

CSEC 604 RESEARCH PROJECT IN CRYPTOGRAPHY AND
AUTHENTICATION
PROJECT REPORT

**QUANTUM KEY DISTRIBUTION. WAYS OF
INCREASING QKD TRANSMISSION
DISTANCE WITHOUT AFFECTING THE
TRANSMITTED DATA**

February 10, 2023

Hem Parekh, Praj Shete, Parth Shukla
Department of Computing Security
College of Computing and Information Sciences
Rochester Institute of Technology
hp5643@rit.edu | ps7600@rit.edu | ps4195@rit.edu

1 Abstract

"Quantum Computers," one of the most quickly growing technologies that can exploit the rules of quantum mechanics and tackle the complicated challenges encountered by traditional supercomputers, have initiated a new era in the world of computing. A traditional computer cannot answer an extremely complicated issue, raising a few technical concerns regarding its capability. Quantum algorithms approach these difficult issues differently, generating a multidimensional space in which pattern linkage occurs. Since traditional infrastructure has begun to transition to quantum infrastructure, it is past time to focus on other elements of computing environments. One such component is "cryptography;" the requirement for quantum-safe cryptography cannot be overstated. We are all unaware of the true capabilities of quantum computers and how they might severely impact standard cryptography systems. Researchers are working on several quantum-safe cryptography systems, but one recurring difficulty is Key Distribution. This study will mostly focus on Quantum Key Distribution. This study will offer responses to some of the following questions: QKD may be used for secure communication in the following ways. What are the various methods for breaking the QKD network? How can it be reduced? Finally, while working on the core problem, we will look at techniques to expand the transmission distance of QKD without affecting or worsening it.

2 Introduction

One of the essential cryptographic challenges is creating safe cryptographic keys across unreliable networks. These fall under the category of theoretically breakable computational security solutions, even if the deployment of public key infrastructure is predicated on computationally challenging mathematical issues and assumptions about the processing capacity of eavesdroppers. As a result, they are in danger as computer power keeps growing and new quantum computing algorithms are developed that can solve some commonly used, computationally challenging mathematical problems in polynomial time. The quantum information theory-based technique known as quantum key distribution, or QKD, enables the creation of information-secure cryptographic keys that are independent of these restrictions, at least at the protocol level. Due to the uniqueness of QKD connections and network structure, QKD networks differ greatly from conventional telecommunication networks. The motivations behind this survey are limitations like limited key generation rate and reachable distance, current lack of quantum repeaters, specialized routing due to the use of public and quantum channels in quantum links, and network organization that must currently use a hop-by-hop key transport approach. In our paper, we will be discussing the entire high-level QKD architecture and its attributes (Section 1.1, Section 1.2, Section 1.3). Going forward we will discuss the different types of QKD networks their advantages and disadvantages and how each of them differs keeping distance as an important factor. Although the research mentioned in the paper achieved outstanding results in terms of

key generation rate, communication distance, QKD network design, and routing algorithm, certain security difficulties still need to be resolved. As a result, the goal of this study is to first outline the QKD network’s developing patterns and outcomes. The difficulties that need to be further researched to perfect QKD networks are then highlighted (Section 4). We’ve also included some workable ideas and approaches for the suggested problems so that researchers might come up with comprehensive remedies. Once the establishment of QKD networks was done, then came the problem of the transmission of keys across these networks.

For this transmission, several different protocols have been introduced. Bennett and Brassard led the foundation of quantum key distribution and provided us with the solution to the most essential problem which is the sharing of the secret key. Since the transmission of this key will take place using the quantum channel it will be secure against any kind of man-in-the-middle attack or any level of computing power. Photon polarization states are used in the protocol. A quantum communication channel in such a system may be open to the public, free space, or optical fiber, accepting any kind of outside interference. Non-orthogonal states are used to encode the data transmitted across the channel. The security of the entire system is ensured by the quantum property that these states cannot be measured without changing the initial state. The phrase “quantum indeterminacy” is frequently used to describe this property. Through the use of polarized photons or qubits, Charles Bennett’s quantum key distribution protocol B92 enables two parties the sender and the receiver to create a perfect secret, a shared and unique key sequence which is the secret key, and the ability to identify whether an eavesdropper has intercepted the quantum channel. Due to the technological shortcomings of the devices used in the exchange of quantum keys, either for the polarization or for reading the polarization of the photons, the protocol’s absolute security cannot be fulfilled [1]. In the case of mdiQKD, the two quantum states used by Alice and Bob were created using weak coherent pulses. They create entangled states from the rectilinear basis for the transmission signals and states from the diagonal basis for the decoy signals. Each side separately creates a signal state or decoy state in their secret laboratories. The prepared entangled states using the basis sent to a third party for a Bell-state measurement. If the measurement was successful, the third party lets Alice and Bob know in which state. The outcomes are then sorted, and the error rates and likelihood of success are computed. They can tell how secure their channel is by using the information they get from the decoy states. This protocol is set up between the communication parties using entanglement, hence the entangled distillation protocol is unnecessary.

Following a discussion of several QKD networks and protocols, we move on to the primary focus of this research study, the distance problem. We examine how each network and protocol deals with the distance problem and how each new version attempts to solve the problem by introducing a new mechanism. Then we’ll go through some of the newer protocols that can send keys across much greater distances. Among these newer protocols are various entanglement-based protocols, MDI, TF-QKD, and many more. We also talk

about why these protocols aren't employed in real-time applications right now. After the discussion about protocols and networks, we will look at some of the solutions suggested by various research publications and how they leverage the existing available resources to extend the transmission distance. Following that, we go over a number of our options, including how we might enhance the distance of key communication by using relays, repeaters, or even satellites. We explore how, if newer protocols are mature enough for real-time applications, they may be utilized to send keys globally through quantum techniques.

3 Literature Review

3.1 QKD Networks

Two or more QKD nodes connected by an optical fiber or free space cables make up a QKD network. The secret keys can be supplied to different users in various locations to ensure forward secrecy and long-term security after being negotiated between any two QKD nodes. A lot of research is done on using QKD networks where papers demonstrate the working architecture of the QKD networks and QKD Nodes. [1] provides an overview of the networking perspectives of the QKD design with certain issues that are developed in the network such as what factors could hamper while increasing the distance. The paper also discusses the issues that may raise while focusing on just increasing the distance. Increasing the distance is not as easy as it seems, different types of networks have different advantages as well as disadvantages. There is always a maximum point to which increasing the distance is feasible.

3.2 Types of QKD Networks

Selecting the proper type of QKD network is essential if one wants processing to work efficiently. Papers [1, 2, 6, 7] discuss the factors affecting the computation, key rate generation, and distance. Every QKD type will affect these factors hence one could use a hybrid model to obtain maximum efficiency in all fields. The papers also discuss the different real-world networks implemented by different countries and institutions, their drawbacks, their results, and possible issues. Selecting the right transmission media also is an important factor in the case of the QKD networks. Using fiber optic or free space also provides variability in whether the distance is to be increased or not.

3.3 Key rate Vs Distance

A very significant relationship between two different aspects of the QKD was proved in [10] where it was discussed how the increase in the distance would hamper the qubit loss and hence lead to a burden in the key generation rate. The key generation rate decreases linearly to some extent and after a certain point, it drops drastically. This was observed in almost all protocols that were implemented

3.4 Beam-Splitting Attack (BS Attack)

[10] discussed SEPM-QKD simulation with varying local coherent light intensity. While the transmission distance rises with increasing attenuation of the coherent light intensity, the key rate falls. The key rate is roughly equal to the square of the coherent state's amplitude when the average photon number is significantly below 1. The percentage of the particle-like correlation between Alice and Bob will likewise rise for coherent states with large intensities. The last key's bit error rate will rise, reducing the transmission distance. There are also two other key rate curves, which match the findings of the fitting without taking BS assaults into account. The key rate will be adversely affected by the BS attack over long transmission distances, it has been discovered.

3.5 Challenges in cost and performance

At the moment, both hardware and software solutions are being sought after in the search for high-performance and affordable QKD systems. [15] discusses these challenges that came ahead of researchers such as its robustness and cost. It also discusses various factors such as how the key rate is directly influenced by the type of detectors used and how wavelength or spatial mode multiplexing could help to increase the key rate. Distance-based issues and their possible solutions such as how single-photon detection masters the point-to-point communication distance were also discussed in the study.

Figure 19 shows how to include a picture in a LaTeX document.

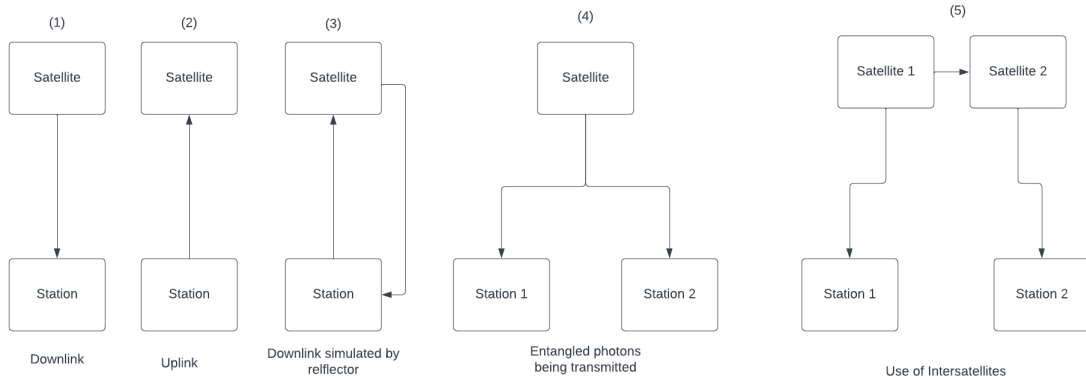


Figure 1: Using Satellite for Quantum Key Distribution.

3.6 Available Solutions to Distance Problem

Recently revealed research demonstrates how far we have come in the realm of QKD and how far we have come in terms of crucial transmission distance using quantum methods. Researchers illustrate how we changed the design of the QKD network and how employing various strategies and means helped boost transmission distance. One of the publications, "Satellite-to-ground quantum key distribution," was the first to propose utilizing satellites to send keys. They discussed how using free space instead of optical fibers would be far more advantageous and how noise attenuation is greatly decreased in space. They detailed the design of the QKD utilizing a satellite and how China used a satellite to transfer keys from China to a distance of 1200km. They modified the very first protocol introduced, known as the BB84 protocol. They described all the challenges they face as well as solutions to those challenges. The maximum distance that this method was able to achieve when they discovered it was 1200km as mentioned. Another study publication, "Progress in satellite quantum key distribution," described how using the entanglement-based protocol for satellite QKD can increase the transmission distance. The key shortcoming of the article was that the entanglement-based protocol is still in the experimental stage and hence not mature enough for real-time use. They successfully explained the architecture as well as illustrations of different platforms that can be used to perform satellite QKD as shown in figure 19.

These were the different methods and research that were done to increase the transmission distance via the use of satellites. Following this, much study has been conducted on the use of relays/repeaters. The architecture of QKD will be discussed in this article. This will help us realize that the architecture of the QKD system itself is the fundamental factor limiting transmission distance. Thus, in the initial study that proposed the use of relays in 1988, the authors go over different methods and the benefits and drawbacks of using relays and repeaters. Later on, there were different methods proposed along with the architecture and their advantages as also which protocols suit the best and which comes up with the maximum transmission distances of the key using the quantum techniques.

4 Introduction to QKD Networks

The QKD network comprises various static nodes having quantum capabilities some of these are storing qubits, creating a single photon or entanglement state, and performing quantum unitary operations [2]. This QKD network is used to extend the QKD protocols which we will be discussing in detail in upcoming sections. These quantum nodes are used to execute the QKD protocols and distribute the local keys between the neighboring nodes. Once the keys are shared then in a hop-by-hop manner the unconditional session keys are distributed between the remote end users and different applications. The entire QKD network is further divided into different attributes and layers. The attributes comprise quantum nodes and links whereas the framework comprises three different layers: a quantum

layer, a key management layer, and a communication layer as presented in Figure 2. The quantum layer consists of different quantum devices which are responsible for sharing local keys with the help of QKD protocols. This layer also consists of an authenticated public classical channel along with the quantum devices [3]. The entire QKD architecture relies on key agreements, hence, situations in which the upper layer requires the high consumption of key materials by different applications are generally not desirable [2]. Therefore, it is the responsibility of the quantum layer to generate key material continuously to maintain the quality of service to the upper layers. The management of keys generated and storing them securely to conveniently utilize the resources provided by the quantum devices in the quantum layer is the key responsibility of the key management layer. Additionally, the key management layer also holds the responsibility to manage the routing protocols and keep a check on the quality of service related to the key infrastructure. The topmost layer is the communication layer uses the key materials generated to encrypt the data traffic using IPSec which is an existing security protocol suite to manage the routing tasks and allows the APIs to be used by the end users or applications for accessing the secure session keys generated [3]. The most important layer here is the quantum layer and we will be focusing on this layer, particularly as the above layer's infrastructure totally depends on the network organization and the communication between the nodes in these two layers can be achieved through standard existing connections such as the internet.

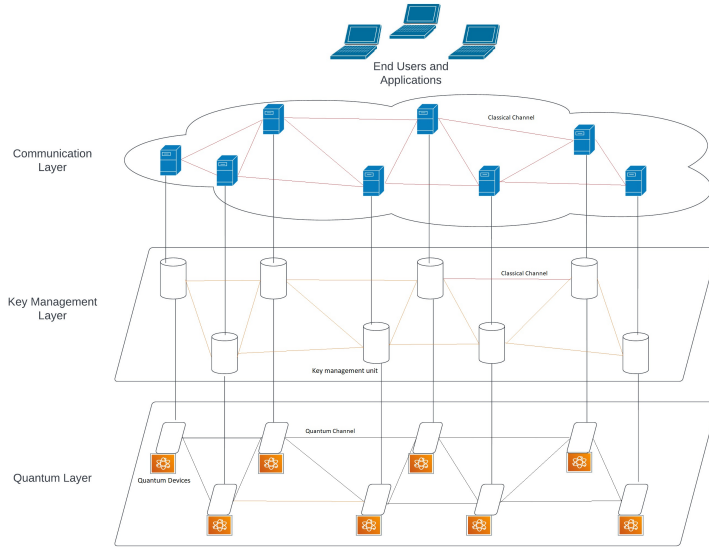


Figure 2: QKD Framework

4.1 QKD Network Attributes

Instead, of relying on the computational assumptions of ostensibly difficult problems, new security methods like QKD. QKD networks, however, need to be integrated into the present environment and follow a set of guidelines and limitations. A list of some of the most common demands made by QKD networks is provided below.

4.1.1 Average Key Rate

The average key rate remains the most important attribute in any given QKD network. The encryption and decryption algorithms can be performed successfully only when there is sufficient key material available in the key storage. The network performance is majorly affected when there is an imbalance between the rate at which the key material is stored and used. We could see a positive development in the key rate sector. The DARPA QKD network was able to achieve a key rate of about 400bps over 10 km [4]. The SECOQC maximum key rate that was achieved was around 3.1 kbps over a 33 km distance [5]. Tokyo in 2009 achieved a key rate of over 304 kbps over 45 km [6]. Beijing âShanghai built a backbone QKD network with devices that could achieve a key rate of almost about 250 kbps over 43 km. Since the past 20 years a steady increase in the key rate, as well as the distance, has been evident practically with the improvements in the infrastructure, especially the optical components and detectors. Optimizing the digital signal processing in FPGA a record high key rate was achieved of key rate around 10 Mbps. Another race of increasing the transmission distance has already begun. With protocol enhancements and technological improvements, this can be thoroughly achieved [7]. Therefore, it is realistic to anticipate that an ideal solution would eventually greatly outperform the current key rate and distance values, even though the race between key material creation and consumption will continue.

4.1.2 Link Length

The maximum length over which secure key material may be created is a QKD link's primary limitation. Scattering and absorption of polarized photons with some other factors place a distance restriction on the reach of quantum channels (direct optical connections or free line of sight) [8, 9]. 29 km connection through the optical switch between Harvard and Boston universities which was made possible using the DARPA QKD Network. Using SECOQC, the maximum length of the link obtained was around 82km. Tokyo recorded a maximum distance of around 90 km between the Koganei-1 and Koganei-2 nodes [10]. The maximum distance that QKD connections may be used efficiently in contemporary optical fiber networks is about 100 km.

4.1.3 Securing the Key Material

The main reason for interest in QKD is the privacy of the established key material. This means that the nodes of a QKD network must be secured with a strong probability that the established key material is unique and inaccessible to third parties. The security of key material is evaluated not only when it is established but also when it is managed, stored, and eventually used. It is therefore important to secure each level of the QKD network architecture.

4.1.4 Key Consumption

If the key generation rate in each network is the bare minimum this will affect the entire communication in the network. Each packet needs the previously established key material [3]. Hence, it is necessary to choose the shortest path for a packet to travel, this will also serve two purposes: (1) the Consumption of keys is reduced, (2) the Chance of an attacker to eavesdrop reduces significantly. Here, distance comes into the picture indirectly, haphazardly increasing the distance cannot be the solution. We need to limit this distance as it will affect side factors as well.

4.1.5 Robustness and Compatibility

It is necessary to design QKD networks such that they ensure robustness and compatibility as the QKD networks will slowly be integrated into traditional telecommunication environments [3]. Additionally, if the exiting nodes are under attack or certain malfunctioning takes place, there should be an alternative path for the packets to travel. Assuming the worst-case scenarios such as the attacker might compromise the entire QKD channel, the design of the network must be such that it can provide rapid responses to such kind of situations.

4.2 Quantum Nodes

Quantum devices that are responsible to execute the QKD protocols are structured together to construct a quantum node. These devices must have the ability to generate qubits, measure qubits and store qubits in specific memory devices. Depending upon the type of QKD protocol used the devices that need to adopt vary. Depending on the functions of quantum nodes, they can be categorized into three following types: (1) the repeater node, (2) the access node, (3) the central control node. The repeater node uses a suitable routing path to transmit the packets of session keys. The access nodes provide the necessary APIs to allow end users or applications to use the transmitted session keys. The entire routing table of the QKD network is controlled and managed by the central control node which plays the role of a routing server in a client-server architecture. Since meeting the balance between the key supply and demand is difficult because of the dynamics in key generation rate and key service demands it is necessary for a quantum node to maintain a buffer also

known as the key storage to temporarily store the local keys [3]. This will accelerate the tolerance levels of the QKD networks. Now the question here is whether the keys that are stored are secure enough or not. For this, it is important to manage and protect key generation, usage, and key storage.

4.3 Quantum Links

A quantum link comprises two channels: (1) Quantum Channel, and (2) Public Channel. This quantum link is a logical connection between the two remote quantum nodes 2. The quantum channel is used to transmit the qubits whereas the public channel also known as the classical channel, is built using classical cryptography technologies such as the universal hash functions. The classical channel is then responsible for post-processing operations such as error corrections, privacy amplification process, etc.

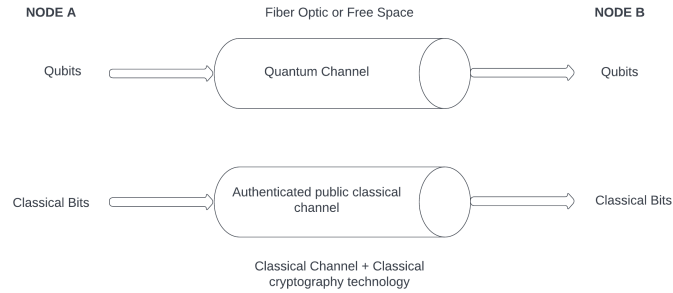


Figure 3: Quantum Links

There are two possible methods that can be implemented: (1) Optical fibers and (2) Free line of sight which is implemented in a P2P (point-to-point manner). The most common technique to transmit qubits is optical fibers but optical fibers are not convenient as well as practical in all situations to execute the QKD protocols. Using free-space links is better, more accurate, and more convenient to execute the QKD protocols but it has some limitations as well. The free space links need specific atmospheric conditions for the qubits to get transported. Additionally, it requires a visible light path, and the signal-to-noise ratio must be within the acceptable range. The same optical fibers can be used between the two QKD nodes to transport both the classical as well as the quantum information. One more advantage of using the free line of sight over the optical fibers is the installation costs required to deploy the optical fibers channel. Different types of QKD protocols require different types of transmission mediums. The discrete-variable-based QKD protocols require the fiber optic channel whereas the continuous-variable-based protocol uses the free space link. Before selecting the most convenient transmission channel type, it is also important to take factors such as the communication distance and the key rate into consideration.

The important relation between the key generation rate and the distance is that the key generation rate decreases as the distance increases, hence improving the performance, the distance and the key generation rate are practically impossible after a specific point (Fig. 2). Using fiber optics channels can improve performance by having more distance and improved key generation rate. But the limitations of using this are the increasing costs of implementing dedicated fibers and single-photon detectors. A previous study [9] has demonstrated successfully to increase in the distance range from 645km to 1200 km. Also, the twin-field QKD (TF-QKD) protocol proposed a range of 550km using the fiber optic cable.

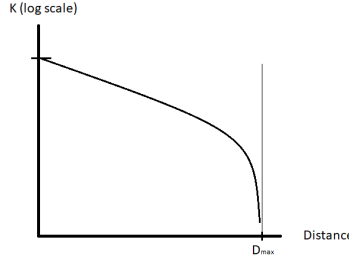


Figure 4: Key Rate Vs Distance

The maximum distance decreases with the increase in losses and the optical detector noise, this maximum distance is the distance over which the key can be generated [10]. Every detector has a count named dark count which is typically an event where a single photon is detected even though there is no photon present. This dark-count rate is constant for every detector. Recent studies have shown that the typical distance used by optical fiber systems is limited to 100kms and the corresponding key rate is a few tens or hundreds of kbps. Since the key rate is limited, it is necessary to install key storage at both endpoints of the channel. When there is a new key incoming it will be filled in this key storage and will be used to encrypt/decrypt data flows. The key consumption rate is determined by the amount of data that needs to be encrypted and the encryption algorithm that is been used. The QKD link can be designated as “Unavailable” when there are not enough keys to perform further cryptographic operations. One more noteworthy feature of the QKD devices is to generate keys continuously until and unless the key storage is full. This will prevent the key storage from going out of key materials.

5 QKD Network Types

The practical experiments and different research conducted have divided the QKD networks into three distinct classes: (1) Active Optical switch networks, (2) trusted node networks, and (3) quantum repeater networks. Although there is no such hard-defined rule to

implement any one type of QKD network, one can implement any kind of QKD network thus making it a hybrid model.

5.1 Active Optical Switch

A direct optical P2P quantum channel is established between any two nodes in the network using the optical switch. Any kind of assistance is not required between either of the two given nodes. (Fig 5a) This kind of design is like the normal switch we use in computer networks. This design brings two limitations into the picture: (1) the distance between the two nodes should be constant and hence cannot be extended which means it cannot exceed the maximum communicable distance between any two nodes in each protocol or network type. (2) consistency in quantum technologies should be maintained between the two nodes. Qubit communication is drastically affected using this type of network as the additional amount of photon loss will lead to a decrease in the distance of the quantum channel.[11]. Hence the type of network plays a key role in maximizing the distance.

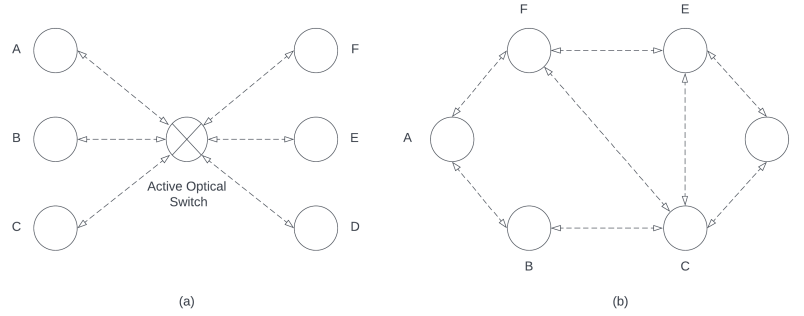


Figure 5: a. Active Optical Switch b. Trusted Node Network

5.2 Trusted Node Network

As opposed to the active optical switch network, in a trusted node network any given quantum node can establish a quantum connection with its neighboring node. Hence, resources and other security materials can be shared only with the neighboring nodes and not the remote nodes [3]. If the remote nodes want to connect and communicate the only way to communicate is to establish a connection in a hop-by-hop manner (Fig 5b). One advantage here in this kind of network is it can avoid a single point of failure just by eliminating the risk of a switch that can be attacked or malfunctioned. However, limitations still exist. Since the qubits are transferred in a hop-by-hop manner, any node in the given path can retain the information regarding the session keys, hence one should

assume that the intermediate nodes are trusted. So, if we want to increase the distance between the nodes, we must protect the nodes coming between those two nodes. Yet, this method is mostly used in current practical scenarios as constraints such as communication distance or node numbers don't come into the picture. Also, one can use different QKD devices to implement different technologies, hence satisfying the purpose of robustness and compatibility.

5.3 Quantum Repeater Network

This type of network is like that of the trusted node network. The major difference between the two is that in the case of a quantum repeater network, each node comprises of the quantum repeater that can use quantum teleportation or entanglement swapping. Nodes are also responsible for routing and forwarding mechanisms considering the lack of quantum repeaters. Although the computational power of this kind of technology is good enough, the quantum repeater technology is not mature yet, and using quantum repeaters is not cost-effective.

6 Key Results of previously deployed QKD networks

To enumerate the major findings in current QKD networks, this section analyses recent research papers and reports. Some nations and academic institutions have poured a lot of money into field trials on QKD networks to demonstrate their viability. The literature focuses on key storage and management solutions, key usage, and the performance of the solution since the quantum optical infrastructure is a major topic in the literature.

6.1 DARPA QKD Network

Developed in December 2002 by BBN technologies, Harvard and Boston Universities became the world's first QKD network. The network consisted of two pairs one transmitter pair (Anna and Alice) and one compatible receiver (Boris and Bob) and one 2 x 2 optical switch that could establish a connection between any sender to a receiver. The DARPA QKD network includes 10 quantum nodes and adopts a hybrid network type comprising of the active optical switch and trusted node networks. The DARPA network generates 400bps across 29 kilometers using the greatest performance thanks to the BB84 protocol suite, which provides the security keys [2, 10]. The DARPA QKD network created a hybrid solution by combining the two kinds which were discussed previously. The DARPA QKD network not only served as a springboard for the advancement of trusted repeater QKD networks, but it also amply illustrated the drawbacks of a switched QKD network type.

6.2 SECOQC QKD Network

Quantum Cryptography (SECOQC) based on European Commission's (EC) compiled with FP6 Project Secure Communication launched a project namely SECOQC QKD Network which defined the practical applications of QKD networks to examine the QKD networks' security, design, architecture, communications protocols, and implementation strategies in more detail. SECOQC makes it abundantly evident that key distribution and secure communication will be supported by QKD networks in future Internet settings. The SECOQC QKD network contains six quantum nodes and uses a trusted node network architecture. In addition, five distinct QKD techniques are utilized to distribute the local keys, and six various technologies (including attenuated laser pulse, one-way weak coherent pulse, entangled photons, and free space) are employed to build quantum linkages [12]. The SECOQC QKD network had the best performance in terms of key generation rate, averaging 3.1 kbps over 33 km.

6.3 Tokyo UQCC

Since 2010, Japan has launched the Tokyo UQCC (Updating Quantum Cryptography and Communication) QKD testbed network. The QKD network's infrastructure is made up of four access nodes and six repeater nodes, and the local keys are distributed via both the BB84 and BBM92 protocols [2, 3]. In October 2010, a live demonstration of secure TV conferencing utilizing this QKD network's key distribution service was given. The Tokyo UQCC QKD network has the best key generation rate performance, at 304 kbps across 45 km.

6.4 Summary of QKD Experiments

Network	DARPA	SECOQC	UQCC	China QKD
Project Year	2002-2006	2004-2008	2010	2014-2017
QKD Network Type	Active optical switch + Trusted Node	Trusted Node	Trusted Node	Trusted Node
QKD Protocol	BB84 Protocol	5 different QKD protocols	BB84 & BBM92	BB84 protocol
Max. Key generating rate	400 bps over 29 km	3.1 kbps over 33 km	304 kbps over 45 km	250 kbps over 43 km

Table 1: Summary of QKD Network Types

7 Challenges and workable solutions in current QKD infrastructure

Although great experimental results have been obtained from the existing studies in terms of the network framework, key generation rate, communication distance, and routing of

different protocols there are still some glitches in the overall QKD architecture that need to solve [3]. This section discusses the issues that were observed by the researchers and their workable solutions. These challenges include:

1. QKD networks lack point-to-multipoint (P2M) mechanisms: Current QKD network architecture only provides point-to-point key distribution service and not point-to-multipoint
2. A multiple-path technique consumes a lot of the resources in a quantum node: Although a multiple-path method can get around the need that each quantum node must be trusted, the multiple-path strategy requires a lot of resources from the quantum nodes (such as the local keys that are required to aid transmit the session key)

7.1 QKD networks lack point-to-multipoint (P2M) mechanisms

The current QKD networks can only provide the P2P key distribution service that can only forward key/session material to only one node. However, some applications majorly require broadcast communication to be done and hence need a P2M key distribution service. Some experiments were performed to achieve this with the P2P mechanism but were susceptible to the consumption of numerous resources of the quantum nodes. For example, in Fig 6, Alice wants to dissipate her session key to three different parties Bob, Charlie, and David. First Alice will send the session key (SA) to one of the nodes let's say N8, node N8 will use its local key to transport the key material to the next node which is N4. Now N4 will have to generate three keys $K(2,4)$, $K(1,4)$, and $K(3,4)$, and perform three different encryptions. This will give performance issues during normal operations at the nodes. To enhance the performance, reducing this overhead on nodes is necessary. Adopting the quantum conference key distribution (QCKD) protocol, which enables a multiparty to concurrently share a conference key, is therefore a workable solution to this problem. If N4 had shared a conference key with N1, N2, and N3 for the job, N4 would only use one conference key and complete the encryption once (Figure 7); hence, a QCKD protocol is necessary for the QKD network [2]. However, there is still much to learn about how to effectively integrate QKD and QCKD protocols into QKD networks. Some physical layer technologies, in addition to the QCKD protocols, can be utilized to address this P2M issue. One appropriate technique is a time-division multiplexing (TDM), instance.

7.2 A multiple-path technique consumes a lot of the resources in a quantum node:

Any node along the path can store and maintain the session key delivered from the source node to the destination node because the QKD network employs the hop-by-hop mechanism to diffuse the session keys to the target node while considering a restriction to the qubit

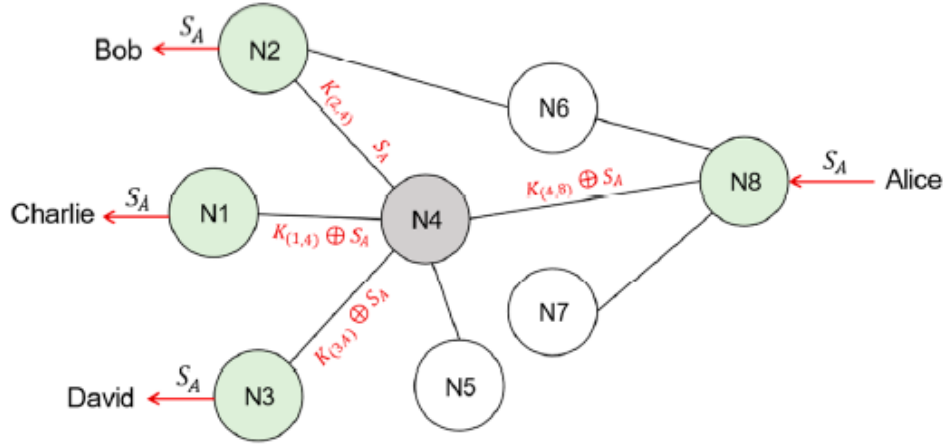


Figure 6: Point to Point Key Distribution Mechanism [2]

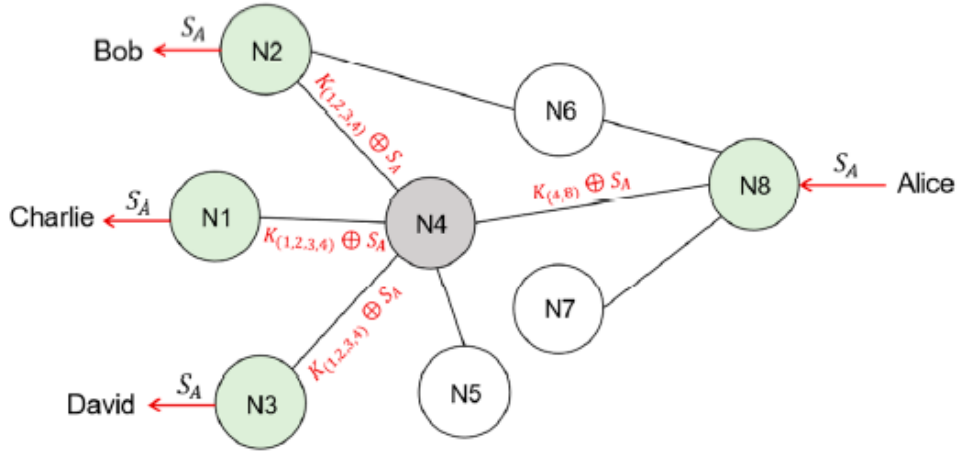


Figure 7: Point to Multipoint Key Distribution Mechanism [2]

transmission distance. The source node that wishes to share the session key sends a reservation request to each of the nodes that are located between the source and destination nodes after the routing path has been decided upon. The intermediate nodes then share the session keys by encrypting the local keys using XOR operations to help the source key. It has been demonstrably demonstrated that if the intermediary nodes were infiltrated, the session key may leak. As seen in Figure 8, the SECOQC QKD network uses a similar approach to broadcast the session key. By using the local key shared by it and the next node, this session key transmission mechanism enables any node in the routing route to

decode the session key's ciphertext before re-encrypting the key and sending new ciphertext to the next node. In other words, each node in the routing path may acquire the session key directly, meaning that if any node in the routing path is hacked, the session key will be made public. In other words, each node in the routing path may simply acquire the session key.

$$K_{(1,2)} \oplus (K_{(1,2)} \oplus K_{(2,3)}) \oplus (K_{(2,3)} \oplus K_{(3,4)}) \oplus (K_{(3,4)} \oplus K_{(4,5)}) \oplus (K_{(4,5)} \oplus SK).$$

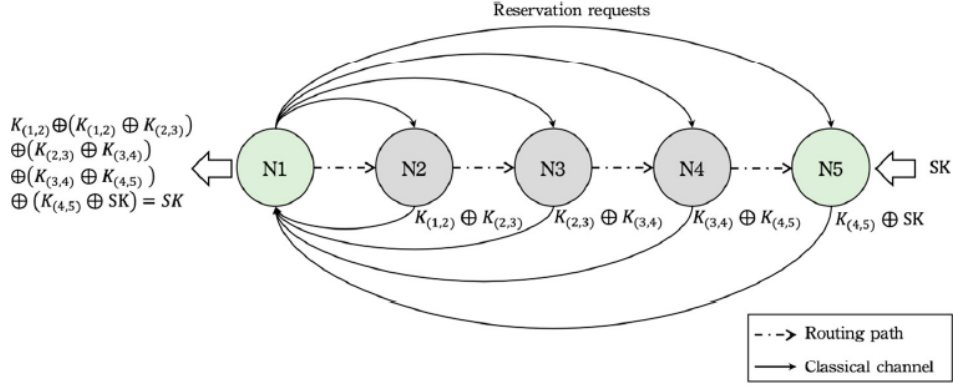


Figure 8: Multipath Issues [2]

Previous research proved that even a multipath strategy can also consume a lot of resources of the quantum nodes if the partial nodes in the path were compromised. One possible solution to this can be that each node will share a secret shadow with the use of QSS protocol [13, 11]. If the node is not on the route, no information about the session key may be taken from this and exposed to anybody Figure 9. The source node won't get the secret shadow from the intermediary nodes if they were hacked, making it impossible to decode the session key data. However, it is still believed that the source and destination nodes are secure and reliable. Additionally, because the routing pathways in the QKD network are dynamic, it is essential to inform every node along the path in order to obtain a hidden shadow from them. Future solutions are still required for this problem.

8 Intro for BB84 Protocol:

In the late 1960s it was understood that the principle of uncertainty could be applied in the field of cryptography. This led to the foundation of quantum cryptography which was led by Stephen Wiesner who was a physicist in 1969. One of the challenges was the problem of quantum key distribution under the principles of quantum mechanics [14, 15]. Bennet and Brassard collaborated with Stephen and proposed the BB84 protocol.

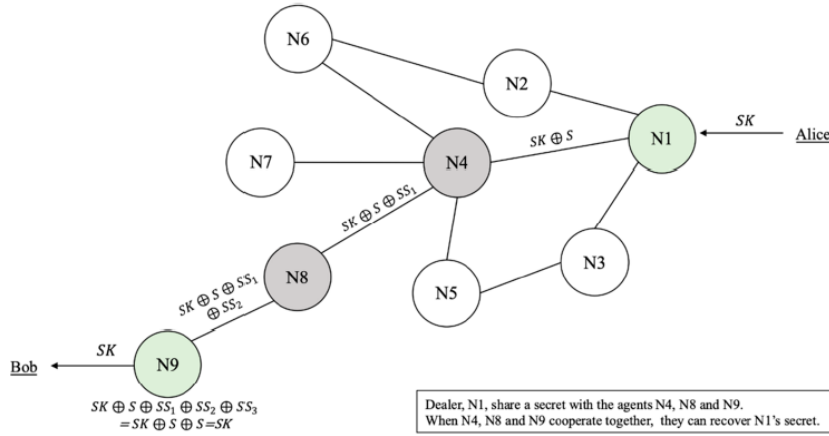


Figure 9: Working of Secret Shadow mechanism [2]

9 Polarizations of photons

There are 2 bases namely the rectilinear base and the diagonal base. A photon is polarized using one of these bases. After polarization, the photon is represented in the form of a qubit. When a photon is polarized in the rectilinear basis at an angle of 0 degrees and in the diagonal basis at an angle of 45 degrees it is represented using the binary 0. Similarly, when a photon is polarized in the rectilinear basis at an angle of 90 degrees and in the diagonal basis at an angle of 135 degrees it is represented using the binary 1. The probability of how a photon works with a polarizer during polarization can be divided into 4 parts (Figure 10) When an unpolarized light passes through a vertical polarizer(basis), its probability is 100 percent when it is produced again in a vertical polarizer When an unpolarized light passes through a vertical polarizer(basis) at an angle of 90 degrees, its probability is 0 percent when it is produced again in a vertical polarizer but at an angle of 0 degrees. When an unpolarized light passes through a vertical polarizer(basis), its probability is 50 percent when it is produced again in a 45-degree diagonal polarizer

10 BB84

Bennett and Brassard protocol (BB84) was proposed in 1984 since it serves as the starting point for many other protocols. This protocol is dependent on Heisenberg's Uncertainty Principle. The purpose behind quantum key distribution is for the sender (Alice) and the receiver (Bob) to establish a secret key over a likely insecure channel. Alice and Bob will hope to communicate with each other over the public channel but they will use the quantum channel to establish a secret key (Figure 11). The quantum channel that is used for the

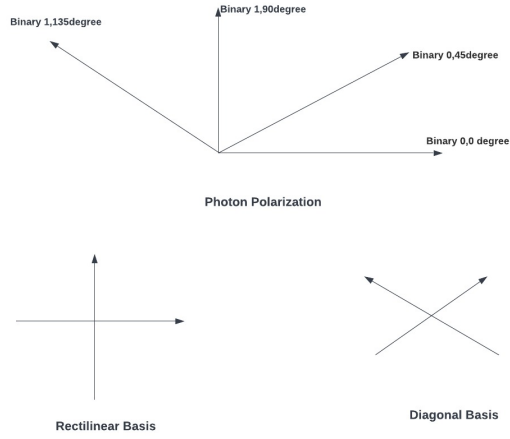


Figure 10: Bases for polarization of photons

purpose of quantum key distribution is either free space or single-mode fiber. BB84 was first introduced to solve the key distribution efficiency [16]. The BB84 protocol can be divided into 5 steps in which a common secret key is established over a quantum channel [14].

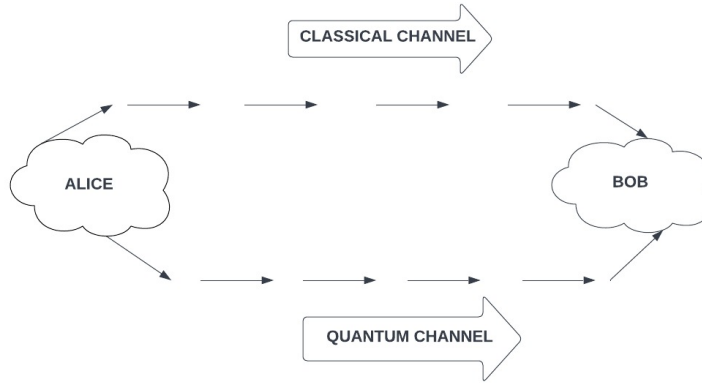


Figure 11: Channels in BB84 Protocol

10.1 Step 1

The sender (Alice) will first begin with establishing a connection with the receiver (Bob). Alice then continues to create a stream of random bits of 0s and 1s. Alice then proceeds

to generate a string of bases which could be either rectilinear bases or it could be diagonal bases. These randomly generated bits and bases are of equal length. Alice polarizes every bit using the randomly chosen polarizer and transmits the photon to Bob.

10.2 Step 2

This step begins with Bob receiving the polarized photons sent by Alice. Bob proceeds to choose either of the measurement basis that is the rectilinear base or the diagonal base. If the base that was chosen by Bob is the same as Alice then the value of the measure will be the same as Alice's. If Bob chooses the wrong base then the value of the measure will have a 50 percent probability. After this step Bob has a stream of bits which is also known as the raw key. This raw key is a string of 0s and 1s that Bob received from Alice after he used his randomly chosen base.

10.3 Step 3

After the quantum communication is finished Bob and Alice communicate with each other through an authenticated public channel. In this step, Bob informs Alice of the basis that he used to measure each received photon. Alice then informs Bob if the detector he used for the measurement were right or wrong. This will help to identify the correct corresponding bit. The bits which have been produced after using the wrong base are discarded. The probability of Bob choosing the correct base is 50 percent thus after the discarding is done at least the bits get matched with Alice's original bit which is called the sifted key. Eavesdropping is one of the major concerns while producing a shared key but in this case, it is possible to detect if there has been any eavesdropping. Let's consider the middle man (Trudy) is trying to copy the key which was sent from Alice to Bob. The only way Trudy can measure these bits is by measuring them using his/her own base. Now, just like Bob the chances of Trudy getting the right base is 50 percent. From the other 50 percent, she can obtain a correct measurement in half the cases. This means that of the bit that is transmitted by Trudy, 75 percent of them are correct and that means 25 percent of them are wrong. These bits are now retransmitted to Bob. Now when Bob compares his basis with the basis of Alice and keeps only the ones that are the same to get the shift key. In this case, the error should be 0 percent but instead, Bob will find out the error percentage to be 25 and thus Bob and Alice will know that there was someone listening and another quantum channel will be established for key exchange. Thus we can see the strength of the BB84 protocol lies in the fact that the sender and the receiver can identify if there was any sort of presence of an eavesdropper.

10.4 Shortcoming of the BB84 protocol

Due to the detectors' imperfections, noises may be heard. This means that even in the absence of eavesdropping, Alice and Bob may disagree when they attempt to establish a

key. Due to the fact that the key can only be used in 25 percent of the stream that was initially generated, many qubits are left unused. This occurs as a result of the basis being chosen at random.

10.5 Possible attacks on the BB84 protocol

It is challenging to put the BB84 theory into practice and make it unbreakable because there will be flaws in the process of producing and measuring photons. Because of this, the protocol is vulnerable to assaults and eavesdropping techniques.

10.5.1 Intercept and Resend

A significantly easier eavesdropping method is intercept-resend. In this scenario, Eve would monitor the data transmission from Alice and take measurements. She would create a new state in the measured polarization based on the results of her measurement and send this to Bob. As an illustration, let's say Alice prepares and sends a quantum state that is a part of the linear basis. Eve would be able to send Bob the correct state of the photon if she intercepted and measured it on the same basis. She would then prepare and send Bob the correct state. So long as Bob measures the state on the proper foundation, Bob identifies the correct state in this since in this case, Eve introduces no error. However, if Eve intercepts and measures the state using a basis, her results will be utterly random, she will gain nothing, and she will cause the most disruption to the transmission

10.5.2 Photon Splitting Attack

Using present methods, it is quite challenging to produce perfectly single photons at a high rate. Because of this, phase-randomized weak coherent pulses are used for the majority of BB84 implementation. Multi-photon pulses will almost certainly be produced by most sources, at least with a minimal probability. Therefore, Eve can intervene and split the photons as they go from Alice to Bob in these multi-photon pulses. One is kept by her, and the other is sent to Bob. Eve would take measurements after Alice and Bob had taken them and made the bases known to the public. She will measure using the same methodology as Bob and, on average, produce data that is identical to Bob (Figure 12).

11 B92 PROTOCOL

In his 1992 publication, "Quantum cryptography employing any two non-orthogonal states" [Bennett92], Charles Bennett put out what is effectively a condensed version of BB84. In contradiction to BB84, where there are a total of four possible polarization states, B92 only requires two states [17]. Identical to the BB84, Alice sends Bob a stream of photons which are encoded with randomly picked bits. Now, the bases that Alice needs to utilize

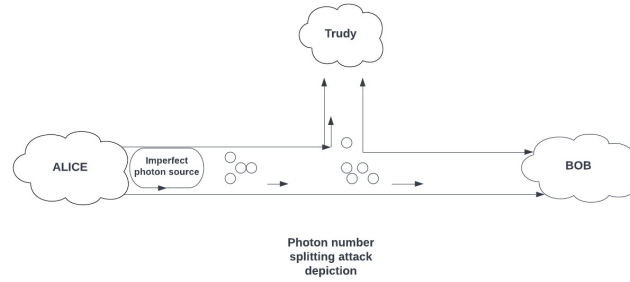


Figure 12: Photon Splitting Attack

are completely dependent on the bits she has selected at random. This is the key difference between the BB84 and B92 protocols. Bob continues to decide on a measurement basis at random, but if he selects the incorrect basis, he will be unable to take any measurements—a situation known as erasure in quantum physics. Bob may easily check his measurements by informing Alice whether they were accurate after each piece she sends [17]. The steps for the B92 protocol are as follows:-

1. The sender which we refer to as Alice will create a random stream of bits. This is referred to as the primary key and let's refer to it as "s"
2. Alice uses the two polarization states that are 0 and 45 degrees to represent the stream of bits x.

SENDER		
Base	L	D
State	0	45
Qbit	→	↗
Bits	0	1

Figure 13: Sender

3. Through the use of a quantum channel, Alice generates a stream of polarized photons, also referred to as qubits and sends it to the recipient (Bob).
4. Bob still has no idea about the bases that were used by Alice for polarization thus he randomly chooses the polarization bases between the linear and the diagonal base

similar to what we did in the BB84 protocol as discussed before.

- Bob measures every bit by the base that he had chosen in step 4. After this, he obtains a raw key.





RECIEVER				
Base	L	D	L	D
State	0	45	90	135
Qbit				
Result	0	0	1	1
Bit	?	?	1	0

Figure 14: Receiver

- After obtaining the raw key each qubit that was detected as 0 gets eliminated from the raw key. Now if Bob used the linear base when detecting the 1, the bit chosen for the key is 0 and if bob used the rectilinear base to detect the 1, the bit chosen for the key is 1.
- Alice eliminates from x the bits when bob detected the 0

11.1 Pseudocode for B92 protocol

```

Sender:
create random bits string s
FOR each bit from s
  IF s[i] = 0 THEN polarize photon in state (0°)
    generate a qbit p[i] = →
  IF s[i] = 1 THEN polarize photon in state (45°)
    generate a qbit p[i] = ↗
  send qbit p[i] to Receiver
ENDFOR
Receiver:
FOR each qbit p[i] received
  pick randomly from ("L", "D") → base b'[i]
  measure qbit p[i] in respect to base b'[i] → v
  IF v = 0
    THEN s'[i] = ?
    eliminate the corresponding bit from s'
    send value '0' to Sender
  ELSE // v = 1
    IF b'[i] = D
      THEN s'[i] = 0
    ELSE // b'[i] = L
      THEN s'[i] = 1
    ENDIF
  ENDIF
ENDFOR

```

Figure 15: Pseudocode

12 Measurement Device Independent Quantum Key Distribution Protocol

Even though in theory QKD is unconditionally secure, there is a significant difference between the assumptions provided in the security proofs of QKD and the actual implementations. This is the case because real devices inherently have flaws that can cause them to behave very differently from the mathematical models that were used to demonstrate security [18]. The bobs measurement scheme contains flaws. Quantum hacking has become more common as a result of this. This occurs as a result of Trudy's ability to communicate with Bob in any way, which makes it challenging for Bob to ensure safety. Therefore, Trudy might take advantage of these flaws to discover the distributed key covertly. Additionally, it is going to be relatively challenging to guarantee that both detectors always have the same detection efficiency because every QKD system requires at least two detectors to measure two separate bit values. In this case, Eve need only modify the timing of each signal's arrival so that one detector detects more accurately than the other. She was able to gather some knowledge regarding the final key as a result while not introducing errors. The detector blinding attack, which is more potent, was just recently established. Eve can learn the entire key while not being noticed because of it. The steps are as follows. Bob's detectors are made to operate in the so-called linear mode by Eve by sending them a strong light signal. As a result, the SPDs function like conventional intensity photo-detectors and are no longer sensitive to single-photon pulses. Eve may now completely control which detector "clicks" by essentially providing Bob with a customized light pulse. The use of this attack against both commercial and academic QKD systems has been successful. Measurement device-independent QKD is the widely explored solution to this problem. This eliminates the qkd's weakest component, which removes the side channel from the measuring unit. Using this with existing technology is also very feasible [18]. Importantly, it enables long-distance QKD with a high key rate.

Before we start understanding how the mdiQKD operates, we must first learn the functioning of how the Einstein-Podolsky-Rosen-based protocol operates [18]. To an unreliable third party, X, Alice, and Bob both prepare an EPR pair, which is a pair of qubits that are in a maximally entangled state. The signals that will be arriving via a Bell State Measurement are planned to be subjected to an entangled swapping by X. (BSM). Following this, X will announce his findings. Following that, Bob and Alice will use the diagonal basis and the rectilinear basis that they randomly chose to measure their EPR pairings. They can determine if X is being honest by employing this method.

12.1 Working of MDI-QKD Protocol

1. Alice creates phase-randomized pulses from weak coherent sources of varying intensities. These two pulses interfere at a beam splitter (BS) with a transmittance of 50 percent, producing two outcome signals with the conventional photon number statistics. Alice

passively creates signals or decoy states.

2. Bob uses two weak coherent sources with different intensities to generate phase-randomized pulses, following the same procedure as Alice.
3. The polarization encoding technique is used in this stage and is based on the BB84 protocol. For each signal, a distinct polarization state of Alice and Bob's phase-randomized WCP is chosen using the polarization modulator (Figure 16). They transmit that to relay X, an unreliable relay, which does a Bell-state measurement. A Bell state measurement is completed when precisely two detectors are detected as being triggered. Through a public channel, X informs Alice and Bob of these results. Now, depending on the results from X, Alice and Bob proceed with the error-correcting process as in the conventional QKD protocol. This will guarantee that Bob and Alice have the same bits.

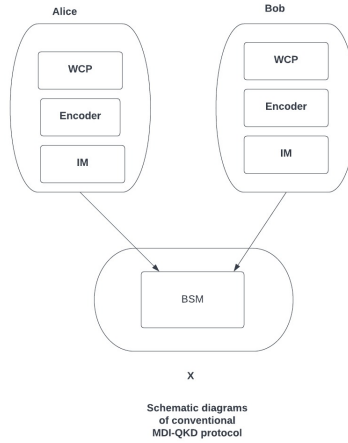


Figure 16: Schematic diagram of Conventional MDI-QKD Protocol

13 Distance Problem and Possible Solutions

So, till now we realized that one major issue Quantum Key distribution has faced is the distribution of keys at a significant distance. Over the past ten to fifteen years lots of different methods, protocols as well as different implementation techniques have been used. Rather than jumping right to the problem and giving a possible solution, we have divided this paper into three parts. The first part included the different networks used to implement Quantum Key Distribution. The second part includes different protocols that have been implemented and how every protocol came up with a different approach to tackle

the distance problem. Before we go on discussing each section, there is one thing about Quantum signals that needs to be cleared. Quantum signals are very vulnerable to different propagations disabilities such as scattering or a loss over transmission through optical fibers. To avoid this one would think that we can amplify the quantum signals so that the loss can be overcome. But, quantum signals cannot be amplified because if one wants to amplify the quantum signals, it would require them to measure and clone the quantum states which is impossible because it is against the laws of physics [?]

13.1 Quantum Transmission Media

First, there are different transmission mediums that a Quantum Key Distribution makes use of. There are specifically two different types of Quantum transmission media that can be used:

- Optical Fiber
- Free Space

As already discussed optical fiber has significantly low loss and very good stability and thus has been a suitable medium for the transmission of photon signals. Even though using optical Fiber has its advantages, the main disadvantage that it has had is that due to its nature of absorption and how it gets affected by the noise during the transmission of quantum signals, it is unable to transmit these signals over a long distance.

When it comes to Free space as the mode of transmission of quantum signals, it can transmit signals over a longer distance and is also flexible. Recently there has been significant progress in the experiments of QKD over free-space optical links. Experiments such as Air-to-ground QKD [19], Satellite-to-ground QKD [20] have been able to increase the distance of QKD up to 1200 km. This owes to the property of free space that the propagation loss scales only quadratically in free space which then becomes negligible in the vacuum above the Earth's atmosphere. However, the only reason Free space is not being used in real-life applications is that it is not mature enough and there is more testing as well as advancement required before it is out in the real world. After talking about QKD transmission media, it is time when we talk about different QKD implementation options. There have been mainly two different implementation options:

- DV-QKD
- CV-QKD

The first method of implementation involves mapping information to the discrete quantum states, like the polarization phase or time bin of a single photon. This method prefers a single photon source. The distance of DV-QKD has been limited mainly because of the performance of single-photon detectors.[21] CV-QKD[22] - This is the complete opposite of

DV-QKD since this makes use of continuous values quantum states which includes quantized electromagnetic fields. The main reason why CV-QKD's transmission distance is limited is because of the efficiency of the post-processing techniques used.

13.2 Protocols

Then comes different types of protocol. Though I will not be explaining the working of these protocols, since it is already done in section 2, I will be just explaining the distance problem that these protocols face and how each protocol dealt with it and what was the maximum transmission distance that it was able to cover. The very first protocol that was introduced and is still in use, with a few modifications, is BB84. The main reason why it has not been able to achieve its maximum capacity is because of the unavailability of a perfect single photon. Instead, it uses a highly attenuated laser source that can generate weak coherent pulses. The second protocol is the MDI protocol. This is one of the recently introduced protocols. The newer, modified versions of MDI such as TF-QKD[23], and PM-QKD[24] protocols have shown to be capable of overcoming key generation rates as well as the distance limitation which is faced by the conventional MDI protocol.

13.3 QKD Networks

Now let us talk about the certain limitation that is faced by different QKD networks. Detailed information about the working and how they are implemented is already discussed in section 4. As discussed there has been a significant development in recent years in different networks that are used for the transmission of keys via quantum channels. We discussed Optical Switching Based QKD. This network method is capable of transmitting the signals via short quantum links without ever interacting with the untrusted nodes. This makes them less vulnerable to any kind of eavesdropping. But since this network method does not make use of any kind of nodes, it can be used only for the transmission of keys for a short distance [25]. Another QKD network that we discussed is a Trusted Relays Based Network. This type of network makes use of trusted nodes. The QKD link is responsible for creating secret keys that are then locally stored at both end nodes. QKD transmission is possible using this network if there is a combination of QKD links in a one-dimensional chain along with a set of trusted relays that are connected using QKD Links. The transmission of keys from one node to another takes place by a hop-by-hop method along the path. Since a long-distance transmission of QKD is possible using this type of network, it has been adopted for the deployment.

The third type of network that is used and is being researched is the Untrusted Relay Network. We already know that this makes use of the untrusted relay and since they are untrusted this type of network requires a more secure protocol. Again we already have seen that MDI and different entanglement protocols have shown promising results in increasing the transmission distance, a combination of this network along with this protocol can

increase the transmission distance by a significant amount. [26] [27]

The fourth and final network that we saw made use of the Quantum Repeater and thus is called Quantum Repeater Based Network. This type of network is capable of increasing the transmission distance way more than the above-discussed networks. The repeaters are capable of creating a longer distance entanglement between the two ends and these nodes make use of the process called entanglement swapping.[28][29][30]

14 Possible solutions to Distance Problem

14.1 Usage of Relays/Repeaters

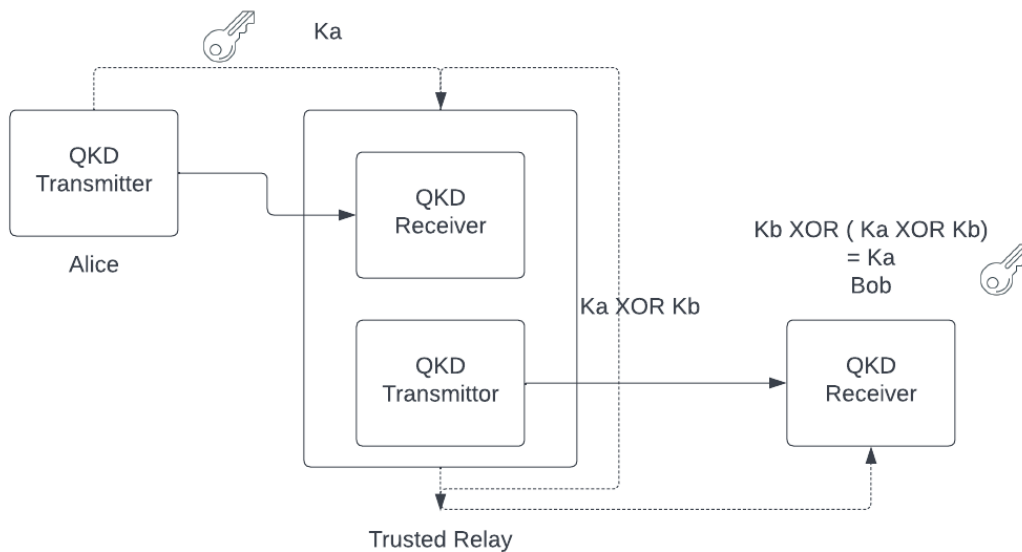


Figure 17: Using Trusted Relays for Quantum Key Distribution.

So far we have realized that the QKD faces two major problems, one being the distance and the other being the secret key rate. This limitation is mainly caused due to several imperfections in the physical layer of the architecture of the QKD. These impairments include scatters, and loss of faint quantum signals transmitted in a quantum channel. One of the solutions to increase the distance of the QKD transmission was through the use of repeaters or relays. The main functionality of the quantum repeaters is to restore the information regarding the quantum signals without actually measuring them [29]. Due to the nature of Quantum repeaters, it has attracted a lot of attention in recent years.

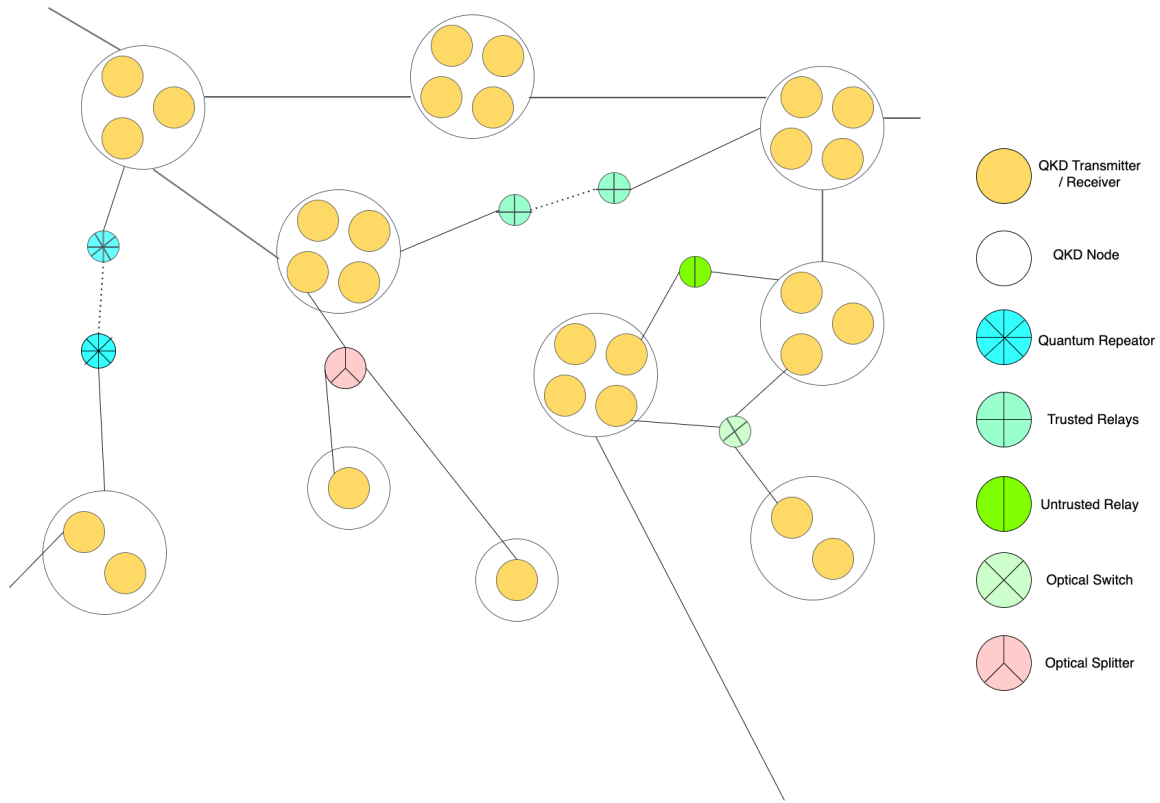


Figure 18: Relaying Options for Increasing Distance.

[31][32][33]. Though there has been no luck in the successful development of a practical Quantum Repeater and thus it has not been deployed in the real world yet. Another solution stated that the distance can be increased if there was a repeaterless scheme such as TF-QKD which does not make use of nodes or relays/repeaters that might be able to successfully conquer the basic distance limit QKD. [34] A third solution, similar to the previous solution came to light when there was a new protocol named, Twin Field - Quantum Key Distribution Protocol, was invented. This protocol does not make use of quantum repeaters and was able to increase the point-to-point secret key capacity.[23] But the distance achieved by TF-QKD was limited up to 605km.[27]

Currently, in the real world, a compromise was made to extend the distance by using trusted relays. Thus, trusted relays have also been widely adopted by many of the real-world QKD Networks. Other reasons why trusted relays have been preferred during the real-world implementation of QKD include the reduced complexity, and also how it readily supports the setup of long-distance QKD networking. Several varieties of trusted relays have been discovered in recent years, each one with its benefits. One such trusted relay simplified its

overhead as well as its security and thus reduced the overhead expense during the relaying process [35]. One solution that holds the promise of increasing the transmission distance is the usage of the entanglement-based approach.

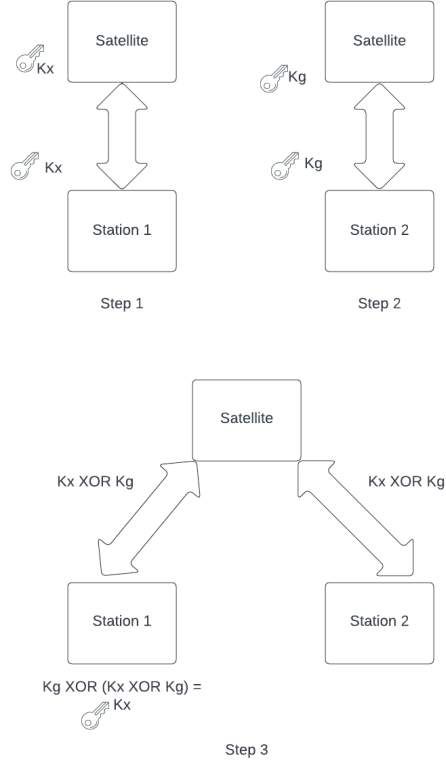


Figure 19: Satellite for QKD Transmission

14.2 Usage of Satellites

The drawbacks of using QKD on the ground led to the usage of satellites for the transmission of Quantum keys. These drawbacks included non-supportive fiber-based QKD on bad terrain. The use of satellites was preferred because of the presence of free space in the vacuum above the earth's atmosphere and how it had less attrition than the earth's atmosphere. With the use of untrusted relays for connecting the networks, present in different locations on the ground, there is a possibility of a significant increase in the key rate as well as an increase in the distance of transmission of keys via free-space links.[36] There are several ongoing research going about the satellite-based QKD, some of them include research by Micius [20], research by Bedington[36], and research by Khan [37], each providing a different approach

to overcome the distance problem through the usage of the satellite. Another reason why the use of satellites was preferred was that it is placed above the Earth's atmosphere and directly link to the stations on the ground stations. According to this solution, the atmospheric attenuation was reduced to 0.07dB per km and almost negligible in the vacuum. This solution was able to increase the transmission distance to a significant distance and thus promising a global transmission of the keys soon if they were able to overcome the drawbacks they faced.[36]. Finally, we came across another research suggesting the use of higher orbit quantum satellites that could be launched along with the establishment of the satellite constellation. This method that the study suggested shows the promise of establishing global QKD. [38]

15 Conclusion

The QKD networks can offer long-term data protection and future-proof security for a wide range of applications, but they also have a lot of unresolved issues. This study offers a thorough analysis of previous successes together with a wide-ranging research viewpoint on QKD networks. We commenced with the introduction of the QKD network its architecture and overall factors that get affected by the increase in distance. In the initial sections, we proved that increasing distance is not a one-shot solution we need to take into consideration the other factors that might get affected. going ahead we discussed different protocols that help execute the QKD Networks and transmit qubits from source to destination. Finally, we provided a few solutions that would help to increase the transmission distance between the nodes. In our future work, we would like to continue to hunt more technical solutions which can be feasible, robust as well as cost-effective.

16 Acknowledgment

We are grateful to Prof. Sumita Mishra for her overall guidance during the semester and for providing us with the chance to present and share our findings with our fellow peers.

References

- [1] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Communications Surveys Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.
- [2] C.-W. Tsai, C.-W. Yang, J. Lin, Y.-C. Chang, and R.-S. Chang, "Quantum key distribution networks: Challenges and future research issues in security," *Applied Sciences*, vol. 11, no. 9, p. 3767, 2021.

- [3] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher *et al.*, “Quantum key distribution: a networking perspective,” *ACM Computing Surveys (CSUR)*, vol. 53, no. 5, pp. 1–41, 2020.
- [4] C. Elliott and H. Yeh, “Darpa quantum network testbed,” BBN TECHNOLOGIES CAMBRIDGE MA, Tech. Rep., 2007.
- [5] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. Towery, and S. Ten, “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” *New Journal of Physics*, vol. 11, no. 7, p. 075003, 2009.
- [6] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nature Photonics*, vol. 9, no. 3, pp. 163–168, 2015.
- [7] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, “Security of trusted repeater quantum key distribution networks,” *Journal of Computer Security*, vol. 18, no. 1, pp. 61–87, 2010.
- [8] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus *et al.*, “Using quantum key distribution for cryptographic purposes: a survey,” *Theoretical Computer Science*, vol. 560, pp. 62–81, 2014.
- [9] W. Li, L. Wang, and S. Zhao, “Phase matching quantum key distribution based on single-photon entanglement,” *Scientific Reports*, vol. 9, no. 1, pp. 1–12, 2019.
- [10] C. Elliott, “The darpa quantum network,” in *Quantum Communications and cryptography*. CRC Press, 2018, pp. 91–110.
- [11] J.-H. Chen, K.-C. Lee, and T. Hwang, “The enhancement of zhou et al.’s quantum secret sharing protocol,” *International Journal of Modern Physics C*, vol. 20, no. 10, pp. 1531–1535, 2009.
- [12] M. Dianati and R. Alléaume, “Architecture of the secoqc quantum key distribution network,” in *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM’07)*. IEEE, 2007, pp. 13–13.
- [13] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, “Practical challenges in quantum key distribution,” *npj Quantum Information*, vol. 2, no. 1, pp. 1–12, 2016.
- [14] P. Winiarczyk and W. Zabierowski, “Bb84 analysis of operation and practical considerations and implementations of quantum key distribution systems,” in *2011 11th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, 2011, pp. 23–26.

- [15] F. Yang and Y.-J. Hao, “The formal study of quantum cryptography protocols,” in *2013 10th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, 2013, pp. 29–33.
- [16] H.-F. Li, L.-X. Zhu, K. Wang, and K.-B. Wang, “The improvement of qkd scheme based on bb84 protocol,” in *2016 International Conference on Information System and Artificial Intelligence (ISAI)*, 2016, pp. 314–317.
- [17] C. Anghel, A. Istrate, and M. Vlase, “A comparison of several implementations of b92 quantum key distribution protocol,” in *2022 26th International Conference on System Theory, Control and Computing (ICSTCC)*, 2022, pp. 374–379.
- [18] F. Xu, M. Curty, B. Qi, and H.-K. Lo, “Measurement-device-independent quantum cryptography,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 148–158, 2015.
- [19] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, “Air-to-ground quantum communication,” *Nature Photonics*, vol. 7, no. 5, pp. 382–386, 2013.
- [20] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.
- [21] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, “Advances in ingaas/inp single-photon detector systems for quantum communication,” *Light: Science & Applications*, vol. 4, no. 5, pp. e286–e286, 2015.
- [22] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, “Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 881–919, 2018.
- [23] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature*, vol. 557, no. 7705, pp. 400–403, 2018.
- [24] X. Ma, P. Zeng, and H. Zhou, “Phase-matching quantum key distribution,” *Physical Review X*, vol. 8, no. 3, p. 031043, 2018.
- [25] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, “Efficient decoy-state quantum key distribution with quantified security,” *Optics express*, vol. 21, no. 21, pp. 24 550–24 565, 2013.
- [26] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin *et al.*, “Sending-or-not-sending with independent lasers: Secure twin-field

- quantum key distribution over 509 km,” *Physical review letters*, vol. 124, no. 7, p. 070501, 2020.
- [27] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, “600-km repeater-like quantum communications with dual-band stabilization,” *Nature Photonics*, vol. 15, no. 7, pp. 530–535, 2021.
 - [28] H. J. Kimble, “The quantum internet,” *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.
 - [29] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, “Quantum repeaters: the role of imperfect local operations in quantum communication,” *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.
 - [30] R. Van Meter and J. Touch, “Designing quantum repeater networks,” *IEEE Communications Magazine*, vol. 51, no. 8, pp. 64–71, 2013.
 - [31] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” *Science*, vol. 362, no. 6412, p. eaam9288, 2018.
 - [32] R. Van Meter, T. D. Ladd, W. J. Munro, and K. Nemoto, “System design for a long-line quantum repeater,” *IEEE/ACM Transactions On Networking*, vol. 17, no. 3, pp. 1002–1013, 2008.
 - [33] S. Kumar, N. Lauk, and C. Simon, “Towards long-distance quantum networks with superconducting processors and optical links,” *Quantum Science and Technology*, vol. 4, no. 4, p. 045003, 2019.
 - [34] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, “Fundamental limits of repeaterless quantum communications,” *Nature communications*, vol. 8, no. 1, pp. 1–15, 2017.
 - [35] W. Stacey, R. Annabestani, X. Ma, and N. Lütkenhaus, “Security of quantum key distribution using a simplified trusted relay,” *Physical Review A*, vol. 91, no. 1, p. 012338, 2015.
 - [36] R. Bedington, J. M. Arrazola, and A. Ling, “Progress in satellite quantum key distribution,” *npj Quantum Information*, vol. 3, no. 1, pp. 1–13, 2017.
 - [37] M. Leslie, “Quantum cryptography via satellite,” *Engineering*, vol. 5, no. 3, pp. 353–354, 2019.
 - [38] T. Vergoossen, S. Loarte, R. Bedington, H. Kuiper, and A. Ling, “Modelling of satellite constellations for trusted node qkd networks,” *Acta Astronautica*, vol. 173, pp. 164–171, 2020.