one translation of the honest-but-curious adversary to the quantum case leads to difficulties. First of all, due to the no-cloning theorem, a quantum adversary cannot copy the states during the interactions with the clients. The honest attribute could, at first sight, be translated as it is. However, if we think of the definition with the auditor, then we should allow the adversary to perform a delayed measurement attack. In such an attack, the adversary ignores the protocol instruction to measure the quantum state. At a later point in the protocol, at least during the audit, the adversary applies the measurement.

This directly leads us to the specious adversaries defined by Dupuis, Nielsen, and Salvail [5]. They call an adversary specious, if at every step in the protocol, the adversary can pass an audit by applying a local operation. It is crucial to consider *every* step in the protocol, because of the no-cloning theorem.

The purification attack is a well known attack in the quantum cryptography community. The adversary implementing the purification attack is usually called a purified adversary. The purified adversary is specious, because at every step in the protocol, the adversary can trace-out the purification quantum registers. By this, the global state, which might be shared between the clients and the adversary, gets reverted to the valid state.

C. Le Gall's adversarial model

The adversary in Le Gall's scheme follows the protocol to the extent of discarding information. In the first step of the protocol, the adversary implicitly measures the input state. In contrast to the classical case, honest-but-curious adversaries never discard information. On the contrary, these adversaries are forced to remember everything they see. The linear PIR lower bound indeed also holds for honest-but-curious adversaries [4].

An explicit attack to break Le Gall's protocol, where the adversary does not measure the input state, can be found in the master's thesis of Ä. B. [1, page 44].

III. PROOF IDEA

The proof of Theorem 1 can be found in our manuscript [2, page 6]. In the proof we first reduce any multi-step QPIR protocol to a single-step QPIR protocol. In a single-step QPIR protocol, the server sends one message to the client, who then extracts the desired bit. This exactly describes quantum random access codes (RAC), where any database item can be retrieved from a quantum state encoding the database. After the reduction, the proof is finished by applying Nayak's lower bound on random access codes [7].

That this reduction is possible is shown in two steps. First, one needs to describe how the reduction is done. The server simulates the client and assumes 1 as the client's index. At the end of the simulation, the state of the simulated client is sent to the real client, who applies a map to change the global state in such a way, as if the server used i as the index. That this can be done is shown using Uhlmann's lemma and the Fuchs-van de Graaf inequalities. This alone is not sufficient to prove the theorem. In order to apply Nayak's RAC lower bound, one also needs to show that the communication complexity of the single-step protocol is at most as large as the communication complexity of the original protocol. This is shown by limiting the Schmidt rank of the state resulting from the simulation, and by Schmidt compressing the client's state.

IV. CONCLUSION

We presented the communication complexity lower bound for information-theoretic single-server Quantum Private Information Retrieval protocols in a non-technical way. Furthermore, we stressed on the rather conceptual contribution, namely that comparing classical and quantum adversaries is not trivial.

[1] Ämin Baumeler. Quantum private information retrieval. Master's thesis, ETH Zurich, 2012.

[2] Ämin Baumeler and Anne Broadbent. Quantum private information retrieval has linear communication complexity. *arXiv: 1304. 5490 [quant-ph]*, 2013.

[3] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the International Conference on Computers, Systems, and Signal Processing*, pages 175–180, 1984.

[4] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. Private information retrieval. *Journal of the ACM*, 45(6):965–981, Nov 1998.

[5] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. In *Proceedings of the 30th Annual Conference on Advances in Cryptology, CRYPTO '10*, pages 685–706. Springer-Verlag, 2010.

[6] François Le Gall. Quantum private information retrieval with sublinear communication complexity. *Theory of Computing*, 8(1):369–374, 2012.

[7] Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science, FOCS '99*, pages 369–376, Washington, DS, USA, 1999. IEEE Computer Society.

[8] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, Nov 1997.