Robustness and device independence of verifiable blind quantum computing

Alexandru Gheorghiu,[1] Elham Kashefi,[1,2] and Petros Wallden[1]

[1] *School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK*
[2] *CNRS LTCI, Departement Informatique et Reseaux, Telecom ParisTech, Paris CEDEX 13, France*

Quantum mechanics opens exciting new prospects in information processing. The most notable examples are the fields of quantum cryptography, where higher level security is possible, and of quantum computation which offers greater computational power. These two fields can be combined in order to perform *secure delegated quantum computation*. In this setting, a computationally weak but trusted client delegates a computation to an untrusted but powerful quantum server. We also require that the client is able to *verify* the correctness of the computation. Verification of quantum computation is on its own right a very important task. Direct verification of quantum computation through simulation is not possible. Instead, the techniques used so far are based on *interactive proof systems* [1, 2].

A major obstacle in implementing quantum information processing devices is the loss of coherence of quantum states due to interaction with the environment. This can be modeled as noise which affects the correct operation of quantum devices. We address this problem for the verifiable blind quantum computation protocol of Fitzsimons and Kashefi (FK) [2]. This leads to three main results. First we prove that the protocol is robust, i.e. it continues to be secure and correct even when there are errors in the preparation of the quantum states. Our proof guarantees that the protocol functions given imperfect states, as long as they are close in trace distance to their ideal values. It also guarantees that an adversary cannot use these imperfections to either learn the computation or deceive the client. This is done by bounding the correlations between the input quantum states and any adversary and thus ensures security against any type of attacks, including coherent attacks. Security against such attacks is not covered in the composability framework described in [3]. We therefore had to address this issue directly in our standalone security setting.

Secondly, we give a fault tolerant construction for the FK protocol. While the protocol is robust, errors on individual qubits during the computation accumulate and we show that for a sufficiently large computation, the client will reject the outcome with high probability. Our solution is to incorporate a topologically protected error-correcting code [4, 5] into the protocol and adapt the verification procedure accordingly. This enables the correction of errors that occur during the computation, corresponding to imperfect operations of the server. We prove the security of this fault-tolerant protocol by showing that no adversary can make the client accept an incorrect output with high probability.

Our third contribution is to make the FK protocol *device independent*. Device independence is the property of a cryptographic protocol where honest participants are secure even if they do not trust their (quantum) devices, i.e. even if the devices are handed to them by adversaries as black-boxes. In our setting, device independence means that the trusted client can verify the quantum computation from the (classical) results of untrusted quantum devices. Having proven the robustness of the FK protocol, we proceed to compose it with another protocol developed by Reichardt, Unger and Vaziarni (RUV) [6]. This protocol achieves verification of two entangled, non-communicating servers using the rigidity of CHSH games. The servers are instructed to alternate between sub-protocols for state tomography, process tomography and gate teleportation. The client verifies this using statistics gathered from each sub-protocol. This approach can be used for verifiable blind quantum computation, but the construction is inefficient. We instead use only the (modified) sub-protocol of state tomography to certify the preparation of the input for the FK protocol. These input states can be made arbitrarily close to their ideal values, up to a local isometry. It is therefore crucial to prove the strong robustness property of the FK protocol. Our resulting hybrid protocol improves the efficiency while retaining device independence. Moreover, the hybrid can be further improved if one provides a more efficient technique for preparing the FK input.

An independent work addressing a similar problem appeared on arxiv [7] on the same day as our paper [8].

[1] D. Aharonov, M. Ben-Or and E. Eban. Interactive proofs for quantum computations. In *Proceedings of Innovations in Computer Science 2010,* ICS2010, p453, 2010.

[2] J. F. Fitzsimons and E. Kashefi. Unconditionally verifiable blind computation, 2012. Eprint:arXiv:1203.5217

[3] V. Dunjko, J. F. Fitzsimons, C. Portmann and R. Renner. Composable security of delegated quantum computation. In Advances in Cryptology, vol 8874 LNCS, p406. Springer Berlin Heidelberg, 2014.

[4] T. Morimae and K. Fujii. Blind topological measurement-based quantum computation. Nat. Commun. 3, 1036, 2012.

[5] R. Raussendorf, J. Harrington and K. Goyal. Topological fault-tolerance in cluster state quantum computation. New J. Phys. 9, 199, 2007.

[6] B. W. Reichardt, F. Unger and U. Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games, 2012. Eprint:arXiv:1209.0448

[7] M. Hajdušek, C. A. Pérez-Delgado and J. F. Fitzsimons. Device-independent verifiable blind quantum computation, 2015. Eprint:arXiv:1502.02563.

[8] A. Gheorghiu, E. Kashefi and P. Wallden. Robustness and device independence of verifiable blind quantum computing, 2015. Eprint:arXiv:1502.02571.