

Article

Cost-Optimization-Based Quantum Key Distribution over Quantum Key Pool Optical Networks

Jie Jia ^{1,2}, Bowen Dong ^{1,2}, Le Kang ^{1,2}, Huanwen Xie ^{1,2} and Banghong Guo ^{1,*} 

¹ Guangdong Provincial Key Laboratory of Nanophotonic Functional Materials and Devices, Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, South China Normal University, Guangzhou 510006, China

² National Quantum Communication (Guangdong) Co., Ltd., Guangzhou 510700, China

* Correspondence: guobh@scnu.edu.cn

Abstract: The Measurement-Device-Independent-Quantum Key Distribution (MDI-QKD) has the advantage of extending the secure transmission distances. The MDI-QKD combined with the Hybrid-Trusted and Untrusted Relay (HTUR) is used to deploy large-scale QKD networks, which effectively saves deployment cost. We propose an improved scheme for the QKD network architecture and cost analysis, which simplifies the number of QKD transmitters and incorporates the quantum key pool (QKP) in the QKD network. We developed a novel Hybrid-QKD-Network-Cost (HQNC) heuristic algorithm to solve the cost optimization problem. Simulations verified that the scheme in this paper could save the cost by over 50 percent and 90 percent, respectively.

Keywords: trusted and untrusted relay; measurement-device-independent quantum key distribution; optical networks; quantum key pool; cost optimization



Citation: Jia, J.; Dong, B.; Kang, L.; Xie, H.; Guo, B. Cost-Optimization-Based Quantum Key Distribution over Quantum Key Pool Optical Networks. *Entropy* **2023**, *25*, 661. <https://doi.org/10.3390/e25040661>

Academic Editors: Avishy Carmi, Eliahu Cohen and Dana Ben Porath

Received: 20 March 2023

Revised: 7 April 2023

Accepted: 7 April 2023

Published: 14 April 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Quantum Key Distribution (QKD) [1,2] technology has caused abundant research and attention from academia and industry. The expansion of multi-user networks [3,4] is an inevitable trend. The transmission distance is from the initial few meters to today's hundreds [5] and even thousands of kilometers [6], as well as the secret key rate from the bit to the Mbps [7] level.

There are many more technologies to widely deploy QKD networks: quantum relay, trusted relay, untrusted relay, and optical switch. In recent years, quantum relay [8–10] technology has made significant progress, but its development has been mainly concentrated on the laboratory setting [9], which is still some distance away from real practicality. The trusted relay [11,12] is the most-widely used relaying technology and the most-mature one. The untrusted relay [13] provides higher security, but limited transmission distance. QKD networks based on optical switches [14] are easy to implement. The optical switch is used as an intermediate node to extend the QKD secure transmission distance within a certain distance range and reduce the deployment cost of QKD networks. Yet, the application range is small and limited by the distance, as well as the number of users.

Multiple-user [3,15] QKD networks are crucial for realizing secure communication in a practical environment. The United States, Europe, and Japan are actively laying out quantum communication networks and applying the to various fields. In fact, the above QKD networks are based on the trusted relay and optical switch. The deployment of quantum relays has not yet been implemented in a mature network. A detailed comparison is given in Table 1.

Table 1. Current actual QKD networks.

Network	Node Number	Relay
DARPA quantum network [16]	10	Trusted relay Optical switch
SECOQC quantum network [17]	6	Trusted relay
Tokyo quantum network [18] network	6	Trusted relay
Space-to-ground quantum network [6]	32	Trusted relay

The Measurement-Device-Independent-Quantum Key Distribution (MDI-QKD) [19,20] closes all detector vulnerabilities and doubles the transmission distance. Based on existing networks, the MDI-QKD [13] network with the Hybrid Trusted and Untrusted Relay (HTUR) extends the transmission distance and improves security further, where untrusted relays do not rely on any assumptions on measurement. We note the introduction of the Quantum Key Pool (QKP) [4,21–23] in QKD networks. The secret keys generated between QKD node pairs are stored in the QKP temporarily to reduce the waste of secret keys. The QKP increases the secret key resource utilization, which thoroughly lowers the deployment of crucial QKD devices and saves costs.

Hence, how to efficiently deploy HTUR QKD networks with the QKP is an essential problem. In this paper, we addressed this issue and focused on the optimization of the deployment cost with the Hybrid QKD Network cost (HQCNC) heuristic algorithm. Our main contributions are as follows

(I) We introduced a new four-layer architecture of the QKD network, in which the QKPs are deployed in the QKD layer temporarily to store the secret keys generated between QKD node pairs.

(II) We propose a new HTUR QKD network structure with the QKP used to illustrate the long-distance secret keys' transmission.

(III) We established a new HTUR QKD network cost model where the deployment costs of various QKD devices are considered.

(IV) We designed an HQNC heuristic algorithm to evaluate the performance through numerical simulation and performed a comparative analysis with the Cost-Optimized QKD Backbone Networking (CO-QBN) and Purely Trusted Relay (PTR) schemes in terms of network device depletion and total deployment cost, respectively.

The rest of this paper is structured as follows: Section 2 briefly describes the QKD network architecture and node structure. Section 3 defines the network model and cost model. Section 4 proposes an efficient HQNC heuristic algorithm, and performs extensive numerical simulations for the performance evaluation. Finally, Section 5 gives the conclusion.

2. QKD Network Architecture

In this section, we introduce a QKD network architecture, as shown in Figure 1. This network architecture consists of a four-layer structure: the Application layer (APP layer), the control layer, the QKD layer, and the optical layer, respectively. Compared with Cao et al. [24], the architecture in this paper adopts the MDI-QKD [19,25,26] protocol and introduces the HTUR for cooperative deployment. The QKPs tentatively store the secret keys generated by the two neighboring nodes. The abbreviations and definitions in this paper are listed in Table 2.

Table 2. Abbreviations and definitions.

Abbreviations	Definitions
QKD	Quantum Key Distribution
MDI	Measurement-Device-Independent
QKP	Quantum Key Pool
SDN	Software-Defined Network
HQNC	Hybrid QKD Network Cost
HTUR	Hybrid Trusted and Untrusted Relay
CO-QBN	Cost-Optimized QKD Backbone Networking
PTR	Purely Trusted Relay
API	Application Programming Interface
QTs	Quantum Transmitters
QRs	Quantum Receivers
KM	Key Management
KS	Key Service
OSs	Optical Switches
EDFA	Erbium-Doped Fiber Amplifiers
MOD	Multiplex/Demultiplex
CS	Current Scenario
FS	Future Scenario
PCh	Public Channel
DCh	Data Channel
QCh	Quantum Channel
NSFNET	National Science Foundation Network
USNET	United States Network

The four layers of the structure collaborate with each other to complete the unconditional secure information encryption transmission. In the APP layer, multiple QKD users randomly send out secret key requests, and each user with specific security requirements requests a certain number of secret keys from the QKD layer. The Software-Defined Network (SDN) controller receives the QKD user's requests through the northbound interface [27] (restful Application Programming Interface (API) protocol). The user requests with a high secret key demand are prioritized and sent to the QKD layer and optical layer via the southbound interface [28] (open flow protocol). In the QKD layer, three different nodes are required: the QKD nodes, the trusted relay nodes, and the untrusted relay nodes. Secret keys are generated between neighboring QKD nodes and trusted relay nodes or between two neighboring trusted relay nodes. Untrusted relay nodes are third-party nodes. The QKD layer sends the secret keys located in the QKP to the optical layer, which is co-located with the QKD layer. Then, the encryption of the security information requested by a specific user is achieved. Finally, the SDN controller sends the completion command to the application layer.

As shown in Figure 2, the trusted relay nodes include the Measurement-Device-Independent-Quantum Transmitters (MDI-QTs), the Key Service (KS), and the Optical Switches (OSs). When the OS and Untrusted Relay 1 are connected, a pair of secret keys K_A is generated between QKD Node 1 and Trusted Relay Node 1, and the generated key pair K_A is temporarily stored in QKP1. When the OS and Untrusted Relay 2 are connected, a pair of secret keys K_B is generated between QKD Node 2 and Trusted Relay Node 1, and the generated secret key pair K_B is temporarily stored in QKP2. For the secret key requirements of more distant node pairs, the staggered deployment of the HTUR is added to the QKD links. Note that only one MDI-QTs device is contained in Trusted Relay Node 1, and we would flexibly utilize the MDI-QTs located in Trusted Relay Node 1 by controlling the OS. The secret keys' transfer process between the remote QKD Node 1 and QKD Node 2 is as follows: the K_A and K_B located in KS3 conduct the bitwise exclusive OR operation, and $k_A \oplus K_B$ is sent to KS2 through a key management (KM) link. According to $K_B \oplus (K_A \oplus K_B) = K_A$, the KS2 retrieves K_A . Then, both KS1 and KS2 would access K_A . Hence, K_A is shared between QKD Node 1 and QKD Node 2.

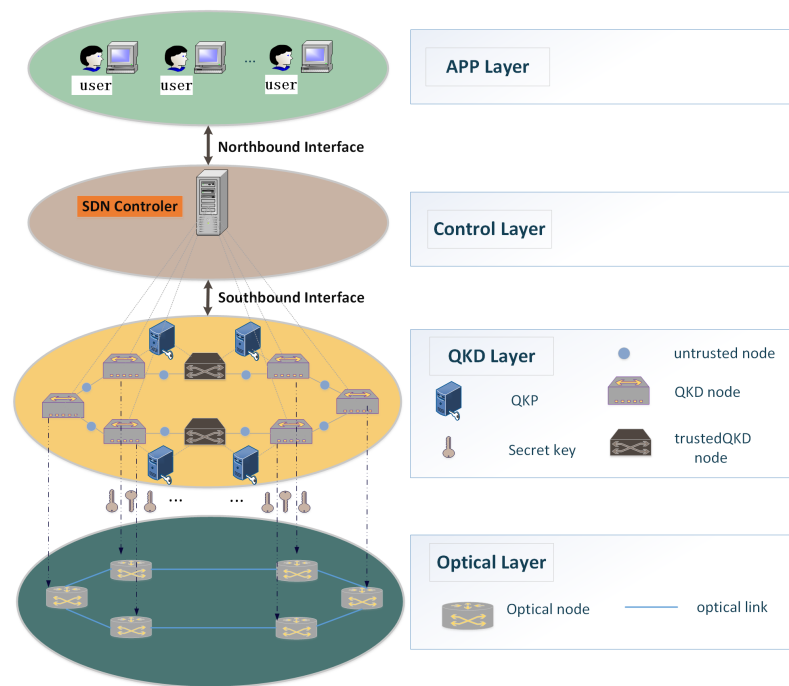


Figure 1. QKD network architecture.

In the QKD network, the Public Channel (PCh) and the Data Channel (DCh) deploy Erbium-Doped Fiber Amplifiers (EDFAs) at every distance of 80 km ($m = 80$ km) [29] on the optical link to enable the long-distance transmission of optical signals, where m denotes the distance between the adjacent QKD node/trusted relay and the untrusted relay. In this paper, we reference the previous literature [13,30]: when the untrusted relay or the trusted relay is deployed at the same physical location as the EDFA, only one Multiplex/Demultiplex (MOD) component can be used for both the EDFA bypass [31] and the multiplexing/demultiplexing QKD, KM, and optical links. Hence, to save the MOD component, we assumed that the trusted and untrusted relays are deployed at the same location as the EDFAs. In the MDI-QKD network, the distances of two adjacent MDI-QTs and trusted–untrusted relays are 160 km and 80 km, respectively.

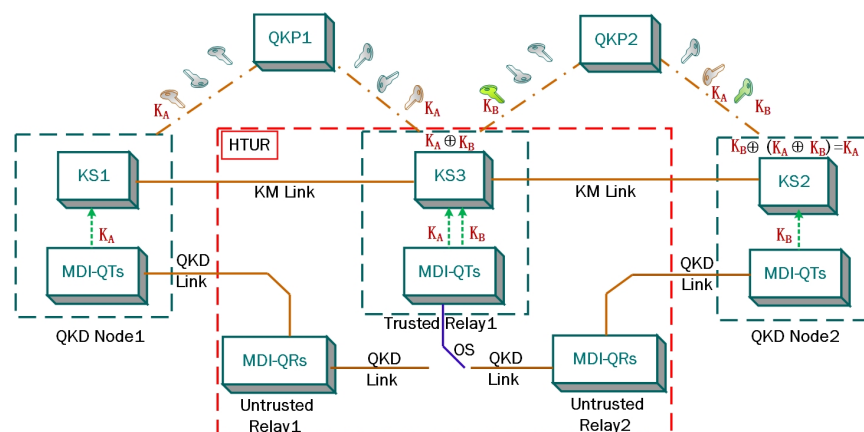


Figure 2. Structure of HTUR QKD layer based on the QKP.

3. Problem and Algorithm Formulation

In this section, we formulate the cost model and the algorithm model to elaborate the QKD network cost less problem. The notations used in this paper are listed and defined in Table 3.

Table 3. Symbols and definitions.

Symbols	Definitions
$G(N, L)$	Optical/QKD network topology
N	Set of optical/QKD nodes
L	Set of QKD links
m	The distance between QKD Node 1/trusted relay and untrusted relay
$r(s_r, d_r, P_r)$	A QKD request between two arbitrary distant QKD nodes
R	Total QKD requests in QKD backbone network
P_r	The number of parallel QKD links of r
E_r	Secret key rate of r
D	The distance of a pair of MDI-QTs
E_D	The secret key rate at distance D
L_r	Set of fiber links on the path of r
L_{sd}	Set of fiber links between QBNs s_r and d_r
γ	The wavelength of QKD link
ω	The wavelength of KM link
(α, β)	Index of QBN nodes in QKD network topology $G(N, L)$. $(\alpha, \beta) \in G(N, L)$
W_Q	Set of wavelength channels planned as QChs
W_{KM}	Set of wavelength channels planned as KM
M_{QT}^r	Required number of MDI-QTs for r
M_{QR}^r	Required number of MDI-QRs for r
M_{KS}^r	Required number of KSs for r
M_{MOD}^r	Required number of pairs of Multiplexes/Demultiplexes (MODs) for r
δ_{QT}^r	Cost of an MDI-QTs for r
δ_{QR}^r	Cost of an MDI-QRs for r
δ_{KS}^r	Cost of a KS for r
δ_{MOD}^r	Cost of a pair of MODs for r
δ_L^r	Cost per kilometer of a wavelength channel on a fiber link
C_{QT}^R	Cost of MDI-QTs for all QKD link requests R
C_{QR}^R	Cost of MDI-QRs for all QKD link requests R
C_{KS}^R	Cost of KS for all QKD link requests R
C_L^R	Cost of QKD and KM link for all QKD link requests R
C_{MOD}^R	Cost of pairs of MODs for all QKD link requests R
C_R	Total cost of deployment QKD backbone network
$B_{(\alpha, \beta), \gamma}^r$	Boolean variable that equals 1 if wavelength γ on link (α, β) is assigned to the QKD link of r , and 0 otherwise
$K_{(\alpha, \beta), \gamma}^r$	Boolean variable that equals 1 if wavelength γ on link (α, β) is assigned to the KM link of r , and 0 otherwise

3.1. QKD Network Model

To ensure the isolation, MODs are utilized in different QKD and KM links in the same fiber [32]. We assumed that the QKD nodes have a co-located deployment with optical nodes. Hence, the topology of the QKD layer is similar to the optical layer. We modeled the network topology as $G(N, L)$, where N and L denote the set of optical/QKD nodes and fiber links, respectively. The QKD links consist of Quantum Channels (QChs) and PChs, and the KM links contain only classical channels. The fiber links in the optical layer comprise the DChs. Different wavelength channels are allocated in the QKD links, where the sets of wavelengths for the quantum and classical channels are denoted as W_Q and W_{KM} , respectively.

3.2. Cost Model

To better illustrate the cost optimization of the QKD network, before analyzing the cost of the QKD network, we define a QKD request parameter $r(s_r, d_r, P_r)$, where s_r and d_r denote the source and destination nodes of the QKD request r , respectively, and P_r denotes the number of parallel QKD links that satisfy the secret key rate requirement of the QKD requests. According to the principle of wavelength division multiplexing [32], multiple

parallel QKD links could be multiplexed in the same fiber to achieve a higher secret key rate and save fiber resources. P_r is defined as

$$P_r = E_r / E_D \quad (1)$$

where E_r denotes the secret key rate requirement for a QKD request r . E_D denotes the secret key rate at distance D ($D = 2$ m) [13], where D represents the distance of a pair of adjacent MDI-QTs. The untrusted relay is placed in a symmetric position of a pair of MDI-QTs. The specific secret key rate of each QKD link was not considered in this work, and here, we only conducted a quantitative analysis.

Based on the network topology, we define a parameter:

$$\eta = \frac{N(N-1)}{2} \quad (2)$$

Here, η denotes the total number of QKD link requests in the network when any QKD node pair hosts one request. N denotes the number of optical/QKD nodes.

The costs of QKD network deployment come from the various devices in the network that support the HTUR with QKP over the network. This section details the following:

(1) Number of MDI-QTs and MDI-QRs and cost:

In this paper, we utilized only the MDI-QKD transceiver to implement the QKD for the whole network. Two MDI-QTs and one MDI-QRs are required to complete a QKD process, due to the MDI-QKD protocol being adopted in the QKD optical network. Therefore, the number of MDI-QTs and MDI-QRs required for an MDI-QKD request is expressed as

$$M_{QT}^r = \left(\left\lceil \frac{L_{sd}}{D} \right\rceil + 1 \right) \cdot P_r \quad (3)$$

$$M_{QR}^r = \left\lceil \frac{L_{sd}}{D} \right\rceil \cdot P_r \quad (4)$$

where the Gaussian brackets here indicate upward rounding, L_{sd} is the physical length of the fiber links between the source node s and the destination node d of the adjacent QKD nodes, P_r is the number of parallel QKD links of r , and D is the distance between a pair of connected MDI-QTs. Based on (3) and (4), the cost of the MDI-QTs and MDI-QRs for all QKD requests R can be expressed as

$$C_{QT}^R = \sum_{r \in R} M_{QT}^r \cdot \delta_{QT}^r \quad (5)$$

$$C_{QR}^R = \sum_{r \in R} M_{QR}^r \cdot \delta_{QR}^r \quad (6)$$

where δ_{QT}^r and δ_{QR}^r denote the cost of an MDI-QTs and MDI-QRs for QKD request r , respectively.

(2) Number of KSs and cost:

From Figure 2, the Key Services (KSs) are placed at the same physical location as the QKD transmitters where the number of KSs required for a QKD request is equal to the MDI-QKD transmitter. Thus, the number of parallel QKD links is not considered when calculating the number of KSs. The number of KSs required for a QKD request r can be expressed as

$$M_{KS}^r = \left(\left\lceil \frac{L_{sd}}{D} \right\rceil + 1 \right) \quad (7)$$

In order to ensure the security of the secret key storage, we assumed that the KS is deployed independently for each QKD request. Therefore, the KS cost of all QKD links in the network can be expressed as

$$C_{KS}^R = \sum_{r \in R} M_{KS}^r \cdot \delta_{KS}^r \quad (8)$$

(3) Number and cost of QKPs:

The QKP [21] technique can achieve the effective management of precious secret key resources and improve the efficiency of the quantum key distribution. Reference [24] showed that the QKPs are abstraction rather than independent devices. Therefore, the specific cost of the QKP was not considered here.

(4) Number and cost of MODs:

To save fiber deployment and reduce the waste of fiber resources, we added MODs to coexist with the QKD links and KS links as single fibers. Our specific implementation was to deploy MOD [20] devices at QKD nodes and trusted and untrusted relay nodes. The equation is expressed as follows:

$$M_{MOD}^r = (2 \cdot \left\lceil \frac{L_{sd}}{D} \right\rceil + 1) \quad (9)$$

Then, the cost of the MODs required for all requests R can be expressed as

$$C_{MOD}^R = \sum_{r \in R} M_{MOD}^r \cdot \delta_{MOD}^r \quad (10)$$

(5) QKD and KM link costs:

In this section, we know there are two channels in the QKD link from Figure 2: the QChs and the PChs are used for quantum key generation and post-processing [31] between QKD nodes, respectively. Besides, there is the KM link along another wavelength channel for long-distance transmission secret keys. Then, the physical length of the QKD and KM links required for a QKD request r is expressed as

$$L_r = (2 \cdot P_r \cdot L_{sd} + L_{KM}) \quad (11)$$

Here, P_r denotes the number of parallel QKD links, and L_{sd} denotes the distance between source node s and destination node d of QKD request r. Parameter 2 refers to a quantum channel and a classical channel included in the QKD link. L_{KM} indicates the physical length of the KM links. We note that the KM and the QKD links' length are equal under the same requests.

Based on Equation (11), the cost of the QKD and KM link for all QKD requests R can be expressed as

$$C_L^R = \sum_{r \in R} L_r \cdot \delta_L^r \quad (12)$$

where δ_L^r denotes the QKD and KM links' cost for each QKD request r.

(6) Total deployment cost:

The total cost of deploying the HTUR QKD network with the QKP is expressed as

$$C_R = C_{QT}^R + C_{QR}^R + C_L^R + C_{MOD}^R + C_{KS}^R \quad (13)$$

The total cost values are calculated based on Equations (5)–(8), (10), (12), and (13), respectively. Other auxiliary equipment (e.g., OSs, etc.) was not considered in this study owing to its low cost value.

3.3. Heuristic Algorithm

Based on the above HTUR QKD network and cost models, we propose an HQNC heuristic algorithm. The details are given in Algorithm 1. We first initialized the parameters C_R , C_r , M_{QT}^r , M_{QR}^r , M_{KS}^r , and L_r . For each arriving QKD request r, the Dijkstra [21,31] algorithm was applied to select the shortest path O_r for r, and the length L_{sd} of the shortest path was calculated after the shortest path was obtained. In the next step, the number of parallel QKD channel wavelengths required under each QKD request r was obtained

from the equation $P_r = E_r / E_D$. After obtaining the shortest path and the required number of wavelengths for a QKD request, we applied the first-fit [21] algorithm to assign the appropriate wavelengths (QKD wavelengths and KM channel wavelengths) to the QKD request r . The first-fit algorithm has the advantage of low computational complexity, and it selects the wavelengths in the lower position among all accessible wavelength sets.

Algorithm 1: Hybrid QKD Network Cost (HQNC) Algorithm.

Input: $G(N, L)$, R , D , W_Q , W_{KM} , δ_{QT}^r , δ_{QR}^r , δ_{KS}^r , δ_L^r , W_{MOD} .

Output: C_R , C_r routing, and wavelength allocation for each QKD request, update QKD network's state:

1. Initialize $C_R \leftarrow 0$; $C_r \leftarrow 0$.
 2. **For** each QKD network request $r \in R$, **do**:
 3. Initialize $M_{QT}^r \leftarrow 0$, $M_{QR}^r \leftarrow 0$, $M_{KS}^r \leftarrow 0$, $L_r \leftarrow 0$.
 4. Routing computation with Dijkstra's shortest path algorithm.
 5. Compute the physical distance L_{sd} between the QBN source node S_r and destination node d_r of the r on the shortest path O_r .
 6. Compute the required number of QChs $P_r = E_r / E_D$.
 7. Search all available wavelength channels, and store them in W_Q as the QChs on the shortest path O_r .
 8. **If** $|W_Q| \geq 2 \cdot P_r$, **then**
 9. Filter $2 \cdot P_r$ wavelength channels from W_Q using first-fit algorithm for QKD request r .
 10. Search all available wavelength channels, and store them in W_{KM} as the KM links on the shortest path O_r .
 11. **If** $|W_{KM}| \geq 1$, **then**
 12. filter one wavelength channel from W_{KM} using first-fit algorithm for QKD request r .
 13. **For** the shortest path O_r of QKD request r , **do**:
 14. Compute the required number of QKD transmitters and R:
 15. $M_{QT}^r \leftarrow (\lceil L_{sd} / D \rceil + 1) \cdot P_r$;
 16. $M_{QR}^r \leftarrow \lceil L_{sd} / D \rceil \cdot P_r$.
 17. Compute the required number of KSs and MODs of the QKD request r :
 18. $M_{KS}^r \leftarrow (\lceil L_{sd} / D \rceil) \cdot P_r$;
 19. $M_{MOD}^r \leftarrow (2 \cdot \lceil L_{sd} / D \rceil) \cdot P_r$.
 20. Compute the required length of links of the QKD request located in:
 21. $L_r \leftarrow 2 \cdot P_r \cdot L_{sd} + L_{KM}$.
 22. **End for**
 23. The total cost:
 24. $C_R \leftarrow C_R + M_{QT}^r \cdot \delta_{QT}^r + M_{QR}^r \cdot \delta_{QR}^r + M_{MOD}^r \cdot \delta_{MOD}^r + M_{KS}^r \cdot \delta_{KS}^r + L_r \cdot \delta_L^r$.
 25. **Else:**
 26. The secret-key rate demand of QKD request r cannot be satisfied.
 27. **Else:**
 28. The secret-key rate demand of QKD request r cannot be satisfied.
 29. **End**
 30. The total cost for all QKD requests $C_R \leftarrow C_R + C_r$.
 31. **Return** C_R , C_r routing, and wavelength allocation for each QKD request, and update QKD links' state.
-

After both the QKD path and the available channel wavelength are defined, the number of MDI-QTs, MDI-QRs, MODs, and KSs and the length of the wavelength links under each QKD request are calculated according to Equations (3), (4), (7), (9), and (11), respectively. The corresponding parts of the heuristic algorithm in Algorithm 1 are Rows 14 to 21.

The cost of MDI-QTs, MDI-QRs, MODs, and KSs and the length of the wavelength links for all QKD requests in the network can be calculated by Equations (5), (6), (8), (10), and (12), respectively. Further, the total deployment cost in the QKD network is obtained from Equation (13). The corresponding parts of the HQNC algorithm in Table 1 are Rows 23 and 30.

In the implementation process in detail, the time complexity of this algorithm mainly depends on the size of the network and the constraints. In the worst case, the time complexity of Rows 3–9 and Rows 10–36 in this algorithm is $O(|N|^2)$ and $O(W_Q \cdot W_{KM})$, respectively. Therefore, the total time complexity of this HQNC algorithm is $O(|N|^2 + W_Q \cdot W_{KM})$.

4. Performance Evaluation and Analysis

In this section, we introduce the HTUR QKD network with the QKP for cost optimization. To illustrate the efficiency and feasibility of the scheme, we conducted an extensive simulation analysis, with PTR [31] and CO-QBN [13] for comparison. Further, the National Science Foundation Network (NSFNET) and United States Network (USNET) topologies shown in Figures 3 and 4 were adopted for the deployment network cost. QKD requests were randomly generated among all QKD node pairs, and the maximum number of QKD requests satisfied by various QKD networks could be calculated according to the formula $|N| \cdot (|N| - 1)/2$. Thus, the maximum number of QKD requests on the NSFNET and USNET is 91 and 276, respectively. We considered the case that there will be more QKD requests in the near future and the existing network users' scale may need to be further expanded. For the simulation, we assumed that the range of QKD requests on the NSFNET and USNET topologies was [20, 200] and [40, 400], respectively. The weight values of two neighboring nodes on the network topology refer to the physical distance (kilometers). We assumed that there are sufficient wavelengths in the links and there is no case of an insufficient number of wavelengths and request allocation failure. To satisfy the different secret key requirements for the QKD requests, the secret key rate was set as $\{k\}$, $\{k, 2k\}$, and $\{k, 2k, 3k\}$ respectively.

The cost values used for the performance evaluation are listed in Table 4. These cost values required in the QKD network were based on reasonable assumptions, which were provided by the vendor. Considering the price fluctuations in cost values due to component reduction as technology advances, we propose two scenarios to analyze the performance: (1) Current Scenario (CS): The cost value of each component is fixed. This is applicable to the current mature deployment of the network. (2) Future Scenario (FS): The cost value of each component is also fixed, but the cost value of the FS is extremely reduced compared to the CS. This scenario helped us to analyze the long-term impact of device cost optimization in the network. The problem of predicting future network costs can be better addressed.

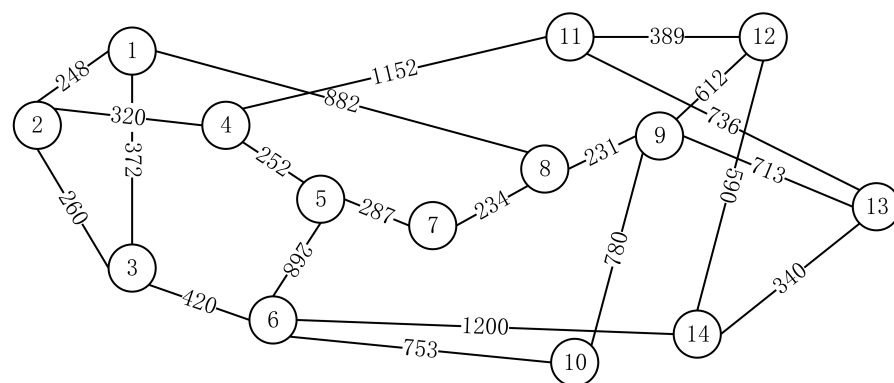


Figure 3. NSFNET topology.

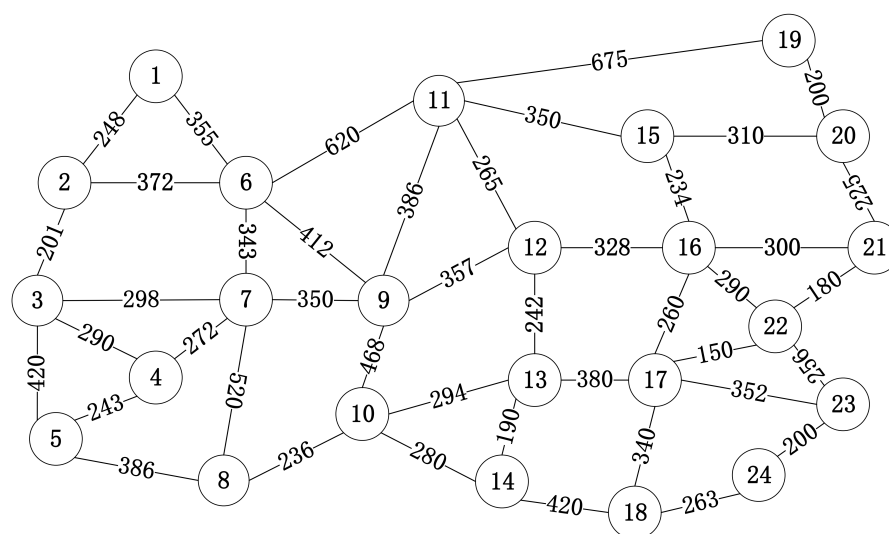


Figure 4. USNET topology.

Table 4. Cost values used for the performance evaluation based on QKD networks.

Different Situations	$ R $	Scenario	δ_{QT}^r (\$)	δ_{QR}^r (\$)	δ_L^r (\$)	δ_{KS}^r (\$)	δ_{MOD}^r (\$)
HQNC	$ R > 0$	CS	6600	15,000	135	5000	200
		FS	3000	8000	60	2500	100
PTR	$ R > 0$	CS	6600	15,000	135	5000	200

4.1. QKD Network Critical Device Requirements Analysis

In this section, we evaluated in detail the various device deployment issues for QKD networks and adopted the number of required QKD transmitters and receivers as examples. Furthermore, we utilized TRN and CO-QBN as the comparison schemes to specify the efficiency of our new proposed HQNC scheme.

QKD Transmitter and Receiver Number

Figures 5 and 6 demonstrate the results between the average number of QKD transmitters/receivers (per QKD request) and QKD network requests under the NSFNET and USNET topologies, respectively. The PTR scheme was used for comparison in Figures 5 and 6. As the secret key rate of QKD requests increases, the average number of corresponding QKD transmitters also increases, and the trend of increasing the number of QKD transmitters and receivers based on both topologies is consistent. The result is that, according to Equations (3) and (4), the average number of QKD transmitters and receivers is related to the secret key rate requirement.

The average number of QKD transmitters required for QKD requests do not show a corresponding linear increase as the QKD requests increase when the secret key rate is $\{k\}$, $\{k, 2k\}$, and $\{k, 2k, 3k\}$, respectively, that is QKD requests are randomly generated among all QKD node pairs. As shown in Figures 5a and 6a, the average number of QKD transmitters/receivers required by the HQNC is smaller than the PTR scheme, which also proves the efficiency of our new proposed method. The advantage of a reduced transmitters/receivers number is especially obvious when the secret key rate is higher. The reason is that the PTR scheme requires more QKD transmitting/receiving devices compared to the HQNC scheme when the secret key rate increases. The number of transmitters/receivers required under the same QKD requests number is slightly larger than the number of receivers. The result is that, adopting the HTUR QKD with the QKP incorporating the MDI-QKD protocol, one more QKD transmitter than QKD receivers is required to complete a QKD request.

From Figures 5b and 6b, we observe that the number of QKD transmitters/receivers shows an irregular variation as the network scale increases. The main reasons are that the average calculation method is used to compute the number of QKD transmitters and receivers, the QKD requests are generated randomly, and the distances between different QKD node pairs are different, and none of the above reasons is related to the network scale.

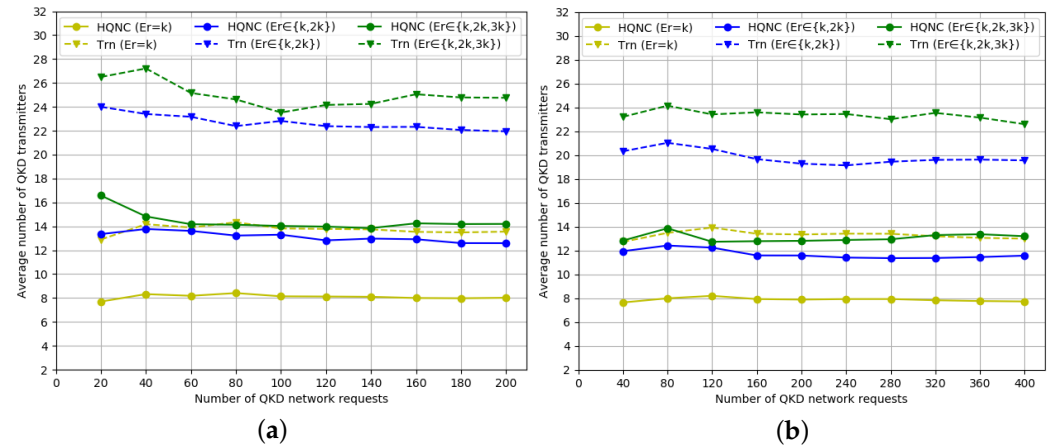


Figure 5. Average number of QKD transceivers versus number of QKD requests compared to TRN based on (a) NSFNET topology and (b) USNET topology.

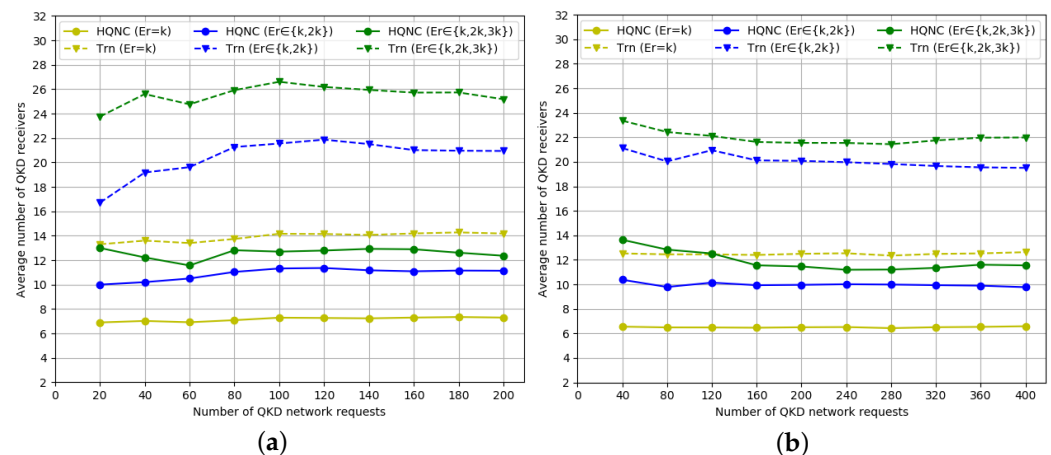


Figure 6. Average number of QKD receivers versus number of QKD requests compared with TRN based on (a) NSFNET topology and (b) USNET topology.

Therefore, the HQNC algorithm can reduce the number of QKD transmitters and receivers to deploy QKD networks to a larger extent; especially when the secret key rate is higher, the advantages of the HQNC scheme are more obvious. Moreover, the HQNC algorithm for reducing QKD transmitters and receivers is related to the distance between QKD node pairs in the network rather than to the network topology scale.

From Figure 7a,b, the number of QKD transmitters in the HQNC is significantly reduced in both the NSFNET and USNET topologies compared to CO-QBN. According to Figure 8a,b, the number of QKD receivers for the HQNC cost optimization solution is similar to the CO-QBN algorithm. The result is that we mainly reduced the deployment of QKD transmitters compared to the CO-QBN algorithm in the network.

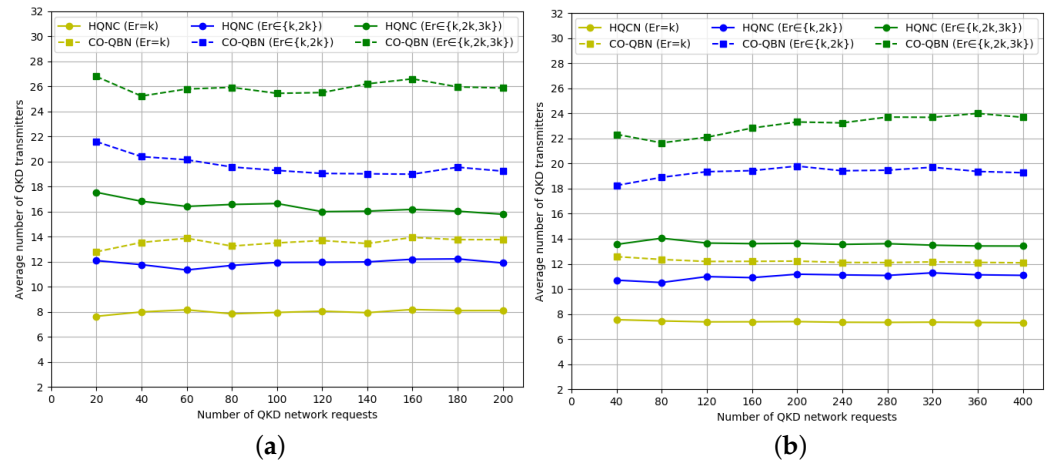


Figure 7. Average QKD transmitters number versus QKD requests number compared to CO-QBN based on (a) NSFNET topology and (b) USNET.

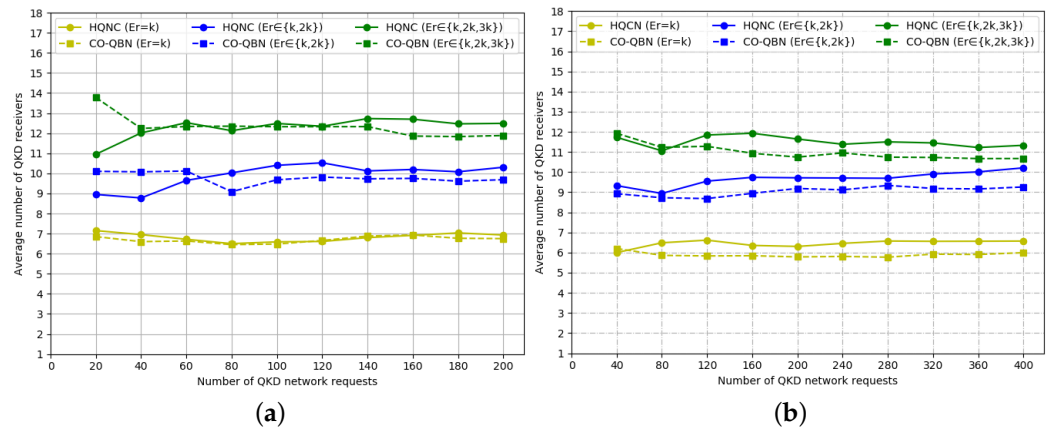


Figure 8. Average QKD receivers number versus QKD requests number compared to CO-QBN based on (a) NSFNET topology and (b) USNET.

4.2. QKD Network Total Deployment Cost Analysis

In this section, we analyzed the QKD network total deployment cost problem in detail. To reflect the generality of the deployment cost, we considered two scenarios (CS and FS) separately, as described below

The total deployment costs of QKD network requests are shown in Figures 9–11, respectively. Figures 9 and 10 show the total QKD request deployment cost on the NSFNET and USNET topologies for the CS, with TRN and CO-QBN as comparisons, respectively. Figure 11 shows the total QKD requests' deployment cost on the NSFNET and USNET network topologies for the FS, compared with the HTUR only.

According to Figures 9 and 10, it can be observed that the total cost value gradually increases as the number of QKD requests increases. In the same scenario (as shown in Table 2), the total cost value improves gradually with the increase of the secret key rate. Compared with the previous TRN and CO-QBN schemes, the HQNC in this paper requires a significantly lower total cost value for the same secret key rate. This phenomenon verifies the efficiency of our new proposed scheme. In Figure 9a,b, the TRN curve is always higher than that of the HQNC when the secret key rate is fixed. As the number of QKD requests increases, the difference of the cost values between TRN and HQNC becomes larger. The reason is that, as the number of QKD requests increases, the cost savings become greater in HQNC compared to TRN. The total cost of QKD network deployment increases gradually with the expansion of the network scale, which is due to the number of QKD requests accommodated. In the CS, the cost savings of the presented HQNC are more than

90 percent and 50 percent compared to the previous TRN and CO-QBN for different secret key rates, respectively.

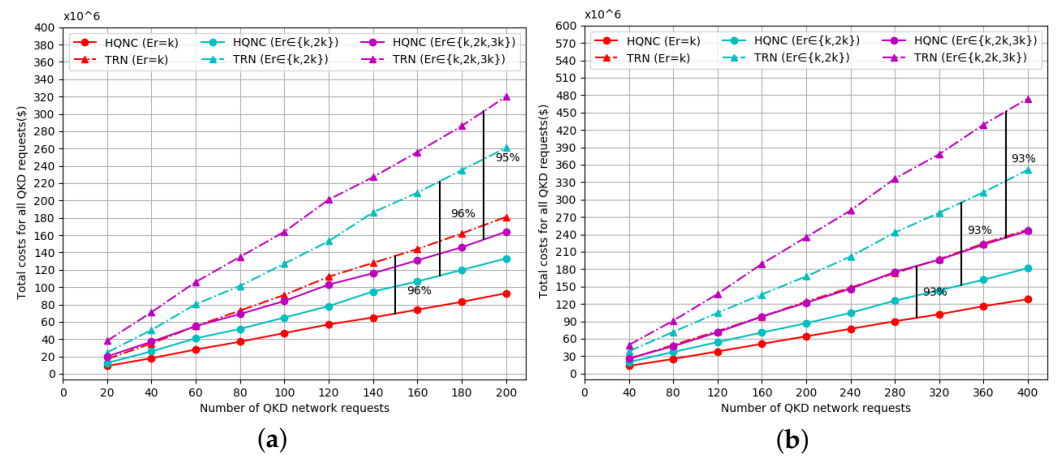


Figure 9. Total QKD network cost versus number of QKD requests compared to TRN in the current scenario based on (a) NSFNET topology and (b) USNET topology.

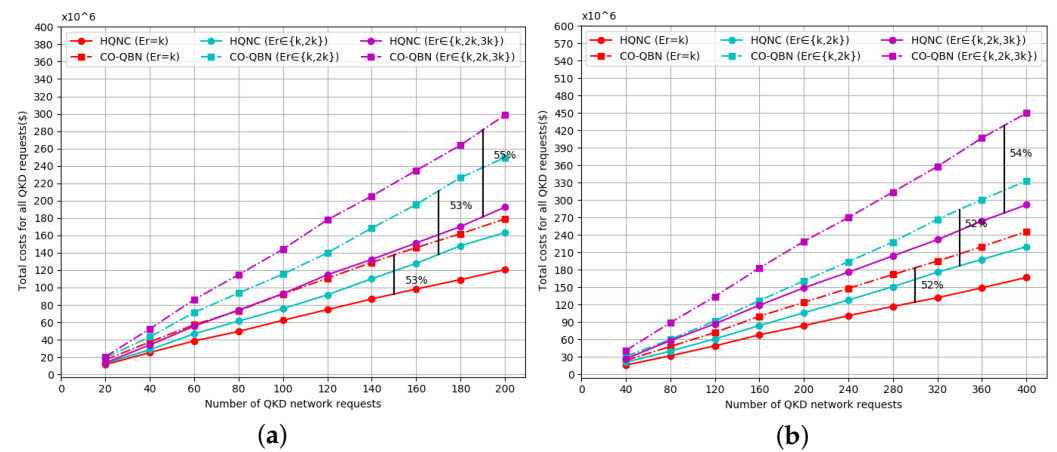


Figure 10. Total QKD network cost versus number of QKD requests compared to CO-QBN in the current scenario based on (a) NSFNET topology and (b) USNET topology.

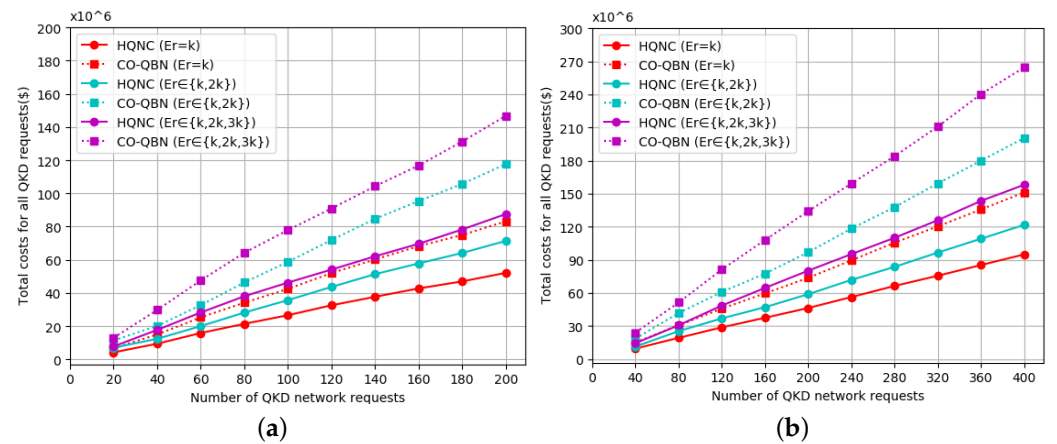


Figure 11. Total QKD network cost versus number of QKD requests compared to CO-QBN in the future scenario based on (a) NSFNET topology and (b) USNET topology.

As shown in Figure 11, we only analyzed the deployment cost of the HQNC in the FS, with CO-QBN for comparison. From Figures 10 and 11, the total cost of the FS is significantly lower than the total cost value of the CS. The main reason for this is that the

definition of each cost value is reduced in the FS from Table 2. Furthermore, the future network cost issue is well predicted.

5. Conclusions

We proposed an HTUR QKD network architecture with QKP integrating the MDI-QKD protocol. Moreover, a new HQCN heuristic algorithm was designed to implement the cost optimization in the QKD network. Two scenarios (i.e., CS and FS) were utilized in the simulation to analyze the total cost of QKD requests. The simulation results demonstrated that, in the CS, the cost savings of the HQCN were more than 90 percent and 50 percent compared to the previous TRN and CO-QBN, which showed the effectiveness of the proposed HQCN heuristic algorithm.

Author Contributions: Conceptualization, J.J.; methodology, J.J., B.D. and L.K.; software, J.J. and B.D.; validation, J.J.; formal analysis, J.J.; investigation, J.J.; resources, B.G.; data curation, J.J.; writing—original draft preparation, J.J.; writing—review and editing, J.J., B.D., L.K., H.X. and B.G.; visualization, J.J.; supervision, B.G.; funding acquisition, B.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Key-Area Research and Development Program of Guangdong Province (Grant No. 2018B030325002).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Special thanks goes to Xiao-Dong Fan, Quan-Hao Niu, and Peng-Cheng Wang for their helpful discussions.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [\[CrossRef\]](#) [\[PubMed\]](#)
- Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [\[CrossRef\]](#)
- Cao, Y.; Zhao, Y.; Yu, X. Multi-tenant provisioning over software defined networking enabled metropolitan area quantum key distribution networks. *J. Opt. Soc. Am.* **2019**, *36*, 3. [\[CrossRef\]](#)
- Cao, Y.; Zhao, Y.; Lin, R.; Yu, X.; Zhang, J.; Chen, J. Multi-tenant secret-key assignment over quantum key distribution networks. *Opt Express* **2019**, *27*, 2544–2561. [\[CrossRef\]](#)
- Chen, J.P.; Zhang, C.; Liu, Y.; Jiang, C.; Zhang, W.; Hu, X.L.; Guan, J.Y.; Yu, Z.W.; Xu, H.; Lin, J.; et al. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. *Phys. Rev. Lett.* **2020**, *124*, 070501. [\[CrossRef\]](#) [\[PubMed\]](#)
- Chen, Y.A.; Zhang, Q.; Chen, T.Y.; Cai, W.; Liao, S.K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.G.; Chen, Z.; et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **2021**, *589*, 214–219. [\[CrossRef\]](#)
- Dynes, J.F.; Wonfor, A.; Tam, W.W.-S.; Sharpe, A.W.; Takahashi, R.; Lucamarini, M.; Plews, A.; Yuan, Z.L.; Dixon, A.R.; Cho, J.; et al. Cambridge quantum network. *NPJ Quantum Inf.* **2019**, *5*, 1. [\[CrossRef\]](#)
- Sangouard, N.; Simon, C.; de Riedmatten, H.; Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **2011**, *83*, 33–80. [\[CrossRef\]](#)
- Li, Z.D.; Zhang, R.; Yin, X.F.; Liu, L.; Hu, Y.; Fang, Y.Q.; Fei, Y.Y.; Jiang, X.; Zhang, J.; Li, L.; et al. Experimental quantum repeater without quantum memory. *Nat. Photonics* **2019**, *13*, 644–648. [\[CrossRef\]](#)
- Kadhim, M.H.; Hasan, J.K.; Alhumaima, R.S. Performance Analysis of Quantum Repeaters Based Hybrid Communications Networks. *IOP Conf. Ser. Mater. Sci. Eng.* **2021**, *1076*, 1. [\[CrossRef\]](#)
- Yu, X.; Liu, Y.; Zou, X.; Cao, Y.; Zhao, Y.; Nag, A.; Zhang, J. Secret-Key Provisioning With Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks. *J. Light. Technol.* **2022**, *40*, 3530–3545. [\[CrossRef\]](#)
- Han, W.; Wu, X.R.; Zhu, Y.; Zhang, W.; Zhou, B. The Trust Relay QKD Network Communication Research. *Adv. Mater. Res.* **2013**, *709*, 421–426. [\[CrossRef\]](#)
- Cao, Y.; Zhao, Y.; Li, J.; Lin, R.; Zhang, J.; Chen, J. Hybrid Trusted/Untrusted Relay-Based Quantum Key Distribution Over Optical Backbone Networks. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 2701–2718. [\[CrossRef\]](#)
- Tayduganov, A.; Rodimin, V.; Kiktenko, E.O.; Kurochkin, V.; Krivoshein, E.; Khanenkov, S.; Usova, V.; Stefanenko, L.; Kurochkin, Y.; Fedorov, A.K. Optimizing the deployment of quantum key distribution switch-based networks. *Opt Express* **2021**, *29*, 24884–24898. [\[CrossRef\]](#)

15. Hua, X.; Hu, M.; Guo, B. Multi-User Measurement-Device-Independent Quantum Key Distribution Based on GHZ Entangled State. *Entropy* **2022**, *24*, 6. [\[CrossRef\]](#)
16. Donkor, E.J.; Elliott, C.; Colvin, A. Current status of the DARPA quantum network (Invited Paper). *Quantum Inf. Comput. III* **2005**, *2005*, 138–149.
17. Peev, M.; Pacher, C.; Alléaume, R.; Barreiro, C.; Bouda, J.; Boxleitner, W.; Debuisschert, T.; Diamanti, E.; Dianati, M.; Dynes, J.F.; et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **2009**, *11*, 075001. [\[CrossRef\]](#)
18. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Tanaka, A.; Yoshino, K.; Nambu, Y.; Takahashi, S.; et al. Field test of quantum key distribution in the Tokyo QKD Network. *arXiv* **2011**, arXiv:1103.3566. [\[CrossRef\]](#)
19. Lo H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [\[CrossRef\]](#)
20. Valivarthi, R.; Umesh, P.; John, C.; Owen, K.A.; Verma, V.B.; Nam, S.W.; Oblak, D.; Zhou, Q.; Tittel, W. Measurement-device-independent quantum key distribution coexisting with classical communication. *Quantum Sci. Technol.* **2019**, *4*, 4. [\[CrossRef\]](#)
21. Cao, Y.; Zhao, Y.; Wu, Y.; Yu, X.; Zhang, J. Time-Scheduled Quantum Key Distribution (QKD) Over WDM Networks. *J. Light. Technol.* **2018**, *36*, 3382–3395. [\[CrossRef\]](#)
22. Yu, X.; Liu, X.; Liu, Y.; Nag, A.; Zou, X.; Zhao, Y.; Zhang, J. Multi-path-based quasi-real-time key provisioning in quantum-key-distribution enabled optical networks (QKD-ON). *Opt. Express* **2021**, *29*, 21225–21239. [\[CrossRef\]](#) [\[PubMed\]](#)
23. Niu, J.; Sun, Y.; Jia, X.; Ji, Y. Key-Size-Driven Wavelength Resource Sharing Scheme for QKD and the Time-Varying Data Services. *J. Light. Technol.* **2021**, *39*, 2661–2672. [\[CrossRef\]](#)
24. Cao, Y.; Zhao, Y.; Colman-Meixner, C.; Yu, X.; Zhang, J. Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). *Opt Express* **2017**, *25*, 26453–26467. [\[CrossRef\]](#)
25. Tang, Y.T.; Yin, H.L.; Zhao, Q.; Liu, H.; Sun, X.; Huang, M.Q.; Zhang, W.J.; Chen, S.J.; Zhang, L.; You, L.; et al. Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network. *Phys. Rev.* **2016**, *6*, 1. [\[CrossRef\]](#)
26. Liu, H.; Wang, W.; Wei, K.; Fang, X.; Li, L.; Liu, N.; Liang, H.; Zhang, S.; Zhang, W.; Li, H.; et al. Experimental Demonstration of High-Rate Measurement-Device-Independent Quantum Key Distribution over Asymmetric Channels. *Phys. Rev. Lett.* **2019**, *122*, 160501. [\[CrossRef\]](#)
27. Cao, Y.; Zhao, Y.; Yu, X.; Wu, Y. Resource Assignment Strategy in Optical Networks Integrated With Quantum Key Distribution. *J. Opt. Commun. Netw.* **2017**, *9*, 11. [\[CrossRef\]](#)
28. Aguado, A.; Lopez, V.; Martinez-Mateo, J.; Peev, M.; Lopez, D.; Martin, V. Virtual Network Function Deployment and Service Automation to Provide End-to-End Quantum Encryption. *J. Opt. Commun. Netw.* **2018**, *10*, 4. [\[CrossRef\]](#)
29. “Understanding Quantum Cryptography,” IDQ White Paper [Online]. Available online: https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf (accessed on 7 April 2023).
30. Cao, Y.; Zhao, Y.; Wang, J.; Yu, X.; Ma, Z.; Zhang, J. Cost-Efficient Quantum Key Distribution (QKD) Over WDM Networks. *J. Opt. Commun. Netw.* **2019**, *11*, 6. [\[CrossRef\]](#)
31. Aleksic, S.; Hipp, F.; Winkler, D.; Poppe, A.; Schrenk, B.; Franzl, G. Perspectives and limitations of QKD integration in metropolitan area networks. *Opt. Express* **2015**, *23*, 10359–10373. [\[CrossRef\]](#)
32. Bahrami, A.; Ld, A.; Spiller, T. Quantum key distribution integration with optical dense wavelength division multiplexing: A review. *IET Quantum Commun.* **2020**, *1*, 9–15. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.