Multiparty Delegated Quantum Computing

Anna Pappa[1,2] and Elham Kashefi[1,3]

[1]*School of Informatics, University of Edinburgh, UK*
[2]*Department of Physics and Astronomy, University College London, UK*
[3]*LIP6, CNRS, University Pierre et Marie Curie, France*

Quantum computing has seen tremendous progress in the past years. However, due to limitations in scalability of quantum technologies, it seems that we are far from constructing universal quantum computers for everyday users. A more feasible solution is the delegation of computation to powerful quantum servers on the network. This solution was proposed in previous studies of Blind Quantum Computation, with guarantees for both the secrecy of the input and of the computation being performed. In this work, we further develop this idea of computing over encrypted data, to propose a multiparty delegated quantum computing protocol in the measurement-based quantum computing framework. We prove security of the protocol against a dishonest Server and against dishonest clients, under the assumption of common classical cryptographic constructions.

Introduction - Since the early days of quantum computing and cryptography, research has been focused on finding secure communication protocols for different cryptographic tasks. However, the no-go results for bit commitment [1, 2] and oblivious transfer [3] soon provided evidence that it is not possible to guarantee perfect security against any type of quantum adversaries [4]. It directly follows that two-party unitaries, and by consequence multi-party ones, cannot be used without further assumptions, to securely implement cryptographic protocols. In previous studies of two-party quantum computation ([5, 6]), access to AND and SWAP gates was required, in order to guarantee security. In the multiparty setting [7], quantum communication between all parties in addition to an honest majority, was required in order to provide security against dishonest participants.

From a different perspective, a lot of research in quantum computing has been focused on secure delegation of computation to powerful servers [8]. This is because the current state-of-the-art is still far from constructing scalable quantum devices, and it seems that the first quantum networks will rely on the use of a limited number of powerful quantum servers.

In this work, we examine the case where a number of clients holding some quantum input, want to perform a unitary operation on the state, but are lacking the computational abilities to do so, and therefore would like to delegate the computation to a Server. To be secure against coalitions of dishonest clients, all participants need to contribute to a quantum encryption process, and are therefore required to be able to create and manipulate single qubits. We use a remote state preparation procedure that does not require quantum communication between the clients and makes our protocol more suitable for a client/server setting. More interestingly, the quantum communication from the clients to the Server can be done in single-qubit rounds, not necessitating any quantum memory from the clients, and takes place only during the preparation (offline) phase, which makes the computation phase entirely classical and therefore more efficient.

As already mentioned, in order to provide any type of security in the multiparty setting, we need to make some assumptions about the dishonest parties. In this work, we will need two assumptions. First, we will assume that the clients have secure access to classical multiparty functionalities, which we will treat as oracles. This is a common construction in classical secure multiparty computation that is built on assumptions like honest majority or difficulty to invert specific one-way functions. The second assumption is that a set of malicious clients cannot corrupt the Server, and the other way around. This means that we only prove security against two adversarial models, against a dishonest Server, and against a coalition of dishonest clients. Security in the more general scenario where a Server and some clients collaborate to cheat, remains as an open question

Finally, we should note that in this work, we are focusing on proving security against malicious quantum adversaries in order to provide a simple protocol for quantum multiparty computation. As such, no guarantee is given on the correctness of the computation outcome. However, in principle, it might be possible to add verification processes in our protocol, by enforcing honest behaviour, following the work of [6] and [9].

Results - We propose a cryptographic protocol that constructs a Multiparty Delegated Quantum Computing resource using quantum and classical communication between n clients and a Server. We want to guarantee that the private data of the clients (i.e. their quantum input and output) remain secret during the protocol. The performed computation also remains hidden from the Server, and can be decided by all clients collectively or a single one, depending on the setting. The protocol consists of two stages, a preparation one, where all the quantum communication takes place, and the computation one, where the communication is purely classical. During the preparation stage, a process named "Remote State Preparation" [10] asks the clients to send quantum states to the Server, who then entangles them and

measures all but one. This process allows the clients to remotely prepare quantum states at the Server's register that are "encrypted" using secret data from all of them, without having to communicate quantum states to each other.

The above process however could allow the clients to affect the input of the other clients by changing the classical values they use throughout the protocol. We therefore ask all clients to commit to using the same classical values for the duration of the protocol by verifiably secret-sharing them. Further, to check that the clients are sending the correct quantum states at the preparation phase of the protocol, they are asked to send many copies of them, which are then (all but one) checked for validity.

At the end of the remote state preparation phase, the Server is left with several quantum states that are "encrypted" using secret data from all the clients. These states will be used to compute the desired functionality, in the Measurement-based Quantum Computing (MBQC) framework [11]. Due to the inherent randomness of the quantum measurements on the entangled state used, there is an unavoidable dependency between the measurement angles of the qubits in the different layers of the computation. This means that the clients need to securely communicate between them and with the Server to jointly compute the updated measurement angles, taking into account the necessary corrections from the previous measurements according to the dependency sets of each qubit. This procedure is purely classical, and uses Verifiable Secret Sharing (VSS) schemes to build a computation oracle that calculates the necessary values at each step of the protocol and enforces honest behavior to the clients.

Finally, in the output phase, each output qubit is naturally encrypted due to the same randomness from previous measurements that propagated during the computation. Each client receives the appropriate encrypted output qubit, and computes the values necessary for the decryption from the previously shared values of all clients.

We use the Abstract Cryptography framework [12] to prove that the protocol is indistinguishable from the ideal functionality that computes the requested unitary on the quantum input of the clients. The proofs are using teleportation and delayed measurement techniques to build a simulator for the dishonest parties, that has at no point of the protocol access to the secret data of the honest parties. This is done in a composable way, by proving that a global distinguisher cannot tell the difference when interacting with the real communication protocol and the ideal functionality.

Conclusion - In this work, we present a quantum multiparty delegated protocol that provides security for clients with limited quantum abilities, therefore extending previous results on two-party [5] and multiparty [7] computation, and combining them with recent work on delegated blind computing [8, 9, 13]. Our protocol requires no quantum memory, entangling operations or measurement devices for the clients, only that they are able (in the general case of quantum input and output) to create single qubits and apply X gates and Z rotations on them. This renders our protocol ready to implement in near-future hybrid quantum-classical networks, since clients with limited quantum abilities will be able to delegate heavy computations to a powerful quantum Server.

It is important to note that the proposed protocol can also be used in parallel or sequentially with other protocols, since security is defined in a composable framework (i.e. Abstract Cryptography). It also seems that it can easily be adapted to any blind computing model, for example the measurement-only model [14], since as mentioned in [13], all protocols with one-way communication from the Server to a client, are inherently secure due to no-signaling.

Our protocol is secure against a dishonest Server and against a coalition of malicious clients, utterly reducing to secure classical multiparty computation and the assumptions it requires to be implemented. It remains to study whether the proposed protocol remains secure against a dishonest coalition between clients and the Server or if there is an unavoidable leakage of information. A possible way to do this would be by extending the results of [15] in the multiparty setting, where both the parties and the Server have inputs in the computation. An even more interesting question is whether we can enhance our protocol to include verifiability in a similar way that is done in [9]. Finally, we have assumed that the clients will choose to act semi-honestly, since any active dishonest activity would be detected with very high probability; however, a quantitative proof of security that considers different types of attacks from the side of the clients would be an natural extention of this work.

[1] Hoi-Kwong Lo and H. F. Chau. "Is quantum bit commitment really possible?". Physical Review Letters, 78(17):3410–3413, 1997.

[2] Dominic Mayers. "Unconditionally secure quantum bit commitment is impossible". Physical Review Letters, 78(17):3414–3417, 1997.

[3] Hoi-Kwong Lo. "Insecurity of quantum secure computations". Physical Review A, 56(2):1154–1162, 1997.

[4] Louis Salvail, Christian Schaffner, Miroslava Sotakova, "On the Power of Two-Party Quantum Cryptography". In Proceedings of ASIACRYPT 2009, LNCS 5912, pages 70–87.

[5] Frédéric Dupuis, Jesper Buus Nielsen, Louis Salvail, "Secure two-party quantum evaluation of unitaries against specious adversaries". In Proceedings of CRYPTO 2010, LNCS 6223, pages 685–706.

[6] Frédéric Dupuis, Jesper Buus Nielsen and Louis Salvail, "Actively Secure Two-Party Evaluation of any Quantum

Operation". In Proc. of CRYPTO 2012, Springer Verlag, pp. 794–811.

[7] Michael Ben-Or, Claude Crépeau, Daniel Gottesman, Avinatan Hassidim, Adam Smith, "Secure Multiparty Quantum Computation with (Only) a Strict Honest Majority". In Proceedings of FOCS 2006, pp. 249-260, IEEE Press.

[8] Anne Broadbent, Joseph Fitzsimons, Elham Kashefi, "Universal blind quantum computation". In Proceedings of FOCS 2009, pp. 517-526.

[9] Joseph F. Fitzsimons, Elham Kashefi, "Unconditionally verifiable blind computation". arXiv:1203.5217 [quant-ph].

[10] Vedran Dunjko, Elham Kashefi, Anthony Leverrier, "Universal Blind Quantum Computing with Weak Coherent Pulses". Phys. Rev. Lett. 108, 200502 (2012).

[11] Robert Raussendorf and Hans J. Briegel, "A One-Way Quantum Computer". Phys. Rev. Lett. 86, 5188, 2001.

[12] Ueli Maurer and Renato Renner, "Abstract cryptography". In Innovations in Computer Science, 2011, Tsinghua University Press.

[13] Vedran Dunjko, Joseph F. Fitzsimons, Christopher Portmann, Renato Renner, "Composable security of delegated quantum computation". In Proceedings of ASIACRYPT2014, pp 406-425.

[14] Tomoyuki Morimae, Keisuke Fujii, "Blind quantum computation protocol in which Alice only makes measurements". Phys. Rev. A 87, 050301(R) (2013).

[15] Elham Kashefi, Petros Wallden, "Garbled Quantum Computation". arXiv:1606.06931 [quant-ph] (2016).