On the implausibility of classical client blind quantum computing

Extended abstract

Scott Aaronson[1], Alexandru Cojocaru[2], Alexandru Gheorghiu[2], and Elham Kashefi[2,3]

[1] Department of Computer Science, University of Texas at Austin,
[2] School of Informatics, University of Edinburgh,
[3] CNRS LIP6, Université Pierre et Marie Curie, Paris

Suppose a large scale quantum computer becomes available over the Internet. Could we delegate universal quantum computations to this server, using only *classical communication* between client and server, in a way that is *information-theoretically blind* (i.e., the server learns nothing about the input apart from its size, with no cryptographic assumptions required)? We give indications that the answer is no. This contrasts with the situation where quantum communication between client and server is allowed — where we now know, from work over the past decade, that such a task is possible using *Universal Blind Quantum Computation* (UBQC) [1] (see Figure 1 for a schematic illustration). It also contrasts with the case where cryptographic assumptions are allowed: there again, it is now known that there are quantum analogues of *fully homomorphic encryption* (though, these also require some quantum communication) [2,3].

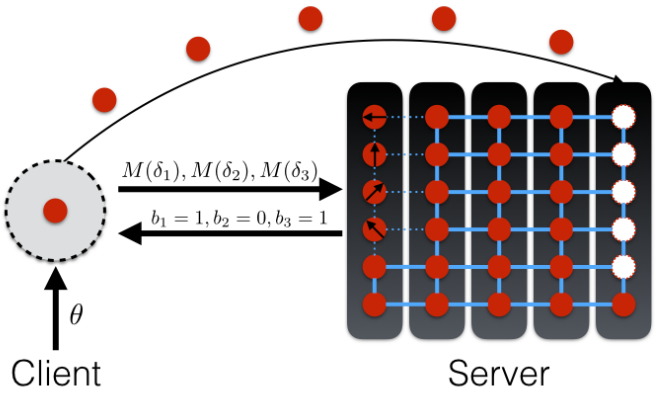
$M(\delta_1), M(\delta_2), M(\delta_3)$
$b_1 = 1, b_2 = 0, b_3 = 1$
θ
Client
Server

Fig. 1: Universal Blind Quantum Computation

In more detail, we observe that, if there exist information-theoretically secure classical schemes for performing universal quantum computations on encrypted data, then we get unlikely containments between complexity classes, such as $\mathsf{BQP} \subset \mathsf{NP/poly}$. This follows from a framework defined by Abadi, Feigenbaum and Killian known as a *generalised encryption scheme* (GES) [4]. A GES is a protocol between a classical client and an unbounded server. The client has an input x for which it wants to compute $f(x)$, but lacks the computational requirements to do so. The client can delegate the computation of $f(x)$ to the server, but would like to keep x hidden in an information-theoretic sense, apart from an upper bound on the size of x. The GES then works as follows:

(1) The client generates a key k and computes an encryption of x, denoted $y \leftarrow E(k, x)$, using a polynomial-time algorithm E.
(2) The client sends y to the server.
(3) The two interact for a number of rounds that is polynomial in the size of x.
(4) The client applies a polynomial-time decryption algorithm D on the server's responses, $\bar{s}$, and on k and x obtaining, with probability at least $1/2 + 1/poly(|x|)$, the desired result $f(x) \leftarrow D(\bar{s}, k, x)$.

Abadi et al. showed that the types of functions which admit such a scheme are contained in the complexity class $\mathsf{NP/poly} \cap \mathsf{coNP/poly}$. Thus, if polynomial-time quantum computations could be performed using a GES, then $\mathsf{BQP} \subset \mathsf{NP/poly} \cap \mathsf{coNP/poly}$. Showing that $\mathsf{BQP} \not\subset \mathsf{NP/poly}$ is no easier than showing that $\mathsf{P} \neq \mathsf{NP}$ so we cannot give a definite proof of this fact. However, we prove two results which indicate why the containment is unlikely.

First, we show that if we fix the advice polynomial of $\mathsf{NP/poly}$, in other words, we consider the class $\mathsf{NP/O(n^d)}$, then we can construct an oracle separating BQP from that class. The oracle is based on a version of the complement of Simon's problem which is also used to separate BQP from NP [5,6].

Our second result concerns *sampling problems* and can, arguably, be considered more compelling than the oracle result. In the case of sampling problems, the input, x, specifies a certain distribution $\mathcal{D}_x$ and the output is a sample from that distribution, in the exact case, or a sample from a distribution $\mathcal{C}_x$ that is close in variation distance to $\mathcal{D}_x$, in the approximate case. We redefine the notion of a GES for the case when the client wishes to delegate sampling problems to the server. We then show that having such a scheme for BosonSampling [7], implies the existence of non-uniform circuits of size $2^{n-\Omega(n/log(n))}$, making polynomially sized queries to an $\mathsf{NP^{NP}}$ oracle, for computing the permanent of an $n \times n$ matrix. We conjecture that such circuits do no exist, given that the best known algorithm for computing the permanent is Ryser's algorithm, developed over 50 years ago, which requires $\mathsf{O}(2^n n)$ arithmetic operations [8].

We then proceed to extend the Abadi et al. result to the setting where one round of quantum communication is allowed between the client and the server, referring to this as a quantum GES (QGES). This is done in order to investigate the complexity theoretic limitations of protocols such as UBQC which is a particular instance of a QGES. We show that for QGES protocols, having an extra property known as *offline-ness*, the functions which can be computed are contained in the class $\mathsf{QCMA/qpoly} \cap \mathsf{coQCMA/qpoly}$. Roughly speaking, an offline protocol is one in which the client does not need to commit to any particular input (of a given size), after having sent the first encrypted message to the server. In other words, there is some efficient (quantum) operation which the client can use to change its input after having initiated communication with the server. This property is satisfied by UBQC. We then use this result to show that, under plausible complexity assumptions, a QGES would be no more useful than a classical GES at delegating NP-hard problems to the server. To be more precise, we show that if $\mathsf{NP} \subset \mathsf{QCMA/qpoly} \cap \mathsf{coQCMA/qpoly}$ then $\mathsf{\Pi_3^P} \subseteq \mathsf{NP^{NP^{PromiseQMA}}}$, which is as close to a collapse of the polynomial hierarchy as one can reasonably hope to get given a quantum hypothesis.

Lastly, we briefly comment on the implications of these results for the prospect of verifying a quantum computation through classical interaction with the server. When the client has a single-qubit preparation device, Fitzsimons and Kashefi showed that the UBQC protocol can be made verifiable [9]. Because of the success of transforming UBQC into a verification protocol the hope was that if one could develop a classical client version of UBQC then that protocol could also be made verifiable. Indeed, blindness seems like a very useful property for a protocol to have if one wishes to make it verifiable. Our result, however, indicates that it is unlikely to have a classical client quantum protocol which relies on blindness.

The motivation for our results is twofold. Firstly, the complexity theoretic approach we use allows us to establish very precise conditions for what is and what is not possible in regards to quantum computing on encrypted data. In particular, given the importance of this application and the need for practical protocols, our "no-go" result for classical clients informs the direction of future research in this field: we either have to consider protocols leaking more information to the server, such as the approach from [10], or consider schemes with computational security, such as the approach from [11].

Secondly, we emphasize the significance of the complexity theoretic upper bound on functions which can be computed with a QGES, as well as the result that NP-hard functions are unlikely to satisfy this bound. Quantum computers could, in principle, solve NP-complete problems quadratically faster than classical computers, thanks to Grover's algorithm [12]. Even though the speedup of Grover's algorithm is only quadratic, from (say) 2^n to $2^{n/2}$, our second no-go theorem is only concerned with the length of the computation performed on the client side, and therefore applies to Grover's algorithm just as it would to a quantum algorithm achieving exponential speedup. Our result shows that clients cannot exploit a Grover speedup on the server side, even when allowing some quantum communication, if we also want to keep their inputs hidden in an information-theoretic sense. Furthermore, the technique used to arrive at the upper bound could prove useful for deriving upper bounds in other settings (for instance when the client sends a logarithmic-size quantum message to the server, instead of a polynomial-size one, or if we leak a different amount of information than just the size of the input).

References

1. Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Proceedings of the 50th Annual Symposium on Foundations of Computer Science*, FOCS '09, pages 517 – 526. IEEE Computer Society, 2009.
2. Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, pages 609–629, 2015.
3. Yfke Dulek, Christian Schaffner, and Florian Speelman. *Quantum Homomorphic Encryption for Polynomial-Sized Circuits*, pages 3–32. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
4. M. Abadi, J. Feigenbaum, and J. Kilian. On hiding information from an oracle. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, pages 195–203, New York, NY, USA, 1987. ACM.
5. Daniel R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997.
6. Scott Aaronson. BQP and the polynomial hierarchy. In *Proceedings of the Forty-second ACM Symposium on Theory of Computing*, STOC '10, pages 141–150, New York, NY, USA, 2010. ACM.
7. Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, STOC '11, pages 333–342, New York, NY, USA, 2011. ACM.
8. Herbert John Ryser. Combinatorial mathematics. In *JSTOR*, volume 14, 1963.
9. Joseph F. Fitzsimons and Elham Kashefi. Unconditionally verifiable blind computation, 2012. Eprint:arXiv:1203.5217.
10. Atul Mantri, Tommaso F. Demarie, Nicolas C. Menicucci, and Joseph F. Fitzsimons. Flow ambiguity: A path towards classically driven blind quantum computation, 2016. Eprint:arXiv:1608.04633.
11. Dan Shepherd and Michael J Bremner. Temporally unstructured quantum computation. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 465, pages 1413–1439. The Royal Society, 2009.
12. Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.