This is the accepted manuscript made available via CHORUS. The article has been published as:

Post hoc Verification of Quantum Computation

Joseph F. Fitzsimons, Michal Hajdušek, and Tomoyuki Morimae

Phys. Rev. Lett. **120**, 040501 — Published 22 January 2018

DOI: 10.1103/PhysRevLett.120.040501

Post hoc verification of quantum computation

Joseph F. Fitzsimons,[1, 2, *] Michal Hajdušek,[1, 2, †] and Tomoyuki Morimae[3, ‡]

[1]*Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372*
[2]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[3]*Department of Computer Science, Gunma University,*
1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan

We propose a set of protocols for verifying quantum computing at any time after the computation itself has been performed. We provide two constructions: one requires five entangled provers and completely classical verifier. The other requires a single prover, a verifier, who is restricted to measuring qubits in the X or Z basis, and one way quantum communication from the prover to the verifier. These results demonstrate that the verification can be achieved independently from the blindness. We also show that a constant round protocol with a single prover and a completely classical verifier is not possible, unless BQP is contained in the third level of the polynomial hierarchy.

As quantum technologies begin to push against the frontier of what is computationally feasible to simulate using conventional computing technologies, the question of whether it is possible to verify a quantum computation performed on untrusted hardware has become increasingly important [1]. This task can be naturally cast in terms of a two party scenario: We take Alice to be a user with limited quantum capabilities, who wishes to delegate a quantum computation to be performed by Bob, who has access to a universal quantum computer. However, Alice does not trust Bob to faithfully perform the computation. In this case, if Alice is to make use of the results obtained via Bob, she requires some method of verifying that he has performed the computation as directed.

In recent years, significant progress has been made in addressing this problem of verification. In the ideal case, Alice would be able to verify Bob's compliance through an entirely classical protocol, freeing her from the requirement of possessing some quantum capability. In computational complexity terms, it means that BQP [31] has an interactive proof system with a BQP prover and a BPP [32] verifier. Such schemes, however, have thus far proven elusive. Current approaches to this problem take one of two approaches, either allowing Alice some limited quantum capability, such as the ability to prepare [2, 3] or measure [4, 5] single qubits, or the possession of a constant sized quantum computer [6], or adding additional entangled provers to the protocol [7–12].

Across both approaches, blind quantum computation [13] has proven itself to be an important building block. Blind quantum computing is a secure quantum computing protocol where a technologically limited Alice can delegate her quantum computing to Bob without leaking the information about her quantum computation. Within the paradigm of blind computation, two distinct approaches have emerged based on the different quantum capabilities assigned to Alice. In the first case, Alice is taken to have the ability to create single qubit states, which can be sent to Bob for processing [13]. In this setting, verification of the delegated computation can be achieved by inserting isolated trap qubits into the computation [2]. In the second approach, Alice is taken to have the ability to perform single qubit measurements, rather than state preparations [14]. In this setting, verification can be achieved through the use of stabilizer measurements on qubits transmitted from Bob to Alice [5]. The relatively low technological requirements for Alice's system have already led to experimental demonstrations of both models of blind computation [15, 16], as well as trap based verification [17].

Up until very recently, all known verification protocols required interaction during the phase when the computation is performed in order to verify its correctness, effectively hiding the computation. In this paper, we propose a new verification scheme where the verification can be done in a "post hoc" way, namely, the verification itself can be done at any later time after the end of the computation. Our scheme does not exhibit blindness, and therefore our result demonstrates that the verification can be achieved independently from blindness. We provide two constructions. One requires five entangled provers and a completely classical verifier. The other requires a single prover, a verifier who has the ability to measure qubits in the X or Z basis, and one way quantum communication from the prover to the verifier. We also show that a constant round protocol with a single prover and a completely classical verifier is not possible, unless BQP is contained in the third level of the polynomial hierarchy. Such a containment is prohibited by a widely accepted conjecture in computer science.

We will restrict our focus to verifying the outcome of decision problems. (As is shown in the Appendix, we can consider more general problems.) Let L be a language in BQP, then for an instance x of size $|x|$, Alice wants to know whether $x \in L$ or $x \notin L$. Since L is in BQP, there exists, for any polynomial r, a uniformly generated polynomial size quantum circuit V_x acting on $n = \text{poly}(|x|)$ qubits such that

- if $x \in L$ then $P_{V_x}(1) \geq 1 - 2^{-r(|x|)}$,
- if $x \notin L$ then $P_{V_x}(1) \leq 2^{-r(|x|)}$,

where $P_{V_x}(1)$ is the probability of obtaining 1 when the first qubit of $V_x|0\rangle^{\otimes n}$ is measured in the computational basis.

Single prover protocol.— We now explain our first construction. Alice, the verifier, is restricted to measure individual qubits in the X or Z basis. In order to decide whether $x \in L$ or $x \notin L$, she asks Bob to run the circuit V_x on his quantum computer. Bob tells Alice the result, $x \in L$ or $x \notin L$.

Let us first consider the case when Bob tells Alice $x \in L$ and wants to make Alice believe the fact. If Bob is honest, x is really in L, but if Bob is dishonest and trying to fool Alice, x is not in L.

Since L is in BQP, it is also in QMA [33] with the trivial witness state $|0\rangle^{\otimes w}$ and the verifying circuit $W_x \equiv I^{\otimes w} \otimes V_x$ acting on $|0\rangle^{\otimes w+n}$. Hence there exists a local Hamiltonian H corresponding to the circuit W_x such that

- if $x \in L$ then the ground energy of H is $\leq a$,
- if $x \notin L$ then the ground energy of H is $\geq b$,

where $b - a \geq \frac{1}{\mathrm{poly}(|x|)}$ [18]. It is known that H can be a 2-local Hamiltonian with only X and Z operators [19].

In order to justify his claim that $x \in L$, Bob also sends a state ρ to Alice. If Bob is honest, it is a ground state of the Hamiltonian H. If we follow a similar construction as in Ref. [20] for the Hamiltonian, then this state will encode the history of the circuit via a Feynman-Kitaev clock [21, 22]. Since the witness state is the trivial state $|0\rangle^{\otimes w}$, Bob can generate such a history state in a polynomial time. If Bob is dishonest, ρ can be any state. Let us write the 2-local Hamiltonian as $H = \sum_S d_S S$, where d_S is a real number and S is a tensor product of Pauli operators where only two operators are Z or X, and others are I. We define the rescaled Hamiltonian

$$H'' = \frac{1}{\sum_S 2|d_S|} H' = \sum_S \pi_S P_S,$$

where $\pi_S = \frac{|d_S|}{\sum_S |d_S|} \geq 0$,

$$\begin{aligned} H' &= H + \sum_S |d_S| = \sum_S |d_S|(I + \mathrm{sign}(d_S)S) \\ &= \sum_S 2|d_S| P_S, \end{aligned}$$

and $P_S = \frac{I + \mathrm{sign}(d_S)S}{2}$.

In order to verify the witness, and hence the computation, Alice randomly chooses S with probability π_S, and measures S. By this we mean that Alice performs single qubit measurements of only two qubits of ρ in the X or Z basis and computes the product of the measurement results, discarding the other qubits of ρ without measuring them. Note that this does not require Alice to have a large quantum memory, as she can receive the qubits one at a time, resetting her system between reception of qubits. If she obtains the result $-\mathrm{sign}(d_S)$, she accepts. It was shown in Ref. [23] that the acceptance probability of such a procedure is

$$p_{acc} = 1 - \frac{1}{\sum_S 2|d_S|} \big(\mathrm{Tr}(H\rho) + \sum_S |d_S|\big),$$

which is

$$p_{acc} \geq \frac{1}{2} - \frac{a}{\sum_S 2|d_S|}$$

when $x \in L$, and

$$p_{acc} \leq \frac{1}{2} - \frac{b}{\sum_S 2|d_S|}$$

when $x \notin L$. Their difference is $1/\mathrm{poly}(|x|)$, and therefore Alice can distinguish the case where $x \in L$ from the case where $x \notin L$ with probability of error bounded to be exponentially small with only polynomially many repetitions. Thus Alice can make use of measurements on the witness state to ensure with arbitrarily high probability of correctness that it is in fact true that $x \in L$, as claimed by Bob.

Let us next consider the case when Bob tells Alice $x \notin L$ and wants to prove that fact. If Bob is honest, x is really not in L, but if Bob is dishonest and trying to fool Alice, x is in L.

Let us define $V_x' \equiv (I^{\otimes n-1} \otimes X)V_x$. Then, because L is in BQP,

- if $x \in L$ then $P_{V_x'}(1) \leq 2^{-r(|x|)}$,
- if $x \notin L$ then $P_{V_x'}(1) \geq 1 - 2^{-r(|x|)}$.

Therefore, there exists a local Hamiltonian H' corresponding to $W_x' \equiv I^{\otimes w} \otimes V_x'$ such that

- if $x \in L$ then the ground energy of H' is $\geq b$,
- if $x \notin L$ then the ground energy of H' is $\leq a$.

This observation is a trivial consequence of the fact that BQP is closed under complement. Running through the same procedure as in the case where $x \in L$, it then follows that the probability of Alice accepting the witness if $x \in L$ can be made exponentially small.

In the above protocol, Alice measures only two qubits of the state that Bob has sent. In principle, however, this does not need to be the case, as Alice is free to measure each incoming qubit. While we do not pursue this approach in the current manuscript, we note that it may be possible to significantly improve the performance of the verification protocol to better estimate the energy of the witness state. This could occur either by making use of the fact that products of different subsets of the results of local Pauli measurements can be used to infer the results for up to $\frac{3}{8}$ of all Pauli terms in the Hamiltonian, or by making use of a modified Hamiltonian in order to leverage gap amplification results [24].

Multi-prover protocol.— Next we explain our second construction. Ji showed that the local Hamiltonian problem has an interactive proof system with five entangled provers and a single purely classical verifier [25]. This approach mirrors that of [26], replacing the code-space and energy tests with versions that can be verified by a purely classical prover.

The code-space test is accomplished using a clever application of CHSH rigidity. Consider the 5-qubit quantum error correction code with generators $\{g_i\}_{i=1}^4$ and let $|\phi\rangle$ be a state from the 2-dimensional stabilised subspace, that is $\langle\phi|g_i|\phi\rangle = 1$ for all i. The structure of the stabiliser generators is such that one of the subsystems, labelled t, always has either a Pauli X or a Pauli Z operator acting on it. Furthermore, due to translational invariance of the 5-qubit error correction code, we have freedom of choosing the subsystem t and then fixing the remaining Pauli operators in g_i appropriately while preserving the 2-dimensional code space. By a repeated use of a reflection operator $W_t = \cos\left(\frac{\pi}{8}\right) X_t + \sin\left(\frac{\pi}{8}\right) Z_t$ on the special subsystem t, we can obtain a set of eight operators $\{h_i\}_{i=1}^8$ satisfying $\langle\phi|\sum_{i=1}^8 h_i|\phi\rangle = 4\sqrt{2}$ and that are related to the original generators by $h_{2i-1} + h_{2i} = \sqrt{2}g_i$. Bipartitioning the 5 provers into non-special provers, labelled as system A, and the special prover t, labelled as B, we obtain the familiar CHSH expressions,

$$\langle\phi|C|\phi\rangle = 2\sqrt{2}, \qquad \langle\phi|C'|\phi\rangle = 2\sqrt{2},$$

where $C = \bar{X}_A H_B^+ + \bar{X}_A H_B^- + \bar{Z}_A H_B^+ - \bar{Z}_A H_B^-$ and $C' = \bar{X}'_A H_B^+ + \bar{X}'_A H_B^- + \bar{Z}'_A H_B^+ - \bar{Z}'_A H_B^-$. The Pauli operators $\bar{X}_A$ and $\bar{X}'_A$ are defined as the generators g_i containing X_t where we replace X_t with the identity operator I. Similarly $\bar{Z}_A$ and $\bar{Z}'_A$ are defined as the generators g_i whose Z_t are replaced with I. Via the rigidity of CHSH games, it can be shown that if the probability of winning the corresponding CHSH game is close to ideal, then the shared state must be close to a state in the code-space.

The energy test is also replaced, making use of the fact that measurements of logical X and Z operators of the code can be performed transversally by appropriate Pauli measurement on each share of the logical qubit. By expanding the Hamiltonian as a sequence of Pauli terms polynomial in n. By choosing randomly to either measure a Pauli term from the Hamiltonian, or make Pauli measurements corresponding to a CHSH game, it is possible to achieve an interactive proof for the local Hamiltonian problem with entirely classical verifier, with a polynomial gap between completeness and soundness, similar to that in [26].

If the direct measurements of the energy in the previous single prover protocol is replaced with this classical interactive proof system, we can achieve the post hoc verification for completely classical verifier.

No-go result.— One defining feature of post hoc verification is that the number of rounds of communication required to verify the computation does not depend on the length of the computation itself. We conclude by showing that verification protocols with a single prover and a classical verifier cannot have this property, unless there is an unexpected collapse in computational complexity.

We proceed by means of contradiction. Let us assume that verification can be achieved with a single prover and a classical verifier, with k rounds of communication between them, for some constant k, such that the probability of Alice accepting an incorrect output of the computation is at most some constant c bounded below $\frac{1}{2}$. This in particular means that for any language $L \in$ BQP, if $x \in L$, Bob can persuade Alice of this fact, whereas if $x \notin L$ Alice cannot be persuaded. In other words, Bob and Alice exchange k classical messages and

- if $x \in L$ there exists a strategy for Bob such that Alice accepts with probability $\geq 1 - c$,
- if $x \notin L$ for any strategy of Bob, Alice accepts with probability $\leq c$.

This is entirely equivalent to the statement that BQP $\subseteq$ IP(k) [34]. However, if we combine this with the known results [27, 28] IP(k) $\subseteq$ AM($k+2$) = AM(2) $\subseteq \Sigma_3^p$, we have to conclude that BQP is contained in the third level of the polynomial hierarchy [35]. Thus, by contradiction, we must conclude that such verification protocols cannot exist unless BQP $\subseteq \Sigma_3^p$. Such an inclusion is considered extremely unlikely given the established relationships between BQP and the entire polynomial hierarchy [29].

Note that although the above rules out constant round verification of quantum computation with a purely classical verifier, it only holds in the case where there is only a single prover. In the case where multiple provers are allowed, a protocol for verification exists as shown in Ref. [26]. Furthermore, this no go result cannot be directly extended to the case of single prover protocols with polynomially many rounds, since BQP is in PSPACE = IP [30] [36]. This does not, however, imply that such protocols must exist, since the only known ways to construct such a proof make use of a prover with power to decide languages believed to be outside of BQP. Thus the question of whether a purely classical verifier can verify a single quantum prover remains an important open problem.

Public verifiability.— To conclude this paper, we mention one interesting advantage of our posthoc verification protocols, namely, a public verifiability. So far, we have considered the case when Alice is honest and Bob might be malicious. In cloud quantum computing, however, Alice, in stead of Bob, might be malicious. She might claim that Bob did not do the correct quantum computing in order to avoid the payment for the could service, although

Bob was actually honest. In our post hoc scheme, such an Alice's malicious attempt does not work, since Bob can easily prove his innocence by just sending the ground state to any trusted third party (such as a court).

TM is supported by the JST ACT-I No.JPMJPR16UP, Grant-in-Aid for Scientific Research on Innovative Areas No.15H00850 of MEXT Japan, and the JSPS Grant-in-Aid for Young Scientists (B) No.26730003 and No. 17K12637. JF acknowledges support from Singapore's Ministry of Education and National Research Foundation, and the Air Force Office of Scientific Research under AOARD grant FA2386-15-1-4082. This material is based on research funded in part by the Singapore National Research Foundation under NRF Award NRF-NRFF2013-01. This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its Competitive Research Programme (CRP Award No.NRF-CRP14-2014-02).

Appendix.— In addition to decision problems, we can turn our approach to several other types of computational problem. For example, let us consider the following problem:

Given a quantum circuit $\mathcal{C}$ composed of initial input state $|0\rangle^{\otimes n}$ followed by a polynomial number of one- and two-qubit gates chosen from some standard gate set, let M be a string obtained by sampling the output of $\mathcal{C}$ in the computational basis. Given a string S, and the promise that either the probability p_S with which $S = M$ is at least $1-\delta$ or at most $1-\delta-\gamma$ for some positive γ, the probability verification problem is to decide which of these is the case.

This problem captures the task of deciding whether S is a likely outcome of the chosen computation described by $\mathcal{C}$ or not. We will restrict attention to the case where γ is bounded from below by some inverse polynomial in the number of qubits strictly greater than zero, since in the case where the gap can be arbitrarily small this problem becomes PP-hard. The problem of verifying that S was produced according to some particular probability distribution is removed. A simple quantum circuit for this decision problem is shown in Fig. 1. Measuring the output qubit in the computational basis results in $|1\rangle$ with probability precisely equal to p_S. Provided that γ is at most polynomially small, this decision problem is then contained within BQP. This procedure can be extended to amplify the probability of accepting only when p_S is above $1-\delta$ as shown in Fig. 2.

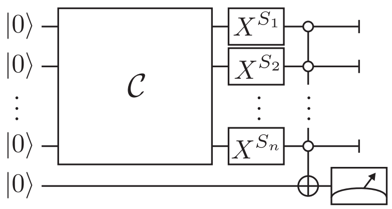

FIG. 1: A quantum circuit for verifying that S is a possible output of computation $\mathcal{C}$. The measured qubit is in state $|1\rangle$ with probability p_S. S_i is ith bit of S.

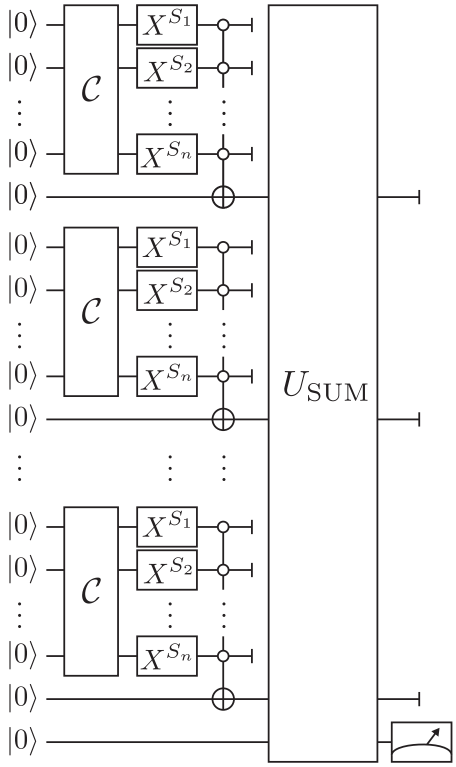

FIG. 2: A quantum circuit for verifying that S is a possible output of computation $\mathcal{C}$ with amplified probability of success. U_{SUM} performs an X gate on the final qubit conditioned on at least a fraction $1-\delta-\frac{\gamma}{2}$ of the other qubits being in state $|0\rangle$. From Hoeffding's inequality, it follows that when $p_S \geq 1-\delta$ that the probability $\tilde{p}_S$ that output qubit is measured to be in state $|1\rangle$ with probability at least $1-\exp(-\frac{N\gamma^2}{2})$, where N is the number of times $\mathcal{C}$ is evaluated. However, when $p_S \leq \epsilon$ then $\tilde{p}_S$ is at most $\exp(-\frac{N\gamma^2}{2})$.

* Electronic address: joseph_fitzsimons@sutd.edu.sg
† Electronic address: hajdusek.michal@gmail.com
‡ Electronic address: morimae@gunma-u.ac.jp

[1] D. Aharonov and U. Vazirani, arXiv preprint arXiv:1206.3686 (2012).

[2] J. F. Fitzsimons and E. Kashefi, Phys. Rev. A **96**, 012303 (2017).

[3] A. Broadbent, arXiv preprint arXiv:1509.09180 (2015).

[4] T. Morimae, Physical Review A **89**, 060302 (2014).

[5] M. Hayashi and T. Morimae, Physical Review Letters **115**, 220502 (2015).

[6] D. Aharonov, M. Ben-Or, and E. Eban, arXiv preprint arXiv:0810.5375 (2008).

[7] B. W. Reichardt, F. Unger, and U. Vazirani, Nature **496**, 456 (2013).

[8] B. W. Reichardt, F. Unger, and U. Vazirani, in *Proceedings of the 4th conference on Innovations in Theoretical Computer Science* (ACM, 2013), pp. 321–322.

[9] M. McKague, Theory of Computing **12**, 1 (2016).

[10] A. Gheorghiu, E. Kashefi, and P. Wallden, New Journal of Physics **17**, 083040 (2015).

[11] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, arXiv preprint arXiv:1502.02563 (2015).

[12] M. Hayashi and M. Hajdusek, arXiv preprint arXiv:1603.02195 (2016).

[13] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on* (IEEE, 2009), pp. 517–526.

[14] T. Morimae and K. Fujii, Physical Review A **87**, 050301 (2013).

[15] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).

[16] C. Greganti, M.-C. Roehsner, S. Barz, T. Morimae, and P. Walther, New Journal of Physics **18**, 013020 (2016).

[17] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Nature Physics **9**, 727 (2013).

[18] J. Kempe, A. Kitaev, and O. Regev, SIAM Journal on Computing **35**, 1070 (2006).

[19] J. D. Biamonte and P. J. Love, Physical Review A **78**, 012352 (2008).

[20] J. F. Fitzsimons and M. Hajdušek, arXiv preprint arXiv:1512.04375 (2015).

[21] R. P. Feynman, Foundations of physics **16**, 507 (1986).

[22] A. Y. Kitaev, A. Shen, and M. N. Vyalyi, *Classical and quantum computation*, vol. 47 (American Mathematical Society Providence, 2002).

[23] T. Morimae, D. Nagaj, and N. Schuch, Phys. Rev. A **93**, 022326 (2016).

[24] D. Aharonov, I. Arad, Z. Landau, and U. Vazirani, in *Proceedings of the forty-first annual ACM symposium on Theory of computing* (ACM, 2009), pp. 417–426.

[25] Z. Ji, arXiv preprint arXiv:1505.07432 (2015).

[26] J. Fitzsimons and T. Vidick, in *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science* (ACM, 2015), pp. 103–112.

[27] S. Goldwasser and M. Sipser, in *Proceedings of the eighteenth annual ACM symposium on Theory of computing* (ACM, 1986), pp. 59–68.

[28] S. Arora and B. Barak, *Computational complexity: a modern approach* (Cambridge University Press, 2009).

[29] S. Aaronson, in *Proceedings of the forty-second ACM symposium on Theory of computing* (ACM, 2010), pp. 141–150.

[30] E. Bernstein and U. Vazirani, SIAM Journal on Computing **26**, 1411 (1997).

[31] BQP is the class of decision problems that are solvable with polynomial-time quantum computing.

[32] BPP is the class of decision problems that are solvable with polynomial-time probabilistic classical computing.

[33] QMA is the class of decision problems that can be verified in polynomial time by a quantum computer with access to a polynomial sized witness state.

[34] IP(k) is the class of decision problems that can be verified with polynomial time classical computation and k rounds of communications with the prover.

[35] AM(k) is a subclass of IP(k) where messages from the verifier are classical random bits.

[36] PSPACE is the class of decision problems that are solvable by a classical computer with a polynomial amount of memory, but unbounded computation time.