Trusted centerによる量子計算の古典検証

森前　智行[1,a)]　竹内　勇貴[2]

概要：The classical channel remote state preparation (ccRSP) is an important two-party primitive in quantum cryptography. Alice (classical polynomial-time) and Bob (quantum polynomial-time) exchange polynomial rounds of classical messages, and Bob finally gets random single-qubit states while Alice finally gets classical descriptions of the states. In [T. Morimae, arXiv:2003.10712], an information-theoretically-sound non-interactive protocol for the verification of quantum computing was proposed. The verifier of the protocol is classical, but the trusted center is assumed that sends random single-qubit states to the prover and their classical descriptions to the verifier. If the trusted center can be replaced with a ccRSP protocol while keeping the information-theoretical soundness, an information-theoretically-sound classical verification of quantum computing is possible, which solves the long-standing open problem. In this paper, we show that it is not the case unless BQP is contained in MA. We also consider a general verification protocol where the verifier or the trusted center first sends quantum states to the prover, and then the prover and the verifier exchange a constant round of classical messages. We show that the first quantum message transmission cannot be replaced with a ccRSP protocol while keeping the information-theoretical soundness unless BQP is contained in AM. Furthermore, we also study the verification with the computational soundness. We show that if a ccRSP protocol satisfies a certain condition even against any quantum polynomial-time malicious prover, the replacement of the trusted center with the ccRSP protocol realizes a computationally-sound classical verification of quantum computing. The condition is weaker than the verifiability of the ccRSP. At this moment, however, there is no known ccRSP protocol that satisfies the condition. If a simple construction of such a ccRSP protocol is found, the combination of it with the trusted center verification model provides another simpler and modular proof of the Mahadev's result. We finally show that the trusted center model and its variant with the ccRSP have extractors for low-energy states. For details, see [T. Morimae and Y. Takeuchi, arXiv:2008.05033]

Classical verification of quantum computing with trusted center

1. Introduction

Whether quantum computing is classically verifiable or not is one of the most important open problems in quantum information science [1], [2], [3]. If the soundness is the computational one, the Mahadev's breakthrough [4] solves the open problem affirmatively. Or, if more than two provers, who are entangled but not allowed to communicate with each other, are allowed, the information-theoretical soundness is possible for a classical verifier [5], [6], [7], [8], [9]. In this paper, we focus on the single prover setup and the information-theoretical soundness (except for Secs. 5 and 6). Furthermore, we require that the honest prover is quantum polynomial-time, and therefore the well-known fact BQP $\subseteq$ IP does not solve the open problem.

In Ref. [10], an information-theoretically-sound non-interactive protocol for the verification of quantum computing was proposed. In this protocol, the verifier is classical, but the trusted center is assumed. The trusted center first sends random BB84 states (i.e., $|0\rangle$, $|1\rangle$, $|+\rangle \equiv \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and $|-\rangle \equiv \frac{|0\rangle-|1\rangle}{\sqrt{2}}$) to the prover, and their classical descriptions to the verifier. The prover then sends a classical

[1] 京都大学基礎物理学研究所
[2] NTT コミュニケーション科学基礎研究所
[a)] tomoyuki.morimae@yukawa.kyoto-u.ac.jp

message to the verifier. The verifier finally does classical polynomial-time computing to make the decision. (For details, see Ref. [10]. In Sec. 2 of this paper, we explain the protocol for the convenience of readers.)

The classical channel remote state preparation (ccRSP) is an important primitive in quantum cryptography. It is a two-party protocol between Alice and Bob where Alice is classical polynomial-time, and Bob is quantum polynomial-time. Alice and Bob exchange polynomial rounds of classical messages, and Bob finally gets random single-qubit states while Alice finally gets their classical descriptions. The concept of the remote state preparation was first introduced in Ref. [11] in the context of blind quantum computing. Ref. [12] studies the remote state preparation in an abstract framework for blind quantum computing. Computationally-secure ccRSP protocols have been constructed under the standard assumption in cryptography that the LWE is hard for quantum computing [13], [14], [15], [16].

If the trusted center of the protocol of Ref. [10] can be replaced with a ccRSP protocol while keeping the information-theoretical soundness, the information-theoretically-sound classical verification of quantum computing is possible, which solves the open problem affirmatively. In this paper, we show that it is not the case unless BQP $\subseteq$ MA. Because BQP $\subseteq$ MA is not believed to happen, our result suggests that the trusted center cannot be replaced with the ccRSP while keeping the information-theoretical soundness. (Actually, what we obtain is a slightly stronger result, BQP $\subseteq \mathrm{MA}_{\mathrm{BQP}}$, where $\mathrm{MA}_{\mathrm{BQP}}$ is MA with honest quantum polynomial-time Merlin. Because $\mathrm{MA}_{\mathrm{BQP}} \subseteq$ MA, we obtain BQP $\subseteq$ MA.)

The no-go result can be shown even for approximate ccRSP protocols where the prover and the verifier succeed with some probability p_{succ} even if the prover is honest, and what the prover gets is close to the ideal state.

Replacing the trusted center of Ref. [10] with the ccRSP is a natural approach to solve the open problem, but our result shows that it does not work. It does not mean the impossibility of the (information-theoretically sound) classical verification of quantum computing, because there might be another approach, but at this moment we do not know any promising approach. (For example, the combination of the FK protocol [17] with the ccRSP will not work, because the malicious unbounded prover can learn all trap information.) On the other hand, showing the impossibility of the (information-theoretically sound) classical verification of quantum computing is also difficult, because it means the separation between BQP and BPP. (If we define $\mathrm{IP}_{\mathrm{BQP}}$ as the set of decision problems that are verified by an IP protocol with an honest quantum polynomial-time prover, we have BPP $\subseteq \mathrm{IP}_{\mathrm{BQP}} \subseteq$ BQP. Therefore, $\mathrm{IP}_{\mathrm{BQP}} \neq$ BQP means BPP $\neq$ BQP.)

We also consider a general verification protocol where the verifier or the trusted center first sends quantum states to the prover, and then the prover and the verifier exchange a constant round of classical messages. We show that the first quantum message transmission cannot be replaced with a ccRSP protocol unless BQP is contained in AM. (More precisely, what we actually obtain is BQP $\subseteq \mathrm{IP}_{\mathrm{BQP}}[const]$, where $[const]$ means a constant round, but it leads to BQP $\subseteq$ AM because $\mathrm{IP}_{\mathrm{BQP}}[const] \subseteq \mathrm{IP}[const] \subseteq$ AM.)

The second proof technique can also be applied to show that replacing the trusted center in the protocol of Ref. [10] with the ccRSP is impossible unless BQP $\subseteq$ AM, but we can show a stronger result, namely, BQP $\subseteq$ MA, by using the specific structure of the protocol of Ref. [10].

We also study the verification with the computational soundness. We show that if a ccRSP protocol satisfies a certain condition even against any quantum polynomial-time malicious prover, the replacement of the trusted center of the protocol of Ref. [10] with the ccRSP protocol realizes a computationally-sound classical verification of quantum computing. The condition is weaker than the verifiability of the ccRSP. It was believed that the verifiability of a ccRSP is necessary if it is used as a subroutine of a protocol of the verification of quantum computing, but this result suggests that it is not necessarily the case. At this moment, however, no ccRSP protocol is known that satisfies the condition. If a ccRSP protocol that satisfies the condition is constructed in a simple way, the combination of it with the protocol of Ref. [10] provides another simpler and modular proof of the Mahadev's result.

We also show that the trusted center model and its variant with the ccRSP have extractors for low-energy states. A quantum proof of quantum knowledge was first introduced in Refs. [18], [19], and a classical proof of quantum knowledge was introduced in Ref. [20].

Finally, let us mention a recent related work. The paper [21] showed three results on the ccRSP in the context of blind quantum computing. First, they showed that the ccRSP cannot be composable secure under the no-cloning theorem. There is, however, a possibility that the BFK protocol [22] combined with a ccRSP protocol is still composable secure. Their second result is that it is not the case unless the no-signaling principle is violated. Finally, they showed that the BFK protocol combined with the Qfactory protocol [15] satisfies the game-based security.

This paper is organized as follows. In Sec. 2, we review the verification protocol of Ref. [10]. In Sec. 3, we show our first result, and then in Sec. 4, we show the second result on the general setup. We study the verification with the computational soundness in Sec. 5. We finally show the existance of extractors in Sec. 6. The computational soundness is considered only in the last two sections. In other sections, we implicitly assume that the malicious prover is unbounded.

2. The verification protocol of Ref. [10]

In this section, we review the verification protocol of Ref. [10]. The protocol is given in Fig. 1. It was shown in Ref. [10] that the protocol can verify any BQP problem:

Theorem 1 For any promise problem $A=(A_{yes},A_{no})$ in BQP, Protocol 1 satisfies both of the following with some c and s such that $c-s\geq\frac{1}{poly(|x|)}$:

- If $x\in A_{yes}$, the honest quantum polynomial-time prover's behavior makes the verifier accept with probability at least c.
- If $x\in A_{no}$, the verifier's acceptance probability is at most s for any (even unbounded) prover's deviation.

3. Replacement of the trusted center

Let us consider Protocol 2, which is the same as Protocol 1 except that the trusted center is replaced with a ccRSP protocol. As a ccRSP, we consider an approximate one: if the prover behaves honestly, the verifier and the prover succeed with probability p_{succ}. If they are successful, the verifier gets $(h,m)\in\{0,1\}^{N+1}$ and the prover gets an N-qubit state $\sigma_{h,m}$ with probability $P(h,m)$, where

$$\frac{1}{2}\Big\|\sum_{h,m}P(h,m)\sigma_{h,m}-\frac{1}{2^{N+1}}\sum_{h,m}\bigotimes_{j=1}^{N}H^h|m_j\rangle\langle m_j|H^h\Big\|_1\leq\epsilon$$

is satisfied for a certain small ϵ. Even if the prover behaves honestly, they fail with probability $1-p_{succ}$. Furthermore, we assume that p_{succ} is samplable in classical polynomial-time, which is a reasonable assumption because the description of the ccRSP protocol is known to the verifier.

We show that such a modified protocol is not an information-theoretically-sound verification protocol unless BQP $\subseteq$ MA$_{\rm BQP}$.

Before stating the result, let us define the class MA$_{\rm BQP}$.

0. The input is an instance $x\in A$ of a promise problem $A=(A_{yes},A_{no})$ in BQP, and a corresponding N-qubit local Hamiltonian
$$\mathcal{H}\equiv\sum_{i<j}\frac{p_{i,j}}{2}\Big(\frac{I^{\otimes N}+s_{i,j}X_i\otimes X_j}{2}+\frac{I^{\otimes N}+s_{i,j}Z_i\otimes Z_j}{2}\Big)$$
with $N=poly(|x|)$ such that if $x\in A_{yes}$ then the ground energy is less than α, and if $x\in A_{no}$ then the ground energy is larger than β with $\beta-\alpha\geq\frac{1}{poly(|x|)}$. Here, $I\equiv|0\rangle\langle 0|+|1\rangle\langle 1|$ is the two-dimensional identity operator, X_i is the Pauli X operator acting on the ith qubit, Z_i is the Pauli Z operator acting on the ith qubit, $p_{i,j}>0$, $\sum_{i<j}p_{i,j}=1$, and $s_{i,j}\in\{+1,-1\}$.
1. The trusted center uniformly randomly chooses $(h,m_1,...,m_N)\in\{0,1\}^{N+1}$. The trusted center sends $\bigotimes_{j=1}^{N}(H^h|m_j\rangle)$ to the prover. The trusted center sends (h,m) to the verifier, where $m\equiv(m_1,...,m_N)\in\{0,1\}^N$.
2. The prover does a POVM measurement $\{\Pi_{x,z}\}_{x,z}$ on the received state. When the prover is honest, the POVM corresponds to the teleportation of a low-energy state $|E_0\rangle$ of the local Hamiltonian $\mathcal{H}$ as if the states sent from the trusted center are halves of Bell pairs. The prover sends the measurement result, (x,z), to the verifier, where $x\equiv(x_1,...,x_N)\in\{0,1\}^N$ and $z\equiv(z_1,...,z_N)\in\{0,1\}^N$.
3. The verifier samples (i,j) with probability $p_{i,j}$, and accepts if and only if $(-1)^{m'_i}(-1)^{m'_j}=-s_{i,j}$, where $m'_i\equiv m_i\oplus(hz_i+(1-h)x_i)$.

図 1 The verification protocol of Ref. [10].

Definition 1 A promise problem $A=(A_{yes},A_{no})$ is in MA$_{\rm BQP}$ if and only if there exists a classical probabilistic polynomial-time verifier such that

- If $x\in A_{yes}$, there exists a quantum polynomial-time prover that sends a classical polynomial-length bit string to the verifier such that the verifier accepts with probability at least $\frac{2}{3}$.
- If $x\in A_{no}$, for any polynomial-length classical bit string from the prover (who can be unbounded), the verifier's acceptance probability is at most $\frac{1}{3}$.

It is easy to show that MA$_{\rm BQP}\subseteq$ MA. Now let us show our first result.

Theorem 2 Assume that Protocol 2 can verify any BQP problem. It means that for any promise problem $A=(A_{yes},A_{no})$ in BQP, Protocol 2 satisfies both of the following with some c and s such that $c-s\geq\frac{1}{poly(|x|)}$:

- If $x\in A_{yes}$, the honest quantum polynomial-time prover's behavior makes the verifier accept with probability at least c.
- If $x\in A_{no}$, the verifier's acceptance probability is at most s for any (even unbounded) prover's deviation.

Then, BQP $\subseteq$ MA$_{\rm BQP}$.

0. The same as the step 0 of Protocol 1.
1. The verifier and the prover run a ccRSP protocol. If the prover behaves honestly, they succeed with probability p_{succ}. If they are successful, the verifier gets $(h, m_1, ..., m_N) \in \{0,1\}^{N+1}$ and the prover gets an N-qubit state $\sigma_{h,m}$ with probability $P(h,m)$. If they fail, the verifier rejects.
2. The same as the step 2 of Protocol 1.
3. The same as the step 3 of Protocol 1.

図 2 The modified protocol.

4. More general setup

In this section, we study a more general setup and show a similar no-go result. Let us consider the verification protocol, Protocol 3. In the first step, the verifier (or the trusted center) generates quantum states $\{\rho_i\}_i$. We assume that this quantum process is a simple one (for example, ρ_i is an N-tensor product of random BB84 states), because the verifier's (or the trusted center's) quantum burden should be minimum. (If the verifier can do complicated quantum computing, there is no point in delegating quantum computing to the prover: the verifier can do the quantum computation by itself. Furthermore, if a trusted center that can do complicated quantum computing is available, the verifier has only to use it instead of interacting with the untrusted prover.)

We show that the first quantum message transmission (step 1) of Protocol 3 cannot be replaced with a ccRSP protocol unless BQP $\subseteq$ IP$_{\rm BQP}[const]$, where IP$_{\rm BQP}[const]$ is the IP with a constant round and a honest quantum polynomial-time prover. Because IP$_{\rm BQP}[const]$ $\subseteq$ IP$[const]$ $\subseteq$ AM, it means BQP $\subseteq$ AM.

Let us consider Protocol 4 that is equivalent to Protocol 3 except that the first quantum step of Protocol 3 is replaced with a ccRSP protocol. We consider a general setup where the ccRSP protocol is an approximate one: even if the prover is honest, they succeed with probability p_{succ}, and what the prover gets is a state ρ_i' with probability p_i', where ρ_i' is close to ρ_i and $\{p_i'\}_i$ is close to $\{p_i\}_i$. Furthermore, we assume that p_{succ} is known, $\{p_i'\}_i$ is samplable in classical polynomial-time, and ρ_i' can be generated in quantum polynomial-time. These assumptions are reasonable, because the description of the ccRSP protocol is known to the verifier, and $\{\rho_i'\}_i$ and $\{p_i'\}_i$ are close to $\{\rho_i\}_i$ and $\{p_i\}_i$, respectively.

Theorem 3 Assume that Protocol 4 can verify any BQP problem. It means that for any promise problem $A = (A_{yes}, A_{no})$ in BQP, Protocol 4 satisfies both of the following with some c and s such that $c - s \geq \frac{1}{poly(|x|)}$:

- If $x \in A_{yes}$, the honest quantum polynomial-time prover's behavior makes the verifier accept with probability at least c.
- If $x \in A_{no}$, the verifier's acceptance probability is at most s for any (even unbounded) prover's deviation.

Then, BQP $\subseteq$ IP$_{\rm BQP}[const]$.

Remark. Again, the theorem requires only the correctness for the ccRSP. Neither the blindness nor the verifiability is required.

1. The verifier generates a state ρ_i with probability p_i, and sends it to the prover. Or, the trusted center generates a state ρ_i with probability p_i, sends it to the prover, and sends its classical description $[\rho_i]$ to the verifier.
2. The prover and the verifier exchange a constant round of classical messages. The honest prover is quantum polynomial-time, but the malicious prover is unbounded. The verifier is classical probabilistic polynomial-time.
3. The verifier finally makes the decision.

図 3 The general protocol with quantum channel.

1. The prover and the verifier run a ccRSP protocol. If the prover is honest, with probability p_{succ}, the prover gets a state ρ_i' with probability p_i', and the verifier gets the classical description $[\rho_i']$ of ρ_i'. With probability $1 - p_{succ}$, they fail, and the prover and the verifier get an error message. If they fail, the verifier rejects.
2. The same as the step 2 of Protocol 3.
3. The same as the step 3 of Protocol 3.

図 4 The general protocol with ccRSP.

5. Computational soundness

We have seen that the replacement of the trusted center in the protocol of Ref. [10] with the ccRSP does not realize the information-theoretically-sound classical verification of quantum computing. What happens if we consider the computational soundness? In this section, we show that if a ccRSP protocol satisfies a certain condition, the protocol of Ref. [10] with the ccRSP is the classical verification of quantum computing (with the computational soundness).

Theorem 4 Assume that a ccRSP protocol satisfies the following: For any quantum polynomial-time malicious prover's deviation, the verifier gets $(h,m) \in \{0,1\}^{N+1}$ with probability

$$P(h,m) \equiv \frac{1}{2}{\rm Tr}\Big[(I_{B_1}^{\otimes M} \otimes |\phi_{h,m}\rangle\langle\phi_{h,m}|_{B_2})\rho_{B_1,B_2} \\ (I_{B_1}^{\otimes M} \otimes |\phi_{h,m}\rangle\langle\phi_{h,m}|_{B_2})\Big],$$

and the prover gets a state

$$\sigma_{h,m} \equiv \frac{1}{2P(h,m)}\mathrm{Tr}_{B_2}\Big[(I_{B_1}^{\otimes M}\otimes|\phi_{h,m}\rangle\langle\phi_{h,m}|_{B_2})\rho_{B_1,B_2} (I_{B_1}^{\otimes M}\otimes|\phi_{h,m}\rangle\langle\phi_{h,m}|_{B_2})\Big]$$

(up to a CPTP map on it), where B_1 is a subsystem of M qubits, B_2 is a subsystem of N qubits, $|\phi_{h,m}\rangle \equiv \bigotimes_{j=1}^N H^h|m_j\rangle$, ρ_{B_1,B_2} is any $(M+N)$-qubit state (that could be chosen by the prover), and Tr_{B_2} is the partial trace over the subsystem B_2. Then, if we replace the trusted center of the protocol of Ref. [10] with the ccRSP protocol, it is the classical verification of quantum computing (with the computational soundness).

We have three remarks. First, note that when

$$\rho_{B_1,B_2} = \Big(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\frac{\langle 00|+\langle 11|}{\sqrt{2}}\Big)^{\otimes N},$$

$P(h,m) = \frac{1}{2^{N+1}}$ for any (h,m) and $\sigma_{h,m} = \bigotimes_{j=1}^N H^h|m_j\rangle\langle m_j|H^h$, which corresponds to the honest prover case.

Second, the above condition is not satisfied against the unbounded malicious prover, because the unbounded malicious prover can get the classical description of $\sigma_{h,m}$ and therefore what the prover gets is not $\sigma_{h,m}$ but, for example, $\sigma_{h,m}\otimes|h,m\rangle\langle h,m|$.

Third, it was believed that the verifiability is neccesary for a ccRSP protocol when it is used as a subroutine of the verification of quantum computing: even if malicious Bob deviates during the ccRSP protocol, it should be guaranteed that the correct state is generated in Bob's place (up to his operation on it). Theorem 4 suggests that it is not necessarily the case: as long as it is guaranteed that Bob does the correct measurement (i.e., the projection $|\phi_{h,m}\rangle\langle\phi_{h,m}|$) on any state, the soundness of the verification protocol holds. It is easy to see that the verifiability is a special case of our condition: In our condition, ρ_{B_1,B_2} is any, but the verifiability requires that ρ_{B_1,B_2} is the N-tensor product of the Bell pair. Our condition is therefore weaker than the verifiability.

6. Extractors

In this section, we show that the trusted center verification protocol of Ref. [10] and its variant with the ccRSP studied in Sec. 5 have extractors for low-energy states.

Theorem 5 The protocol of Ref. [10] has a quantum polynomial-time extractor that satisfies the following. When a prover P^* makes the verifier accept an instance $x\in A$ with probability at least $1-\epsilon$, the extractor that oracle accesses to P^* outputs a state η whose expectation energy $\mathrm{Tr}(\eta\mathcal{H})$ on the local Hamiltonian $\mathcal{H}$ corresponding to x is less than ϵ.

Theorem 6 Assume that a ccRSP protocol satisfies the conditions of Theorem 4, and ρ_{B_1,B_2} can be generated in quantum polynomial-time. Then, the protocol of Ref. [10] with the ccRSP has a quantum polynomial-time extractor that satisfies the following. When a prover P^* makes the verifier accept an instance $x\in A$ with probability at least $1-\epsilon$, the extractor that oracle accesses to P^* outputs a state η whose expectation energy $\mathrm{Tr}(\eta\mathcal{H})$ on the local Hamiltonian $\mathcal{H}$ corresponding to x is less than ϵ.

参考文献

[1] D. Gottesman, 2004.
[2] D. Aharonov and U. Vazirani, Is quantum mechanics falsifiable? A computational perspective on the foundations of quantum mechanics. arXiv:1206.3686
[3] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Verification of quantum computation: an overview of existing approaches. Theory of Computing Systems **63**, 715-808 (2019); arXiv:1709.06984
[4] U. Mahadev, Classical verification of quantum computations. IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), Paris, 2018, pp.259-267; arXiv:1804.01082
[5] M. McKague, Interactive proofs for BQP via self-tested graph states. Theory of Computing **12**, 1 (2016).
[6] Z. Ji, Classical verification of quantum proofs. Proceedings of the 48th annual ACM symposium on Theory of Computing (STOC 2016) p.885 (2016).
[7] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems. Nature **496**, 456 (2013).
[8] A. B. Grilo, A simple protocol for verifiable delegation of quantum computation in one round. 46th International Colloquium on Automata, Languages, and Programming (ICALP 2019).
[9] A. Coladangelo, A. B. Grilo, S. Jeffery, and T. Vidick, Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. arXiv:1708.07359; EUROCRYPT 2019.
[10] T. Morimae, Information-theoretically-sound non-interactive classical verification of quantum computing with trusted center, arXiv:2003.10712
[11] V. Dunjko, E. Kashefi, and A. Leverrier, Blind quantum computing with weak coherent pulses, Phys. Rev. Lett. **108**, 200502 (2012).
[12] V. Dunjko and E. Kashefi, Blind quantum computing with two almost identical states. arXiv:1604.01586
[13] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick, A cryptographic test of quantumness and certifiable randomness from a single quantum device. IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), (2018); arXiv:1804.00640
[14] A. Gheorghiu and T. Vidick, Computationally-secure and composable remote state preparation. IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS), Baltimore, MD, USA, 2019, pp. 1024-1033; arXiv:1904.06320

[15] A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, QFactory: classically-instructed remote secret qubits preparation. ASIACRYPT 2019; arXiv:1904.06303

[16] T. Metger and T. Vidick, Self-testing of a single quantum device under computational assumptions. arXiv:2001.09161

[17] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind computation. Phys. Rev. A **96**, 012303 (2017).

[18] A. Broadbent and A. B. Grilo, Zero-knowledge for QMA from locally simulatable proofs, arXiv:1911.07782

[19] A. Coladangelo, T. Vidick, and T. Zhang, Non-interactive zero-knowledge arguments for QMA, with preprocessing. arXiv:1911.07546

[20] T. Vidick and T. Zhang, Classical proofs of quantum knowledge. arXiv:2005.01691

[21] C. Badertscher, A. Cojocaru, L. Colisson, E. Kashefi, D. Leichtler, A. Mantri, and P. Wallden. Security limitations of classical-client delegated quantum computing. arXiv:2007.01668

[22] A. Broadbent, J. Fitzsimons, and E. Kashefi, in Proceedings of the 50th Annual IEEE Symposiumon Foundations of Computer Science (IEEE Computer Society, Los Alamitos, CA, USA, 2009), pp. 517-526.