Hybrid quantum edge computing network

Lijun Ma, Leah Ding

Lijun Ma, Leah Ding, "Hybrid quantum edge computing network," Proc. SPIE 12238, Quantum Communications and Quantum Imaging XX, 122380F (4 October 2022); doi: 10.1117/12.2633020

SPIE.

Event: SPIE Optical Engineering + Applications, 2022, San Diego, California, United States

Hybrid Quantum Edge Computing Network[1]

Lijun Ma[a] and Leah Ding[b]

[a]Information Technology Laboratory, National Institute of Standards and Technology,
100 Bureau Dr., Gaithersburg, MD 20899
lijun.ma@nist.gov

[b]Computer Science Department, American University
4400 Massachusetts Ave NW, Washington, DC 20016
ding@american.edu

ABSTRACT

Edge computing network and quantum network are two emerging technologies in current communication fields. Edge computing has emerged to support the computational demand of delay-sensitive applications in which substantial computing and storage are deployed at the network edge close to data sources. Quantum network supports distributed quantum computing, which could provide exponentially computation capabilities for certain problems. The vision of a hybrid quantum-edge is to provide a fundamentally new computing paradigm by expanding the computing capabilities and security of edge computing with quantum computing and quantum communications. The distributed nature of edge computing networks will also enable new scalable quantum networking schemes and applications. Such a hybrid computing paradigm will achieve unparalleled capabilities that are provably impossible by using only classical computing or quantum computing schemes alone. In this paper, we introduce the concept of hybrid quantum-edge computing network and discuss its challenges and opportunities.

Keywords: Edge computing network, Quantum computing, Quantum network.

1. INTRODUCTION

Edge computing has emerged to enable in-situ computing in the post-cloud era, where a large quality of data is generated at the network edge (with respect to the cloud), and more applications are being deployed at network edge to consume such data [1]. In edge computing networks, data is stored, processed, analyzed, and acted upon close to data sources. Physical proximity impacts end-to-end latency, energy, communication bandwidth, and data privacy and security. Recent

[1] The identification of any commercial product or trade name does not imply endorsement or recommendation by the National Institute of Standards and Technology.

Quantum Communications and Quantum Imaging XX, edited by Keith S. Deacon, Ronald E. Meyers
Proc. of SPIE Vol. 12238, 122380F · © 2022 SPIE · 0277-786X · doi: 10.1117/12.2633020

work has demonstrated the benefits of edge computing such as reduced response time [2-4], improved energy efficiency[5] , effective data security [6]. In addition, Artificial Intelligence (AI) applications have become one of the top use cases of edge computing [7-9].

In the past decade, there has been tremendous progress in quantum information technology [10], which applies unique properties of quantum mechanics into information technology in ways that greatly exceed classical capabilities. These unique quantum properties include the uncertain principle, quantum interference, quantum entanglement, quantum superposition and quantum squeezing.

Quantum information technology has three fields, quantum computing, quantum communication, and quantum sensing. Quantum computing was first proposed by Feynman in the 1980's and has greatly motivated by Shor's quantum algorithm for factoring large numbers [11]. Quantum computers use quantum bits, or qubits, which can exist as zeros and ones at the same time, and give them the potential to perform many calculations simultaneously. Therefore, Quantum computing can realize calculation for certain problems exponentially faster than classical computers. The quantum computational advantage, or quantum supremacy, had been first demonstrated by Google in 2019 [12] for a problem called "random circuit sample" and more quantum computers with faster speed have been demonstrated in 2020 and 2021 [13-15]. Quantum communication was first proposed by Bennett and Brassard in 1984[16], and since then it has been developed rapidly. Quantum communication includes quantum key distribution (QKD) [17] and quantum entanglement distribution [18]. QKD provides secure communication over unsecured communication links, and its security is guaranteed by the principles of quantum mechanics and is un-hackable by any mathematical methods[19], while the quantum entanglement distributions communicate between quantum computers and quantum sensors at different locations [20]. Many quantum communication networks through optical fibers and free-space with satellites, planes, and drones have been demonstrated. An integrated space-to-ground quantum communication network over 4,600 kilometers has been reported recently [21]. Quantum sensing utilizes the properties of quantum mechanics to realize higher precision measurement and beat the current limits of classical measurement methods [22, 23]. With the recent rapid advances in quantum computing, communication, sensing, and related technologies, quantum internet has been proposed [24, 25]. In quantum internet, quantum information is generated, processed, and stored locally in quantum nodes. These nodes are linked by quantum communication links, which transport quantum states from site to site with high fidelity and distribute entanglement across the entire system. The quantum internet will support distributed quantum computing/sensing networks and provide exponential computation ability and ultra-high precision measurement, which promises to be a game-changing technology when fully realized at scale.

Quantum computing will exponentially expand the computation capabilities of edge computing in certain problems, such as factoring, searching, sampling and simulation, and quantum sensing can provide more precision and accurate measurement data for edge computing. The quantum communication and network support distributed quantum computing and sensing to further enhance the abilities and strengthen the security of edge computing.

2. HYBRID QUANTUM EDGE COMPUTING ARCHITECTURE

We design the hybrid quantum-edge computing paradigm by introducing quantum information processors (such as quantum-powered clouds, quantum-powered servers, quantum computers), and quantum networking devices (quantum repeaters and quantum switches). In this hybrid computing paradigm, computing units will include both classical edge units and quantum units, which requires a mix of quantum and classical communication capabilities and platform configurations.

Figure 1 illustrates the three-layer architecture. Different from existing edge computing environments, quantum processing units and computing units are introduced to all three layers to enable quantum information processing and computing capabilities. In addition, quantum repeaters and quantum switches are introduced to enable quantum networking for both inter-layer and cross-layer communications.

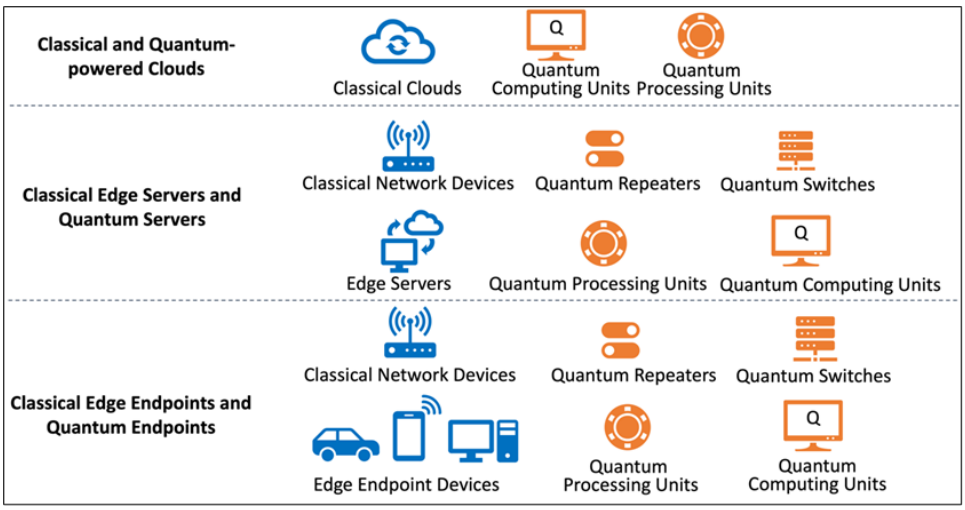

Figure 1. Three-layer architecture of hybrid quantum-edge computing paradigm.

In the hybrid architecture, edge endpoints include classical endpoints and quantum endpoints. Classical endpoints (such as classical computers, mobile devices, smart devices, wearable devices, automobiles, etc.) generate and consume data. Different endpoints have different computing and storage resources, as well as communication bandwidths. The endpoint layer also consists of network devices, such as routers, gateways, switches, and base stations to provide network connections. Some real-time and latency-sensitive applications are being moved from clouds to edge servers and endpoints. We envision that with quantum endpoints and quantum edge servers, more applications will be moved towards the edge of the network.

In this new computing paradigm, quantum endpoints include quantum computing units, quantum processing units, quantum repeaters, and quantum switches. The quantum computing units are quantum computers, which can solve certain computational problems at a speed much faster than classical computers. There are two types of quantum computers: special one and general one. A special quantum computer only performs a certain computational task, while a general quantum computer is programmable and can perform different algorithms by quantum coding.

Quantum processing units are key components and devices for quantum information processing, storage, and communication, such as entangled photon sources, the Bell state and the Greenberger-Horne-Zeilinger state analyzers[26] [27], quantum memories [28], quantum interfaces [29], quantum gates, quantum state measurement, and photon detection. Different from quantum computing units, quantum processing units do not perform the computational tasks directly. They usually work for crucial functions of quantum communication and networks. These functions include quantum entanglement distribution, quantum teleportation and swapping, quantum entanglement purification/distillation [30, 31], and quantum state storage and retrieval. Some quantum processing units can work with classical computing units to generate and distribute quantum secured keys for classical communication.

The no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state [32]. The no-cloning theorem provides the basis of quantum secure communication, but it also makes it impossible to copy or amplify the quantum state of single photons. The inevitable attenuation or loss of photons in transmission links greatly limits the transmission distance of quantum communication. Therefore, the quantum repeater plays important role in the quantum network [33-35]. Different from a classical amplifier or repeater, a quantum repeater does not copy or amplify the signal. There are two types of quantum repeaters: trusted-node repeaters and true quantum repeaters. Trusted-node repeater works only for QKD system with the additional assumption that the repeater node is trusted. In the trusted-node repeater, secured data was decrypted from the previous link and encrypted with quantum secured keys for the next link. The true quantum repeater is based on quantum teleportation/swapping [36] and quantum error corrections, which allow the end-to-end generation of quantum entanglement and the end-to-end transmission of qubits. The true quantum repeater can be used for both QKD and the distributed quantum computing/sensing network.

The quantum switch is used for entanglement routing of quantum links in a quantum network [37, 38]. The quantum switch is similar to the optical switch in a classical optical network, but it requires transparence for quantum states of photons and has much less insertion loss.

Classical edge servers and quantum-powered edge servers reside between edge endpoints and centralized clouds. Traditional cloud computing infrastructures can be extended to edge servers, such as Cloudlet, Micro Could, application servers, regional data hosting servers. Thus, extending the cloud computing services to the edge of the network. Edge servers with various computing capabilities can be deployed to different places within the network. For instance, numerous

small cloudlets can be placed at the network edge (for example, one-hop communication distance from the endpoint devices). Alternatively, fewer, but larger cloudlets can be placed deeper in the network.

The classical clouds and quantum-powered clouds form an aggregated computing and storage layer to provide various applications from a global perspective. Compared to conventional clouding computing, edge-quantum computing is distributed in the sense that there is no centralized cloud to manage resources, data, and applications. Edge servers and endpoints self-organize to collaboratively perform computing tasks and provide real-time services to users [39]. Those edge servers are typically deployed at certain locations, and endpoints can be static or move from a geographic location to another. They are location-aware, for example, their locations can be traced actively or passively to support real-time applications [40].

In this hybrid computing paradigm, geographically distributed classical computing units (edge endpoints, edge servers, and clouds) will enable quantum computing units and quantum processing units to form a scalable quantum network to carry out large-scale calculations for high performance computing.

.

3. A SCALABLE HYBRID QUANTUM EDGE COMPUTING SCENARIO

Existing edge computing architecture uses various communication links for networking, including wired communication (such as Ethernet, optical fiber), wireless communication (such as LTE/5G, ZigBee, IEEE 802.11 a/b/c/g/n/, satellite links, Bluetooth, etc.), or a combination of both [41].

Future hybrid quantum and edge computing paradigms will require quantum connectivity for multi-hop delivery of qubits for distributed computation. Teleportation and blind quantum computation can ensure that remote quantum computing units are connected to edge computing systems for on-demand high performance computing.

As illustrated in Figure 2, classical communication links are also essential for two reasons. First, quantum links are established through classical links. For all quantum communication protocols, whether the quantum key distribution or the entanglement distribution, classical channels are necessary for exchanging necessary information in bits, such as measurement bases or measurement results.

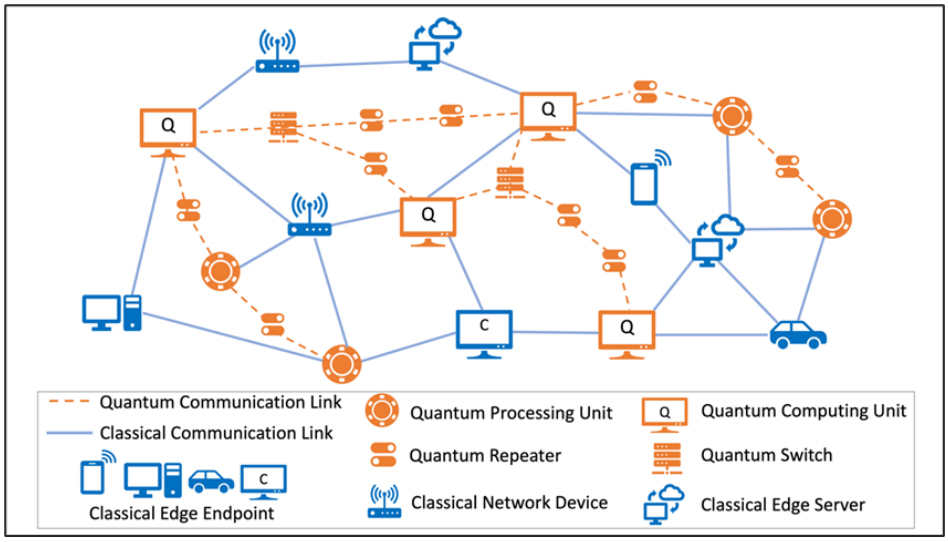

Figure 2. Illustration of integrated quantum and classical communication links

Secondly, while quantum computing units provide the additional computational capability to the hybrid edge computing paradigm, classical computing units (such as endpoint devices, edge servers, clouds, etc.) will remain as essential computing units for many computation tasks. Quantum computing units usually only perform certain tasks greatly surpassing the classical computing units, and the remaining tasks still need classical computing units. Therefore, the integration of quantum and classical communication links is of importance in the hybrid edge computing paradigm.

Finally, security and privacy approaches will be needed to keep communication secure and protect data at rest and in transit in such hybrid environments. The quantum state of a single photon cannot be copied or amplified, which guarantees the security of the communication but also limits the transmission distance. Before full function quantum repeaters have not been realized, currently quantum communication and network systems need trusted relay nodes to extend the

Although a quantum computer promises to solve certain computational tasks exponentially faster than classical computers, its physical implementation is also technically difficult. For example, a superconducting-based quantum computer requires a liquid helium temperature environment in a cryostat. Therefore, the number of qubits in an individual quantum computer is limited. Computation needs to be distributed to multiple entangled quantum computers in a network for complex computation [42-44]. For example, IBM's roadmap for a large-scale quantum computer with 1 million qubits is planned to have a set of interconnected quantum computers [45].

Edge networks can enable distributed computing at scale. Figure 3 illustrates a scalable quantum-edge computing scenario. In this scenario, entities in edge networks from one or more layers (as shown in Figure 1) can provide classical communication links as well as quantum communication links for network routing. Once connected coherently, multiple

quantum processing units, quantum computing units, and classical computing units can form a large-scale quantum computer that can perform more complex computational tasks.

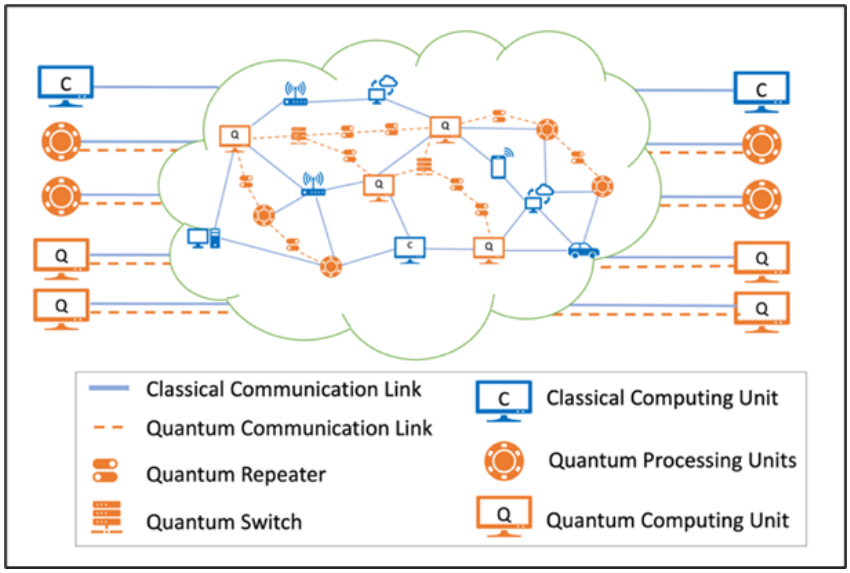

Figure 3. Illustration of a scalable quantum-edge computing scenario.

Geo-distributed classical edge endpoints, servers, and clouds provide agile networking and storage for the delivery of classical information bits. Quantum processing units, quantum computing units, quantum repeaters, and quantum switches provide quantum connectivity for multi-hop delivery of qubits.

In such a scalable quantum-edge computing scenario, geographically distributed computing units (both classical and quantum) are connected via the edge networks and work cooperatively together as a single integrated computing resource. The connections can be dynamic or static depending on the network topology, availability of network entities (edge endpoints, servers, and clouds), communication link quality, computation workload, application demands, etc.
Edge computing is a more secure architecture than cloud computing due to a few reasons. For example, data is transiently stored and analyzed close to data sources, which decreases data leakage during transmission. However, edge computing is vulnerable to various security threats such as eavesdropping [46].

A hybrid quantum-edge computing environment will have enhanced security and privacy as quantum communication can boost communication security and create more secure communication networks. As discussed in previous section, QKD allows secure communication by establishing an encryption key whose security relies only on the laws of quantum mechanics. QKD provides a solution to the task of generating a secure encryption key between two communication parties. Since QKD does not depend on the factorization of large numbers in prime numbers, the encryption keys generated by

QKD cannot be broken by the Shor algorithm running on a quantum computer or by other fast algorithms for prime factorization.

However, it is known that even by using quantum communication, there is no guarantee that the implementation is secure without imposing assumptions on the power of the adversary [47-49]. In addition, different attacks can be launched by adversaries to attack the classical communication links to disrupt the establishment of quantum communication links. For example, an adversary can launch a denial-of-service attack to flood the classical communication links with superfluous requests and prevent the requests from quantum computing units on the classical communication links.

Therefore, it cannot be deemed secure. Effective security and privacy proception need to be studied in such hybrid computing environments.

4. CHALLENGES AND OPEN PROBLEMS

Known key research challenges and open problems related to how to share quantum states among geographically distributed quantum devices such as quantum processing units and quantum computing units need to be addressed. For example, how to preserve quantum information against decoherence, how to improve quantum fidelity, and how to enable long-distance entanglement distribution and quantum teleportation, and so on.

Moreover, given the coexistence nature of quantum and classical devices and communication links in this hybrid paradigm, future research and prototyping are needed to better understand the performance of such distributed systems, data security and privacy, and implementation considerations. Future research topics include, but are not limited to:

- Scalable and flexible network protocols where new quantum nodes can be attached or removed to edge computing clusters with ease.
- Approaches to introducing new quantum computing units and algorithms while ensuring edge computing systems remain interoperable.
- Data-centric security approaches to protect data at rest and in transit in such a hybrid communication environment with mixed classical and quantum entities.
- Privacy-preserving methods to avoid privacy exposure in data aggregation and computing.
- Prototyping experiments for overall system performance benchmark and implementation considerations for different integration schemes and configurations.

5. CONCLUSION

More and more computing tasks are pushed from the cloud to the edge of the network. Quantum computing can expand the capability of edge computing as it has demonstrated advantages over classical computing. On the other hand, connected quantum information processors can achieve distributed quantum computing, and the distributed nature of edge computing networks can enable a new quantum networking scheme. In this paper, we propose a new hybrid quantum-edge computing paradigm where quantum and edge computing complement each other paradigm to achieve unparalleled capabilities that are provably impossible by using only classical computing or quantum computing scheme alone. We also discuss the challenges and opportunities that are worth working on to inspire more research in this direction.

REFERENCES

[1] W. Shi, J. Cao, Q. Zhang *et al.*, “Edge computing: Vision and challenges,” IEEE internet of things journal, 3(5), 637-646 (2016).

[2] S. Yi, Z. Hao, Q. Zhang *et al.*, "Lavea: Latency-aware video analytics on edge computing platform." 1-13.

[3] S. Yi, Z. Hao, Z. Qin *et al.*, "Fog computing: Platform and applications." 73-78.

[4] K. Ha, Z. Chen, W. Hu *et al.*, "Towards wearable cognitive assistance." 68-81.

[5] J. Xu, L. Chen, and S. Ren, “Online learning for offloading and autoscaling in energy harvesting mobile edge computing,” IEEE Transactions on Cognitive Communications and Networking, 3(3), 361-373 (2017).

[6] L. Ding, and M. B. Salem, "A novel architecture for automatic document classification for effective security in edge computing environments." 416-420.

[7] X. Wang, Y. Han, V. C. Leung *et al.*, “Convergence of edge computing and deep learning: A comprehensive survey,” IEEE Communications Surveys & Tutorials, 22(2), 869-904 (2020).

[8] E. Li, L. Zeng, Z. Zhou *et al.*, “Edge AI: On-demand accelerating deep neural network inference via edge computing,” IEEE Transactions on Wireless Communications, 19(1), 447-457 (2019).

[9] Z. Zhou, X. Chen, E. Li *et al.*, “Edge intelligence: Paving the last mile of artificial intelligence with edge computing,” Proceedings of the IEEE, 107(8), 1738-1762 (2019).

[10] S. X. Ng, A. Conti, G.-L. Long *et al.*, “Guest editorial advances in quantum communications, computing, cryptography, and sensing,” IEEE Journal on Selected Areas in Communications, 38(3), 405-412 (2020).

[11] T. D. Ladd, F. Jelezko, R. Laflamme *et al.*, “Quantum computers,” nature, 464(7285), 45-53 (2010).

[12] F. Arute, K. Arya, R. Babbush *et al.*, “Quantum supremacy using a programmable superconducting processor,” Nature, 574(7779), 505-510 (2019).

[13] H.-S. Zhong, H. Wang, Y.-H. Deng *et al.*, “Quantum computational advantage using photons,” Science, 370(6523), 1460-1463 (2020).

[14] Y. Wu, W.-S. Bao, S. Cao *et al.*, “Strong quantum computational advantage using a superconducting quantum processor,” Physical review letters, 127(18), 180501 (2021).

[15] H.-S. Zhong, Y.-H. Deng, J. Qin *et al.*, “Phase-programmable gaussian boson sampling using stimulated squeezed light,” Physical review letters, 127(18), 180502 (2021).

[16] C. H. Bennet, and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing."
[17] N. Gisin, G. Ribordy, W. Tittel *et al.*, "Quantum cryptography," Reviews of modern physics, 74(1), 145 (2002).
[18] J. I. Cirac, P. Zoller, H. J. Kimble *et al.*, "Quantum state transfer and entanglement distribution among distant nodes in a quantum network," Physical Review Letters, 78(16), 3221 (1997).
[19] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf *et al.*, "The security of practical quantum key distribution," Reviews of modern physics, 81(3), 1301 (2009).
[20] R. Horodecki, P. Horodecki, M. Horodecki *et al.*, "Quantum entanglement," Reviews of modern physics, 81(2), 865 (2009).
[21] Y.-A. Chen, Q. Zhang, T.-Y. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature, 589(7841), 214-219 (2021).
[22] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," Reviews of modern physics, 89(3), 035002 (2017).
[23] Z. Zhang, and Q. Zhuang, "Distributed quantum sensing," Quantum Science and Technology, 6(4), 043001 (2021).
[24] H. J. Kimble, "The quantum internet," Nature, 453(7198), 1023-1030 (2008).
[25] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," Science, 362(6412), eaam9288 (2018).
[26] Y.-H. Kim, S. P. Kulik, and Y. Shih, "Quantum teleportation of a polarization state with a complete Bell state measurement," Physical Review Letters, 86(7), 1370 (2001).
[27] J.-w. Pan, and A. Zeilinger, "Greenberger-horne-zeilinger-state analyzer," Physical Review A, 57(3), 2208 (1998).
[28] A. I. Lvovsky, B. C. Sanders, and W. Tittel, "Optical quantum memory," Nature photonics, 3(12), 706-714 (2009).
[29] K. Hammerer, A. S. Sørensen, and E. S. Polzik, "Quantum interface between light and atomic ensembles," Reviews of Modern Physics, 82(2), 1041 (2010).
[30] J.-W. Pan, C. Simon, Č. Brukner *et al.*, "Entanglement purification for quantum communication," Nature, 410(6832), 1067-1070 (2001).
[31] P. G. Kwiat, S. Barraza-Lopez, A. Stefanov *et al.*, "Experimental entanglement distillation and 'hidden'non-locality," Nature, 409(6823), 1014-1017 (2001).
[32] W. K. Wootters, and W. H. Zurek, "A single quantum cannot be cloned," Nature, 299(5886), 802-803 (1982).
[33] H.-J. Briegel, W. Dür, J. I. Cirac *et al.*, "Quantum repeaters: the role of imperfect local operations in quantum communication," Physical Review Letters, 81(26), 5932 (1998).
[34] N. Sangouard, C. Simon, H. De Riedmatten *et al.*, "Quantum repeaters based on atomic ensembles and linear optics," Reviews of Modern Physics, 83(1), 33 (2011).
[35] S. Muralidharan, L. Li, J. Kim *et al.*, "Optimal architectures for long distance quantum communication," Scientific reports, 6(1), 1-10 (2016).
[36] C. H. Bennett, G. Brassard, C. Crépeau *et al.*, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Physical review letters, 70(13), 1895 (1993).
[37] M. Pant, H. Krovi, D. Towsley *et al.*, "Routing entanglement in the quantum internet," npj Quantum Information, 5(1), 1-9 (2019).

[38] K. Chakraborty, F. Rozpedek, A. Dahlberg *et al.*, “Distributed routing in a quantum internet,” arXiv preprint arXiv:1907.11630, (2019).
[39] L. M. Vaquero, and L. Rodero-Merino, “Finding your way in the fog: Towards a comprehensive definition of fog computing,” ACM SIGCOMM computer communication Review, 44(5), 27-32 (2014).
[40] J. Shropshire, “Extending the cloud with fog: Security challenges & opportunities,” (2014).
[41] V. K. Sehgal, A. Patrick, A. Soni *et al.*, [Smart human security framework using internet of things, cloud and fog computing] Springer, (2015).
[42] L. Gyongyosi, and S. Imre, “Scalable distributed gate-model quantum computers,” Scientific reports, 11(1), 1-28 (2021).
[43] R. Van Meter, and S. J. Devitt, “The path to scalable distributed quantum computing,” Computer, 49(9), 31-42 (2016).
[44] A. S. Cacciapuoti, M. Caleffi, F. Tafuri *et al.*, “Quantum internet: networking challenges in distributed quantum computing,” IEEE Network, 34(1), 137-143 (2019).
[45] “https://research.ibm.com/blog/ibm-quantum-roadmap ”.
[46] J. Ni, K. Zhang, X. Lin *et al.*, “Securing fog computing for internet of things applications: Challenges and solutions,” IEEE Communications Surveys & Tutorials, 20(1), 601-628 (2017).
[47] D. Mayers, “Unconditionally secure quantum bit commitment is impossible,” Physical review letters, 78(17), 3414 (1997).
[48] H.-K. Lo, and H. F. Chau, “Is quantum bit commitment really possible?,” Physical Review Letters, 78(17), 3410 (1997).
[49] H.-K. Lo, “Insecurity of quantum secure computations,” Physical Review A, 56(2), 1154 (1997).