Security Limitations of Classical-Client Delegated Quantum Computing

Christian Badertscher, Alexandru Cojocaru, Léo Colisson,
Elham Kashefi, Dominik Leichtle, Atul Mantri, Petros Wallden

Secure delegated quantum computing is a two-party cryptographic primitive, where a computationally weak client wishes to delegate an arbitrary quantum computation to an untrusted quantum server in a privacy-preserving manner. Communication via quantum channels is typically assumed such that the client can establish the necessary correlations with the server to securely perform the given task. This has the downside that all these protocols cannot be put to work for the average user unless a reliable quantum network is deployed.

Therefore the question becomes relevant whether it is possible to rely solely on classical channels between client and server and yet benefit from its quantum capabilities while retaining privacy. Classical-client remote state preparation protocols ($\mathsf{RSP}_{\mathsf{CC}}$) [CCKW18, CCKW19, GV19] are promising candidates to achieve this because they enable a client, using only classical communication resources, to remotely prepare a quantum state. However, the privacy loss incurred by employing $\mathsf{RSP}_{\mathsf{CC}}$ as sub-module to avoid quantum channels is unclear.

To characterize these losses, different models of security can be used. While game-based security is useful to characterize a precise property of a protocol, the security is not guaranteed when the protocol is composed with others arbitrary protocols. In this work, we investigate the question of the security of $\mathsf{RSP}_{\mathsf{CC}}$ protocols in a stronger model of security, namely the Constructive Cryptography framework by Maurer and Renner [MR11]. Protocols proven secure in this model can be composed with arbitrary protocols, both sequentially and in parallel. We first identify the goal of $\mathsf{RSP}_{\mathsf{CC}}$ as the construction of ideal RSP resources from classical channels, we give a very general caracterization of these RSP resources that encompasses all previous usages, and then we reveal the security limitations of using $\mathsf{RSP}_{\mathsf{CC}}$ in general and in specific applications:

1. We uncover a fundamental relationship between constructing ideal RSP resources (from classical channels) and the task of cloning quantum states with auxiliary information. Any classically constructed ideal RSP resource must leak to the server the full classical description (possibly in an encoded form) of the generated quantum state, even if we target computational security only.
   As a consequence, we find that *the realization of common* RSP *resources*, without weakening their guarantees drastically, *is impossible* due to the no-cloning theorem.

2. The above result does not rule out that a specific $\mathsf{RSP}_{\mathsf{CC}}$ protocol can replace the quantum channel at least in some applications, such as the Universal Blind Quantum Computing (UBQC) protocol [BFK09]. However, we show that *the resulting* UBQC *protocol cannot maintain its proven composable security as soon as* $\mathsf{RSP}_{\mathsf{CC}}$ *is used as a subroutine.*

3. We show that *replacing the quantum channel* of the above UBQC protocol by the $\mathsf{RSP}_{\mathsf{CC}}$ protocol QFactory of [CCKW19], *preserves the weaker, game-based, security of* UBQC.

Therefore, fully composable security for classical-client $\mathsf{RSP}_{\mathsf{CC}}$ or UBQC protocols is unachievable in the plain model, and a weaker model of security must be used.

The full paper can be found in [BCC+20].

References

[BCC+20] Christian Badertscher, Alexandru Cojocaru, Léo Colisson, Elham Kashefi, Dominik Leichtle, Atul Mantri, and Petros Wallden. Security Limitations of Classical-Client Delegated Quantum Computing. *arXiv preprint arXiv:2007.01668*, 2020.

[BFK09] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 517–526. IEEE, 2009.

[CCKW18] Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. On the possibility of classical client blind quantum computing. *arXiv preprint arXiv:1802.08759*, 2018.

[CCKW19] Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. Qfactory: Classically-instructed remote secret qubits preparation. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 615–645. Springer International Publishing, 2019.

[GV19] Alexandru Gheorghiu and Thomas Vidick. Computationally-secure and composable remote state preparation. *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1024–1033, 2019.

[MR11] Ueli Maurer and Renato Renner. Abstract cryptography. In *In Innovations in Computer Science*. Citeseer, 2011.