Quantum Information and Computation, Vol. 19, No. 3&4 (2019) 0214–0221

IMPOSSIBILITY OF PERFECTLY-SECURE ONE-ROUND DELEGATED QUANTUM COMPUTING 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
Department of Computer Science, Gunma University
1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan
tomoyuki.morimae@yukawa.kyoto-u.ac.jp

TAKESHI KOSHIBA

Faculty of Education and Integrated Arts and Sciences, Waseda University
Nishi-waseda 1-6-1, Shinjuku-ku, Tokyo 169-8050, Japan
tkoshiba@waseda.jp

Received November 13, 2018
Revised February 27, 2019

Blind quantum computing protocols enable a client, who can generate or measure single-qubit states, to delegate quantum computing to a remote quantum server protecting the client's privacy (i.e., input, output, and program). With current technologies, generations or measurements of single-qubit states are not too much burden for the client. In other words, secure delegated quantum computing is possible for "almost classical" clients. However, is it possible for a "completely classical" client? Here we consider a one-round perfectly-secure delegated quantum computing, and show that the protocol cannot satisfy both the correctness (i.e., the correct result is obtained when the server is honest) and the perfect blindness (i.e., the client's privacy is completely protected) simultaneously unless BQP is in NP. Since BQP is not believed to be in NP, the result suggests the impossibility of the one-round perfectly-secure delegated quantum computing.

Keywords: blind quantum computing
Communicated by: R Jozsa & J Eisert

1 Introduction

Imagine that Alice who does not have any sophisticated quantum technology wants to factorize a large integer. She has a rich friend, Bob, who owns a full-fledged scalable quantum computer. Alice wants Bob to do the factoring for her. However, the problem is that Alice does not trust Bob, and therefore she does not want to reveal her input, output, and the program (in this case Shor's factoring algorithm) to Bob. Can she delegate her quantum computation to Bob while protecting her privacy?

Broadbent, Fitzsimons, and Kashefi [1] theoretically showed that such a secure delegated quantum computing is indeed possible if some minimum quantum technology is assumed for the client. In the protocol of Ref. [1] (Fig. 1), Alice, a client, has a device that emits

randomly rotated single qubit states. She sends these states to Bob, the server, who has the full quantum technology. Alice and Bob are also connected with a two-way classical channel. Bob performs quantum computing by using qubits sent from Alice and classical messages exchanging with Alice via the classical channel. After finishing his quantum computation, Bob sends the output of his computation, which is a classical message, to Alice. This message encrypts the result of Alice's quantum computing, which is not accessible to Bob. Alice decrypts the message, and obtains the desired result of her quantum computing. (Ref. [1] also proposed a quantum input and quantum output protocol.) It was shown in Ref. [1] that whatever Bob does, he cannot learn anything about the input, the program, and the output of Alice's computation (except for some unavoidable leakage, such as upperbounds of the sizes of the input, output, and program, etc.). Proof-of-principle experiments were also done with photonic qubits [2, 3, 4]. The composable security of the protocol was also shown in Ref. [5].

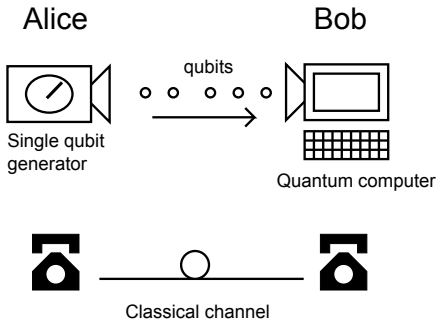

Fig. 1. The blind quantum computing protocol proposed in Ref. [1]. Alice possesses a device that emits randomly-rotated single-qubit states. Bob has a universal quantum computer. Alice and Bob share a two-way classical channel.

In the protocol, the client has to possess a device that generates single qubit states. Generations of single qubit states are ubiquitous in today's laboratories, and therefore not too much burden for the client. In other words, "almost classical" client can enjoy secure delegated quantum computing.

However, isn't it possible to realize secure delegated quantum computing for a "completely classical" client (Fig. 2)? Motivated by this question (and by other important questions such as the verifiability [6]), many variant protocols for blind quantum computing have been proposed [8, 6, 7, 10, 11, 12, 13, 14, 15, 9, 16, 17, 28]. For example, it was shown that, instead of single-qubit states, the client has only to generate weak coherent pulse states if we add more burden to the server [7]. Coherent states are considered as "more classical" than single-photon states, and therefore it enables secure delegated quantum computing for "more classical" client. It was also shown that secure delegated quantum computing is possible for a client who can only measure states [8, 9] (Fig. 3). A measurement of a bulk state with a threshold detector is sometimes much easier than the single-photon generation, and therefore the protocol also enables "more classical" client. However, these protocols still require the client to have some minimum quantum technologies, namely the generation of weak coherent pulses or measurements of quantum states. In fact, all protocols proposed so far require the client to have some minimum quantum abilities, such as generations or measurements of quantum states. (If we have two quantum servers, a completely classical

client can delegate quantum computing [1], but in this case, we have to assume that two servers cannot communicate with each other.)

In short, the possibility of a perfectly-secure delegated quantum computing for a completely-classical client is open. (Note that the perfect security means that an encrypted text gives no information about the plain text [18]. It is a typical security notion in the information theoretical security.)

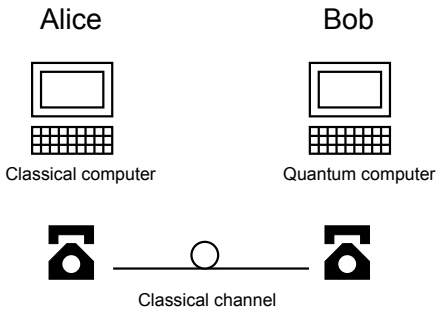

Fig. 2. The secure delegated quantum computing for a classical client. Alice has only a classical computer, whereas Bob has a universal quantum computer. Alice and Bob share a two-way classical channel.

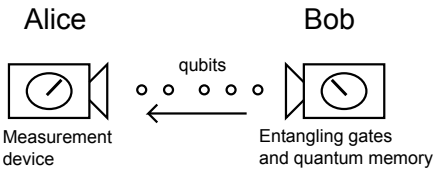

Fig. 3. The blind quantum computing protocol proposed in Refs. [8, 9]. Alice possesses a device that measure qubits. Bob has the ability of generating and storing entangled many-qubit states.

In this paper, we consider one-round perfectly-secure delegated quantum computing for a completely-classical client. We show that unless BQP $\subseteq$ NP it is impossible to satisfy both the correctness and the blindness simultaneously (Theorem below). The definitions of the correctness and blindness are given in Definition 1 and Definition 2 below, respectively. The containment of BQP in NP is not believed to happen [25, 26], and therefore the result suggests the impossibility of one-round perfectly-secure delegated quantum computing for a completely-classical client.

2 Setup

We first explain one-round perfectly-secure delegated quantum computing for a completely-classical client. Alice is completely classical, i.e., she has only a probabilistic polynomial-time Turing machine. Alice wants to solve a BQP problem. In other words, she wants to decide whether $x \in L$ or $x \notin L$ for an instance x of a language L in BQP. However, Alice cannot do it by herself (unless BQP = BPP), and therefore she delegates the computation to Bob as follows.

1. Alice generates a private key $k \in K$, where K is the set of valid keys. The key generation

operation can be done in classical polynomial time. We assume that checking the validness of a key can be done in classical polynomial time. (Or, we assume that all bit strings are valid keys.) She then encrypts L and x as $E_k(L,x)$, where E is the encryption operation, which is deterministic and in classical polynomial time. She sends $E_k(L,x)$ to Bob.

2. Bob sends Alice 0 with probability $p_{Bob}(0|E_k(L,x))$ and 1 with probability $p_{Bob}(1|E_k(L,x)) = 1 - p_{Bob}(0|E_k(L,x))$.

3. Alice calculates the decrypting bit $d_k(L,x) \in \{0,1\}$, which can be calculated deterministically and in classical polynomial time. (It can be computed before she receives a bit from Bob.) She accepts if and only if

$$d_k(L,x) \oplus (\text{the bit sent from Bob}) = 1.$$

When $d_k(L,x) = 0$, Bob has to send 1 to make Alice accept. On the other hand, if $d_k(L,x) = 1$, Bob has to send 0 to make Alice accept. In other words, Bob's bit has to be equal to $d_k(L,x) \oplus 1$ to make Alice accept. Therefore, for fixed L, x, and k, Alice's acceptance probability $p_{Alice}(acc|L,x,k)$ is

$$p_{Alice}(acc|L,x,k) = p_{Bob}(d_k(L,x) \oplus 1|E_k(L,x)).$$

We define the correctness and blindness as follows.

Definition 1 [Correctness] We say that a protocol is correct if the following is satisfied. For any language $L \in$ BQP, instance x, and private key $k \in K$, if $x \in L$ then

$$p_{Alice}(acc|L,x,k) \geq c,$$

while if $x \notin L$ then

$$p_{Alice}(acc|L,x,k) \leq s,$$

where $c > \frac{1}{2}$, $0 \leq s < c \leq 1$, and $c - s \geq 1/poly(|x|)$.

Definition 2 [Blindness] Informally, blindness means that Bob cannot learn anything about Alice's (L,x) from $E_k(L,x)$. More formaly, we say that an encryption is blind if the following is satisfied. For any $L_1, L_2 \in$ BQP, valid key k_1, $x_1 \in L_1$, and $x_2 \in L_2$, there exists a valid key k_2 such that

$$E_{k_1}(L_1,x_1) = E_{k_2}(L_2,x_2).$$

Note that the above delegation protocol is not the most general one. First, the encryption operation by Alice is deterministic and symmetric. It is open whether we can consider more generalized encryptions. Second, Bob sends only a single bit of message to Alice. (Regarding this point, see the Discussion section.) Finally, Alice's decryption operation is not the most general one.

3 Result

Now we show our main result:

Theorem If the above protocol satisfies both the correctness and blindness simultaneously, then BQP $\subseteq$ NP.

Proof.— Let L be a language in BQP. We show that the following NP protocol can verify L.

1. Merlin sends polynomial-length classical bit strings w and w_0 to Arthur. If Merlin is honest, w_0 is any private key from K, and w is a key from K that satisfies

$$E_{w_0}(L_0, 0) = E_w(L, x), \tag{1}$$

   where

$$L_0 \equiv \{x \in \{0,1\}^* \mid \text{the first bit of } x \text{ is } 0\}.$$

   Obviously, $0 \in L_0$ and $L_0 \in$ BQP. Note that such w always exists for any w_0, since otherwise Bob can learn that Alice's computation is not (L, x) when he receives $E_{w_0}(L_0, 0)$, which contradicts the blindness.

2. Arthur checks whether w and w_0 are valid keys. (We have assumed that the check can be done in classical polynomial time, or all bit strings are valid keys.) If at least one of them is invalid, Arthur rejects and aborts.

3. Arthur calculates $E_w(L, x)$ and $E_{w_0}(L_0, 0)$, which can be done deterministically and in classical polynomial time. Arthur rejects and aborts if

$$E_w(L, x) \neq E_{w_0}(L_0, 0).$$

4. Arthur calculates $d_w(L, x)$ and $d_{w_0}(L_0, 0)$, which can be done deterministically and in classical polynomial time. Arthur accepts if and only if

$$d_w(L, x) = d_{w_0}(L_0, 0).$$

We show that this NP protocol can verify L. Note that due to the correctness,

$$p_{Bob}(d_k(L_0, 0) \oplus 1 | E_k(L_0, 0)) \geq c \tag{2}$$

for any key $k \in K$.

First let us consider the case of $x \in L$. In this case, due to the correctness,

$$p_{Bob}(d_k(L, x) \oplus 1 | E_k(L, x)) \geq c \tag{3}$$

for any key $k \in K$. Furthermore, Arthur never rejects at steps 2 and 3. Finally, we can show $d_w(L, x) = d_{w_0}(L_0, 0)$ and therefore Arthur accepts. In fact, if $d_w(L, x) \neq d_{w_0}(L_0, 0)$, which means

$$d_{w_0}(L_0, 0) = d_w(L, x) \oplus 1, \tag{4}$$

then

$$\begin{aligned} c &\leq p_{Bob}(d_{w_0}(L_0,0)\oplus 1|E_{w_0}(L_0,0)) \quad \text{(from Eq. (2))} \\ &= p_{Bob}(d_{w_0}(L_0,0)\oplus 1|E_w(L,x)) \quad \text{(from Eq. (1))} \\ &= p_{Bob}(d_w(L,x)|E_w(L,x)) \quad \text{(from Eq. (4))} \\ &= 1-p_{Bob}(d_w(L,x)\oplus 1|E_w(L,x)) \\ &\leq 1-c \quad \text{(from Eq. (3))}, \end{aligned}$$

which contradicts to $c > \frac{1}{2}$. Therefore, Arthur accepts when $x \in L$.

Next let us consider the case of $x \notin L$. In this case, due to the correctness,

$$p_{Bob}(d_k(L,x)\oplus 1|E_k(L,x)) \leq s \tag{5}$$

for any key $k \in K$. If Arthur arrives at step 4, w and w_0 are valid keys, and

$$E_w(L,x) = E_{w_0}(L_0,0) \tag{6}$$

is satisfied. Let us assume that

$$d_w(L,x) = d_{w_0}(L_0,0). \tag{7}$$

Then,

$$\begin{aligned} c &\leq p_{Bob}(d_{w_0}(L_0,0)\oplus 1|E_{w_0}(L_0,0)) \quad \text{(from Eq. (2))} \\ &= p_{Bob}(d_{w_0}(L_0,0)\oplus 1|E_w(L,x)) \quad \text{(from Eq. (6))} \\ &= p_{Bob}(d_w(L,x)\oplus 1|E_w(L,x)) \quad \text{(from Eq. (7))} \\ &\leq s \quad \text{(from Eq. (5))}, \end{aligned}$$

which contradicts to $s < c$. Therefore, $d_w(L,x) \neq d_{w_0}(L_0,0)$, which means that Arthur rejects. In summary, we have shown that L is in NP.

4 Discussion

In this paper, we have shown that unless BQP $\subseteq$ NP one-round perfectly-secure delegated quantum computing cannot satisfy both the correctness and the perfect blindness simultaneously.

If we relax the requirement of the perfect security to a computational one, for example, there would be several ways of secure delegated quantum computing for a classical client [19, 20, 21, 22]. For example, the fully-homomorphic encryption scheme [19] might be able to achieve secure delegated quantum computing for a classical client. Recently, a secure delegated quantum computing protocol for a completely classical client has been proposed by using the Learning With Errors problem [20].

In our proof, we do not assume $c - s \geq 1/poly$. Therefore, a similar proof shows that if PP can be solved in the protocol, then the polynomial hierarchy collapses.

Finally, we point out that a related result was obtained in Ref. [23], where an impossibility result of an information-theoretically-secure quantum homomorphic encryption was derived

by showing that the size of the sending message from Alice to Bob must be exponentially large to hide polynomial-size quantum circuits. We also mention that after uploading the first version of this paper on arXiv, more general results on the impossibilities of secure delegated quantum computing with a completely classical client have been obtained [24]. In particular, Ref. [24] considers more general case where polynomial-length messages are exchanged in polynomial-round between the server and the client, while the present paper considers the limited case where only a single bit is sent from the server to the client. On the other hand, the complexity conjecture, BQP $\not\subseteq$ NP, that our result is based on has an oracle separation [25, 26], while that of Ref. [24], BQP $\not\subseteq$ NP/poly $\cap$ coNP/poly, does not [24]. It is not clear how to generalize our result to the more general case where the server sends a polynomial-length bit string without introducing advice.

We also mention that Refs. [24, 27] consider delegations of sampling of output probability distributions of sub-universal quantum computing models, while here we consider delegations of decision problems in BQP, which does not seem to be directly applied to the sampling.

Acknowledgements

TM is supported by MEXT Q-LEAP, JST PRESTO No.JPMJPR176A and JSPS Grant-in-Aid for Young Scientists (B) No.JP17K12637. TK is supported by JSPS Grant-in-Aid for Scientific Research (A) JP16H01705 and for Scientific Research (B) JP17H01695.

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. 517 (2009).
2. S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Demonstration of blind quantum computing. Science **335**, 303 (2012).
3. S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Experimental verification of quantum computation. Nature Phys. **9**, 727 (2013).
4. C. Greganti, M. Roehsner, S. Barz, T. Morimae, and P. Walther, Demonstration of measurement-only blind quantum computing. New J. Phys. **18**, 013020 (2016).
5. 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).
6. J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind computation. Phys. Rev. A **96**, 012303 (2017).
7. V. Dunjko, E. Kashefi, and A. Leverrier, Blind quantum computing with weak coherent pulses. Phys. Rev. Lett. **108**, 200502 (2012).
8. T. Morimae and K. Fujii, Blind quantum computation for Alice who does only measurements. Phys. Rev. A **87**, 050301(R) (2013).
9. M. Hayashi and T. Morimae, Verifiable measurement-only blind quantum computing with stabilizer testing. Phys. Rev. Lett. **115**, 220502 (2015).
10. T. Morimae, V. Dunjko, and E. Kashefi, Ground state blind quantum computation on AKLT state. Quant. Inf. Comput. **15**, 0200 (2015).
11. T. Morimae and K. Fujii, Blind topological measurement-based quantum computation. Nature Communications **3**, 1036 (2012).
12. T. Morimae, Continuous-variable blind quantum computation. Phys. Rev. Lett. **109**, 230502 (2012).
13. V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Efficient universal blind computation. Phys. Rev. Lett. **111**, 230501 (2013).
14. A. Mantri, C. Pérez-Delgado, J. F. Fitzsimons, Optimal blind quantum computation. Phys. Rev.

Lett. **111**, 230502 (2013).
15. T. Sueki, T. Koshiba, and T. Morimae, Ancilla-driven universal blind quantum computation. Phys. Rev. A **87**, 060301(R) (2013).
16. Y. Takeuchi, K. Fujii, T. Morimae, and N. Imoto, arXiv:1607.01568
17. T. Morimae and K. Fujii, Secure entanglement distillation for double-server blind quantum computation. Phys. Rev. Lett. **111**, 020502 (2013).
18. D. R. Stinson, *Cryptography: Theory and Practice*, (Chapman & Hall / CRC, 2006).
19. C. Gentry, Fully homomorphic encryption using ideal lattices, Symposium on the Theory of Computing (STOC) pp.169 (2009).
20. U. Mahadev, Classical homomorphic encryption for quantum circuits. IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS) (2018).
21. A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, On the possibility of classical client blind quantum computing. arXiv:1802.08759
22. Z. Brakerski, Quantum FHE (Almost) As Secure As Classical. Advances in Cryptology, CRYPTO 2018. Lecture Notes in Computer Science, vol 10993, pp67-95 (2018).
23. L. Yu, C. A. Pérez-Delgado, and J. F. Fitzsimons, Limitations on information-theoretically-secure quantum homomorphic encryption. Phys. Rev. A **90**, 050303(R) (2014).
24. S. Aaronson, A. Cojocaru, A. Gheorghiu, and E. Kashefi, On the implausiblity of classical client blind quantum computing. arXiv:1704.08482
25. J. Watrous, Succinct quantum proofs for properties of finite groups. Proceedings of IEEE FOCS'2000, pp.537-546 (2000).
26. R. Raz and A. Tal, Oracle separation of BQP and PH. ECCC TR18-107 (2018).
27. T. Morimae, H. Nishimura, Y. Takeuchi, and S. Tani, Impossibility of blind quantum sampling for classical client. arXiv:1812.03703
28. V. Dunjko and E. Kashefi, Blind quantum computing with two almost identical states. arXiv:1604.01586