Quantum Distributed Deep Learning Architectures: Models, Discussions, and Applications

†Yunseok Kwak, †Won Joon Yun, †Jae Pyoung Kim, *Hyunhee Cho, †Jihong Park, ‡Minseok Choi, §Soyi Jung, †Joongheon Kim*

†School of Electrical Engineering, Korea University, Seoul, Republic of Korea
*School of Electronic and Electrical Engineering, Sungkyunkwan University, Suwon, Republic of Korea
‡Department of Electronic Engineering, Kyung Hee University, Yongin, Republic of Korea
§School of Software, Hallym University, Chuncheon, Republic of Korea

Abstract

Although deep learning (DL) has already become a state-of-the-art technology for various data processing tasks, data security and computational overload problems often arise due to their high data and computational power dependency. To solve this problem, quantum deep learning (QDL) and distributed deep learning (DDL) has emerged to complement existing DL methods. Furthermore, a quantum distributed deep learning (QDDL) technique that combines and maximizes these advantages is getting attention. This paper compares several model structures for QDDL and discusses their possibilities and limitations to leverage QDDL for some representative application scenarios.

Keywords: Quantum deep learning, distributed deep learning, quantum secure communication

1. Introduction

As deep learning (DL) has explosively attracted extensive attention for various data processing tasks, e.g., images, audios, and videos, it has been maturing up to the present [1, 2]. Basically, the classical DL method requires a large amount of training data, and furthermore, datasets are very complicated and privacy-sensitive especially in some research fields, e.g., finance and medicine. In these fields, the classical DL approach is difficult to be applied because of its high demand for computational power and the lack of personal data privacy. Recently, two methods have been considered as promising methods to deal with these limitations: Quantum Deep Learning (QDL) [3] and Distributed Deep Learning (DDL). Quantum computing utilizes principles in quantum mechanics such as entanglements and superposition, to increase computing efficiency and to save the power consumption. The most representative QDL techniques that apply quantum computing to DL is Variational Quantum Circuit (VQC) [4], which imitates the classical neural networks with lesser parameters. Also, several studies have shown that QDL can be applied to achieve more efficient and scalable training of classification tasks [5] and deep reinforcement learning (DRL) algorithms [6, 7].

In parallel, DDL has been studied to solve problems that originate from the centralized setting of storing and computing whole datasets in the classical DL system [8]. DDL deals with the computational overhead problem and the data security issue at once. It utilizes the computational power of numerous local devices by operating relatively small models in devices instead of collecting and training all the data at a central server. In Federated Learning (FL) [9], local devices train the model with their datasets only and send the locally trained model parameters to the server instead of their datasets. Meanwhile, Split Learning (SL) divides the ANN model, and distributes the front part and the latter one to the local device and the server. Each device then transmits latent variables to the server and the server gives gradients back to the device for
training the split model. Both FL and SL accomplish reducing computational overhead and protecting data security. Thus, FL and SL have been applied to such research areas that handle privacy-sensitive data, e.g., medicine [10, 11, 12], finance [13], and facial recognition [14].

In this trend, Quantum Distributed Deep Learning (QDDL), which combines the advantages of QDL and DDL, attracts the attention of many researchers. QDDL can strengthen data security from external attacks by utilizing secure quantum communication protocols between the server and client.

Specifically, Federated Quantum Machine Learning [15] and Quantum Federated Learning (QFL) through blind quantum computing [16] utilize QDL algorithms in a federated setting to boost the computational efficiency while ensuring the data privacy and security. In addition, a study [17] proposed the first version of fully-quantum QFL framework by employing quantum federated dataset.

This paper investigates various QDDL techniques and discusses their limitations and challenges. Compared to the conventional QDL and DDL studies, QDDL is still in its infancy and there is no agreements on promising research directions and appropriate architectures. Therefore, this paper broadens this area of study and leverages QDDL for autonomous mobility, a representative application scenario requiring less computations, communication efficiency, and security.

2. Background

Quantum Deep Learning. QDL operates numerical calculations of the ANN with the help of quantum computing [18]. Recently, there have been numerous attempts to replace the classical DL architectures such as Deep Neural Network (DNN), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN) with quantum-based models as follows.

• Variational Quantum Circuits: A variational quantum circuit (VQC) is a quantum circuit that has parameters that can be optimized through the classical DL method [19]. Fig. 1 shows the structure of VQC by comparing it with a classical deep neural network. First, training datasets are encoded to have quantum states expressed by qubits. These quantum states are fed into the VQC, which simulate classical neural networks. Then, the output quantum states are measured and collapsed into one of the basic quantum states. Lastly, the output quantum states are converted back into data that we can read and process. VQC can be trained and optimized like any other neural network. VQC, despite its limited size, can be more expressive than classical neural networks while carrying out similar numbers of parameters or with similar learning speeds. To utilize quantum circuits, a quantum encoder is required. Quantum encoders transform classical vectors into quantum states needed as inputs to the quantum circuits. Therefore, quantum encoders play an essential part in the hybrid quantum-classical model because noisy intermediate-scale quantum (NISQ) devices cannot handle large input datasets. Only a limited number of qubits can be used as inputs. Thus, we need highly efficient quantum encoders to express large datasets with few qubits.

• Quantum Convolutional Neural Networks (QCNN): The QCNN is the quantum circuit with the convolution layer and pooling layer and works in the following five steps [20]. First, input data is encoded into its corresponding qubit state and transformed through rotation operator gates. Second, the convolution layer with quasi-local unitary gates filters the input data into a feature map, and the pooling layer with controlled rotation operators downsizes the feature map. Third, this process is repeated, and the fully connected layer acts on the transformed qubit state as classical CNN models. Fourth, the qubit is measured and decoded back into its original classical data form. Finally, circuit parameters are updated by a gradient descent-based optimizer. Through this process, QCNN can process image information as conventional CNN does.

Quantum Secure Communication. The current classical security protocols are particularly vulnerable to attacks utilizing quantum computing. For example, the Rivest-Shamir-Adleman (RSA) public-key cryptosystem, which uses the inability of classical computers to factorize large numbers in a short time to defend against attacks, can be easily defeated by a quantum computer using Shor’s algorithm [21]. Therefore, the post-quantum cryptography [22] is necessary to protect against quantum computing-based attacks, and a quantum communication security protocol using quantum entanglement and superposition has been popular for defending against such attacks. This paper introduces two well-known quantum secure communication systems, quantum key distribution (QKD) [23] and quantum secure direct communication (QSDC).
Figure 1. The structure of Variational Quantum Circuit (VQC) and classical deep neural network. The parameters and connections with activation function composing classical deep neural network are mapped to the ‘Rotation’ gate and ‘Controlled Not’ gate parameters in the quantum circuit.

- **Quantum Key Distribution**: Quantum key distribution is a secure communication method based on quantum mechanical phenomena instead of mathematical complexity, and functions as a way to generate a random secret key. In BB84 [24], a representative protocol using QKD, the sender and the receiver use polarization filters to generate and measure photons, and verify the signal in the public channel to use it as a quantum secret key. In communications using QKD, the presence of an eavesdropper is not only known to the sender and the receiver, but also the eavesdropper cannot overhear the accurate information. The security of QKD is based on the characteristic of photons that are non-replicable and collapse when they are measured.

- **Quantum Secure Direct Communication**: Quantum secure direct communication (QSDC) [25] is another important branch of quantum cryptography. In QSDC, the secret information can be transmitted through a quantum channel directly without sharing a private key. Since QSDC achieves security through coding in quantum terminals, its communication capacity is more efficient than that of QKD because there is no need to manage quantum keys [26]. At the beginning, the two-step QSDC method has been proposed, which requires two rounds for transmitting photons. This scheme consists of a checking round and a message coding round. In the checking round, the receiver verifies whether the current channel is secure or not, and if the channel security is guaranteed, the receiver directly reads out the encoded message in the message coding round. Recently, the one-step protocol [27] has appeared that combines two steps of checking and message coding into one by using polarization-spatial hyperentanglement. This one-step method enables quantum communications at a longer distance compared to existing techniques.

3. Quantum Distributed Deep Learning Architectures

**Federated Quantum Machine Learning.** Chen et al. [15] proposes the first QML model in the federation setting. Specifically, they considered the VQC and Quantum Neural Networks (QNN) coupled with classical pre-trained convolutional neural networks. Fig. 2 shows the illustration of QFL. These hybrid quantum-classical classifiers perform training in a federated setting by using the FedAvg algorithm [28]. This work demonstrated for the first time that QDDL can be implemented in practice by giving following experiments and schematic results.

- **Variational Quantum Federated Learning**: While existing quantum communication security protocols are based on quantum photonic computing, implementation of QDDL is mostly based on ion trapping or superconducting quantum gate operations. Therefore, [15] selects the VQC instead of quantum communication security protocols to operate the quantum federated learning algorithm in practical scenarios, and demonstrates its performance for binary classification of the CIFAR image dataset.

- **Hybrid Quantum-Classical Transfer Learning**: The NISQ device is still limited in processing large-sized data due to its insufficient computing and error correction capability. Therefore, [15] uses and transfers the learning results of a pre-trained classical neural network to learn a quantum neural network. This method first transforms images into small-dimensional data using a classical
CNN, and then processes it in a quantum circuit. Here, a pre-trained VGG16 model [29] is used for the feature extraction.

**QFL through Blind Quantum Computing.** The quantum protocol for distributed learning with remote quantum servers without exposing the private data of local devices has been developed to pursue exponential speedups and privacy protection. Furthermore, according to [16], applying blind quantum computing [30] to QFL ensures differential privacy and can safely act under external gradient attacks.

- **Blind Quantum Computation:** Blind quantum computation allows clients to offload calculations of the ANN to a remote quantum server without sharing any sensitive information. In this protocol, the client is assumed to prepare random qubits chosen from a finite set and send them to the server; therefore, the client does not require any quantum computational power. Then, a two-way secure communication channel is set up where the client gives single-qubit measurement instructions to the server. After all the instructions are delivered, the server computes the received clients qubits under the instructions that the client informs, and finally the client receives the desired output from the server. In this process, the server does not receive any data from the client. If there is only a single client, privacy is perfectly protected, and the client can safely utilize the quantum classifier. However, when multiple clients use the identical quantum classifier, attackers can employ the information of the quantum classifier and its updates to retrieve the client’s data.

- **Single Client:** A single-user system can guarantee the perfect security while providing reliable results. The quantum server is perfectly ignorant about the client’s quantum classifier from the beginning to the end. Thus, additional security measures are not needed in a single-user environment.

- **Multiple Clients:** If there are multiple clients, they share the identical quantum classifier model. Transmission of parameters, e.g., gradients, to the quantum server for computation could be vulnerable to attacks. If the transmitting parameters are revealed, they can be used for gradient attacks. If the updated parameters are leaked, they can be used in a gradient attack. In a gradient attack, the revealed information can be reverse engineered to estimate the inputs of the system to which unauthorized entities are not allowed to have access. To counteract this problem, we use the differential privacy, which adds Gaussian or Laplacian noise to the information being transmitted. With the appropriately designed noise mechanism, the attacker cannot extract the critical information from the transmitting signal, while the client still can retrieve the data.

- **Gradient Attack:** If the attacker overhears the transmitted signal from the client to the server, the attacker can use this information to recover the circuit’s input. The attacker can then use this information to recover the circuit’s input. The attacker measures the distance between the current gradient and the target to get the information. However, if the differential privacy is considered, the attacker’s gradient attack loss function is interrupted because the noise replaces the target gradient. This decreases the accuracy of recovering the input; therefore, the attacker gets the limited information about the input to the system.

4. Challenges

**Quantum Compatibility Problem.** QML is not stable unlike deep learning and its application has not been used widely yet. It is still limited by the quantum noise without quantum correction when the model exceeds a specific size [31]. A representative method to overcome this limitation is to use a classical ANN as an auxiliary role for quantum computation, as shown in classical-quantum hybrid transfer learning in [15]. In addition, most of the quantum secure communication protocols are difficult to be implemented using NISQ devices. Therefore, implementation of a complete QDDL architecture including QDL and quantum secure communication protocols on NISQ devices is an important issue.

**Data Privacy Problem.** When the sensitive data, e.g., financial and medical data, is handled, it is critical...
to prevent unauthorized users as well as participants of the training process from having access to other clients’ data. In [32], the server and the client use QKD-based quantum communications to exchange information safely. However, the server could still easily identify the client; therefore, this method is not suitable for situations where the security is of paramount importance. On the other hand, in [15], the client and the server did not exchange any data. However, no quantum security protocol is also considered; therefore, this model was especially vulnerable to Byzantine attacks. The model proposed in [16] overcomes this challenge by employing the differential privacy technique to block any attacks during data transmission from the client to the server. At the same time, it also proposed a secure communication protocol to prevent the server from identifying which user transmits the data. Other possible solutions to the data security issue include SL, first introduced in [33]. In an SL setting, a part of the entire training network is stored in the client device, and the client and the server exchange latent data and gradients instead of the actual data. As a result, data privacy is protected. This method generally shows faster algorithmic convergence than federated Learning, and application of this SL setting to QNN is expected to ensure the efficient training and data privacy.

Data Scalability Problem. It is widely known that the problem of the barren plateau occurs in large-scale QNNs [34], which vanishes the quantum gradient and leads to local convergence. This means that even if the size of the VQC is large enough and many parameters become available, its optimal convergence may become difficult. It is known that this phenomenon is affected not only by the size of the quantum circuit, but also by the quantum calculation error rate, the type of gradient descent method, and the ansatz of the quantum circuit. Therefore, the effective design of quantum circuit ansatz to solve these problems is a big challenge facing whole quantum deep learning research field. To this end, research on efficient quantum encoding [35] of classical information or research on processing more information inside qubits by constructing a quantum circuit as a tensor network [36] has been conducted.

5. Potential Application for Autonomous Mobility

The vast amount of data is occurs from mobility platforms (e.g., autonomous driving or advanced aerial mobility) such as visual data (e.g., image, point cloud, scene graph), communication (e.g., wireless communication, quantum communication), and the positional data (e.g., IMU data, GPS data, SLAM). To achieve automated mobility, cognition, communication, and control should be considered as follows.

Cognition. For an autonomous mobility platform, a machine should be cognitive to collected data. QCNN has shown successful operation in the image classification task, where the image size is small (e.g., MNIST, FashionMNIST, CIFAR10) [37]. The basis of cognition around circumstances is object detection. Even the author of [38] has suggested object detection using QAOA, the object detection of QDL version is not discussed yet. The VQC-based object detection is an expected topic and it enables QDDL.

Communication. Building a low-latency secure communication network is essential in creating an autonomous mobile platform. Quantum communication is expected to play a vital role in making such future networks, and research on terrestrial [39], drone [40] and satellite-based [41] quantum networks has been extensively conducted. Current satellite-drone-terrestrial integrated quantum network research uses a method of transmitting encrypted quantum information using a QKD-based security protocol [42]. Combining such an integrated quantum network and QDDL technology is expected to play a decisive role in autonomous mobile-based distributed learning.

Control. Quantum reinforcement learning (QRL) has been actively studied. [43] have proposed the hybrid computing methods, i.e., the controller policy is based on VQC, and the evaluator-side network (i.e., critic) is based on a classical neural network. In addition, [44] have proposed an utterly quantum version of the reinforcement learning regime. Since there are many simulation APIs, e.g., Airsim [45] for aerial mobility CARLA [46] for autonomous driving, the implementation of QRL is expected technology soon. In addition, based on the studies mentioned above, quantum multi-agent distributed reinforcement learning, where the basis is QDDL, is an expected key solution for autonomous mobility platforms.

6. Conclusion

In this work, we first introduced the QDDL studies and their substructures. We also discussed the pros and cons of these studies from multiple perspectives, with a particular focus on data security. We also explored the fields of applications for the research domain and the possibilities of new methodologies. We believe this contribution will definitely help conduct future quantum distributed AI research.
References

[1] J. Park, S. Samarakoon, A. Elgabli, J. Kim, M. Bennis, S.-L. Kim, M. Debbah, Communication-efficient and distributed learning over wireless networks: Principles and applications, Proceedings of the IEEE 109 (5) (2021) 796–819.

[2] S. Ahn, J. Kim, E. Lim, W. Choi, A. Mohaisen, S. Kang, Sim-Caffe: A distributed deep learning platform with shared memory buffer for HPC architecture, in: ICDCS, 2018.

[3] N.Wiebe, A. Kapoor, K. M. Svore, Quantum deep learning, CoRR abs:1412.3489.

[4] J. Biamonte, Universal variational quantum computation, Physical Review A 103 (3) (2021) L030401.

[5] J.-M. Liang, S.-Q. Shen, M. Li, L. Li, Variational quantum algorithms for dimensionality reduction and classification, Physical Review A 101 (3) (2020) 032323.

[6] S. Y.-C. Chen, C.-H. H. Yang, J. Qi, P.-Y. Chen, X. Ma, H.-S. Goan, Variational quantum circuits for deep reinforcement learning, IEEE Access 8 (2020) 141007–141024.

[7] W. J. Yun, S. Jung, J. Kim, J.-H. Kim, Distributed deep reinforcement learning for autonomous aerial eVTOL mobility in drone taxi applications, ICT Express 7 (1) (2021) 1–4.

[8] O. Lockwood, M. Si, Playing atari with hybrid quantum-classical reinforcement learning, CoRR abs:2107.04114.

[9] H. Baek, W. J. Yun, Y. Kwak, S. Jung, J. J. M. M. Bennis, J. Park, J. Kim, Joint superposition coding and training for federated learning over multi-width neural networks, CoRR abs:2112.02543.

[10] Y. J. Ha, M. Yoo, G. Lee, S. Jung, S. W. Choi, J. Kim, S. Yoo, Spatio-temporal split learning for privacy-preserving medical platforms: Case studies with COVID-19 CT, X-ray, and Cholesterol data, IEEE Access 9 (2021) 121046–121059.

[11] Y. J. Ha, G. Lee, M. Yoo, S. Jung, S. Yoo, J. Kim, Feasibility study of multi-site split learning for privacy-preserving medical systems under data imbalance constraints in COVID-19, X-ray, and cholesterol dataset, Scientific Reports 12 (1) (2022) 1–11.

[12] J. Jeon, J. Kim, J. Kim, K. Kim, A. Mohaisen, J.-K. Kim, Privacy-preserving deep learning computation for geo-distributed medical big-data platforms, in: DSN, IEEE, 2019.

[13] G. Long, Y. Tan, J. Jiang, C. Zhang, Federated learning for open banking, in: Federated learning, Springer, 2020, pp. 240–254.

[14] J. Kim, T. Park, H. Kim, S. Kim, Federated learning for face recognition, in: 2021 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2021, pp. 1–2.

[15] S. Y.-C. Chen, S. Yoo, Federated quantum machine learning, Entropy 23 (4) (2021) 460.

[16] W. Li, S. Lu, D.-L. Deng, Quantum federated learning through blind quantum computing, Science China Physics, Mechanics & Astronomy 64 (10) (2021) 1–8.

[17] M. Chehimi, W. Saad, Quantum federated learning with quantum data, CoRR abs:2106.00005.

[18] M. Schuld, I. Sinayskiy, F. Petruccione, An introduction to quantum machine learning, Contemporary Physics 56 (2) (2015) 172–185.

[19] Z. Abothoshima, M. Elhosen, E. H. Houssein, W. M. Mohamed, Classification with quantum machine learning: A survey, CoRR abs:2006.12270.

[20] S. Oh, J. Choi, J. Kim, A tutorial on quantum convolutional neural networks (qcnns), in: ICTC, IEEE, 2020, pp. 236–239.

[21] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: FOCS, IEEE, 1994, pp. 124–134.

[22] D. J. Bernstein, T. Lange, Post-quantum cryptography, Nature 549 (7671) (2017) 188–194.

[23] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, The security of practical quantum key distribution, Reviews of Modern Physics 81 (3) (2009) 1301.

[24] C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, arXiv preprint arXiv:2003.06557.

[25] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, G.-C. Guo, Quantum secure direct communication with quantum memory, Physical Review Letters 118 (22) (2017) 220501.

[26] G.-L. Long, X.-L. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, Physical Review A 65 (3) (2002) 032302.

[27] Y.-B. Sheng, L. Zhou, G.-L. Long, One-step quantum secure direct communication, Science Bulletin 67 (4) (2022) 367–374.

[28] B. McMahan, E. Moore, D. Ramage, S. Hampson, B. A. y Arcas, Communication-efficient learning of deep networks from decentralized data, in: AISTATS, Vol. 54, 2017, pp. 1273–1282.

[29] K. Simonyan, A. Zisserman, Very deep convolutional networks for large-scale image recognition, CoRR abs:1409.1556.

[30] S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, P. Walther, Demonstration of blind quantum computing, Science 335 (6066) (2012) 303–308.

[31] J. Preskill, Quantum computing in the NISQ era and beyond, Quantum 2 (2018) 79.

[32] Y.-B. Sheng, L. Zhou, Distributed secure quantum machine learning, Science Bulletin 62 (14) (2017) 1025–1029.

[33] O. Gupta, R. Raskar, Distributed learning of deep neural network over multiple agents, JCNA 116 (2018) 1–8.

[34] J. R. McLean, S. Boixo, V. N. Smelyanskiy, R. Babbush, H. Neven, Barren plateaus in quantum neural network training landscapes, Nature Communications 9 (1) (2018) 1–6.

[35] Y. Shee, P.-K. Tsai, C.-L. Hong, H.-C. Cheng, H.-S. Goan, A qubit-efficient encoding scheme for quantum simulations of electronic structure, CoRR abs:2110.04112.

[36] J. Qi, C.-H. H. Yang, P.-Y. Chen, Qtn-vqc: An end-to-end learning framework for quantum neural networks, CoRR abs:2110.03861.

[37] S. Oh, J. Choi, J. Kim, A tutorial on quantum convolutional neural networks (qcnns), in: ICTC, 2020, pp. 236–239.

[38] J. Li, M. Alam, A. A. Saki, S. Ghosh, Hierarchical improvement of quantum approximate optimization algorithm for object detection, in: ISQED, IEEE, 2020, pp. 335–340.

[39] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, H. Takesue, Entanglement distribution over 300 km of fiber, Optics express 21 (20) (2013) 23241–23249.

[40] H.-Y. Liu, S.-N. Zhu, Optical-relayed entanglement distribution using drones as mobile nodes, Physical Review Letters 126 (2) (2021) 020503.

[41] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, et al., Satellite-based entanglement distribution over 1200 kilometers, Science 356 (6343) (2017) 1140–1144.

[42] A. D. Hill, J. Chapman, K. Herndon, C. Chopp, D. J. Gauthier, P. Kwiat, Drone-based quantum key distribution, Urbana 51 (2017) 61801–63003.

[43] Y. Kwak, W. J. Yun, S. Jung, J.-K. Kim, J. Kim, Introduction to quantum reinforcement learning: Theory and penny-based implementation, in: ICTC, IEEE, 2021, pp. 416–420.

[44] S. Jerbi, L. M. Trenkwalder, H. P. Nautrup, H. J. Briegel, V. Dunjko, Quantum enhancements for deep reinforcement learning in large spaces, PRX Quantum 2 (1) (2021) 010328.

[45] S. Shah, D. Dey, C. Lovett, A. Kapoor, Airsim: High-fidelity visual and physical simulation for autonomous vehicles, CoRR abs/1705.05065.

[46] A. Dosovitskiy, G. Ros, F. Codevilla, A. M. López, V. Koltun, CARLA: An open urban driving simulator, CoRR abs/1711.03938.