Quantum Information and Computation, Vol. 19, No. 9&10 (2019) 0793–0806
© Rinton Press

IMPOSSIBILITY OF BLIND QUANTUM SAMPLING FOR CLASSICAL CLIENT

TOMOYUKI MORIMAE
Yukawa Institute for Theoretical Physics, Kyoto University
Kitashirakawa Oiwakecho, Sakyo-ku, Kyoto 606-8502, Japan
JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama 332-0012, Japan
tomoyuki.morimae@yukawa.kyoto-u.ac.jp

HARUMICHI NISHIMURA
Graduate School of Informatics, Nagoya University
Furocho, Chikusaku, Nagoya, Aichi, 464-8601, Japan
hnishimura@i.nagoya-u.ac.jp

YUKI TAKEUCHI
NTT Communication Science Laboratories, NTT Corporation
3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan
yuki.takeuchi.yt@hco.ntt.co.jp

SEIICHIRO TANI
NTT Communication Science Laboratories, NTT Corporation
3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan
seiichiro.tani.cs@hco.ntt.co.jp

Received April 4, 2019
Revised June 22, 2019

Blind quantum computing enables a client, who can only generate or measure single-qubit states, to delegate quantum computing to a remote quantum server in such a way that the input, output, and program are hidden from the server. It is an open problem whether a completely classical client can delegate quantum computing blindly (in the information theoretic sense). In this paper, we show that if a completely classical client can blindly delegate sampling of subuniversal models, such as the DQC1 model and the IQP model, then the polynomial-time hierarchy collapses to the third level. Our delegation protocol is the one where the client first sends a polynomial-length bit string to the server and then the server returns a single bit to the client. Generalizing the no-go result to more general setups is an open problem.

Keywords: blind quantum computing, sampling, sub-universal model
Communicated by: R Jozsa & J Eisert

1 Introduction

Blind quantum computing [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20] enables a client (Alice), who can access to only a limited quantum technology, to delegate her quantum computing to a remote quantum server (Bob) in such a way that Alice's input, output, and program are hidden from Bob. The blind quantum computing protocol proposed by Broadbent, Fitzsimons, and Kashefi [1] requires Alice to do only preparations of randomly-rotated single-qubit states. (See also Refs. [2, 3, 4].) It is open whether the requirement can be removed: it is open whether a completely classical Alice can blindly delegate quantum computing to Bob (in the information theoretic sense). Several other blind quantum computing protocols have been proposed to ease Alice's burden. For example, generating weak coherent pulses was shown to be enough instead of the single-qubit state generation [10]. Furthermore, it was shown that blind quantum computing is possible for Alice who can do only single-qubit measurements [11]. Measuring quantum states is sometimes easier than generating quantum states. However, all previous results require some minimum quantum technologies for Alice, and the possibility of blind quantum computing for completely classical Alice remains open. (Note that we are interested in the information-theoretic security. If we consider the computational one, a recent breakthrough showed that secure delegated quantum computing for completely classical Alice is possible [21]. (See also Refs. [22, 23, 24]). Furthermore, an information theoretically secure scheme (that leaks information to some extent) was also considered [25].)

Morimae and Koshiba showed that if certain one-round perfectly-secure delegated quantum computing is possible for BQP with a completely classical client, then BQP $\subseteq$ NP [26]. Since BQP is not believed to be in NP, the result suggests the impossibility of such a delegation. In their protocol, only a single round of message exchange is done between Alice and Bob, and what is sent from Bob to Alice is only a single bit. Aaronson, Cojocaru, Gheorghiu, and Kashefi considered a more general setup where poly-length messages are exchanged in poly-rounds between Alice and Bob [27, 28].

In this paper, we consider a classical blind delegation of sampling of subuniversal models. We show that the delegation is impossible unless the polynomial-time hierarchy collapses to the third level. The result holds for any subuniversal model that does not change the complexity class NQP (or that is universal under postselections, see Sec. 5). Examples are the DQC1 model [31], the IQP model [32], the depth-four model [33], the Boson Sampling model [34], the random circuit model [35], and the HC1Q model [36], etc. In our protocol, only a single-round of message exchange is done and what Bob sends to Alice is only a single bit. It is an open problem whether our no-go result is generalized to more general setups (for discussion on this point, see Sec. 6). One might think that in the case when Bob sends only a single bit to Alice, a no-go result could be shown unconditionally. However, some computational assumptions seem to be necessary. In fact, the blind delegation of BPP sampling can be done unconditionally: Alice has only to do it by herself.

This paper is organized as follows. In the next section, Sec. 2, we give some preliminaries. In Sec. 3, we explain the delegation protocol we consider. In Sec. 4, we show the no-go result for the DQC1 model. In Sec. 5, we generalize the result to other subuniversal models. Finally, in Sec. 6, we give some discussions.

2 Preliminaries

In this section, we provide some preliminaries necessary to understand the main result.

2.1 DQC1

Let us first explain the DQC1 model. The DQC1 model is a restricted model of quantum computing where all but a single input qubit are maximally mixed. It was introduced by Knill and Laflamme originally to model NMR quantum computing [31]. It is known that the

DQC1 model can efficiently solve several problems whose classical efficient solutions are not known, such as the calculation of Jones polynomials [37]. Furthermore, it was shown that output probability distributions of the DQC1 model cannot be classically efficiently sampled unless the polynomial-time hierarchy collapses [38, 39, 40, 41, 42].

Let V be a quantum circuit on n qubits. We define the probability distribution $p_V^{DQC1}:\{0,1\}\to[0,1]$ by

$$\begin{aligned} p_V^{DQC1}(0) &= \mathrm{Tr}\Big[(|0\rangle\langle 0|\otimes I^{\otimes n-1})V\Big(|0\rangle\langle 0|\otimes\frac{I^{\otimes n-1}}{2^{n-1}}\Big)V^\dagger\Big],\\ p_V^{DQC1}(1) &= \mathrm{Tr}\Big[(|1\rangle\langle 1|\otimes I^{\otimes n-1})V\Big(|0\rangle\langle 0|\otimes\frac{I^{\otimes n-1}}{2^{n-1}}\Big)V^\dagger\Big], \end{aligned}$$

where $I\equiv|0\rangle\langle 0|+|1\rangle\langle 1|$ is the two-dimensional identity operator. In this paper we consider the classical delegation of sampling of $\{p_V^{DQC1}(z)\}_{z\in\{0,1\}}$. It is known that if $\{p_V^{DQC1}(z)\}_{z\in\{0,1\}}$ is sampled in classical polynomial time with a multiplicative error $0\le\epsilon<1$, then the polynomial-time hierarchy collapses to the second level [40, 41]. Here, we say that a probability distribution $\{p_z\}_z$ is sampled in classical polynomial time with a multiplicative error ϵ if there exists a classical probabilistic polynomial-time algorithm that outputs z with probability q_z such that

$$|p_z-q_z|\le\epsilon p_z$$

for all z.

2.2 IQP

We next explain the IQP model [32, 43]. An n-qubit IQP circuit is a quantum circuit in the form of $H^{\otimes n}UH^{\otimes n}$, where H is an Hadamard gate and U is a quantum circuit that consists of only Z-diagonal gates, such as Z, CZ, CCZ, and $e^{i\theta Z}$. Here

$$\begin{aligned} Z &\equiv |0\rangle\langle 0|-|1\rangle\langle 1|,\\ CZ &\equiv I^{\otimes 2}-2|11\rangle\langle 11|,\\ CCZ &\equiv I^{\otimes 3}-2|111\rangle\langle 111|. \end{aligned}$$

Let V be an n-qubit IQP circuit. For an $m\le n$, we define the probability distribution $p_V^{IQP,m}:\{0,1\}\to[0,1]$ by

$$\begin{aligned} p_V^{IQP,m}(1) &= \big\|(|1^m\rangle\langle 1^m|\otimes I^{\otimes n-m})V|0^n\rangle\big\|^2,\\ p_V^{IQP,m}(0) &= 1-p_V^{IQP,m}(1). \end{aligned}$$

In this paper we consider the classical delegation of sampling of $\{p_V^{IQP,m}(z)\}_{z\in\{0,1\}}$ with $m=poly(n)$. It is known that if $\{p_V^{IQP,m}(z)\}_{z\in\{0,1\}}$ is sampled for certain $m=poly(n)$ in classical polynomial time with a multiplicative error $0\le\epsilon<1$, then the polynomial-time hierarchy collapses to the second level [40, 41]. (It is also known that $\{p_V^{IQP,m}(z)\}_z$ can be exactly sampled in classical polynomial time if $m=O(\log(n))$ [32].)

2.3 NQP

The complexity class NQP is a quantum version of NP and defined as follows [44]:

Definition 1. *A problem $A = (A_{yes}, A_{no})$ is in NQP if and only if there exists a polynomial-time uniformly generated family $\{V_x\}_x$ of quantum circuits such that*

- *If $x \in A_{yes}$ then $p_{V_x}(1) > 0$.*
- *If $x \in A_{no}$ then $p_{V_x}(1) = 0$.*

Here, $p_{V_x}(1) \equiv \langle 0^n|V_x^\dagger(|1\rangle\langle 1| \otimes I^{\otimes n-1})V_x|0^n\rangle$, and $n = poly(|x|)$.

It is important to point out that quantum computing in the above definition of NQP can be restricted to some subuniversal models, such as the DQC1 model or the IQP model [40, 41]. Let us define the following classes.

Definition 2. *A problem $A = (A_{yes}, A_{no})$ is in $\mathrm{NQP}_{\mathrm{DQC1}}$ if and only if there exists a polynomial-time uniformly generated family $\{V_x\}_x$ of quantum circuits such that*

- *If $x \in A_{yes}$ then $p_{V_x}^{DQC1}(1) > 0$.*
- *If $x \in A_{no}$ then $p_{V_x}^{DQC1}(1) = 0$.*

Here,

$$p_{V_x}^{DQC1}(1) \equiv \mathrm{Tr}\Big[(|1\rangle\langle 1| \otimes I^{\otimes n-1})V_x\Big(|0\rangle\langle 0| \otimes \frac{I^{\otimes n-1}}{2^{n-1}}\Big)V_x^\dagger\Big],$$

and $n = poly(|x|)$.

Definition 3. *A problem $A = (A_{yes}, A_{no})$ is in $\mathrm{NQP}_{\mathrm{IQP}}$ if and only if there exists a polynomial-time uniformly generated family $\{V_x\}_x$ of IQP circuits such that*

- *If $x \in A_{yes}$ then $p_{V_x}^{IQP,m}(1) > 0$.*
- *If $x \in A_{no}$ then $p_{V_x}^{IQP,m}(1) = 0$.*

Here $p_{V_x}^{IQP,m}(1) \equiv \|(|1^m\rangle\langle 1^m| \otimes I^{\otimes n-m})V_x|0^n\rangle\|^2$, $n = poly(|x|)$, and $m \leq n$.

Then we can show the following equivalences.

Theorem 1. [40, 41] $\mathrm{NQP} = \mathrm{NQP}_{\mathrm{DQC1}}$.

Theorem 2. [40, 41] $\mathrm{NQP} = \mathrm{NQP}_{\mathrm{IQP}}$.

For the convenience of readers, their proofs are given in Appendix A and Appendix B, respectively.

2.4 $\widehat{\mathrm{BP}}$ operator

Let K be a complexity class. The class $\widehat{\mathrm{BP}} \cdot \mathrm{K}$ is defined as follows [45].

Definition 4. *A problem $A = (A_{yes}, A_{no})$ is in $\widehat{\mathrm{BP}} \cdot \mathrm{K}$ if and only if for any polynomially bounded function $q : \mathbb{N} \to \mathbb{N}$, there exist a problem $B = (B_{yes}, B_{no})$ in K and a polynomially bounded function $r : \mathbb{N} \to \mathbb{N}$ such that for every $x \in \{0,1\}^*$, it holds that*

- *If $x \in A_{yes}$ then*

$$|\{z \in \{0,1\}^{r(|x|)} \mid \langle x, z\rangle \in B_{yes}\}| \geq (1 - 2^{-q(|x|)})2^{r(|x|)}.$$

- *If $x \in A_{no}$ then*

$$|\{z \in \{0,1\}^{r(|x|)} \mid \langle x, z\rangle \in B_{no}\}| \geq (1 - 2^{-q(|x|)})2^{r(|x|)}.$$

2.5 Advice classes

We also use advice classes [46]. Let K be any complexity class.

Definition 5. *A problem $A = (A_{yes}, A_{no})$ is in* K/poly *if and only if there exist a problem $B = (B_{yes}, B_{no})$ in* K, *an advice function $f : \mathbb{N} \to \{0,1\}^*$, and a polynomial p such that $|f(n)| \le p(n)$ for all n, and*

- *If $x \in A_{yes}$ then $\langle x, f(|x|)\rangle \in B_{yes}$.*
- *If $x \in A_{no}$ then $\langle x, f(|x|)\rangle \in B_{no}$.*

We also use a complexity class with probabilistic advice.

Definition 6. *A problem $A = (A_{yes}, A_{no})$ is in* NP/rpoly *if and only if there exist a classical probabilistic polynomial-time algorithm M and a family $\{q_s\}_{s\in\mathbb{N}}$ of probability distributions $q_s : \{0,1\}^{poly(s)} \to [0,1]$ such that*

- *If $x \in A_{yes}$ then $\Pr(M \text{ accepts}) > 0$.*
- *If $x \in A_{no}$ then $\Pr(M \text{ accepts}) = 0$.*

Here, M takes (x, b) as the input, where $b \in \{0,1\}^{poly(|x|)}$ is sampled from the probability distribution $q_{|x|}$.

3 Delegation protocol

In this section we explain the delegation protocol we consider. Let V_x be a quantum circuit on n qubits with a parameter $x \in \{0,1\}^*$. Alice wants to sample the probability distribution $\{p_{V_x}^{DQC1}(z)\}_{z\in\{0,1\}}$, where

$$p_{V_x}^{DQC1}(z) \equiv \mathrm{Tr}\Big[(|z\rangle\langle z| \otimes I^{\otimes n-1})V_x\Big(|0\rangle\langle 0| \otimes \frac{I^{\otimes n-1}}{2^{n-1}}\Big)V_x^\dagger\Big].$$

However, she is completely classical (i.e., her computational ability is classical probabilistic polynomial-time), so she delegates the sampling to Bob. Bob's computational ability is unbounded. She wants to hide the parameter x from Bob up to its size $|x|$.

Our delegation protocol consists of the following elements:

- A classical probabilistic polynomial-time key generation algorithm K. On input $x \in \{0,1\}^*$, the algorithm K outputs $k \leftarrow K(x)$ with certain probability, where $k \in \{0,1\}^{poly(|x|)}$ is a key.
- A classical deterministic polynomial-time encryption algorithm E. On input $(x,k) \in \{0,1\}^* \times \{0,1\}^{poly(|x|)}$, it outputs $a = E(x,k)$, where $a \in \{0,1\}^{poly(|x|)}$.
- A classical deterministic polynomial-time decryption algorithm D. On input $(x,k,b) \in \{0,1\}^* \times \{0,1\}^{poly(|x|)} \times \{0,1\}$, it outputs $\tau = D(x,k,b)$, where $\tau \in \{0,1\}$.

Our delegation protocol runs as follows:

1. On input $x \in \{0,1\}^*$, Alice runs the key generation algorithm K to get a key k.
2. Alice computes $a = E(x,k)$, and sends a to Bob.

3. Bob sends Alice $b \in \{0,1\}$ with probability $q_a(b)$.

4. Alice computes $\tau = D(x,k,b)$.

We require that this delegation protocol satisfies both the correctness and blindness simultaneously. Here, the correctness and blindness are defined as follows.

Definition 7. *We say that the above protocol is ϵ-correct if for any circuit V_x, any parameter x, and any key k for x, i.e., $k \leftarrow K(x)$,*

$$\begin{aligned} \left|Pr(\tau=0) - p_{V_x}^{DQC1}(0)\right| &\leq \epsilon p_{V_x}^{DQC1}(0), \\ \left|Pr(\tau=1) - p_{V_x}^{DQC1}(1)\right| &\leq \epsilon p_{V_x}^{DQC1}(1). \end{aligned}$$

Here,

$$\Pr(\tau = z) \equiv \sum_{b\in\{0,1\}} q_{E(x,k)}(b)\delta_{z,D(x,k,b)}$$

for $z \in \{0,1\}$.

It means that Alice can sample $\{p_{V_x}^{DQC1}(z)\}_{z\in\{0,1\}}$ with a multiplicative error ϵ.

Definition 8. *We say that the above protocol is blind if the following is satisfied: Let x_1 be any parameter, and k_1 be any key for x_1, i.e., $k_1 \leftarrow K(x_1)$. For any parameter x_2 such that $|x_2| = |x_1|$, the probability that $K(x_2)$ outputs k_2 such that $E(x_2,k_2) = E(x_1,k_1)$ is non-zero.*

In other words, let $P_x(a)$ be the probability that $K(x)$ outputs k such that $a = E(x,k)$. Then, the blindness means that supports of P_{x_1} and P_{x_2} are the same for any x_1 and x_2. The intuition behind Definition 8 is that if such k_2 is never generated then Bob can learn that Alice's parameter is not x_2 when he receives $E(x_1,k_1)$ from Alice.

To conclude this section, we provide several remarks. First, our delegation protocol is similar to the generalized encryption scheme (GES) of Refs. [47, 27]. However, the GES is a protocol that enables a client to delegate the calculation of $f(x)$ for a function f and input x with success probability larger than $1/2 + 1/poly(|x|)$. The computation of the value of $p_{V_x}^{DQC1}(1)$ could be delegated by using the GES, but it is stronger than what Alice wants to do, i.e., the sampling of $\{p_{V_x}^{DQC1}(z)\}_{z\in\{0,1\}}$. Second, what Bob does in our protocol is only sending a single bit to Alice, while the GES considers a more general setup: Bob sends Alice poly-length bit strings, and multiple rounds of message exchanges are done between Alice and Bob. It is an open problem whether we can generalize our no-go result for more general setups (see Sec. 6). Third, our definition of the blindness given above is a minimum one, and in fact it is a necessary condition for the more general definition of the blindness in Refs. [47, 27]. Our no-go result can be shown with any reasonable definition of the blindness as long as it includes the above definition of the blindness as a necessary condition. Finally, in our protocol, we have assumed that a valid key is always obtained. We can generalize it to the following: on input x, the key generation algorithm K outputs $(k,f) \leftarrow K(x)$. If $f = success$, k is a valid key. If $f = fail$, k is an invalid key. The probability that the key generation algorithm K outputs $f = success$ is at least $1/2 + 1/poly(|x|)$. In this case, Alice has only to run K until she gets $f = success$.

4 Result

The main result of the present paper is the following.

Theorem 3. *If the above delegation protocol satisfies both the ϵ-correctness and blindness simultaneously with* $0 \le \epsilon < 1$*, then* $\mathrm{NQP} \subseteq \mathrm{NP/poly}$*.*

Proof. Let $A = (A_{yes}, A_{no})$ be a problem in NQP. Then, from Theorem 1, A is in $\mathrm{NQP}_{\mathrm{DQC1}}$. Therefore, there exists a polynomial-time uniformly generated family $\{V_x\}_x$ of quantum circuits such that

- If $x \in A_{yes}$ then $p_{V_x}^{DQC1}(1) > 0$.
- If $x \in A_{no}$ then $p_{V_x}^{DQC1}(1) = 0$.

Let s be a natural number. Let k_s be any key for 1^s, i.e., $k_s \leftarrow K(1^s)$. Let $a_s = E(1^s, k_s)$. Bob sends Alice $b \in \{0,1\}$ with probability $q_{a_s}(b)$ when he receives a_s from Alice. Let us consider the following probabilistic algorithm with advice.

1. On input x with $|x| = s$, receive $(a_s, q_{a_s}(0))$ as advice. Note that it is advice, because both a_s and $q_{a_s}(0)$ depend only on s. (Note that we consider only quantum circuits whose acceptance probabilities can be represented exactly in poly-length bit strings, such as circuits consisting of H and Toffoli.)
2. Run the key generation algorithm K on input x. Let k be the obtained key, i.e., $k \leftarrow K(x)$. Run the encryption algorithm E on input (x, k). If $E(x,k) \neq a_s$, reject. If $E(x,k) = a_s$, then generate $b \in \{0,1\}$ with probability $q_{a_s}(b)$, and run the decryption algorithm D on input (x, k, b). Let $\xi = D(x,k,b)$, where $\xi \in \{0,1\}$. If $\xi = 1$, accept. If $\xi = 0$, reject.

Because of the correctness,

$$\left|\Pr(\xi = 1) - p_{V_x}^{DQC1}(1)\right| \quad \le \quad \epsilon p_{V_x}^{DQC1}(1)$$

for a certain $0 \le \epsilon < 1$. The acceptance probability p_{acc} of the above probabilistic algorithm with advice is

$$p_{acc} = \eta \times \Pr(\xi = 1),$$

where η is the probability that the key generation algorithm K on input x outputs a key k such that $a_s = E(x,k)$. Because of the blindness, $\eta > 0$. Hence, if $x \in A_{yes}$ then

$$p_{acc} \ge \eta(1-\epsilon) p_{V_x}^{DQC1}(1) > 0.$$

If $x \in A_{no}$ then

$$p_{acc} \le \eta(1+\epsilon) p_{V_x}^{DQC1}(1) = 0.$$

Therefore, A is in NP/poly, and we have shown $\mathrm{NQP} \subseteq \mathrm{NP/poly}$. □

The consequence, $\mathrm{NQP} \subseteq \mathrm{NP/poly}$, leads to the collapse of the polynomial-time hierarchy to the third level due to the following lemma. Because the polynomial-time hierarchy is not believed to collapse, Theorem 3 suggests the impossibility of the classical blind DQC1 sampling.

Lemma 1. *If* $\mathrm{NQP} \subseteq \mathrm{NP/poly}$*, then the polynomial-time hierarchy collapses to the third level.*

Proof. Note that

$$\mathrm{coNP} \subseteq \mathrm{PH} \subseteq \widehat{\mathrm{BP}} \cdot \mathrm{coC_{=}P} = \widehat{\mathrm{BP}} \cdot \mathrm{NQP} \subseteq \widehat{\mathrm{BP}} \cdot \mathrm{NP/poly} \subseteq \mathrm{NP/poly}.$$

Here, the second inclusion is from Corollary 2.5 of Ref. [45]. The third equality is from $\mathrm{coC_{=}P} = \mathrm{NQP}$ of Ref. [48]. The proof of the last containment, $\widehat{\mathrm{BP}} \cdot \mathrm{NP/poly} \subseteq \mathrm{NP/poly}$, is similar to that of $\mathrm{BPP} \subseteq \mathrm{P/poly}$ (see Appendix C). Finally, $\mathrm{coNP} \subseteq \mathrm{NP/poly}$ leads to the collapse of the polynomial-time hierarchy to the third level [49]. (Actually, $\mathrm{coNP} \subseteq \mathrm{NP/poly}$ leads to the stronger result $\mathrm{PH} = \mathrm{S_2^{NP}}$ [50], where $\Sigma_2^p \cup \Pi_2^p \subseteq \mathrm{S_2^{NP}} \subseteq \Sigma_3^p$.) □

5 Generalizations

In this paper, we have shown that if a classical client can blindly delegate the DQC1 sampling then the polynomial-time hierarchy collapses to the third level. It is clear that the same result holds for another subuniversal model M if $\mathrm{NQP} = \mathrm{NQP_M}$ is satisfied, where $\mathrm{NQP_M}$ is the NQP whose quantum circuits are restricted to the model M. For example, we can show the following:

Theorem 4. *If the sampling of* $\{p_V^{IQP,m}(z)\}_{z\in\{0,1\}}$ *can be classically delegated satisfying both the* ϵ*-correctness and blindness simultaneously with* $0 \leq \epsilon < 1$*, then* $\mathrm{coNP} \subseteq \mathrm{NP/poly}$*.*

Furthermore, it is clear that the same result holds for other subuniversal models M, such as the Boson Sampling model [34], the depth-4 model [33], and the random circuit model [35], because $\mathrm{NQP} = \mathrm{NQP_M}$ for these models. (It is known that these models are universal under a postselection. If we accept when the postselection is successful and the original circuit accepts, then the acceptance probability is proportional to the acceptance probability of a universal circuit. See Appendix B.)

6 Discussion

In this paper, we have considered the delegation protocol where Bob sends only a single bit to Alice. It is an open problem whether we can generalize our no-go result for more general delegation protocols. For example, what happens if Bob sends a poly-length bit string to Alice? (It is easy to see that Theorem 3 can be generalized to the delegation protocol where Bob sends Alice a log-length bit string.) Furthermore, what happens if multiple rounds of message exchanges are done between Alice and Bob?

The argument used in the proof of Theorem 3 does not seem to be directly applied to these generalized cases. For example, let us modify our delegation protocol in such a way that, instead of the single bit, Bob sends Alice a poly-length bit string $b \in \{0,1\}^{poly(|x|)}$ with probability $q_a(b)$ when he receives $a \in \{0,1\}^{poly(|x|)}$ from Alice. Then we can show the following.

Theorem 5. *If such a modified delegation protocol satisfies both the* ϵ*-correctness and blindness simultaneously with* $0 \leq \epsilon < 1$*, then* $\mathrm{NQP} \subseteq \mathrm{NP/rpoly}$*.*

Proof. Let $A = (A_{yes}, A_{no})$ be a problem in NQP. Then, from Theorem 1, A is in $\mathrm{NQP_{DQC1}}$. Therefore, there exists a polynomial-time uniformly generated family $\{V_x\}_x$ of quantum circuits such that

- If $x \in A_{yes}$ then $p_{V_x}^{DQC1}(1) > 0$.
- If $x \in A_{no}$ then $p_{V_x}^{DQC1}(1) = 0$.

Let s be a natural number. Let k_s be any key for 1^s, i.e., $k_s \leftarrow K(1^s)$. Let $a_s = E(1^s, k_s)$. Bob sends Alice $b \in \{0,1\}^{poly(s)}$ with probability $q_{a_s}(b)$ when he receives a_s from Alice. Let us consider the following probabilistic algorithm with probabilistic advice.

1. On input x with $|x| = s$, receive a_s and the probability distribution $\{q_{a_s}(b)\}_{b\in\{0,1\}^{poly(s)}}$ as advice. Note that they are advices, because both a_s and $\{q_{a_s}(b)\}_{b\in\{0,1\}^{poly(s)}}$ depend only on s.
2. Run the key generation algorithm K on input x. Let k be the obtained key, i.e., $k \leftarrow K(x)$. Run the encryption algorithm E on input (x,k). If $E(x,k) \neq a_s$, reject. If $E(x,k) = a_s$, then sample $b \in \{0,1\}^{poly(s)}$ from $\{q_{a_s}(b)\}_{b\in\{0,1\}^{poly(s)}}$, and run the decryption algorithm D on input (x,k,b). Let $\xi = D(x,k,b)$, where $\xi \in \{0,1\}$. If $\xi = 1$, accept. If $\xi = 0$, reject.

Because of the correctness,

$$\left|\Pr(\xi = 1) - p_{V_x}^{DQC1}(1)\right| \quad \leq \quad \epsilon p_{V_x}^{DQC1}(1)$$

for a certain $0 \leq \epsilon < 1$. The acceptance probability p_{acc} of the above algorithm is

$$p_{acc} = \eta \times \Pr(\xi = 1),$$

where η is the probability that the key generation algorithm K on input x outputs a key k such that $a_s = E(x,k)$. Because of the blindness, $\eta > 0$. Hence, if $x \in A_{yes}$ then

$$p_{acc} \geq \eta(1-\epsilon)p_{V_x}^{DQC1}(1) > 0.$$

If $x \in A_{no}$ then

$$p_{acc} \leq \eta(1+\epsilon)p_{V_x}^{DQC1}(1) = 0.$$

Therefore, A is in NP/rpoly, and we have shown NQP $\subseteq$ NP/rpoly. □

However, it can be shown that NP/rpoly = ALL (for a proof, see Appendix D) [52]. Therefore we cannot conclude any unlikely consequence, such as the collapse of the polynomial-time hierarchy.

Acknowledgements

TM thanks A. Gheorghiu for sending his Ph.D. thesis and answering to some questions. TM is supported by MEXT QLEAP, JST PRESTO No.JPMJPR176A and JSPS Grant-in-Aid for Young Scientists (B) No.JP17K12637. HM is supported by JSPS KAKENHI grants No. 26247016, No. 16H01705 and No. 16K00015. YT is supported by MEXT QLEAP.

References

1. A. Broadbent, J. F. Fitzsimons, and E. Kashefi, Universal blind quantum computation. Proc. of the 50th Annual IEEE Sympo. on Found. of Comput. Sci. pp.517-526 (2009).
2. A. Childs, Secure assisted quantum computation. Quant. Inf. Comput. **5**, 456 (2005).
3. P. Arrighi and L. Salvail, Blind quantum computation. Int. J. Quant. Inf. **4**, 883 (2006).
4. D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev, Interactive proofs for quantum computations. arXiv:1704.04487

5. S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Demonstration of blind quantum computing. Science **335**, 303 (2012).
6. S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Experimental verification of quantum computation. Nature Phys. **9**, 727 (2013).
7. C. Greganti, M. Roehsner, S. Barz, T. Morimae, and P. Walther, Demonstration of measurement-only blind quantum computing. New J. Phys. **18**, 013020 (2016).
8. V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, Composable security of delegated quantum computation. ASIACRYPT 2014, LNCS Volume 8874, pp.406-425 (2014).
9. J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind computation. Phys. Rev. A **96**, 012303 (2017).
10. V. Dunjko, E. Kashefi, and A. Leverrier, Blind quantum computing with weak coherent pulses. Phys. Rev. Lett. **108**, 200502 (2012).
11. T. Morimae and K. Fujii, Blind quantum computation for Alice who does only measurements. Phys. Rev. A **87**, 050301(R) (2013).
12. M. Hayashi and T. Morimae, Verifiable measurement-only blind quantum computing with stabilizer testing. Phys. Rev. Lett. **115**, 220502 (2015).
13. T. Morimae, V. Dunjko, and E. Kashefi, Ground state blind quantum computation on AKLT state. Quant. Inf. Comput. **15**, 0200-0234 (2015).
14. T. Morimae and K. Fujii, Blind topological measurement-based quantum computation. Nature Communications **3**, 1036 (2012).
15. T. Morimae, Continuous-variable blind quantum computation. Phys. Rev. Lett. **109**, 230502 (2012).
16. V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Efficient universal blind computation. Phys. Rev. Lett. **111**, 230501 (2013).
17. A. Mantri, C. Pérez-Delgado, and J. F. Fitzsimons, Optimal blind quantum computation. Phys. Rev. Lett. **111**, 230502 (2013).
18. T. Sueki, T. Koshiba, and T. Morimae, Ancilla-driven universal blind quantum computation. Phys. Rev. A **87**, 060301(R) (2013).
19. Y. Takeuchi, K. Fujii, T. Morimae, and N. Imoto, Fault-tolerant verifiable blind quantum computing with logical state remote preparation. arXiv:1607.01568
20. T. Morimae and K. Fujii, Secure entanglement distillation for double-server blind quantum computation. Phys. Rev. Lett. **111**, 020502 (2013).
21. U. Mahadev, Classical homomorphic encryption for quantum circuits. arXiv:1708.02130
22. A. Gheorghiu and T. Vidick, Computationally-secure and composable remote state preparation. arXiv:1904.06320
23. A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, QFactory: classically-instructed remote secret qubits preparation. arXiv:1904.06303
24. A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, On the possibility of classical client blind quantum computing. arXiv:1802.08759
25. A. Mantri, T. F. Demarie, N. C. Menicucci, and J. F. Fitzsimons, Flow ambiguity: a path towards classically driven blind quantum computation. Phys. Rev. X **7**, 031004 (2017).
26. T. Morimae and T. Koshiba, Impossibility of perfectly-secure delegated quantum computing for classical client. arXiv:1407.1636
27. S. Aaronson, A. Cojocaru, A. Gheorghiu, and E. Kashefi, On the implausiblity of classical client blind quantum computing. arXiv:1704.08482
28. Theorem 3 of Ref. [27], which roughly says that "if a classical blind delegation of Boson Sampling is possible, then the polynomial-time hierarchy collapses to the fourth level", contains an error [29]. On the other hand, another result, which roughly says that "if a classical blind delegation of Boson Sampling is possible, then the permanent can be computed with a small size circuit" is shown in Ref. [30].
29. A. Gheorghiu, private communications.
30. A. Gheorghiu, Ph.D. thesis, University of Edinburgh (2018).

31. E. Knill and R. Laflamme, Power of one bit of quantum information. Phys. Rev. Lett. **81**, 5672 (1998).
32. M. J. Bremner, R. Jozsa, and D. J. Shepherd, Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. Proc. R. Soc. A **467**, 459 (2011).
33. B. M. Terhal and D. P. DiVincenzo, Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games. Quant. Inf. Comput. **4**, 134-145 (2004).
34. S. Aaronson and A. Arkhipov, The computational complexity of linear optics. Theory of Computing **9**, 143-252 (2013).
35. A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, On the complexity and verification of quantum random circuit sampling. Nat. Phys. 2018
36. T. Morimae, Y. Takeuchi, and H. Nishimura, Merlin-Arthur with efficient quantum Merlin and quantum supremacy for the second level of the Fourier hierarchy. Quantum **2**, 106 (2018).
37. P. W. Shor and S. P. Jordan, Estimating Jones polynomials is a complete problem for one clean qubit. Quant. Inf. Comput. **8**, 681-714 (2008).
38. T. Morimae, Hardness of classically sampling one clean qubit model with constant total variation distance error. Phys. Rev. A **96**, 040302(R) (2017).
39. T. Morimae, K. Fujii, and H. Nishimura, Power of one non-clean qubit. Phys. Rev. A **95**, 042336 (2017).
40. K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Impossibility of classically simulating one-clean-qubit model with multiplicative error. Phys. Rev. Lett. **120**, 200502 (2018).
41. K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Power of quantum computation with few clean qubits. Proceedings of 43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016), pp.13:1-13:14 (2016).
42. T. Morimae, K. Fujii, and J. F. Fitzsimons, Hardness of classically simulating one clean qubit model. Phys. Rev. Lett. **112**, 130502 (2014).
43. M. J. Bremner, A. Montanaro, and D. J. Shepherd, Average-case complexity versus approximate simulation of commuting quantum computations. Phys. Rev. Lett. **117**, 080501 (2016).
44. L. Adleman, J. DeMarrais, and M. Huang, Quantum computability. SIAM J. Comput. **26**, 1524-1540 (1997).
45. S. Toda and M. Ogiwara, Counting classes are at least as hard as the polynomial-time hierarchy. SIAM Journal on Computing **21**, 316-328 (1992).
46. R. M. Karp and R. J. Lipton, Some connections between nonuniform and uniform complexity classes. Proceedings of the twelfth annual ACM symposium on theory of computing (STOC '80), pp.302-309 (1980).
47. M. Abadi, J. Feigenbaum, and J. Kilian, On hiding information from an oracle. Journal of Computer and System Sciences **39**, 21-50 (1989).
48. S. Fenner, F. Green, S. Homer, and R. Pruim, Determining acceptance probability for a quantum computation is hard for the polynomial hierarchy. Proceedings of the Royal Society A **455**, 3953-3966 (1999).
49. C. K. Yap. Some consequences of non-uniform conditions on uniform classes. Theoretical Computer Science 26, 287-300 (1983).
50. J. Y. Cai, V. T. Chakaravarthy, L. A. Hemaspaandra, and M. Ogihara, Competing provers yield improved Karp-Lipton collapse results. Information and Computation **198**, 1-23 (2005).
51. S. Aaronson, Limitations of quantum advice and one-way communication. Theory of Computing **1**, pp.1-28 (2005).
52. One might think that this seems strange as MA/rpoly = NP/poly [53] while NP is in MA. However, adding randomized (or quantum) advice may change the inclusion order of the original complexity classes. In our case, the definition of NP based on a probabilistic Turing machine (the unbounded-error acceptance criterion) is crucial to make NP/rpoly = ALL.
53. S. Aaronson, QMA/qpoly is contained in PSPACE/poly: De-Merlinizing quantum protocols. In Proceedings of IEEE Complexity 2006, pp.261-273 (2006).

Appendix A Proof of Theorem 1

The inclusion NQP $\supseteq$ NQP$_{\rm DQC1}$ is trivial. Let us show the other inclusion NQP $\subseteq$ NQP$_{\rm DQC1}$. Let $A=(A_{yes},A_{no})$ be a problem in NQP. Then, there exists a polynomial-time uniformly generated family $\{V_x\}_x$ of quantum circuits such that

- If $x\in A_{yes}$ then $p_{V_x}(1)>0$.
- If $x\in A_{no}$ then $p_{V_x}(1)=0$.

Here, $p_{V_x}(1)\equiv \|(|1\rangle\langle 1|\otimes I^{\otimes n-1})V_x|0^n\rangle\|^2$. Let us define the $(n+2)$-qubit circuit W_x as is shown in Fig. A.1. Then,

- If $x\in A_{yes}$ then $0<p_{W_x}(1)<1$.
- If $x\in A_{no}$ then $p_{W_x}(1)=0$.

Here, $p_{W_x}(1)\equiv \|(|1\rangle\langle 1|\otimes I^{\otimes n+1})W_x|0^{n+2}\rangle\|^2$. From W_x, we construct the DQC1 model of Fig. A.2. By the straightforward calculation, it is clear that the probability $\tilde{p}$ of obtaining 1 when the first qubit of the DQC1 model of Fig. A.2 is measured in the computational basis is

$$\tilde{p}=\frac{4p_{W_x}(1)(1-p_{W_x}(1))}{2^{n+2}}.$$

Therefore, if $x\in A_{yes}$ then $\tilde{p}>0$, and if $x\in A_{no}$ then $\tilde{p}=0$, which means that A is in NQP$_{\rm DQC1}$. Hence we have shown NQP $\subseteq$ NQP$_{\rm DQC1}$.

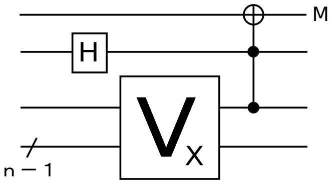

Fig. A.1. The circuit W_x. M means the computational-basis measurement. The line with the slash / means the set of $n-1$ qubits.

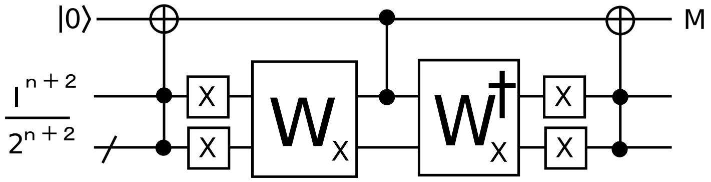

Fig. A.2. The DQC1 model constructed from W_x. The line with the slash / means the set of $n+1$ qubits. A gate acting on this line is applied on each qubit. M is the computational-basis measurement.

Appendix B Proof of Theorem 2

Since NQP $\supseteq$ NQP$_{\rm IQP}$ is trivial, let us show NQP $\subseteq$ NQP$_{\rm IQP}$. Let $A=(A_{yes},A_{no})$ be a problem in NQP. Then there exists a polynomial-time uniformly generated family $\{V_x\}_x$ of quantum circuits such that

- If $x \in A_{yes}$ then $p_{V_x}(1) > 0$.
- If $x \in A_{no}$ then $p_{V_x}(1) = 0$.

Here, $p_{V_x}(1) \equiv \|(|1\rangle\langle 1| \otimes I^{\otimes n-1})V_x|0^n\rangle\|^2$. Since the IQP model is universal under a postselection, for any V_x there exist an IQP circuit W_x and $s = poly(|x|)$ such that

$$\frac{(|1^s\rangle\langle 1^s| \otimes I^{\otimes n})W_x|0^{n+s}\rangle}{\sqrt{2^{-s}}} = |1^s\rangle \otimes (V_x|0^n\rangle).$$

Therefore

$$p_{W_x}^{IQP,s+1}(1) = \left\|(|1^{s+1}\rangle\langle 1^{s+1}| \otimes I^{\otimes n-1})W_x|0^{n+s}\rangle\right\|^2 = \frac{p_{V_x}(1)}{2^s}.$$

Therefore if $x \in A_{yes}$ then $p_{W_x}^{IQP,s+1}(1) > 0$, and if $x \in A_{no}$ then $p_{W_x}^{IQP,s+1}(1) = 0$. Hence A is in $\mathrm{NQP}_{\mathrm{IQP}}$, and we have shown $\mathrm{NQP} \subseteq \mathrm{NQP}_{\mathrm{IQP}}$.

Appendix C Proof of $\widehat{\mathrm{BP}} \cdot \mathrm{NP/poly} \subseteq \mathrm{NP/poly}$

One way of showing it is to combine Lemma 2.12 of Ref. [45], $\widehat{\mathrm{BP}} \cdot \mathrm{K} \subseteq \mathrm{K/poly}$, with $(\mathrm{K/poly})/\mathrm{poly} \subseteq \mathrm{K/poly}$.

Here, for the convenience of readers, we provide a direct proof. Let $A = (A_{yes}, A_{no})$ be a problem in $\widehat{\mathrm{BP}} \cdot \mathrm{NP/poly}$. Then, for any polynomially bounded function $q : \mathbb{N} \to \mathbb{N}$, there exist a problem $B = (B_{yes}, B_{no})$ in NP/poly and a polynomially bounded function $r : \mathbb{N} \to \mathbb{N}$ such that for every $x \in \{0,1\}^*$ it holds that

- If $x \in A_{yes}$, then
$$\left|\{z \in \{0,1\}^{r(|x|)} \mid \langle x, z\rangle \in B_{yes}\}\right| \geq 2^{r(|x|)}(1 - 2^{-q(|x|)}).$$
- If $x \in A_{no}$, then
$$\left|\{z \in \{0,1\}^{r(|x|)} \mid \langle x, z\rangle \in B_{no}\}\right| \geq 2^{r(|x|)}(1 - 2^{-q(|x|)}).$$

Let us take $q(n) = n + 1$. For each $x \in A_{yes} \cap \{0,1\}^n$, the number of $z \in \{0,1\}^r$ such that $\langle x, z\rangle \notin B_{yes}$ is at most $2^{r(n)-q(n)}$. For each $x \in A_{no} \cap \{0,1\}^n$, the number of $z \in \{0,1\}^r$ such that $\langle x, z\rangle \notin B_{no}$ is at most $2^{r(n)-q(n)}$. Therefore, there exists at least one $z \in \{0,1\}^r$ such that for all $x \in \{0,1\}^n$

- If $x \in A_{yes}$ then $\langle x, z\rangle \in B_{yes}$.
- If $x \in A_{no}$ then $\langle x, z\rangle \in B_{no}$.

Let $\tilde{z}_n$ be such z. Then, there exists an advice $\{\tilde{z}_n\}_n$ such that for all $x \in \{0,1\}^*$

- If $x \in A_{yes}$ then $\langle x, \tilde{z}_{|x|}\rangle \in B_{yes}$.
- If $x \in A_{no}$ then $\langle x, \tilde{z}_{|x|}\rangle \in B_{no}$.

Since $B = (B_{yes}, B_{no})$ is in NP/poly, there exists a problem $C = (C_{yes}, C_{no})$ in NP and advice $\{\eta_n\}_n$ such that

- If $y \in B_{yes}$ then $\langle y, \eta_{|y|} \rangle \in C_{yes}$.
- If $y \in B_{no}$ then $\langle y, \eta_{|y|} \rangle \in C_{no}$.

Therefore,

- If $x \in A_{yes}$ then $\langle x, \tilde{z}_{|x|}, \eta_{|\langle x, \tilde{z}_{|x|} \rangle|} \rangle \in C_{yes}$.
- If $x \in A_{no}$ then $\langle x, \tilde{z}_{|x|}, \eta_{|\langle x, \tilde{z}_{|x|} \rangle|} \rangle \in C_{no}$.

Hence we have shown A is in NP/poly.

Appendix D Proof of NP/rpoly = ALL

Here we show NP/rpoly = ALL. The proof is essentially the same as that of PP/rpoly = ALL [51].

Let $A = (A_{yes}, A_{no})$ be any problem. Let $f : \{0,1\}^* \to \{0,1,\perp\}$ be a function such that $f(x) = 1$ if and only if $x \in A_{yes}$, and $f(x) = 0$ if and only if $x \in A_{no}$. Let $q_s : \{0,1\}^s \times \{0,1,\perp\} \to [0,1]$ be the probability distribution such that

$$q_s(x,y) = \begin{cases} \frac{1}{2^s} & y = f(x) \\ 0 & y \neq f(x) \end{cases}$$

for all $(x,y) \in \{0,1\}^s \times \{0,1,\perp\}$. Let us consider the following probabilistic algorithm with probabilistic advice:

1. On input x with $|x| = s$, receive the probability distribution q_s as advice.
2. Sample (x', y) from q_s. If $x' \neq x$, reject. If $x' = x$, see y. If $y = 1$, accept. If $y \neq 1$, reject.

If $x \in A_{yes}$, the acceptance probability p_{acc} is

$$p_{acc} = \frac{1}{2^s} \times 1 > 0.$$

If $x \in A_{no}$, the acceptance probability p_{acc} is

$$p_{acc} = \frac{1}{2^s} \times 0 = 0.$$

Therefore, A is in NP/rpoly.