Blind Quantum Computation against collective noise

Yuki Takeuchi[1,*], Keisuke Fujii[2,3], Rikizo Ikuta[1], Takashi Yamamoto[1], and Nobuyuki Imoto[1]
[1] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[2] *The Hakubi Center for Advanced Research, Kyoto University, Yoshida-Ushinomiya-cho, Sakyo-ku, Kyoto 606-8501, Japan*
[3] *Graduate School of Science, Kyoto University, Kitashirakawa Oiwake-cho, Sakyo-ku, Kyoto 606-8502, Japan*
[*] *takeuchi@qi.mp.es.osaka-u.ac.jp*

Introduction.— First-generation fully fledged quantum computers will be realized by large enterprises and/or governments. It is supposed that due to their sizes and/or the difficulty of maintaining them, clients, who want to utilize the quantum computer, delegate quantum computation to the quantum servers held in the enterprises and/or governments using poor quantum devices for universal quantum computation. In such a situation, the clients can employ blind quantum computation (BQC) to guarantee unconditional security of their inputs, algorithms, and outputs of quantum computations [1, 2].

Since BQC essentially employs quantum communication between clients and quantum servers [3], the reliable quantum communication is important for BQC. Several BQC protocols such as the double-server BQC protocol [4] have been proposed in order to resolve the noise problem of a quantum channel. However, in the double-server BQC protocol, it is prohibited that two quantum servers communicate with each other. If two quantum servers communicate with each other, clients' secrets are completely exposed to the quantum servers. While fault-tolerant BQC [5, 6] may be employed, their threshold values are possibly too low to tolerate quantum noise during quantum communication. This is because the degree of noise depends on the fluctuation of the quantum channel of long distance, which is supposed to be much higher than the noise threshold. Accordingly, a complete solution of the noise problem of the quantum channel in BQC is still open.

Our protocol.— In this work, we resolve the problem of the collective noise, which means arbitrary collective single-qubit noise in the quantum channel for BQC. Specifically, we make use of the fact that photons are commonly used as carriers of information in quantum communication, and optical fibers are employed as quantum channels. In such a situation, the noise in the quantum channel is regarded as the collective noise as confirmed in experiments [7]. Decoherence-free subspace (DFS) has been known to be immune to such a noise [8–10], and its validity has already been demonstrated experimentally [11].

We propose protocols to employ DFS for BQC, namely DFS-BQC protocols (see Ref. [12] for the details). We show that by making clever use of both polarization and spatial modes of photons (and coherent light pulses), parties can protect the quantum state, which is sent from the client (Alice) to the server (Bob) for BQC against the collective noise with few changes in the state preparation and communication parts of the BFK protocol [1], while Bob needs to perform additional operations. Since the BFK protocol ensures unconditional security against Bob's arbitrary operations, this construction substantially relaxes the proof of blindness of DFS-BQC.

We consider three variations of DFS-BQC protocols. The first one is the entanglement-based DFS-BQC protocol, where Alice is assumed to be able to generate Bell pairs. In the field of BQC, such a requirement is too demanding for Alice. Then, as the second one, we propose the single photon-based DFS-BQC protocol, which successfully replaces the entanglement generation process with a single-photon generation, and the postselection at Bob's side. The success probability of these two protocols are $O(T^2)$. In order to achieve the efficient dependency $O(T)$, we propose the third one, that is, coherent light-assisted protocol, where a single photon for utilizing the DFS in the second one is replaced by a coherent light pulse. All of these protocols ensure unconditional security.

Our protocols contribute to an experimentally feasible realization of BQC. In contrast to quantum key distribution, where both participants are assumed to mainly use linear optics, Bob is supposed to have a fully fledged quantum computer in the BQC scenario, which allows us to understand more general usage of DFS in quantum cryptography.

Acknowledgments.— We thank Y. Nagamatsu for helpful discussions. This work was supported by Program for Leading Graduate Schools: "Interactive Materials Science Cadet Program," and JSPS Grant-in-Aid for Scientific Research(A) 25247068 and (B) 15H03704.

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

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

[3] T. Morimae and T. Koshiba, arXiv:1407.1636v1.

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

[5] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007).

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

[7] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).

[8] P. Zanardi and M. Rasetti, Phys Rev. Lett. **79**, 3306 (1997).

[9] T. Yamamoto, J. Shimamura, Ş. K. Özdemir, M. Koashi, and N. Imoto, Phys. Rev. Lett. **95**, 040503 (2005).

[10] H. Kumagai, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **87**, 052325 (2013).

[11] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, Science **290**, 498 (2000).

[12] Y. Takeuchi, K. Fujii, R. Ikuta, T. Yamamoto, and N. Imoto, arXiv:1505.04248v1.