Hindawi
Quantum Engineering
Volume 2022, Article ID 6345981, 6 pages
https://doi.org/10.1155/2022/6345981

*Research Article*

# QNUS: Reducing Terminal Resources in Quantum Secure Direct Communication Network Using Switches

**Peng-Hao Niu**,[1,2,3] **Fei-Hao Zhang**,[1] **Xiu-Wei Chen**,[1] **Min Wang**,[1] **and Gui-Lu Long**[1,2,3,4]

[1]*Beijing Academy of Quantum Information Sciences, Beijing, China*
[2]*State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing, China*
[3]*Frontier Science Center for Quantum Information, Beijing, China*
[4]*Beijing National Research Center for Information Science and Technology, Beijing, China*

Correspondence should be addressed to Gui-Lu Long; gllong@tsinghua.edu.cn

Received 5 May 2022; Accepted 29 June 2022; Published 4 August 2022

Academic Editor: Shi Hai Dong



The quantum network is an indispensable step toward multiuser and wide-area information interchange in the course of the development of quantum technology. When designing and deploying a quantum network, availability, robustness, flexibility, and expenditure need to be considered in a balanced way. In this article, we propose a network connected through optical switches, QNUS, that requires only terminals in the number of nodes in a quantum network, which is a great saving of resources.

## 1. Introduction

Quantum cryptography and communication have been developing for several decades. In 1984, the first quantum key distribution (QKD) protocol where secure keys are agreed was proposed [1]. It has grown maturely and is developing fast [2–7]. Another important quantum communication branch, quantum secure direct communication (QSDC) [8–10], was proposed in 2000. QSDC is one kind of quantum communication that transmits confidential information in quantum channels directly without establishing secure keys in advance. It has been developing fast in recent years both in theory and experiment [11–21], and an experimental prototype has also been completed [22]. It has been shown that using a procedure called INCUM, QSDC can be performed with the same distance and transmission rate as QKD [15]. The distance of QSDC has been extended gradually in the past few years, and it has reached 100 km in low-loss fiber [16]. By combining QSDC with classical cryptography, a classical secure-repeater can be constructed, prolonging the distance endlessly with end-to-end security [17]. A 15-user QSDC network was reported in [21].

The quantum network is a vital avenue for multiuser and wide-scale applications. The quantum network led by DARPA [23] is the first field test of the QKD network on a metropolitan scale. In 2007, a four-node QKD network was set up in the commercial fiber network in Beijing [24]. Four users can be connected to each other with the help of wavelength division multiplexing, and all quantum sources are set at one node. Then, in 2009, a seven-user quantum network was constructed in Wuhu, Anhui, China [25]. The Wuhu quantum network contains five nodes with one node also used as a trusted relay connected with a subnetwork. This network expands to a quantum network linked up with three cities and two metropolitan areas, which is named as Hefei-Chaohu-Wuhu wide-area networks [26]. Los Alamos National Laboratory (LANL) also built a quantum network using an approach called "network-centric quantum communication (NQC)" [27]. It forms a "hub-and-spoke" topology, a trusted authority (TA) is at the hub node, and other nodes connect to this TA hub. Any node that wants to communicate needs to execute the QKD process with TA, and then use the secure key to transmit messages to each other. In Europe, SEcure COmmunication based on Quantum Cryptography (SECOQC) was established with six

nodes connected by eight links in Vienna [28]. The SECOQC utilizes different kinds of QKD protocols, including coherent pulses, entanglement-based, continuous-variable, and free-space. Besides, a four-node quantum network was built in Tokyo [29] with six different QKD systems and achieves secure TV conferencing over a 45 km distance. Quantum networks in a wide area have also been researched in long-distance telecom fiber and free-space links [30].

Network topology is important when constructing a quantum network. It involves the interrelationship between nodes, placement of links and facilities, and finally the cost of building a multi-user quantum network. At present, quantum communication equipment is costly [31]. Therefore designing a quantum network with reduced resources is very important at the present stage, and one way to achieve it is by utilizing optical switches which allow sharing of resources of quantum devices in a quantum network [32]. Here, we propose a scheme for constructing quantum networks with reduced resources. The scheme decreases the number of quantum transceivers, meanwhile holding the availability, flexibility, and robustness. In this article, current quantum networks' topology and structure will be discussed in Section 2, then followed by the details of our scheme in Section 3. Finally, we will discuss our scheme and compare it with other quantum networks design in Section 4.

## 2. Quantum Network Schemes

*2.1. QKD Network.* One type of QKD network topology is the star shape, where there is a central node, to which all other nodes are connected, as shown in Figure 1. Most quantum network topology is designed as a star network, such as DARPA's QKD network [23], LANL's NQC network [27], the Tokyo QKD network [29], the four-node quantum network in Beijing [24], and the five-node quantum network in Wuhu [25, 33]. The central node can serve as a trusted authority (TA) [27] or an optical router with the help of optical components [25, 34]. The other nodes will be connected to the user's terminal or used as a trusted relay to connect to another subnetwork [24].

Another kind of quantum network topology is the ring shape, such as the SECOQC QKD network [35] and the Swiss Quantum QKD network [36]. It is worth noting that sometimes mixtures of star and ring shapes are used, for instance, the SECOQC network forms a ring shape with four nodes and there are diagonal links, so it is a mesh topology. In the ring topology, to achieve the interconnection of nodes, some nodes will be used as relays and some nodes need many sets of quantum transmitters or receivers. For example, in Figure 2, it is a three-node QKD network that forms a ring. Each node needs a quantum transmitter or a quantum receiver to interconnect to the other two nodes. It is easy to generalize this to a four-node ring quantum network. In a four-node ring shape QKD network, each node is connected to other two nodes if there are no diagonal links. Then, each node needs two quantum transmitters or receivers to achieve the interconnection of these four nodes. If two diagonal nodes need to connect directly, either the link should go through a third node between them, and the third node serves as a trusted relay, or diagonal links should

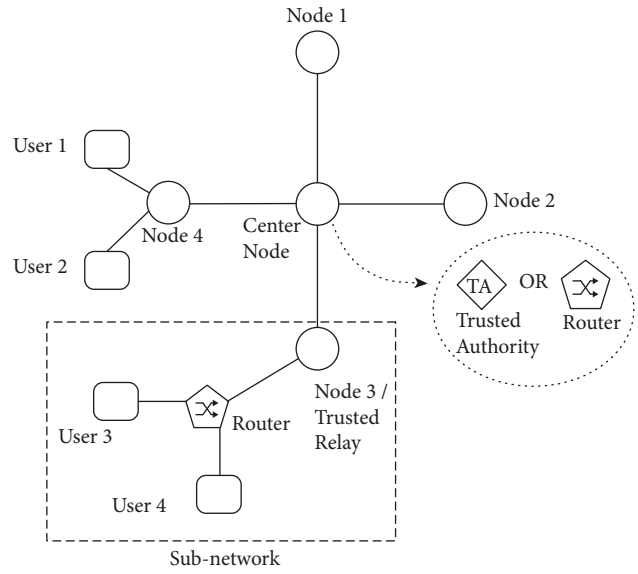


Figure 1: The star topology QKD network.

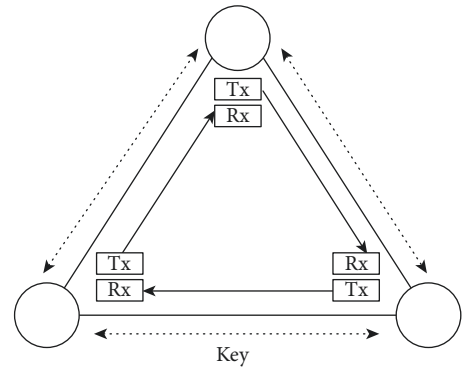


Figure 2: The ring topology QKD network. Each node needs only one transmitter or receiver to connect with another node.

be established and each node will need three quantum transmitters and receivers [35].

In QKD architecture, the resulting keys are symmetric between quantum transmitters (Tx) and quantum receivers (Rx), they only need one quantum transmitter and one quantum receiver for a link.

*2.2. QSDC Network.* Confidential messages are transmitted directly in a quantum channel from sender to receiver, which means it has a direction. Therefore, if two parties want to have a bidirectional communication, each of them needs a QSDC transmitter and a receiver, that is, a QSDC transceiver.

Let us discuss the situation of quantum networks of QSDC. In the star network, each node that connects to the central node is deployed with a QSDC transceiver to communicate with the central node, and the central node will need to deploy $m$ quantum transceivers where $m$ is the number of nodes connected to the central node. The star network is convenient to construct, whereas considering the

robustness, if the central node is in a breakdown, the whole network will be in paralysis, like the QKD network too.

The ring network can offer some kind of robustness. Nodes are relatively equal, so the breakdown of one node will not affect the whole network, and one link's failure will not interrupt communications, which will be explained in Section 3. However, the amount of quantum transceivers deployed in the ring network increases obviously, as shown in Figure 3. In a three-node ring network of QSDC, each node connects with the other two nodes and needs two quantum transceivers to have a bidirectional communication, which means four quantum terminals at each node. The quantities of quantum terminals at each node will increase to six in a four-node ring network with diagonal links, that is, a mesh network. Therefore, it requires a new way to address the quantity issue in the ring or mesh QSDC network while maintaining the advantage of robustness and availability.

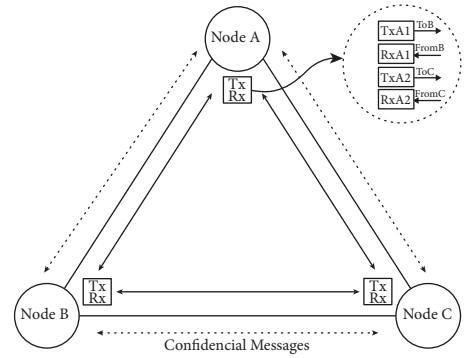


Figure 3: The ring topology QSDC network. Each node needs one transmitter and one receiver at the same time to connect with another node for mutual communication.

## 3. QSDC Network Using Switches (QNUS)

We take the mesh topology as an example to illustrate our idea. In Figure 4, if node $A$ wants to communicate with node $C$, then the link could be $A\leftrightarrow 3\leftrightarrow C$ or $A\leftrightarrow 1\leftrightarrow 4\leftrightarrow C$ or $A\leftrightarrow 2\leftrightarrow 5\leftrightarrow C$, which provides multiple paths. The strength of this topology is if link 3 is a breakdown, node $A$ and node $C$ can still use another link to prevent a communication interruption. Links 1 and 4 can connect directly at node $B$ using optical switches, so node $B$ would not need to serve as a relay when node $A$ is communicating with node $C$. This will not only save the number of relays but also avoids the security shift from quantum to classical protection at the relay station. In the usual realization, each link needs two transceivers, hence the number of transceivers required is 10 in Figure 4.

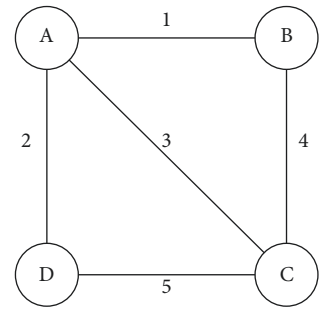


Figure 4: A mesh topology QSDC network.

Now, we describe the structure of nodes in the QNUS and show how this QNUS scheme reduces the number of QSDC transceivers. The key point is to give the links switchover capability in the network. Figure 5 shows the inside structure of node $A$ of Figure 4. The optical switch forms a quantum router that can connect different links as required. Each optical switch is a $1\times 3$ switch and the input port can only connect to one output port of the three at a time. For example, node $A$ can communicate with node $C$ through link 3 if the switch connects $a\leftrightarrow a-c\leftrightarrow c$. Node $A$ can also communicate with node $B$ or $D$ through $a\leftrightarrow a-b\leftrightarrow b$ or $a\leftrightarrow a-d\leftrightarrow d$, whereas only one quantum transceiver is needed.

The optical switch used in node $B$ is a $1\times 2$ switch, as shown in Figure 6. Node $B$ can communicate with other nodes with the help of quantum routers, and only one quantum transceiver is deployed. It should note that link 1 and link 4 can be connected at node $B$ through $a\leftrightarrow a-c\leftrightarrow c$, which means node $A$ and node $C$ are connected directly without a relay. When node $A$ communicates with node $C$ through node $B$, node $B$ cannot talk to nodes $A$ or $C$. Structures of nodes $C$ and $D$ are similar to nodes $B$ and $A$.

Quantum routers at different nodes can cooperate to achieve a required links' connection, and then each node can communicate with other nodes bidirectionally. At the same time, the total amounts of quantum transceivers needed in the four-node QSDC network reduce to four rather than ten.

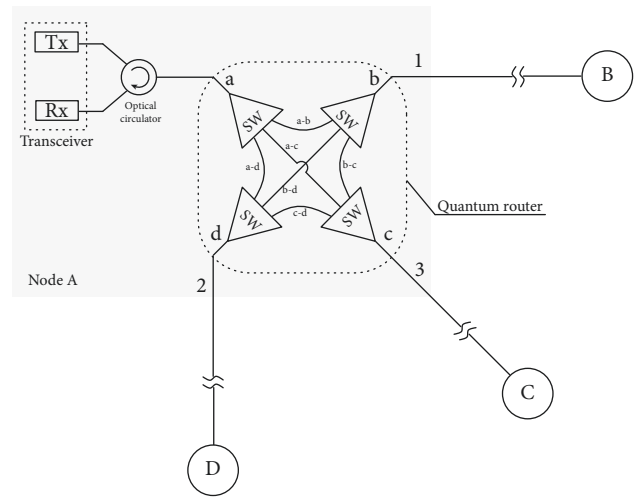


Figure 5: Structure of node $A$ in Figure 4. The light gray area indicates node $A$ which connects to node $B$, $C$, and $D$ through links 1, 2, and 3. SW: optical switch. Tx and Rx: QSDC transmitter and receiver.

This means that each node needs only one transceiver (a transmitter and a receiver). This kind of scheme can also generalize to other mesh topology networks with more nodes. For a node with $n$ links connected, $n+1$ optical switches with $1\times n$ size are needed to construct a quantum router. The $1\times n\,(n>1)$ switch can also be made with $n-1$ optical switches with $1\times 2$ size, as shown in Figure 7.

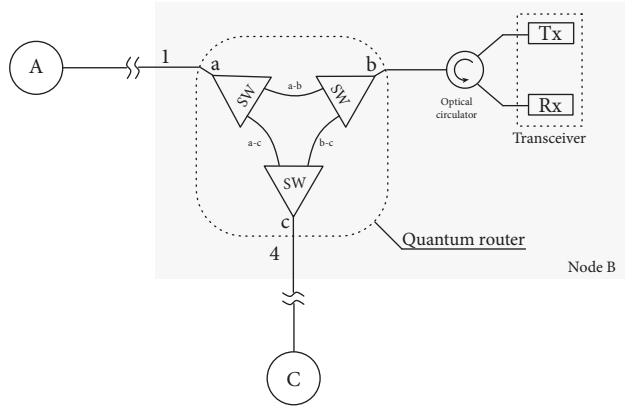


Figure 6: Structure of node $B$ in Figure 4. The light gray area indicates node $B$ which connects to nodes $A$ and $C$ through links 1 and 4. SW: optical switch. Tx and Rx: QSDC transmitter and receiver.

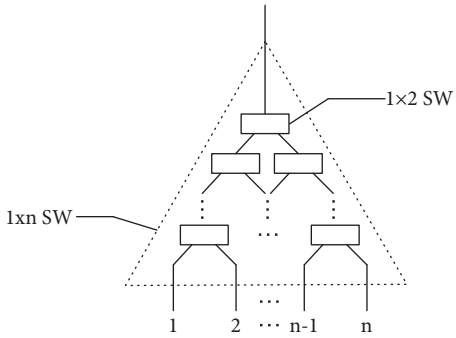


Figure 7: The $1 \times n$ switch made with $1 \times 2$ switch.

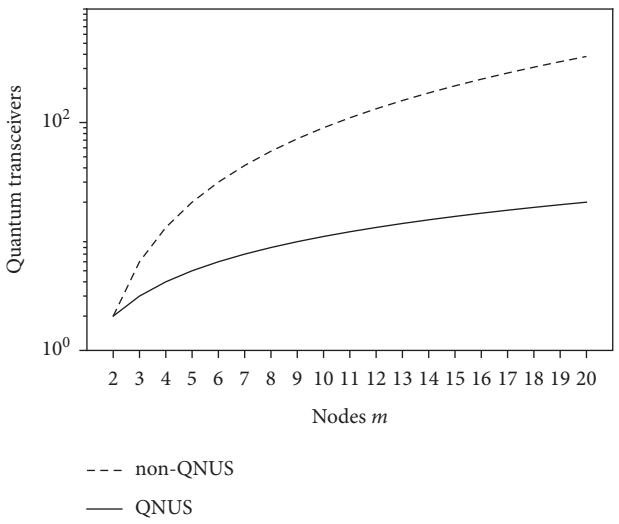


Figure 8: The number of quantum transceivers required in a full-mesh quantum network under QNUS and non-QNUS. $m$ is the amount of nodes.

## 4. Discussion

We proposed a scheme of QSDC networks with optical switches, namely QNUS. The scheme utilizes optical switches to form quantum routers and deploys them in a distributed manner across nodes. Compared with the network without optical switches, this scheme reduces the number of transceivers from $2N_l$ to $N_n$, where $N_l$ is the number of links and $N_n$ is the number of nodes in a network. Usually, the number of links is a quadratic function of $N_n$, thus QNUS could lead up to a square-root reduction of the transceivers' number in a quantum network, as shown in Figure 8.

However, such a dramatic saving also has a price to pay, for example, before setting up a telephone call, one must exchange the connection information to set up the links between related nodes through optical switches, which may cause some delays. In order to estimate the delay roughly, we assume there are a user Alice as the sender and a user Bob as the receiver. Usually, Alice will make a phone call with a user-oriented terminal, and the calling signal will be sent to a network management system (NMS) at the nearest node. We simplify the model as shown in Figure 9(a), calling signal will transmit to the NMS firstly with time $t_1$, then the NMS at both nodes addresses and establishes connections via the classical network, thus specifying the two parties of the quantum communication, which will cost time of $t_2$. Voice messages will then be transmitted to the QSDC transmitter with time $t_3$, then through the quantum channel with time $t_4$, and then to the node of the receiver and finally received by Bob with time $t_5 + t_6$. This is the situation of the non-QNUS network. In QNUS, as shown in Figure 9(b), after NMSs confirm participants of the quantum communication, the NMS at each node will set up the optical switches in the quantum router. We note the time required to finish this process is $t_2'$. This time $t_2'$ includes the transmission time of the control signal from the NMS to the quantum router, and the switching delay of optical switches. The typical delay of optical switching is about 10~100 $\mu$s [37]. Then, voice messages will be sent to the QSDC transmitter following a similar process as in Figure 9(a). It should be noted that we assume the time spent on the internal optical path in a quantum router is ignored. We can now figure out that the delay $\Delta$ caused by QNUS compared with non-QNUS is $\Delta \leq 2t_2'$.

In addition, compared to the non-QNUS quantum network, there may be more than one transceiver in the node of such network, which can support more than one

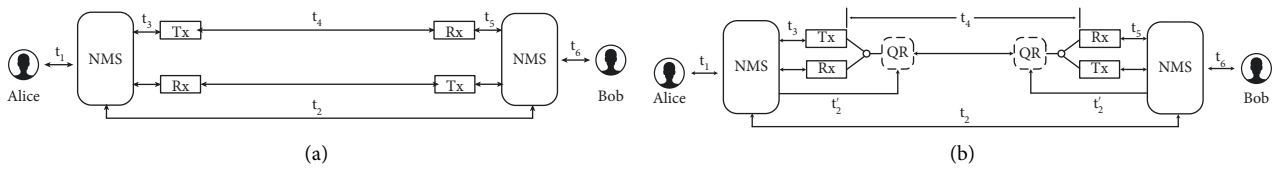


Figure 9: Comparison of delays between the (a) non-QNUS and (b) QNUS. QR: quantum router.

communication process at the same time, whereas this is achieved at a higher cost.

The QNUS scheme can be generalized to other quantum networks, provided that the information transmitted in the corresponding network links has directional requirements.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work was supported by the National Key R & D Program of China (2017YFA0303700), the Key R & D Program of Guangdong Province (2018B030325002), the Tsinghua University Initiative Scientific Research Program, the National Natural Science Foundation of China under Grants No. 61727801 and No. 11974205, and in part by the Beijing Advanced Innovation Center for Future Chip (ICFC).

## References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 175–179, 1984.

[2] L. C. Kwek, L. Cao, W. Luo et al., "Chip-based quantum key distribution," *AAPPS Bulletin*, vol. 31, no. 1, p. 15, 2021.

[3] G. Z. Tang, C. Y. Li, and M. Wang, "Polarization discriminated time-bin phase-encoding measurement-device-independent quantum key distribution," *Quantum Engineering*, vol. 3, no. 4, p. e79, 2021.

[4] G. J. Fan-Yuan, S. Wang, Z. Q. Yin et al., "Afterpulse analysis for passive decoy quantum key distribution," *Quantum Engineering*, vol. 2, no. 4, p. e56, 2020.

[5] G. Chai, D. Li, Z. Cao, M. Zhang, P. Huang, and G. Zeng, "Blind channel estimation for continuous-variable quantum key distribution," *Quantum Engineering*, vol. 2, no. 2, p. e37, 2020.

[6] S. P. Kish, E. Villaseñor, R. Malaney, K. A. Mudge, and K. J. Grant, "Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-earth channel," *Quantum Engineering*, vol. 2, no. 3, 2020.

[7] Y. Zhang and Q. Ni, "Design and analysis of random multiple access quantum key distribution," *Quantum Engineering*, vol. 2, no. 1, 2020.

[8] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Physical Review A*, vol. 65, no. 3, Article ID 032302, 2002.

[9] F. G. Deng, G. L. Long, and X. S. Liu, "Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block," *Physical Review A*, vol. 68, no. 4, Article ID 042317, 2003.

[10] F. G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Physical Review A*, vol. 69, no. 5, Article ID 052319, 2004.

[11] J. Wu, Z. Lin, L. Yin, and G. L. Long, "Security of quantum secure direct communication based on wyner's wiretap channel theory," *Quantum Engineering*, vol. 1, no. 4, 2019.

[12] J. Y. Hu, B. Yu, M. Y. Jing et al., "Experimental quantum secure direct communication with single photons," *Light: Science & Applications*, vol. 5, no. 9, Article ID e16144, 2016.

[13] W. Zhang, D. S. Ding, Y. B. Sheng, L. Zhou, B. S. Shi, and G. C. Guo, "Quantum secure direct communication with quantum memory," *Physical Review Letters*, vol. 118, no. 22, Article ID 220501, 2017.

[14] F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, "Experimental long-distance quantum secure direct communication," *Science Bulletin*, vol. 62, no. 22, pp. 1519–1524, 2017.

[15] G. L. Long and H. Zhang, "Drastic increase of channel capacity in quantum secure direct communication using masking," *Science Bulletin*, vol. 66, no. 13, pp. 1267–1269, 2021.

[16] H. Zhang, Z. Sun, R. Qi, L. Yin, G. L. Long, and J. Lu, "Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states," *Light: Science & Applications*, vol. 11, no. 1, p. 83, 2022.

[17] G. L. Long, D. Pan, Y. B. Sheng, Q. Xue, J. Lu, and L. Hanzo, "An evolutionary pathway for the quantum internet relying on secure classical repeaters," 2022, https://arxiv.org/pdf/2202.03619.pdf.

[18] C. Y. Gao, P. L. Guo, and B. C. Ren, "Efficient quantum secure direct communication with complete bell-state measurement," *Quantum Engineering*, vol. 3, no. 4, 2021.

[19] C. Wang, "Quantum secure direct communication: intersection of communication and cryptography," *Fundamental Research*, vol. 1, no. 1, pp. 91-92, 2021.

[20] R. X. Wang, "Quantum secure data transfer with pulse shape encoded optical qubits," *Quantum Engineering*, vol. 3, no. 4, 2021.

[21] Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, "A 15-user quantum secure direct communication network," *Light: Science & Applications*, vol. 10, no. 1, p. 183, 2021.

[22] R. Qi, Z. Sun, Z. Lin et al., "Implementation and security analysis of practical quantum secure direct communication," *Light: Science & Applications*, vol. 8, no. 1, 2019.

[23] C. Elliott, D. Pearson, and G. Troxel, *Quantum Cryptography in Practice*ACM Press, Karlsruhe, Germany, 2003.

[24] W. Chen, Z.-F. Han, T. Zhang et al., "Field experiment on a "star type" metropolitan quantum key distribution network,"

*IEEE Photonics Technology Letters*, vol. 21, no. 9, pp. 575–577, 2009.

[25] F. Xu, W. Chen, S. Wang et al., "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chinese Science Bulletin*, vol. 54, no. 17, pp. 2991–2997, 2009.

[26] S. Wang, W. Chen, Z. Q. Yin et al., "Field and long-term demonstration of a wide area quantum key distribution network," *Optics Express*, vol. 22, no. 18, Article ID 21739, 2014.

[27] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, "Network-centric quantum communications with application to critical infrastructure protection," 2013, https://arxiv.org/abs/1305.0305.

[28] A. Poppe, M. Peev, and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna," *International Journal of Quantum Information*, vol. 6, no. 2, pp. 209–218, 2008.

[29] M. Sasaki, M. Fujiwara, H. Ishizuka et al., "Field test of quantum key distribution in the Tokyo QKD network," *Optics Express*, vol. 19, no. 11, Article ID 10387, 2011.

[30] T. Y. Chen, X. Jiang, S. B. Tang et al., "Implementation of a 46-node quantum metropolitan area network," *Npj Quantum Information*, vol. 7, no. 1, p. 134, 2021.

[31] E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *Npj Quantum Information*, vol. 2, no. 1, Article ID 16025, 2016.

[32] A. Tayduganov, V. Rodimin, E. O. Kiktenko et al., "Optimizing the deployment of quantum key distribution switch-based networks," *Optics Express*, vol. 29, no. 16, pp. 24884–24898, 2021.

[33] S. Wang, W. Chen, Z. Q. Yin et al., "Field test of wavelength-saving quantum key distribution network," *Optics Letters*, vol. 35, no. 14, p. 2454, 2010.

[34] C. Elliott, "The DARPA quantum network," 2004, https://arxiv.org/abs/quant-ph/0412029.

[35] M. Peev, C. Pacher, R. Alléaume et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, no. 7, Article ID 075001, 2009.

[36] D. Stucki, M. Legré, F. Buntschu et al., "Long-term performance of the swissquantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, Article ID 123001, 2011.

[37] S. Nakamura, K. Sekiya, S. Matano et al., "High-speed and on-chip optical switch based on a graphene microheater," *ACS Nano*, vol. 16, no. 2, pp. 2690–2698, 2022.