Arbitrable blind quantum computation

Go Sato1 · Takeshi Koshiba2 · Tomoyuki Morimae3,4

Received: 7 March 2018 / Accepted: 19 October 2019 / Published online: 30 October 2019© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract
Blind quantum computation (of a single-server case) is a two-party cryptographic protocol which involves a quantum computation server Bob and a client Alice who wants to delegate her quantum computation to Bob without revealing her quantum algorithms and her input to and output from the algorithms. Since Bob may be truant and pretend to execute some computation, Alice wants to verify Bob’s honesty on computation. To resolve this problem, the notion of the verifiability has been considered in the literature and several protocols of verifiable blind computation have been developed. Verifiable blind quantum computation enables Alice to check whether Bob is cheating or not. In addition to the above problem, another problem could arise. If Alice pretends to be a client and is actually a competitor against Bob, then she might slander Bob by fabricating his dishonesty. Therefore, if either Alice or Bob is cheating, then a “neutral” referee other than Alice and Bob should judge which is honest. The standard definition of the verifiability guarantees that only Alice can verify Bob’s computation, and thus, it should be called private verifiability. If Bob claims his innocence though he is actually cheating, then Alice cannot persuade any others that Bob is really cheating while Alice can recognize Bob’s cheating. In this paper, we incorporate arbitrators as the third party into blind quantum computation to resolve the above problems and give an arbitrable blind quantum computation scheme, which provides public verifiability in some sense.
1 Introduction

Secure computation involves several parties who want to evaluate functions over their private inputs without compromising privacy. Since the notion of secure computation was invented by Yao, there have been many proposals to implement secure computation. The first scheme by Yao [1] was realized as a combination of encrypted circuits (garbled circuits) to evaluate a function and oblivious transfer protocols and its security relied on an unproven computational complexity theoretic assumption. Unfortunately, unconditionally secure computation for general functionalities is impossible in the classical setting [2] and even in the quantum setting [3]. Thus, we have to consider special cases where unconditionally secure computation can be realized. As a special case of secure computation, a protocol (BFK09 protocol) for unconditionally secure delegated computation was shown by Broadbent, Fitzsimons and Kashefi [4]. Secure delegated computation (of the single-server case) in the quantum setting [a.k.a. blind quantum computation (BQC)] is a two-party protocol between a client (Alice) and a server (Bob): Bob is capable of carrying out any quantum computation and Alice wants to delegate her computational tasks to Bob without revealing her secret, that is, her algorithms and their inputs/outputs. Secure delegated computation of several servers has been also investigated. After Broadbent et al’s seminal work, BQC protocols in different settings and models have been proposed and discussed [5–17].

While BQC protocols ensure Alice’s privacy, Alice may not detect Bob’s cheating behaviors even if Bob neglects Alice’s request and pretends to execute her algorithm. To overcome this problem, some BQC protocols support the verifiability which enables Alice to detect Bob’s dishonest behavior if Bob is cheating. The Fitzsimons–Kashefi protocol (FK17 protocol) [18] is a verifiable variant of the BFK09 one, and the Hayashi–Morimae protocol (HM15 protocol) [19] is a verifiable variant of the Morimae–Fujii BQC one (MF13 protocol) [5]. Even if Alice can verify Bob’s execution of Alice’s algorithm, there still exists a problem. The problem is that Alice can detect Bob’s dishonesty, but others outside the protocol may not believe what Alice says. For example, Alice pays a service fee to Bob if Bob honestly provides the delegated computation service. On the other hand, Alice does not want to pay anything if Bob is cheating. The cheating Bob may charge Alice even for his cheating service. In addition to the above problems, yet another problem could arise. If Alice pretends to be a client and is actually a competitor against Bob, then she might slander Bob by fabricating his dishonesty. Any person outside the protocol (e.g., the FK17 protocol or the HM15 protocol) cannot decide which one is honest.

The notion of verifiability given in [18] is what we call private verifiability. We have observed that private verifiability does not resolve the above dispute. To resolve this dispute problem, we rather need a mechanism where any public outsider or a specific third party can verify if Bob honestly provides a delegated computation service. In [20], Honda proposed the notion of public verifiability for BQC and provided a publicly verifiable BQC protocol by using a classical computational cryptography, which relies on an unproven computational assumption. In this paper, we take a different approach from [20] and provide a protocol which does not rely on computational assumptions. To do this, we incorporate arbitrators as the third party into the HM15 protocol and give an unconditionally secure arbitrable blind quantum computation protocol. We
may consider that the existence of an honest third party is a strong assumption. Since we do not know whether the public verifiability in the information-theoretic sense without such an assumption is achievable, we should make this compromise. In classical cryptography, the existence of the honest third party (e.g., Certification Authority in Public Key Infrastructure) is often assumed [21]. The public verifiability of our protocol depends on the non-interactiveness of the HM15 protocol. The flow of quantum states, from Bob to Alice, in the MH15 protocol is different from the one in the FK17 protocol (and many others). If we employ the MH15 protocol, the arbiter can check Bob’s honesty from the quantum information only from Bob. This means that the verification process does not depend on the algorithm Alice has. This fact enables us to construct an arbitrable BQC protocol by a simple adaptation of the MH15 protocol. On the other hand, if we employ the interactive BQC protocols, then the arbiter generally uses information from both Alice and Bob, which would make a construction of arbitrable BQC protocols complicated.

For implementing BQC, there is another approach by using homomorphic encryptions. In the classical setting, Gentry devised a fully homomorphic encryption [22] under some computational assumption. Even in the quantum settings, some possibilities of homomorphic encryptions have been discussed [23–25], while there is a limitation [26] on information-theoretic secure quantum homomorphic encryption.

2 Preliminaries

As mentioned, we will give an arbitrable blind quantum computation protocol. First, we briefly review the MF13 protocol on which we base our protocol. In our protocol, we need a procedure (i.e., honesty test) to decide if a given state is actually a graph state. For such an honesty test, we may use the Morimae–Nagaj–Schuch test (MNS16 test) [27] or tests in [19,28,29] and the security can be proved by using quantum de Finetti Theorem under measurements that are implementable by fully-one-way local operations and classical communication (LOCC) [30].

2.1 MF13 and HM15 protocols

A client Alice has only a measurement device, and a server Bob prepares a resource state of measurement-based quantum computation. For the MF13 protocol, any resource state (e.g., two-dimensional cluster state or three-dimensional cluster state for topological quantum computation) can be used. The MF13 protocol is as follows: (1) Bob prepares a universal resource state; (2) Bob sends a particle of the resource state to Alice via the quantum channel; (3) Alice measures the particle with respect to the basis which is determined by her algorithm. They repeat (2) and (3) until the computation halts.

The HM15 protocol is a privately verifiable version of the MF13 protocol. In the HM15 protocol, Bob first prepares $k + 1$ copies of the resource state (represented as a bipartite graph). $k$ out of $k + 1$ copies are used for stabilizer tests for the verifiability. The
remaining one copy is used for the computation where Alice’s algorithm is performed via the MF13 protocol.

2.2 Honesty test

Morimae, Nagaj and Schuch [27] gave a verification procedure (MNS16 test) that checks whether a given quantum state $\rho$ is close to a graph state $|G\rangle$. The probability that the MNS16 test passes is described as $(1 + \langle G|\rho|G\rangle)/2$. While the honesty test in [19] is for bipartite graph states, the MNS16 test and also tests in [28,29] are for any graph states. In the protocol description, given in Sect. 3, we mention the MNS16 test for the honesty test. Alternatively, we may use other tests in [19,28,29].

The description of the MNS16 test is as follows: Given an $n$-qubit state $\rho$, the verifier does the following:

1. Generate a random $n$-bit string $k \equiv (k_1, ..., k_n) \in \{0, 1\}^n$.
2. Measure the operator

$$s_k \equiv \prod_{j=1}^{n} g_{j}^{k_j},$$

which can be done with only single-qubit measurements of Pauli $X$, $Y$, and $Z$ operators, because $s_k$ is the tensor product of them. Here, $g_j$ is the $j$th stabilizer of the graph state.
3. Accept if the measurement result is $+1$.

It is clear that the acceptance probability is

$$\frac{1}{2^n} \sum_k \text{Tr}\left(\frac{I + s_k}{2}\rho\right) = \frac{1 + \langle G|\rho|G\rangle}{2}.$$   

3 Protocol

As in the standard BQC protocols, we assume that Alice, a client, would like to securely delegate her computation to Bob, a server. We assume that Bob can prepare a universal $n$-qubit graph state $|G\rangle$. Besides Alice and Bob, we assume that there exists a trusted third party Charlie who acts as an arbitrator. In this paper, we assume that Charlie always obeys the protocol and stands neutral. Our protocol is given in Protocol 1.

Remark 1 It is not essential that Charlie has quantum memory in the protocol. If Charlie does not have quantum memory, he can take the option in STEP 3. Moreover, if Alice considers that her private verification suffices, Charlie does not have to be involved in the protocol. In that case, Bob may directly send $k + m + 1$ graph states (instead of $2k + m + 1$ graph states) to Alice in STEP 1; Alice applies a random permutation to $k + m + 1$ graph states and discards $m$ graph states in STEP 2; and STEP 3 and STEP 6 can be omitted.
Protocol 1 Arbitrable BQC protocol

STEP 1: Bob generates $|G\rangle^{\otimes 2k+m+1}$ and sends them to Charlie, where $|G\rangle$ is an $n$-qubit graph state.

STEP 2: Charlie applies a random permutation to $2k + m + 1$ graph states and discards $m$ graph states. (Optionally, Charlie may execute $k$ MNS16 tests as in STEP 6. If the $k$ tests are not passed, Charlie judges that Bob is cheating.)

STEP 3: Charlie keeps $k$ graph states in his memory and sends the remaining $k + 1$ graph states $\rho$ to Alice.

STEP 4: Alice receives a graph states $\rho$ and applies the MNS16 tests to randomly chosen $k$ graph states from $k + 1$ graph states $\rho$. Let $\rho_{\text{comp}}$ be the remaining one graph state. Alice executes the algorithm on $\rho_{\text{comp}}$ by measuring the particle with respect to the basis which is determined by the description of Alice’s algorithm.

STEP 5: If those $k$ tests pass, then Alice accepts the computation. Otherwise, Alice rejects the computation. Charlie does not anything if Alice accepts.

STEP 6: If Bob claims that Alice is cheating and Alice claims that Bob is cheating, then Charlie executes $k$ MNS16 tests by using $k$ graph states stored in his memory. If those $k$ tests are passed, Charlie judges that Alice is cheating. Otherwise, Charlie judges that Bob is cheating.

Remark 2 In STEP 2, Charlie discards $m$ graph states after applying a random permutation over received quantum states. This STEP convinces Charlie that the remaining $2k + 1$ copies look like some identical copies. Based on this conviction, Charlie can decide that Bob is a cheater if Bob is actually a cheater, as we will discuss later.

For the protocol, we assume that $k \geq 4n^2 - 1$ and $m \geq (2 \ln 2)k^n n^5$. Recall that $n$ is the qubit size of the universal graph state $|G\rangle$. Bob needs to prepare many copies of the graph state. After applying a random permutation over the copies and discarding some of them, the remaining copies look some identical copies (possibly other than the copies of $|G\rangle$) even if Bob does not honestly prepare many copies of $|G\rangle$. The parameter $m$ specifies how many copies should be discarded to guarantee that the remaining copies are sufficiently close to some identical copies. The parameter $k$ is related to the reliability of the test that Alice executes to check whether the remaining copies look like the copies of $|G\rangle$. The larger the $k$ becomes, the more reliable the test result is. From the viewpoint of reliability, larger values of $k$ and $m$ are better. But, taking too large values of $k$ and $m$ causes the inefficiency of the protocol execution.

Then, Protocol 1 satisfies the following two properties.

Completeness
If Bob sends $|G\rangle^{\otimes 2k+m+1}$ to Alice (via Charlie), then Alice passes the test with probability 1.

Soundness
If Alice passes the test, $\rho_{\text{comp}}$ satisfies $\langle G | \rho_{\text{comp}} | G \rangle \geq 1 - \frac{1}{n}$ with probability $1 - \frac{1}{n}$ at least.

The completeness just comes from the construction of Protocol 1. The soundness can be similarly discussed as in [28]. For self-containment, we show a brief proof. First, for any $n$-qubit quantum state $\sigma$, we can show that

\[
\text{Tr}[(T^{\otimes k} \otimes P_G^+)\sigma^{\otimes k+1}] \leq \frac{1}{2n^2},
\]
where $T$ is a POVM which corresponds to a pass by the honesty test and

$$
\Pi_G^\perp = I^\otimes n - |G\rangle\langle G|.
$$

Since

$$
\text{Tr}(T\sigma) = \frac{1}{2} + \frac{1}{2}\langle G|\sigma|G\rangle,
$$

we can say that

$$
\text{Tr}(\Pi_G^\perp\sigma) = 1 - \langle G|\sigma|G\rangle = 2(1 - \text{Tr}(T\sigma)).
$$

Thus, we have

$$
\text{Tr}[(T^\otimes k \otimes \Pi_G^\perp)\sigma^\otimes k] = \text{Tr}(T\sigma)^k\text{Tr}(\Pi_G^\perp\sigma)
= 2\text{Tr}(T\sigma)^k(1 - \text{Tr}(T\sigma)).
$$

When $\text{Tr}(T\sigma) = \frac{k}{k+1}$, the above takes the maximum value

$$
2\left(\frac{k}{k+1}\right)^k \left(1 - \frac{k}{k+1}\right) \leq \frac{2}{k+1} \leq \frac{1}{2n^2}.
$$

The remaining $(k+1)$ qubits quantum state $\rho$ after the trace out can be obtained as follows by using the quantum de Finetti theorem with respect to the one-way LOCC norm

$$
\text{Tr}[(T^\otimes k \otimes \Pi_G^\perp)\rho]
\leq \int d\mu(\sigma)\text{Tr}[(T^\otimes k \otimes \Pi_G^\perp)\sigma^\otimes k] + \frac{1}{2}\sqrt{\frac{2k^2n\ln 2}{m}}
\leq \frac{1}{2n^2} + \frac{1}{2n^2} = \frac{1}{n^2}.
$$

Since

$$
\text{Tr}[(T^\otimes k \otimes \Pi_G^\perp)\rho] = \text{Tr}(\Pi_G^\perp\rho_{\text{comp}})\text{Tr}(T^\otimes k \rho),
$$

$\text{Tr}(\Pi_G^\perp\rho_{\text{comp}}) \geq \frac{1}{n}$ implies that $\text{Tr}(T^\otimes k \rho) \leq \frac{1}{n}$. This means that if Alice accepts, then it holds that $\langle G|\rho_{\text{comp}}|G\rangle \geq 1 - \frac{1}{n}$ with probability $1 - \frac{1}{n}$ at least. Thus, the soundness holds.

In Eq. (1), we suppose that $T$ is a POVM for Alice in STEP 5. On the other hand, we can provide another interpretation for Eq. (1) and consider that $T$ is a POVM for Charlie in STEP 6. Even in this interpretation, we have a similar consequence, that is,
if Charlie passes the test, $\rho_{\text{comp}}$ satisfies $\langle G | \rho_{\text{comp}} | G \rangle \geq 1 - \frac{1}{n}$ with probability $1 - \frac{1}{n}$ at least. In other words, if Alice accepts the computation, then Charlie can endorse her acceptance. Thus, we can say that Charlie works as an arbitrator.

4 Conclusion

The public verifiability for blind quantum computation can resolve the dispute between the client and the server. In this paper, we have provided a protocol for blind quantum computation with public verifiability in the information-theoretic sense. However, we assume the existence of an honest third party (as an arbitrator). We leave open the question whether publicly verifiable blind quantum computation is achievable without the existence of an honest third party.

From the cryptographic point of view, the universal composability [31] is one of the most important properties. It is shown that the private verifiability of the BFK04 protocol and the MF13 protocol is universally composable [32,33]. The universal composability of public verifiability could be an interesting topic.

Acknowledgements

TK is supported in part by JSPS Grant-in-Aids for Scientific Research (A) 16H01705 and for Scientific Research (B) 17H01695. TM is supported by JST ACT-I No.JPMJPR16UP and a JSPS Grant-in-Aid for Young Scientists (B) 17K12637.

References

1. Yao, A. C.-C.: How to generate and exchange secrets. In: Proceedings of the 27th Annual Symposium of Foundations of Computer Science, IEEE Computer Society, pp.162–167 (1986)
2. Cleve, R.: Limits on the security of coin flips when half the processors are faulty. In: Proceedings of the 18th Annual Symposium on Theory of Computing, ACM, pp.364–369 (1986)
3. Lo, H.-K.: Insecurity of quantum secure computations. Phys. Rev. A 56(2), 1154–1162 (1997)
4. Broadbent, A., Fitzsimons, J., Kashefi, E.: Universal blind quantum computation. In: Proceedings of the 50th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, pp.517–526 (2009)
5. Morimae, T., Fujii, K.: Blind quantum computation for Alice who does only measurements. Phys. Rev. A 87, 050301(R) (2013)
6. Sueki, T., Koshiba, T., Morimae, T.: Ancilla-driven universal blind quantum computation. Phys. Rev. A 87, 060301(R) (2013)
7. Morimae, T., Fujii, K.: Blind topological measurement-based quantum computation. Nat. Commun. 3, 1036 (2012)
8. Morimae, T.: Continuous-variable blind quantum computation. Phys. Rev. Lett. 109, 230502 (2012)
9. Dunjko, V., Kashefi, E., Leverrier, A.: Universal blind quantum computing with weak coherent pulses. Phys. Rev. Lett. 108, 200502 (2012)
10. Giovannetti, V., Maccone, L., Morimae, T., Rudolph, T.G.: Efficient universal blind quantum computation. Phys. Rev. Lett. 111, 230501 (2013)
11. Mantri, A., Perez-Delgado, C.A., Fitzsimons, J.F.: Optimal blind quantum computation. Phys. Rev. Lett. 111, 230502 (2013)
12. Morimae, T., Fujii, K.: Secure entanglement distillation for double-server blind quantum computation. Phys. Rev. Lett. 111, 020502 (2013)
13. Li, Q., Chan, W.H., Wu, C., Wen, Z.: Triple-server blind quantum computation using entangle swapping. Phys. Rev. A 89, 040302(R) (2014)
14. Sheng, Y.B., Zhou, L.: Deterministic entanglement distillation for secure double-server blind quantum computation. Sci. Rep. 5, 7815 (2015)
15. Morimae, T., Dunjko, V., Kashefi, E.: Ground state blind quantum computation on AKLT state. Quantum Inf. Comput. 15(3&4), 200–234 (2015)
16. Fitzsimons, J.F.: Private quantum computation: an introduction to blind quantum computing and related protocols. NPJ Quantum Inf. 3, 23 (2017)
17. Morimae, T., Koshiba, T.: Impossibility of perfectly-secure one-round delegated quantum computing for classical client. Quantum Inf. Comput. 19, 214–221 (2019)
18. Fitzsimons, J., Kashefi, E.: Unconditionally verifiable blind quantum computation. Phys. Rev. A. 96, 012303 (2017)
19. Hayashi, M., Morimae, T.: Verifiable measurement-only blind quantum computing with stabilizer testing. Phys. Rev. Lett. 115, 220502 (2015)
20. Honda, K.: Publicly verifiable blind quantum computation. arXiv:1604.00116 (2016)
21. The existence of Certificate Authorities is a standard setting in PKI (Public-Key Infrastructure). This setting is described in many documents on PKI. For example, you may consult with Microsoft documents on PKI, which is available from https://docs.microsoft.com/en-us/windows/desktop/seccertenroll/public-key-infrastructure. Also, you may see some textbook on PKI (e.g., Public Key Infrastructure: Building Trusted Applications with Web Services by J. R. Vacca, CRC Press (2004))
22. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual Symposium on Theory of Computing, ACM, pp.169–178 (2009)
23. Broadbent, A., Jeffery, S.: Quantum homomorphic encryption for circuits of low T-gate complexity. In: Proceedings of CRYPTO 2015, Part II, Lecture Notes in Computer Science, pp.609–629. Springer, vol.9216 (2015)
24. Dulek, Y., Schaffner, C., Speelman, F.: Quantum homomorphic encryption for polynomial-sized circuits. In: Proceedings of CRYPTO 2016, Part III, Lecture Notes in Computer Science, pp.3–32. Springer, vol.9816 (2016)
25. Mahadev, U.: Classical homomorphic encryption for quantum circuits. In: Proceedings of the 59th Annual Symposium on Foundations of Computer Science, IEEE, pp.332–338 (2018)
26. Yu, L., Perez-Delgado, C.A., Fitzsimons, J.F.: Limitations on information theoretically secure quantum homomorphic encryption. Phys. Rev. A 90, 050303 (2014)
27. Morimae, T., Nagaj, D., Schuch, N.: Quantum proofs can be verified using only single qubit measurements. Phys. Rev. A 93, 022326 (2016)
28. Morimae, T., Takeuchi, Y., Hayashi, M.: Verified measurement-based quantum computing with hypergraph states. Phys. Rev. A 96, 062321 (2017)
29. Takeuchi, Y., Morimae, T.: Verification of many-qubit states. Phys. Rev. X 8, 021060 (2018)
30. Li, K., Smith, G.: Quantum de Finetti theorem under fully-one-way adaptive measurements. Phys. Rev. Lett. 114, 160503 (2015)
31. Canetti, R.: Universal composability security: a new paradigm for cryptographic protocols. In: Proceedings of the 42nd Annual Symposium on Foundations of Computer Science, IEEE, pp.136–145 (2001)
32. Morimae, T., Koshiba, T.: Composable security of measuring-Alice blind quantum computation. arXiv:1306.2113 (2013)
33. Dunjko, V., Fitzsimons, J.F., Portmann, C., Renner, R.: Composable security of delegated quantum computation. In: Proceedings of ASIACRYPT 2014, Part II, Lecture Notes in Computer Science, pp.406–425. Springer, vol.8874 (2014)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.