On The Round Complexity of Two-Party Quantum Computation

James Bartusek Andrea Coladangelo Dakshita Khurana Fermi Ma

1 Introduction

Secure computation is a cornerstone of modern cryptography. It allows mutually distrusting parties to compute arbitrary functions on their private inputs, revealing only the outputs of the computation while hiding all other private information [Yao86, GMW87, BGW88, CCD88].

With the emergence of quantum computers, it becomes important to understand the landscape of secure *quantum* computation over distributed, private quantum (or classical) states. Specifically, our work focuses on the two party setting, where Alice and Bob hold (possibly entangled) quantum inputs $\mathbf{x}_A$ and $\mathbf{x}_B$ respectively, and would like to evaluate a quantum circuit Q on their joint input $(\mathbf{x}_A, \mathbf{x}_B)$. The output is of the form $Q(\mathbf{x}_A, \mathbf{x}_B) = (\mathbf{y}_A, \mathbf{y}_B)$, so at the end of the protocol Alice and Bob hold the (possibly entangled) output states $\mathbf{y}_A$ and $\mathbf{y}_B$ respectively. One of the most practically relevant properties of a two-party computation protocol is its *round complexity*, i.e. the number of rounds of interaction between Alice and Bob. In this work, we make substantial progress on the following question:

How many rounds of interaction are necessary for general-purpose two-party quantum computation?

Our work studies this question in the setting of *malicious* attackers. We would like to ensure that a malicious Alice (resp. Bob) who may arbitrarily deviate from the protocol specifications (1) can only hold information that is efficiently computable from either her input or output at any point during the protocol execution, and (2) cannot cause Bob (resp. Alice) to obtain an incorrect outcome of the protocol without being detected. These guarantees are formalized via a simulation-based security notion, which requires that no adversary can recover any information in the real world that it cannot recover in an ideal world where it simply hands its input to a trusted party who then returns the output.

The problem of secure quantum computation on distributed quantum states has a strong tradition in the quantum cryptography literature. It was first studied by [CGS02, BCG+06], who obtained unconditional maliciously-secure general *multi-party* quantum computation with honest majority. The setting where half (or more) of the players are malicious requires computational assumptions due to the impossibility of unconditionally secure quantum bit commitment [May97, LC98, DSWK06]. In the computational setting, [DNS10] gave a two-party quantum computation (2PQC) protocol secure against the quantum analogue of semi-honest adversaries (specious adversaries); this was later extended to the malicious setting by [DNS12]. A recent work of [DGJ+20] constructed maliciously-secure general multi-party quantum computation with *dishonest* majority from any maliciously-secure post-quantum classical MPC. *Importantly, all of the above protocols have round complexity polynomial in the size of the quantum circuit.*

In this work, we show that various flavors of maliciously-secure two-party quantum computation are possible in *two* or *three* rounds, in a setting where parties have access to a common random string (CRS). Along the way, we give a two-message protocol in the setting where only one party receives output — a quantum analogue of Yao's celebrated two-party computation protocol [Yao86] in the malicious setting. Additionally, we study barriers to achieving two-round secure computation where both parties obtain output, which are inherent to the quantum setting.[1]

[1] Indeed, two-round protocols are known from minimal assumptions in the classical setting.

1.1 Our Results

As mentioned, we consider the setting of two-party quantum computation where parties have access to a trusted setup, like a common random string (CRS). We study two possible models of interaction: (1) the sequential messages model, where only one party speaks in each round (i.e. Bob sends a message to Alice, in the next step Alice sends a message to Bob, and so forth), and (2) the simultaneous messages model, where in each round both parties simultaneously send messages to each other (i.e. Bob's round i message does not depend on Alice's round i message, and vice versa).

Recently, [BY20] introduced and constructed quantum garbled circuits. As an application, they describe a general-purpose three-message 2PQC and conjecture its security against *specious* (semi-honest) adversaries (a formal proof of security was outside the scope of their work). The starting point of our work is a garbling technique sketched in [BY20, §2.7], which the authors present as a simpler alternative to their main quantum garbled circuit construction. While this alternative construction sacrifices some of the efficiency guarantees of the main construction in [BY20], it enables *classical* garbling of quantum circuits. This feature turns out to be crucial for our constructions of *maliciously*-secure 2PQC.

First Result: A Round-Optimal Protocol in the Sequential Messages Model. Our first result is in the setting of sequential messages, where we obtain a 3-message protocol for two-party quantum computation, assuming post-quantum OT. This round complexity is *optimal* for the sequential message setting.

Theorem 1.1. *(Informal) There exists a 3-message (resp. 2-message) protocol for two-party quantum computation in the CRS model that delivers an output to both parties (resp. one party). This protocol satisfies simulation-based security against malicious adversaries assuming the existence of post-quantum maliciously-secure two-message oblivious transfer with straight-line simulation in the CRS model (which is known from the quantum hardness of learning with errors (QLWE)).*

We note that (two-message) secure computation of general two-party quantum functionalities where exactly one party obtains output implies (two-message) zero-knowledge arguments for QMA as a special case. Recall that zero-knowledge arguments for QMA allow a prover to convince a verifier of the validity of a QMA statement while revealing no additional information about the quantum witness. An important goal in the study of zero-knowledge protocols is to minimize interaction; while post-quantum non-interactive zero-knowledge (NIZK) arguments for NP are known in the CRS model [CCH+19, PS19], the analogous task for QMA remains open. Given the apparent difficulty of constructing NIZK arguments for QMA, many recent works have focused on this problem in the *preprocessing* setting [BG19, CVZ20, ACGH19, Shm20]. One such setting considers *designated-verifier* NIZKs, where the prover and verifier share a common *uniformly random* string, and the verifier generates a public key that the prover must use to generate proofs; verification is private and requires the corresponding secret key.

We show that the techniques underlying our malicious 2PQC also imply (reusable) malicious designated verifier (MDV-)NIZKs for QMA in the CRS model. The "malicious" requirement asks that zero knowledge hold against verifiers that generate the public key maliciously, and the "reusable" requirement states that soundness holds for multiple proofs (of potentially different statements) computed with respect to the same setup, even when the prover learns whether or not the verifier accepted each proof. This is referred to as multi-theorem security in [Shm20]. In order to obtain reusable security, we instantiate our protocol with a *reusable* classical two-party computation protocol. Such a reusable 2PC can be based on post-quantum OT (of the type needed for Theorem 1.1) plus a reusable MDV-NIZK for NP, which is known from QLWE [LQR+19]. We therefore also obtain the following.

Theorem 1.2. *(Informal) There exists a reusable MDV-NIZK for QMA with a classical CRS and classical proving key assuming the existence of post-quantum maliciously-secure two-message oblivious transfer with straight-line simulation in the CRS model, plus post-quantum reusable MDV-NIZK for NP (both of which are known from QLWE).*

The only two previous results to achieve *reusable* designated-verifier NIZKs for QMA are by Shmueli [Shm20] and Alagic et al [ACGH19]. The former is in the CRS model and assumes sub-exponential security of QLWE,

while the latter is in the quantum random oracle model (QROM), and also assumes sub-exponential security of QLWE. Crucially, both of these results require the QMA prover to have access to *many copies* of the QMA witness. We achieve reusable MDV-NIZK for QMA that only requires the prover to be in possession of a single copy of the QMA witness.

Second Result: A Two-Round Protocol with (Quantum) Preprocessing in the Simultaneous Messages Model. As discussed above, the other natural model is that parties communicate in rounds, and both players may simultaneously send each other a message in every round. In this simultaneous message model, the three-round lower bound discussed above is inapplicable and two-round protocols may conceivably exist (although one-round protocols cannot).

Our first result in this setting is a two-round protocol in a *preprocessing model*, where both players participate in an "offline" preprocessing step without knowledge of their inputs. Once inputs are available, the "online" phase of the protocol requires just two rounds of interaction (with simultaneous messages). We obtain the following:

Theorem 1.3. *There exists a protocol for two-party quantum computation with two simultaneous rounds of communication in the preprocessing model, assuming the sub-exponential quantum hardness of learning with errors (QLWE).*

In fact, we construct a *three-round protocol* in the CRS model with only two rounds of *online* communication, which implies the above theorem. A crucial ingredient that allows us to remove one round of *online* communication is quantum teleportation. To prove security of our protocol, we develop a novel delayed simulation technique, which we call "simulation via teleportation", and may be of independent interest.

Third Result: Barriers and Approaches to Two-Round Protocols with Simultaneous Messages in the CRS Model. A natural next question is whether we can remove the preprocessing step. In other words, we ask: in the simultaneous message model, is it possible to construct a two-round maliciously secure 2PQC protocol with just a common random string (CRS)?

This appears to be a fairly challenging question, and we do not fully resolve it in this work. However, we provide both negative and positive partial results, which we hope will lead to future progress on this question.

Theorem 1.4. *(Informal) Under the conjecture that there exists a quantum functionality that does not admit an instantaneous nonlocal quantum computation protocol with polynomial-size pre-processing, there exists a quantum functionality that cannot be securely computed in two rounds in the classical CRS model with an oblivious simulator.*

Towards getting around this potential barrier, we give a proof-of-concept construction of a protocol with non-oblivious simulation. Specifically, we assume a (strong) form of VBB obfuscation for quantum circuits that contain unitary and measurement gates, where the former may be classically controlled on the outcome of measurement gates. We point out, however, that VBB-obfuscation of circuits with measurement gates is potentially even more powerful than the VBB obfuscation for unitaries that was formalized in [AF16] (further discussion on this is available in the full version). Under this assumption, we obtain a two-round two-party secure quantum computation protocol in the CRS model.

Theorem 1.5. *(Informal) Two-round two-party secure quantum computation in the CRS model exists assuming a strong form of VBB or ideal obfuscation for quantum circuits as discussed above.*

We remark that while there exist (contrived) examples of functionalities that cannot be VBB obfuscated [AF16, ABDS20, ALP20], it is still plausible that many quantum functionalities can be obfuscated. However, without any candidate constructions of obfuscation for quantum circuits, we stress that our result should only be taken as a proof-of-concept.

References

[ABDS20] Gorjan Alagic, Zvika Brakerski, Yfke Dulek, and Christian Schaffner. Impossibility of quantum virtual black-box obfuscation of classical circuits. *arXiv preprint arXiv:2005.06432*, 2020.

[ACGH19] Gorjan Alagic, Andrew M Childs, Alex B Grilo, and Shih-Han Hung. Non-interactive classical verification of quantum computation. *arXiv*, pages arXiv–1911, 2019.

[AF16] Gorjan Alagic and Bill Fefferman. On quantum obfuscation. *ArXiv*, abs/1602.01771, 2016.

[ALP20] Prabhanjan Ananth and Rolando L La Placa. Secure software leasing. *arXiv preprint arXiv:2005.05289*, 2020.

[BCG+06] Michael Ben-Or, Claude Crépeau, Daniel Gottesman, Avinatan Hassidim, and Adam Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *47th FOCS*, pages 249–260. IEEE Computer Society Press, October 2006.

[BG19] Anne Broadbent and Alex B Grilo. Zero-knowledge for qma from locally simulatable proofs. *arXiv preprint arXiv:1911.07782*, 2019.

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *20th ACM STOC*, pages 1–10. ACM Press, May 1988.

[BY20] Zvika Brakerski and Henry Yuen. Quantum garbled circuits. *arXiv preprint arXiv:2006.01085*, 2020.

[CCD88] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (abstract) (informal contribution). In Carl Pomerance, editor, *CRYPTO'87*, volume 293 of *LNCS*, page 462. Springer, Heidelberg, August 1988.

[CCH+19] Ran Canetti, Yilei Chen, Justin Holmgren, Alex Lombardi, Guy N. Rothblum, Ron D. Rothblum, and Daniel Wichs. Fiat-Shamir: from practice to theory. In Moses Charikar and Edith Cohen, editors, *51st ACM STOC*, pages 1082–1090. ACM Press, June 2019.

[CGS02] Claude Crépeau, Daniel Gottesman, and Adam Smith. Secure multi-party quantum computation. In *34th ACM STOC*, pages 643–652. ACM Press, May 2002.

[CVZ20] Andrea Coladangelo, Thomas Vidick, and Tina Zhang. Non-interactive zero-knowledge arguments for qma, with preprocessing. In *Annual International Cryptology Conference*, pages 799–828. Springer, 2020.

[DGJ+20] Yfke Dulek, Alex B. Grilo, Stacey Jeffery, Christian Majenz, and Christian Schaffner. Secure multi-party quantum computation with a dishonest majority. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part III*, volume 12107 of *LNCS*, pages 729–758. Springer, Heidelberg, May 2020.

[DNS10] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 685–706. Springer, Heidelberg, August 2010.

[DNS12] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Actively secure two-party evaluation of any quantum operation. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012. Proceedings*, volume 7417 of *LNCS*, pages 794–811. Springer, 2012.

[DSWK06] Giacomo Mauro D'Ariano, D Schlingemann, RF Werner, and D Kretschmann. Quantum bit commitment revisited: the possible and the impossible. Technical report, 2006.

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987.

[LC98] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1-2):177–187, 1998.

[LQR+19] Alex Lombardi, Willy Quach, Ron D. Rothblum, Daniel Wichs, and David J. Wu. New constructions of reusable designated-verifier NIZKs. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 670–700. Springer, Heidelberg, August 2019.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414, 1997.

[PS19] Chris Peikert and Sina Shiehian. Noninteractive zero knowledge for NP from (plain) learning with errors. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part I*, volume 11692 of *LNCS*, pages 89–114. Springer, Heidelberg, August 2019.

[Shm20] Omri Shmueli. Multi-theorem (malicious) designated-verifier nizk for qma, 2020.

[Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *27th FOCS*, pages 162–167. IEEE Computer Society Press, October 1986.