Practically verifiable blind quantum computation with error tolerance

Yuki Takeuchi[1], Keisuke Fujii[2], Tomoyuki Morimae[3], and Nobuyuki Imoto[1]
[1]*Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2]*Photon Science Center, Graduate School of Engineering,*
The University of Tokyo, 2-11-16 Yayoi, Bunkyo-ku, Tokyo 113-8656, Japan
[3]*ASRLD Unit, Gunma University, 1-5-1 Tenjin-cho, Kiryu-shi, Gunma 376-0052, Japan*

Introduction.— A first-generation fully fledged quantum computer will be realized by a large enterprise or a government. It is supposed that, due to its scale and/or the difficulty of maintenance, a client (Alice), who wants to utilize the quantum computer, delegates quantum computation to a server (Bob), who has the quantum computer, using relatively poor quantum devices. In such a situation, the security of Alice's information is of prime importance as is the case for the current (classical) cloud computing system. Blind quantum computation (BQC) guarantees unconditional security of Alice's input, quantum algorithm, and output of quantum computation [1]. Besides unconditional security, there is an important concept, verifiability, i.e., an ability of Alice with poor quantum devices to certify whether or not Bob honestly does the task delegated by Alice [2]. A verification protocol for BQC attracts attention not only as a cryptographic protocol, but also to know our limitation on fundamental understanding of quantum physics [3]. While experimental verifiability or falsifiability of theory is an important factor as physics, since quantum many-body systems observed become complex, it is highly nontrivial for us as classical observers to verify whether or not the experimental output honestly satisfies our theoretical prediction [3]. The verification problem in BQC can also be viewed as an abstract theoretical model of this situation.

In the existing verifiable BQC protocols [2, 4–11], if Bob performs any deviation on trap qubits sneaked by Alice, Bob's output can be rejected by Alice. Therefore even when Bob performs a little deviation, or when the quantum channel is subject to noise, the acceptance rate of the output decreases exponentially in the number of trap qubits. This degrades the practicability of the verifiable BQC protocol. In order to avoid this scenario, the trap qubits might be encoded by the quantum error-correcting code. However, in the BQC setting, Alice's quantum ability is rather limited, and hence state preparations [2, 4, 5, 9] or measurements [6–8, 10, 11] in the randomly rotated logical bases are not available. Similarly to the privacy amplification in quantum key distribution (QKD) [12], a systematic way to amplify the acceptance rate by the almost classical Alice is now highly desired to make verifiable BQC practical.

Our protocol.— We propose a practically verifiable BQC protocol, where the acceptance rate can be successfully amplified, with keeping verifiability, by the almost classical Alice under Bob's deviation including imperfections of Bob's devices and quantum channel noise [13]. To this end, we develop a $\{X, Z\}$-basis-measurement-only remote blind single-qubit preparation (RBSP) protocol. Here, X and Z represent Pauli X and Z, respectively. We show that not only blindness and correctness, which are necessary requirements for BQC, but verifiability is also guaranteed even when the RBSP protocol is further followed by the FK (Fitzsimons-Kashefi) protocol for verification [2]. Since the requirement on Alice is only $\{X, Z\}$-basis measurements, we can employ the CSS codes [14, 15], and Alice can perform error correction via classical processing after transversal $\{X, Z\}$-basis measurements similarly to BB84 protocol [16] for QKD. Specifically, if Bob's operation is perfect, and if the channel noise is given by independent X and Z errors, the proposed protocol tolerates the error rate up to $\sim 11\%$ [14].

In our poster, we will first show that the ten states $\{|0\rangle, |1\rangle, |+_{k\pi/4}\rangle \equiv (|0\rangle + e^{ik\pi/4}|1\rangle)/\sqrt{2}\}$ $(0 \le k \le 7)$ used in the FK protocol can be prepared remotely for Alice who can prepare the eigenstates of X and Z ($\{X, Z\}$-basis states) and can access to a quantum channel (P1) without degrading blindness and verifiability. Here, $|0\rangle$ ($|1\rangle$) is $+1$ (-1) eigenstate of Z. Secondary, the preparation of the $\{X, Z\}$-basis state can be replaced, with keeping verifiability, by Bob's preparation of the Bell pair and Alice's measurement in $\{X, Z\}$-basis (P2). In order to show the blindness and verifiability of P2, we utilize following two facts. First, we can construct a virtual protocol P2', which is exactly the same as P2 from Bob's view point. Second, the blindness and verifiability of P1 is guaranteed for any Bob's deviation represented by (completely positive and trace-preserving) CPTP map independent on Alice's input. By using this second fact, P2' is further regarded as a special case of P1, where blindness and verifiability have already been guaranteed. The detail of our protocol is given in Ref. [13].

Our contributions.— Our protocol contributes to making a verifiable BQC practical. By using our protocol, almost classical Alice can amplify the acceptance rate even in the presence of Bob's deviation or quantum channel noise with keeping verifiability. The double-server BQC protocols [1, 17, 18], which are thought to be the most classical for Alice, implicitly require unconditionally secure classical communication, which can be, for example, satisfied by QKD. In this sense, our protocol requires Alice as minimum devices as possible. While Alice's requirement is minimum, she can tolerate quantum channel noise as much as the CSS codes can. Note that the existing fault-tolerant BQC protocol [19] has not achieved the bound of the CSS codes even without verifiability with more powerful Alice.

As another contribution, since the requirements of our protocol for the client are the same as that for the BB84, our protocol facilitates the integration of quantum computing and quantum secure communication network allowing quantum secure cloud computing practically [20, 21].

Acknowledgments.— We thank Akihiro Mizutani for helpful discussion. YT is supported by Program for Leading Graduate Schools: “ Interactive Materials Science Cadet Program. ”KF is supported by KAKENHI No. 16H02211. TM is supported by the Grant-in-Aid for Scientific Research on Innovative Areas No.15H00850 of MEXT Japan, and the Grant-in-Aid for Young Scientists (B) No.26730003 of JSPS. NI is supported by JSPS KAKENHI Grants No. 16H02214.

[1] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, USA, 2009), p. 517.

[2] J. F. Fitzsimons and E. Kashefi, arXiv:1203.5217.

[3] D. Aharonov, M. Ben-Or, and E. Eban, in *Proceedings of Innovations in Computer Science 2010* (Tsinghua University Press, Beijing, China, 2010), p. 453.

[4] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Nat. Phys. **9**, 727 (2013).

[5] T. Kapourniotis, E. Kashefi, and A. Datta, arXiv:1403.1438.

[6] T. Morimae, Phys. Rev. A **89**, 060302(R) (2014).

[7] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, arXiv:1502.02563.

[8] A. Gheorghiu, E. Kashefi, and P. Wallden, New J. Phys. **17**, 083040 (2015).

[9] E. Kashefi and P. Wallden, arXiv:1510.07408.

[10] M. Hayashi and T. Morimae, Phys. Rev. Lett. **115**, 220502 (2015).

[11] M. Hayashi and M. Hajdusek, arXiv:1603.02195.

[12] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. Comput. **17**, 210-229 (1988).

[13] Y. Takeuchi, K. Fujii, T. Morimae, and N. Imoto, arXiv:1607.01568.

[14] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).

[15] A. M. Steane, Proc. R. Soc. London A **452**, 2551-2577 (1996).

[16] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.

[17] Y.-B. Sheng and L. Zhou, Sci. Rep. **5**, 7815 (2015).

[18] T. Morimae and K. Fujii, Phys. Rev. Lett. **111**, 020502 (2013).

[19] T. Morimae and K. Fujii, Nat. Commun. **3**, 1036 (2012).

[20] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Phys. Rev. Lett. **111**, 230501 (2013).

[21] V. Dunjko and E. Kashefi, arXiv:1604.01586.