Quantum computing meets federated learning

Kaifeng Bu^{*}

Department of Physics, Harvard University, Cambridge MA 02138, USA

Received September 7, 2021; accepted September 14, 2021; published online November 8, 2021

Citation: K. Bu, Quantum computing meets federated learning, *Sci. China-Phys. Mech. Astron.* **65**, 210331 (2022), <https://doi.org/10.1007/s11433-021-1788-3>

Quantum machine learning is an emerging interdisciplinary field that explores the interplay between machine learning and quantum physics, holding the potential to revolutionize a number of aspects of artificial intelligence [1]. Meanwhile, blind quantum computing (BQC) protocols, which are proposed for private quantum computation, promise to handle delegated computing tasks without revealing clients' private data [2]. The combination of quantum machine learning and blind quantum computing may shed light on multiparty federated learning tasks.

In ref. [3], the authors explore possible quantum advantages from the security perspective and introduce a new quantum protocol for federated learning based on BQC, where several clients can collaboratively train a shared quantum learning model while hiding their sensitive data. The basic quantum model is a variational quantum classifier, which can be naturally implemented on the BQC platform for supervised learning tasks. In federated learning, however, if a public model is trained with good performance, there must be “effective” information flowing from the clients to the public server, and the private information may be revealed by some reverse engineering methods such as gradient attack [4]. To overcome this problem, the authors adapt the idea of differential privacy [5] to the quantum federated learning protocol by randomizing the uploaded data, which has information-theoretical guarantee for privacy protection. The performance of this defense strategy has been further tested by a hybrid quantum-classical “gradient attack” and it turns out to be effective against these malicious attacks. In

summary, this work provides a new framework for quantum federated learning and combines the strengths of both classical centralized learning and federated learning. Meanwhile, the benchmark tests provided, e.g., the robustness of the protocol to different noise strengths, the performance of the protocol with differential privacy, and different encoding strategies, may provide valuable guidance for the experiments with the NISQ devices.

Furthermore, this work also raises an important question that may trigger further exploration. With the rapid development of quantum machine learning algorithms, some of these algorithms promise to bring speedups in supervised or unsupervised learning tasks. In ref. [3], the authors mainly explore the feasibility of quantum federated learning with variational quantum classification tasks. To extend this framework, it will be intriguing if some algorithms, such as the quantum support vector machine and generative models, can be adapted to the quantum federated learning setting with speedups over the classical counterparts.

- 1 J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, *Nature* **549**, 195 (2017), arXiv: [1611.09347](https://arxiv.org/abs/1611.09347).
- 2 A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Blind Quantum Computing: 2009 50th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, Atlanta, 2009), pp. 517-526.
- 3 W. Li, S. Lu, and D.-L. Deng, *Sci. China-Phys. Mech. Astron.* **64**, 100312 (2021).
- 4 L. Zhu, Z. Liu, and S. Han, in *Deep Leakage from Gradients: Advances in Neural Information Processing Systems* (Curran Associates, Inc., 2019), pp. 14774-14784.
- 5 C. Dwork, in *Differential Privacy: A Survey of Results: International Conference on Theory and Applications of Models of Computation* (Springer, Berlin, Heidelberg, 2008), pp. 1-19.

^{*}Corresponding author (email: kfbu@fas.harvard.edu)