Accepted Manuscript

Article

Distributed secure quantum machine learning

Yu-Bo Sheng, Lan Zhou

PII: S2095-9273(17)30325-0
DOI: http://dx.doi.org/10.1016/j.scib.2017.06.007
Reference: SCIB 165

To appear in: *Science Bulletin*

Received Date: 15 May 2017
Revised Date: 19 June 2017
Accepted Date: 20 June 2017

Please cite this article as: Y-B. Sheng, L. Zhou, Distributed secure quantum machine learning, *Science Bulletin* (2017), doi: http://dx.doi.org/10.1016/j.scib.2017.06.007

Distributed secure quantum machine learning

Yu-Bo Sheng[1*] and Lan Zhou[2]
[1]*Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China*
[2]*College of Mathematics & Physics, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

(Dated: Received:15-May-2017; revised: 19-Jun-2017; Accepted: 20-Jun-2017;)

Distributed secure quantum machine learning (DSQML) enables a classical client with little quantum technology to delegate a remote quantum machine learning to the quantum server in such an approach that the privacy data is preserved. Moreover, DSQML can be extended to a more general case that the client does not have enough data, and resorts both the remote quantum server and remote databases to perform the secure machine learning. Here we propose a DSQML protocol that the client can classify two-dimensional vectors to different clusters, resorting to a remote small-scale photon quantum computation processor. The protocol is secure without leaking any relevant information to the Eve. Any eavesdropper who attempts to intercept and disturb the learning process can be noticed. In principle, this protocol can be used to classify high dimensional vectors and may provide a new viewpoint and application for future "big data".

Keywords: Quantum machine learning; Quantum communication; Quantum computation; Big data

PACS numbers:

I. INTRODUCTION

Quantum communication, such as quantum teleportation [1–3], quantum key distribution (QKD) [4–6], quantum secure direct communication (QSDC) [7–11], and other important protocols [12, 13] have been paid widely attention, for they can perform absolutely secure communication in principle. Quantum computing has also attracted much interest because of the discovery of applications that outperform the best-known classical counterparts. For example, Shor's algorithm for integer factorization [14], Grover's algorithm [15], and the optimal Long's algorithm for unsorted database search [16], all have displayed the great computing power of quantum computers. Vast technological developments have been made for small-scale quantum computers in ions [17], photons [18], superconduction [19], and some other important quantum systems [20].

Machine learning (ML) is a branch of artificial intelligence [21]. It can learn from previous experience to optimize performance, which is widely used in computer sciences, robotics, bioinformatics, and financial analysis. Recently, ML can be also used to realize the precise quantum measurement and discriminate quantum measurement trajectories [22, 23]. ML depends on the database to perform the training. The more data the computer can process, the more accurate of the ML model is. In ML, an important algorithm in mathematical picture can be described as follows: it is to evaluate the distance and inner product between two vectors. For high-dimensional vectors, such task requires large time proportional to the size of the vectors. Therefore, the vector size will become a challenge for modern rapid growing big data and the limitation of Moore's law in a classical computer.

In 2013, Lloyd et al. [24] showed that the quantum computer can be used to perform the ML. Subsequently, several quantum machine learning (QML) protocols and experimental realization were reported [25–34]. In 2014, Rebentrost et al. [25] discussed the quantum support vector machine for big data classification. They showed that the support vector machine, can be implemented on a quantum computer. Bang et al. [26] proposed an interesting method for quantum algorithm design assisted by ML. Yoo et al. [27] compared quantum and classical machines designed for learning an N-bit Boolean function. They concluded that quantum superposition enabled quantum learning is faster than classical learning. Cross et al. [29] discussed the quantum learning which is robust against practical noise. They showed that the class of parity functions can be learned in logarithmic time from corrupted quantum queries. Cai et al. [31] realized the first entanglement-based ML on a quantum computer. Li et al. [32] demonstrated the quantum learning algorithm for artificial intelligence on a four-qubit quantum processor.

In this paper, we will discuss another practical application for QML. Alice (client) has some important and confidential data and wants to implement QML with the learning algorithm of distance evaluation. However, she does not have enough quantum ability. Fortunately, Al-

*shengyb@njupt.edu.cn