Multi-photon 3-Stage QKD for Practical Quantum Networks

Nitin Jha
Kennesaw State University
Abhishek Parakh (✉ aparakh@kennesaw.edu)
Kennesaw State University
Mahadevan Subramaniam
University of Nebraska at Omaha

Research Article

Keywords: Quantum networks, quantum key distribution, multi-photon transmissions, 3-stage protocol, network topologies

Posted Date: January 10th, 2024

DOI: https://doi.org/10.21203/rs.3.rs-3826628/v1

Additional Declarations: No competing interests reported.

Title Page

Title

Multi-photon 3-Stage QKD for Practical Quantum Networks

Authors

Nitin Jha, Computer Science Department, Kennesaw State University, USA, email: njha1@students.kennesaw.edu

Abhishek Parakh, Computer Science Department, Kennesaw State University, USA, email: aparakh@kennesaw.edu

Mahadevan Subramaniam, Computer Science Department, University of Nebraska Omaha, USA, email: msubramaniam@unomaha.edu

Corresponding author

Abhishek Parakh, Computer Science Department, Kennesaw State University, USA, email: aparakh@kennesaw.edu

Multi-photon 3-Stage QKD for Practical Quantum Networks

Author 1[1], Author 2[1*], Author 3[2]

Abstract

Quantum key distribution (QKD) will most likely be an integral part of any practical quantum network setup in the future. However, not all QKD protocols can be used in today's networks because of the lack of single photon emitters and noisy intermediate quantum hardware. Attenuated photon transmission typically used to simulate single photon emitters severely limits the achievable transmission distances and the integration of QKD into existing classical networks that use tens of thousands of photons per bit of transmission. Furthermore, it has been found that different protocols perform differently in different network topologies. In order to remove the reliance of QKD on single photon emitters and increase transmission distances, it is worthwhile exploring QKD protocols that do not rely on single-photon transmissions for security, such as the 3-stage QKD protocol; the 3-stage protocol can tolerate multiple photons in each burst without leakage of information. This paper compares and contrasts the 3-stage QKD protocol and its efficiency in different network topologies and conditions. Further, we establish a mathematical relationship between achievable key rates for increasing transmission distances in various topologies. Our results provide insight to a network engineer in designing QKD networks of the future.

Keywords: Quantum networks, quantum key distribution, multi-photon transmissions, 3-stage protocol, network topologies

1 Introduction

Quantum information theory has been of great interest to researchers in the last few decades, enabling numerous new computing, networking, and sensing applications [1–3]. Under certain hardware assumptions, Quantum networks promise to provide a more secure means of communication [4] compared to classical networks alone. Quantum key distribution, despite some of its limitations [5], is a cornerstone for building the future quantum internet. In doing so, the ideas from quantum mechanics play an integral part in designing "low-noise electromagnetic networks" [6]. In the current era, various research projects are focused on building near-ideal quantum hardware, establishing end-to-end network security through quantum key distribution (QKD), and managing several possible eavesdropping attacks [6–8]. Experiments conducted through established QKD networks such as the DARPA network, several networks in Europe [9] and Tokyo [10] show the practicality of quantum network research in the last decades. In a more recent work, an entire inter-European private quantum network was set up with two sender and two receiver nodes during the 2021 G20 Summit held in Trieste [11]. Between 2003 and 2016, the Chinese Academy of Sciences (CAS) developed and launched a satellite and ground-based quantum key distribution network. The experiment involved the use of a low-earth-orbit satellite equipped with a decoy-state QKD transmitter and distributed encryption keys securely over a distance of 7600 km [12] including a video conferencing session. With the rapid development of quantum computing technologies, quantum cryptography will ensure large-scale secure connections over quantum networks [8, 13].

QKD is governed by the overall laws of quantum physics, which makes it “future proof”, i.e., the eavesdropper has no way of keeping a log of this transmission, unlike the classical transmission [14–18]. Because of this, QKD will likely be an integral part of future communication techniques, which will include a combination of *quantum-resistant classical algorithms* (also called post-quantum cryptography) and *quantum cryptography* (mostly QKD) solutions [19] enabling future secure networks for smart grids, financial institutions, and defense agencies. However, there are several practical challenges associated with creating larger quantum networks. These challenges are both theoretical and physical in nature, such as the possibility of protections against photon number splitting attacks (PNS) for single-photon transmissions, inconsistencies in the behavior of underlying hardware [20, 21], and practical security issues arising from the existing “loopholes” related to the Bell inequality tests [22]. Apart from the possibility of attacks, the currently existing techniques are facing a lot of practical engineering challenges in building optical switches, trusted nodes, etc. The presence of optical switches reduces the transmission distance over the optical fiber [23]. Losing a trusted node, i.e., it being compromised, can lead to the network being prone to even more attacks, thus making the entire network vulnerable.

One of the significant hurdles in the adoption of quantum key distribution protocols is the low key rate and the requirement of single photon emitters and detectors for ideal security characteristics. While several schemes have been proposed to make quantum key distribution techniques robust to multi-photon bursts [24], these still assume that the multi-photon bursts are few in number and are discarded in the end. The security is still reliant on single photons. In other words, these schemes cannot be securely integrated with existing classical networks that use tens of thousands of photons per bit of transmission. One possible solution is the use of a new generation of multi-photon quantum key distribution techniques that do not rely on single photons for security and can tolerate high photon burst rates, such as the 3-stage QKD protocol [25]. However, later, it was proved that the three-stage protocol could be used for quantum secure direct communication [26]. Investigation into this 3-stage QKD protocol is the central theme of this work.

This paper looks at three different QKD protocols, i.e., the Decoy-state, the 3-stage, and the E91 protocols. Our study describes the efficiencies of the above protocols on different topologies such as direct, line, grid, ring, and torus topology. We vary network parameters such as entanglement swapping success probability, decoherence probability, and signal attenuation during transmission. We move on to analyze in detail the performance of E91 and the 3-stage protocol on the torus topology. To establish the significance of the multi-photon bursts in current practical scenarios, we analyze multi-photon bursts up to a burst size of a million qubits. This analysis led to defining a mathematical relationship between the size of the multi-photon burst used and the maximum distance of stable transmission between Alice and Bob.

This paper is laid out as follows - section 2 explores the theoretical aspects of the QKD protocols that are relevant for multi-photon transmissions study conducted in this paper such as 3-stage protocol proposed by Kak [25, 27], and E91 protocol, which is entanglement based protocol and use of quantum repeaters, which are of essential importance and are being heavily researched by scientists [28–32]. In section 3, we explore various topologies of interest and briefly describe the different topological quantum networks associated with our study. In section 4, we go over the modifications made to the network simulator presented in [33] and some of the simulation parameters relevant to our analysis. In section 5, we present the results and analysis of our study for the 3-stage protocol and E91 protocol to establish a relationship between the size of the multi-photon burst and the distance of stable transmission. Furthermore, we also study the performance of several protocols for a torus topology. Section 6 concludes the paper and proposes some future directions for research.

2 QKD Protocols

QKD protocols can be classified based on the detection techniques used to retrieve the key information encoded in the photons being used. Discrete-Variable (DV) protocols use the polarization (or phase) of weak coherent pulses to encode the information, which simulates a true single-photon state [19]. Protocols such as Decoy-state and BB84 use the single photon-encoding scheme where the information is encoded in the polarization of the photon being used, i.e., these are prime examples of DV protocols. Another category of protocols is called Continuous-Variable QKD, a technique where photon-counters are replaced with general p-i-n photo-diodes, which are known to be faster [34]. The detection techniques used in the above are based on *"homodyne detection"*. Figure 1 represents a general setup of the quantum cryptography model, which consists of two channels - a quantum channel for emitting and receiving the qubits and a classical channel for authenticating the encryption-decryption, depicting the sender (Alice), the receiver (Bob), and the possible-attacker (Eve). Eve, in QKD protocols, is assumed to be an active attacker.

2.1 The Decoy State Protocol

The Decoy-state protocol counteracts PNS attacks that can compromise BB84 security [17] by sending out random decoy photon bursts. Eve, the attacker, has no idea which of these transmitted states are real and which are decoys. Thus, Alice and Bob use statistical analysis to establish if an attacker is present. In reality, decoy state protocols are implemented using weak coherent pulses with varying probabilities of transmitting

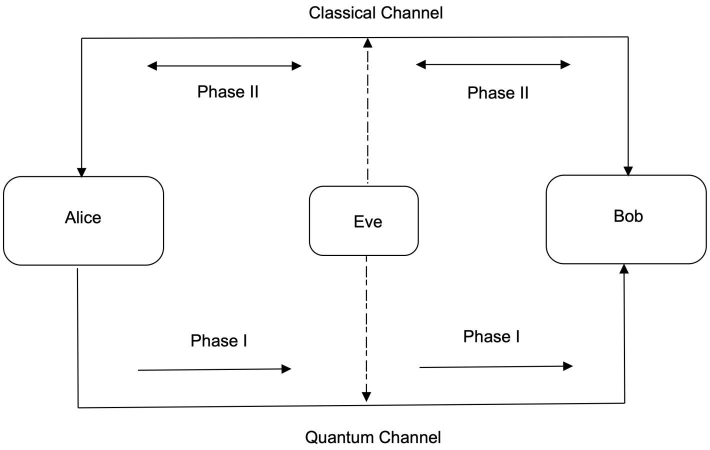


Fig. 1: Quantum Communication Representation Model [35]

.

distinct amounts of photons. In our work and for comparison, the Weak+Vacuum Decoy-state procedure, as described in [36, 37], is simulated. The signal, weak decoy, and vacuum decoy states are all used in the Weak+Vacuum Decoy-state. The weak decoy state has a probability N_ν with the intensity of photon per burst being ν, where $\mu > \nu$ (see below). The vacuum decoy state has a probability N_0 with the intensity of photon per burst being zero, i.e., it allows the parties to detect any possible background noise [38]. The protocol follows the steps of the $BB84$ protocol, which is as follows:

1. Alice generates a random string sequence, y, and encodes each of them using one of the two non-orthogonal bases X or Z.
2. Alice transmits each of the bits from the sequence y using a weak-laser of intensity μ, ν, or zero with photon probabilities as N_μ, N_ν, and N_0 respectively.
3. Depending upon the number of photons that Bob receives, he performs one of the following,
   - If Bob receives zero photons, he records an empty measurement.
   - If Bob receives one photon, he records the measurement in one of the basis from $\{X, Z\}$.
   - If Bob receives more than one photon, he randomly records one of the measurements obtained from all of the received photons.

Once Alice has transmitted all the bits from the generated sequence, y, both Alice and Bob share their basis choices and respective intensities of detection over an authenticated classical channel. Based on this shared information, relevant estimations for the detection can be made, and thus, an attacker's presence can be identified. The following are the parameters used for simulation based on [38].

- The burst intensities for the real-state and weak decoy-state are $\mu = 0.5$ and $\nu = 0.152$, respectively.

- The probabilities of real, weak-decoy, and vacuum-decoy states are $N_\mu = 0.635$, $N_\nu = 0.203$, and $N_0 = 0.162$ respectively.
- The multi-photon burst has probability of 0.038, single-photon burst has probability of 0.38, and no photon burst has probability of 0.57.
- Since the choice of measurement basis by Bob has a probability of 0.5 (either X or Z), Bob has a probability of adding a key of 0.5 in case of a successful photon transmission.

2.2 The Three-stage Multi-photon Protocol

One of the main protocols as a possible option for practical quantum networks is the three-stage multi-photon protocol. In this protocol, every qubit is encrypted using a private secret key similar to the classical *double-lock encryption* [33]. Alice starts by encoding her key/message using orthogonal states, for example $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ or may choose to simply send an arbitrary quantum state $|X\rangle$ (denoted X below for simplicity). Alice and Bob now choose secret unitary operations, U_A and U_B, which commute, i.e., $[U_A, U_B] = 0$. The following are the steps of the protocol,

1. Alice has a quantum state X she wants to transmit. She chooses a secret random transformation matrix U_A.
2. Alice applies U_A and transmits $U_A(X)$ to Bob.
3. Bob receives the transmission and applies his secret transformation, U_B, and sends $U_B(U_A(X))$ back to Alice.
4. Alice now applies $U_A^\dagger$ to Bob's transmission, i.e., $U_A^\dagger(U_B(U_A(X)))$. As we know $[U_A, U_B] = 0$, the transmission signal renders down to $U_B(X)$ as $U_A^\dagger U_A = 1$. Alice sends back this message to Bob.
5. Bob receives the transmission and applies the dagger operation for his transformation operation, i.e., $U_B^\dagger$. Thus, Bob recovers the original quantum state X.

In the above discussion, one of the unitary operations conducted can be the rotational operation, i.e.,

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \tag{1}$$

In eq 1, we can notice that the unitary operation fits our criteria, i.e., $[U_A, U_B] = 0$ and $R^\dagger(\theta) = R(\theta)$. The above protocol is vulnerable to a man-in-the-middle attack like any other key distribution technique and requires the use of authenticated quantum channels [33]. However, the protocol does not have any classical phase and is an all-quantum protocol.

2.3 The E91 Protocol

Similar to the BB84 and B92 protocols, the E91 protocol is also executed with the assumption of single-photon transmissions. However, unlike BB84 and B92 protocols, E91 is an entanglement-based protocol. In this protocol, each of the parties gets a qubit from an entangled pair. Both Alice and Bob perform measurements by utilizing one of the two orthogonal bases, i.e., $\{X, Z\}$ and the following steps,

1. Both Alice and Bob receive a qubit from entangled Bell pair $(|00\rangle \pm |11\rangle)/\sqrt{2}$.

2. Alice measures her qubit using one of the randomly chosen basis, and she records the measurement.
3. Bob also measures using one of the randomly chosen basis and records his measurement results.

The above steps are repeated for a larger number of entangled pairs. Alice and Bob share their measurement using the classical channel to authenticate the transmitted qubits. Measurement results are retained where the same basis was used by both Alice and Bob. To account for the possibility of an attacker, a fraction of the remaining qubits are openly compared and discarded. One thing to point out is that the E91 Protocol uses the Bell-Inequality test to determine the presence of an eavesdropper [39], and therefore, our discussion above is a simplified version of it. Once all of the above has been done, error correction and privacy amplification are performed.

2.4 Security of QKD Protocols

The main security concern with multi-photon transmissions is the PNS attack. We can define the probability of finding $n-$coherent photons as the Poisson distribution [40],

$$P(n,\mu) = \frac{\mu^n e^{-\mu}}{n!} \tag{2}$$

The zero, first, and second-order expansion for our photon distribution are,

$$P(0) \approx 1 - \mu + \frac{\mu^2}{2};\ P(1) \approx \mu - \mu^2;\ P(2) \approx \frac{\mu^2}{2} \tag{6}$$

Now, for a burst containing more than 1 photon, i.e., $n \geq 2$, we can write the Poisson distribution for photons as [40],

$$P(n \geq 2) \approx \frac{\mu}{2} + \frac{\mu^2}{4} \tag{7}$$

2.4.1 Eavesdropping Strategies

Reference [40] discusses several possible scenarios of attacks by Eve while going undetected.

- The first strategy is where Eve intercepts and analyses all of the photons transmitted by Alice. Eve then transmits the measurement results to a source close to Bob, which only transmits certain plausible states to Bob (maintaining the photon statistics to avoid suspicion). The maximum ratio between mutual information between Eve and Alice and QBER was found to be 6.83 [40]. Furthermore, if *infinitesimal splitting* was considered, the mutual information of Alice and Eve was shown to be ideally equal to 1, i.e., “full information” is known to Eve [40].
- The second strategy used by Eve can be described as using a beamsplitter, i.e., instead of taking out one of the photons in a 2 photon burst, Eve can take a fraction λ out of each pulse using a beamsplitter and replacing the photon-line with a line having lower loss. Doing this, the mutual information between Alice

and Eve can be written as [40],

$$I(A,E) = \frac{\mu}{2}(2\lambda(1-\lambda))\frac{1}{2}, \tag{8}$$

where $\mu/2$ is $P(2)$ as described earlier in eq 3. In this approach, we see that the maximum $I(A,E) = \mu/8$ when $\lambda = 1/2$, which corresponds to a gain of 3 dB [40].

2.5 Eavesdropping and Stable Transmission Distance

The key rate and the distance over which these key rates are stable are highly correlated to the presence of an eavesdropper in the system. The efficiency of the key distribution is highly dependent on the Quantum Bit Error Rate (QBER) and the mutual information between Alice and Eve, $I(A,E)$. With today's equipment, the major problem is the higher detector noise, which leads to high QBER at large distances; thus, the maximum distance of stable transmission drastically decreases [40].

3 Topologies

One important aspect of developing efficient quantum networks is the efficiency of transmissions in different network topologies. Apart from studying some of the basic topologies, such as *line*, *star*, *ring*, and *grid*, we designed a *toroidal topology* (Torus) for our network simulator.

Table 1: Comparison of Different Topologies

Topology	Advantages	Disadvantages
Line	Offers one path between Alice and Bob, i.e., minimum control-layered overhead	• Impractical over long ranges. • Not reliable.
Gird	• Provides multiple path between Alice and Bob. • Nodes are geographically isolated.	Maximum control-layer overhead needed.
Ring	Provides two paths between Alice and Bob with lesser control-layer overhead.	Less reliable than grid topology.
Star	Allows several user nodes at once.	Reduces overall performances and increased risk.
Torus	Higher connectivity due to multiple available paths, and comparatively easier expansion without much reconstruction	Higher initial and overall maintenance due to complex structure architecture.

3.1 The Direct Topolgy

A direct topology can be considered as the most simple case of creating a network, i.e., consisting of a connection between Alice and Bob. Since it is a direct connection between the two users and the key rates are noted to have an exponentially inverse co-relation with the distance, this particular topology is rendered impractical over large distances. However, for simulation purposes, this simple topology offers a chance to evaluate the efficiency of each of the QKD protocols without having us to worry about other parameters, such as network connection optimizations. Thus, the direct topology serves as the basis for the creation and understanding of other following bigger and more complex topologies.

3.2 The Line Topology

The line topology is an extension, more practical, representation of direct topology in which we add a third node between Alice and Bob. All of the transmissions are directed through the middle node to Bob. This middle node is either a trusted node or a quantum repeater. This is beneficial as this decreases the exponential loss of qubits by decreasing the successive lengths of fiber optics from one node to another.

3.3 The Grid Topology

The grid is an extension of collections of nodes with intermediate quantum repeaters. This consists of Alice and Bob and a series of intermediate trusted nodes or quantum repeaters on a rectangular grid. This allows the senders to transmit more than one qubit for each simulation round, due to the presence of different paths [33]. Due to the presence of multiple accessible paths, this topology accounts for more secure connections for a practical Eve, who now needs to account for various geographically separated devices to get the transmission information. Even if a grid topology provides for a more secure connection, we would require ideal routers and a much more financially heavy structure.

3.4 The Torus Topology

A Torus is a 3-dimensional wrapped structure where the endpoints of the grid topology are connected in both horizontal and vertical fashion. Figure 2 defines the 2-dimensional representation of the Torus created in our network simulator.

Figure 2 represents the horizontal and vertical wrapping of nodes of a simple 2-dimensional grid structure to create a 3-dimensional torus structure. In our simulations, we perform and present the results of the 3-stage protocol operated on a torus topology.

3.5 The Ring Topology

The ring topology, similar to the grid topology, offers multiple paths of key transmission, and it consists of combinations of several trusted nodes or quantum repeaters.

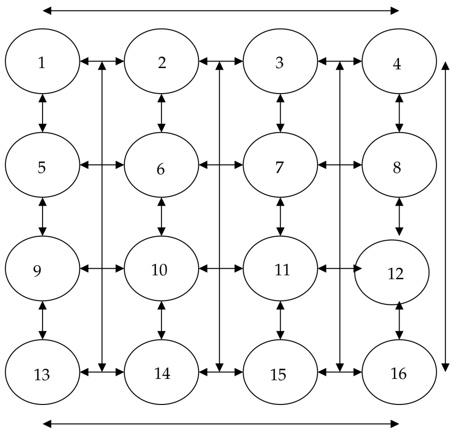


Fig. 2: Representation of the node connections to form a torus consisting of 4 × 4 nodes. For our simulation, we are using a basic 3×3 torus topology, and the arrowhead represents the connections between two given nodes.

This consists of two paths between Alice and Bob with 4 hops. However, this topology takes a toll on the overall reliability of the network due to the simplification of the coordination of various network resources [33].

3.6 The Star Topology

The star topology is one of the most popular and reliable topologies when talking about designing any network. In this case, a star topology accounts for several user nodes (apart from Alice and Bob), which is achieved using an optical switch or a quantum repeater. However, the star topology is not very efficient for direct quantum communication as it requires a *point-to-point* connection due to the limitation of the no-cloning principle. Due to multiple users connected to the same transmitter, the risk of sensitive information being released also increases. A star topology can be implemented using optical switches.

4 The Network Simulator

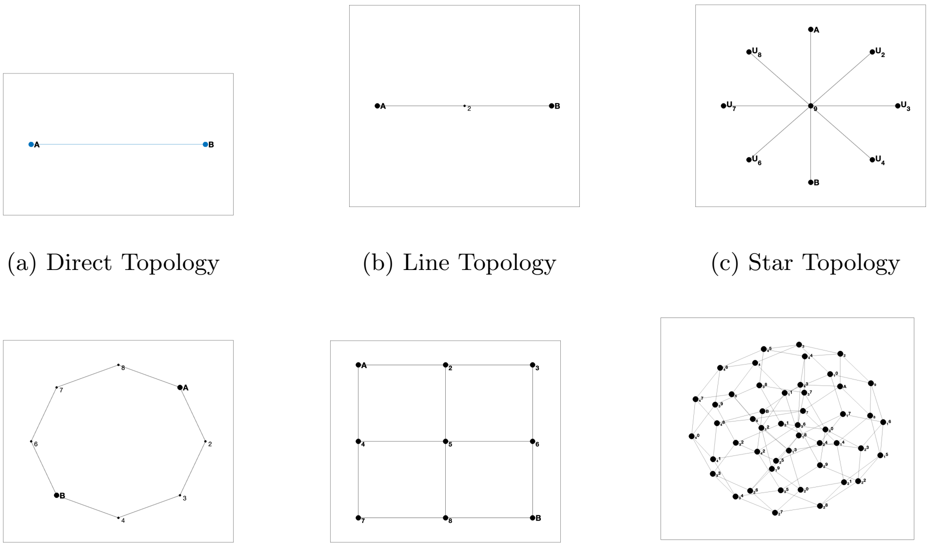
The Network Simulator developed for this study was written in Matlab. The network simulator was enhanced using the simulator presented in [41].

4.1 Network Communication

The connections between each of the involved nodes are achieved by simulating fiber-optic cables with transmission probability as given in eq 9.

$$P(L) = 10^{-\alpha L/10}, \tag{9}$$

where L is the fiber length in kilometers, and α is the attenuation coefficient of the fiber-optic cable used. It's evident from eq 9 that as we increase the distance between



(a) Direct Topology (b) Line Topology (c) Star Topology

(d) Ring Topology (e) Grid Topology (f) 7×7 Torus Topology

Fig. 3: Different topologies used in our QKD simulations (all of the topology profiles are generated through our simulations directly).

the nodes or the length of fiber required, the success of transmission would drastically decrease. For the purpose of our simulation, we keep the value of $\alpha = 0.15\ km^{-1}$ unless otherwise specified.

Any network consists of different types of nodes. For our simulation, we also have a couple of different kinds of nodes. Trusted nodes (including Alice and Bob) are the important bits of the network, and these try to establish connections to each of the other trusted nodes through an accessible path. Each of the successfully transmitted qubits is stored in the form of a raw key pool, $(RK)_{i,j}$ where i, j defines the i^{th} and j^{th} trusted node pair. Optical Switches were also simulated for the link neighboring nodes along a peer-to-peer path. Even though switches are good for creating dynamic connections between given nodes, we see that there's a performance deterioration. By using the E91 Protocol, we also aimed to simulate quantum repeaters. Similar to classical repeaters, quantum repeaters increase the effective range of communications as these serve as intermediate points of transmission, and thus, the relative length between each successive node of transmission is decreased. Unlike classical repeaters, quantum repeaters cannot clone the data and then transmit it to the next node, as it will violate the no-cloning principle of quantum mechanics. This is achieved by using the principle of quantum entanglement and by performing entanglement swapping between the successive nodes. Referring to eq 9, we can note that the probability of successful transmission between each of these repeater nodes is higher as the effective distance between two successive transmissions is reduced. However, the overall probability of successful transmission, i.e., from Alice to Bob, is the same as the probability of successful transmission between each of these repeater nodes is considered as independent event, i.e., $p(n) = p(1) \times p(2) \times p(3) \times ...p(n+1)$. To overcome this mathematical difficulty, we simulate redundancy by attempting five Bell state transmissions at once, which facilitates the previously described entanglement swapping [42]. Figure 4 represents how a quantum repeater uses two entangled Bell pairs to create and perform entanglement swapping between the initial and final trusted node by using an external Bell pair through the intermediate quantum repeater.

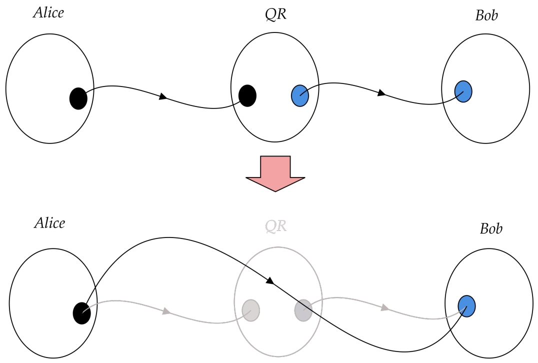


Fig. 4: Working of the quantum repeater: Starts with two sets of entangled bell-pair between Alice-QR and QR-Bob. Then, we perform an entanglement swap between the nodes to create a final entangled Bell state pair between Alice and Bob. The curly line represents an entangled pair.

In our simulator, entanglement swapping has been performed using the following steps,

1. Every quantum repeater tries to share 5 Bell pairs with neighboring devices, and this is deemed successful if one of the Bell pairs is successfully transmitted, each having a probability of transmission given by eq 9. Here, L is the distance between the quantum repeater and the node it's trying to share the Bell pair with.
2. For those repeaters which successfully shared Bell states (as described in [41]), they now try to link to the nearest trusted nodes using entanglement swapping by performing Bell state measurements. We set the success probability of a Bell state measurement to $B = 0.85$. Every measurement must be successful in establishing a final entangled pair, i.e., if there are n repeaters present between two nodes, the probability of success is given by B^n.

Once entanglement swapping is performed and the trusted nodes are connected, they proceed with the QKD protocol as if the qubits have been successfully transmitted.

4.2 QKD Protocol Simulation

Once a transmission is simulated (either through the quantum repeater chain or direct fiber-optic cables), we move on with the simulation specific to particular QKD Protocols as described in section 2. After a given set of QKD rounds (on the order of $10^5 - 10^6$) are completed, error correction is simulated before deriving the final key between Alice and Bob. We have used the decoherence value of $D = 0.02$ to account for quantum-state decoherence that happens due to environmental noise. All of the qubits in transmissions are effected by this decoherence noise of the cables. Any decohered are noted down as *erreneous*, and we calculate the error rate Q for each of the given key pools. Performing the error correction, we derive the final key pool, $K_{i,j}$ between the i^{th} and j^{th} trusted node pair using eq 10.

$$K_{i,j} = R(1 - 2h(Q_{i,j})), \tag{10}$$

where $h(Q)$ is the binary entropy function. Every pair of trusted nodes initially shares a key pool. They then use XOR operations to send key material to Alice and Bob securely. Alice and Bob also utilize the key material they directly share. Consider a network with three nodes: Alice, T_2, and Bob. Alice and Bob have their own key material in the final key pool $K_{A,B}$, while T_2 holds the key pools $K_{A,2}$ and $K_{2,B}$ for Alice and Bob, respectively. T_2 sends the result of $K_{A,2} \oplus K_{2,B}$ to Bob, who can retrieve $K_{A,2}$ by applying XOR with $K_{2,B}$ as described in eq 11. It's important to note that the amount of key material transmitted depends on the smaller of the two key pools. The total key material Alice and Bob receive from all trusted nodes is estimated using a max-flow algorithm.

$$K_{A,2} = (K_{A,2} \oplus K_{2,B}) \oplus K_{2,B} \tag{11}$$

Finally, we calculate the overall key rate, which is basically the size of the final key pool divided by the total number of QKD rounds performed. This represents the maximum theoretical efficiency of the QKD protocol.

5 Results

In this section, we'll go over the results obtained through our simulations for different QKD Protocols as mentioned in section 2 and over different Topologies mentioned in section 3.

5.1 Performance over Direct Topology

We first looked at the performance of different QKD Protocols over direct topology as it serves as the most basic case of topology without any complexities. Thus, it serves as a good baseline for our further analysis. Fig 5 shows the performance of different QKDs as obtained. In this case, we simulated E91 in two cases, i.e., with and without using quantum repeaters. From fig 5, we can clearly see that using quantum repeaters increased the distance of stable key rates significantly to the case without any quantum repeaters.

As discussed in section 2.1, and as shown from figure 5, Decoy state protocol offers the lowest key rates as there are multiple QKD Rounds conducted, which does not

Table 2: Summary of quantum communication protocol simulation parameters.

Parameter	**Description**
α	Fiber attenuation coefficient. $\alpha = 0.15$. $\alpha = 0.4$ for optical switches.
L	Length of fiber segments in kilometers.
Burst Size	Frequency of photons in one burst. The default values are as follows, • Decoy State: A probability distribution between 0 and 2. • Three-Stage: 10 photons sent in the first burst, then subsequent numbers. • E91: 5 parallel Bell-state attempting between each quantum repeater.
B	Probability of successful Bell state measurements for each of the quantum repeaters in between Alice and Bob. $B = 0.85$.
D	Probability of quantum state decoherence due to channel noise. $D = 0.02$.

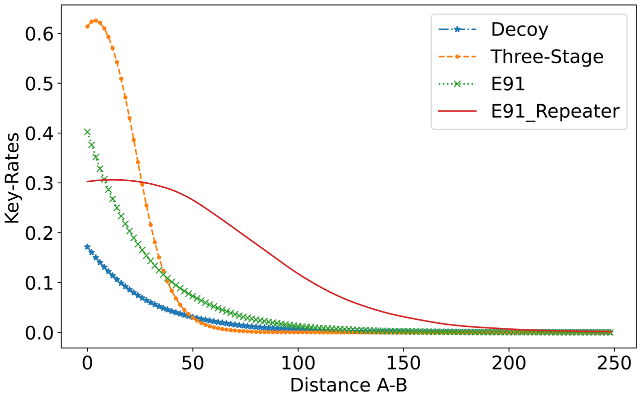


Fig. 5: Comparison of Performance of different QKD Protocols over Direct Topology.

contribute towards the final key-pool. Decoy-state only demonstrates higher key rates compared to 3-stage after around the distance of $L = 50$ km, as it does not require three consecutive transmissions. The 3-stage protocol provides the highest key rates unless we separate Alice and Bob by over 40 km. As it requires three consecutive transmissions, increasing this distance directly correlates to much more significant fiber loss than any other protocol. For the E91 protocol, we require only one successful key-bit transfer per transmission; thus, it seems to show a lower decline than the 3-stage protocol after around 50 km. When we include quantum repeaters in the E91 setup, we notice that while the key rates are stable for a longer distance, it's much lesser than

E91 without any repeaters at smaller distances, contributing to the fact that quantum repeaters also introduce another scope of failure, i.e., entanglement swapping failure.

5.2 Performance of QKD Protocols over Different Topologies

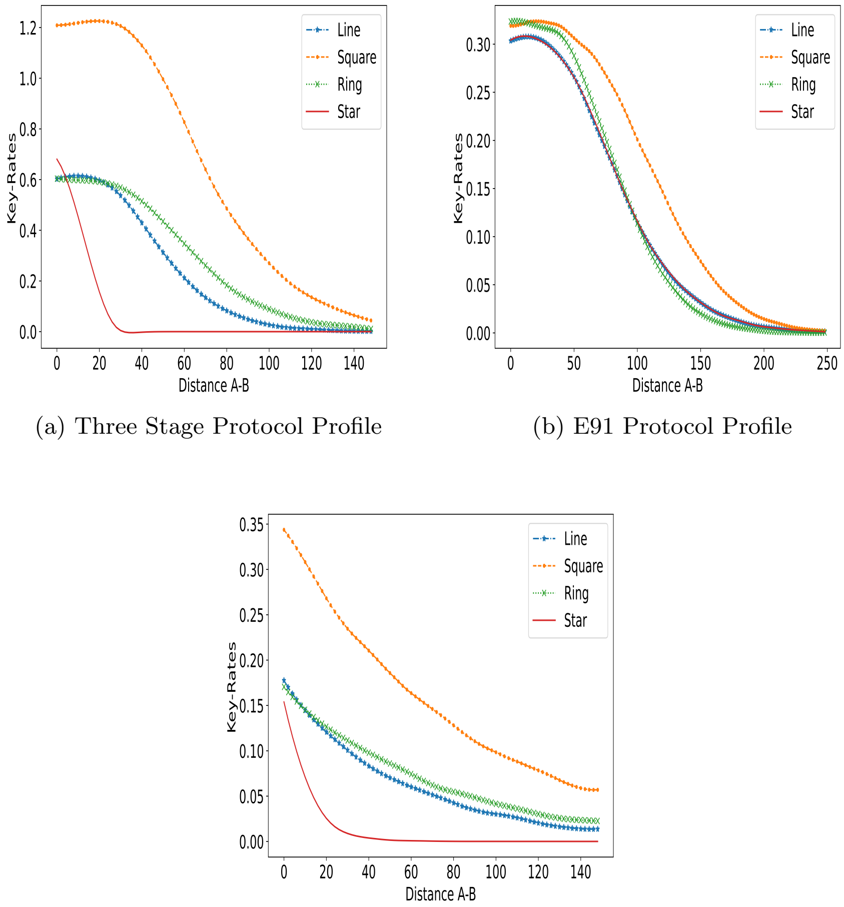
This section explores the performance of different QKD protocols on different Topologies described in section 3. We compare the changing key rates over various distances between Alice and Bob for the 3-stage protocol (section 2.2), the E91 protocol (section 2.3), and decoy-state protocol(section 2.1). As seen in fig 6, Decoy-State does not offer very stable transmission distances, and the decay is more rapid than the other two protocols. One other interesting thing to note is that the grid topology (3.3) offers significantly higher key rates for 3-stage protocol due to the availability of multiple paths for key distribution, i.e., the possibility of more than one key being distributed each round as described in section 4, because of the presence of multiple trusted nodes.

5.3 Performance of the Decoy-State Protocol

From figure 6c, we can see that the grid topology offers the highest key rates than the rest of the topologies due to the presence of multiple paths and multiple trusted nodes contributing to more than a single key per simulation round. The grid topology also seems to be more durable over time due to the fact that the fiber segments between trusted nodes are shorter compared to other topologies used. Ring topology also offers multiple paths, but it seems to be just slightly better than line topology. However, over time, ring topology seems to show a better key rate with a lower decline rate than the line topology. For star topology, the higher attenuation coefficient ($\alpha = 0.4$ because of optical switches) results in significantly more fiber loss than any other topologies as described by eq (9).

5.3.1 Performance of the Three-Stage Protocol

From figure 6a, we can notice that the grid topology, yet again, offers higher key rates than the rest of the topologies and is overall more robust than the rest of the topologies over time due to the presence of multiple paths having multiple trusted nodes contributing to a higher final key pool. Comparing the performance of 3-stage protocol over direct topology and line topology, figures 5 and 6a point to the fact that the presence of the intermediate trusted node in line topology offers for a lower decline in key-rates than direct topology over longer range, as the fiber segments between Alice and Bob are relatively shorter thus probability of successful transmission increases according to eq 9. At shorter distances, both line and ring topologies show similar key rates. However, for longer ranges, we can see that Ring topology seems to be more robust by offering lesser key-rate decay than line topology. For star topology, we can see that even though it starts with a higher key-rate value than both line and ring topology, it decays much faster due to the higher value of the attenuation coefficient (α) as it's simulating an optical switch.



(a) Three Stage Protocol Profile

(b) E91 Protocol Profile

(c) Decoy-State Protocol Profile

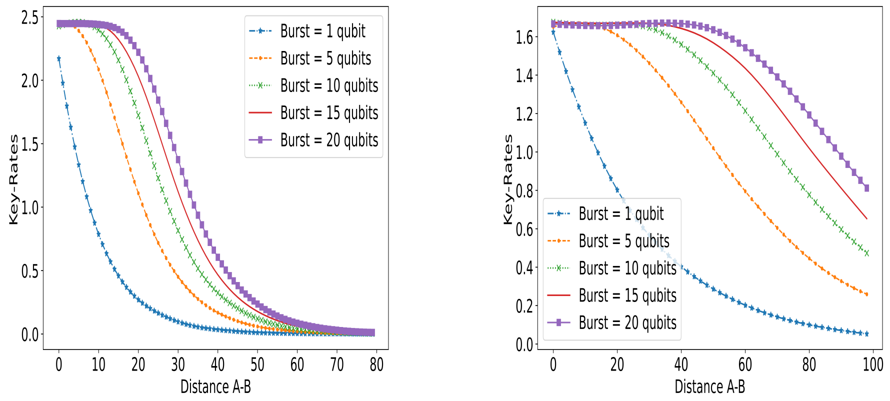
Fig. 6: Performance of different QKD Protocols over Different Topologies

5.3.2 Performance of E91 Protocol

From figure 6b, we can see that almost all of the topologies have similar performances for E91. However, we can see that the grid (defined as "square") is more robust, and the decay is slower than all of the other topologies due to the presence of multiple paths and a series of multiple repeaters (3 in the shortest path). However, we can also note that ring topology offers higher key rates at very small distances due to fewer repeaters in the path than the grid topology, thus having lesser chances of failed entanglement swapping. As we can see, the benefits of having multiple paths are overturned by the errors associated with failing quantum repeaters. In the star network topology, the central quantum repeater can set up pathways between any two user nodes. It does this by selectively creating Bell states with chosen nodes, eliminating the need for an optical switch. This method enables the star network to achieve efficiency comparable to a direct line topology, as both rely on a single quantum repeater to bridge the distance between two points, such as Alice and Bob.

5.3.3 QKD Protocol Performance over Torus Topology

We have presented results for the performance of different QKD Protocols over different topologies. We now explore the extension of the grid topology with a three-dimensional wrapping, i.e., torus topology. In this section, we explore the performance of the 3-stage protocol and E91 protocol over our torus topology.



(a) 3- Stage QKD Protocol Performance over a 3 × 3 Torus Topology.

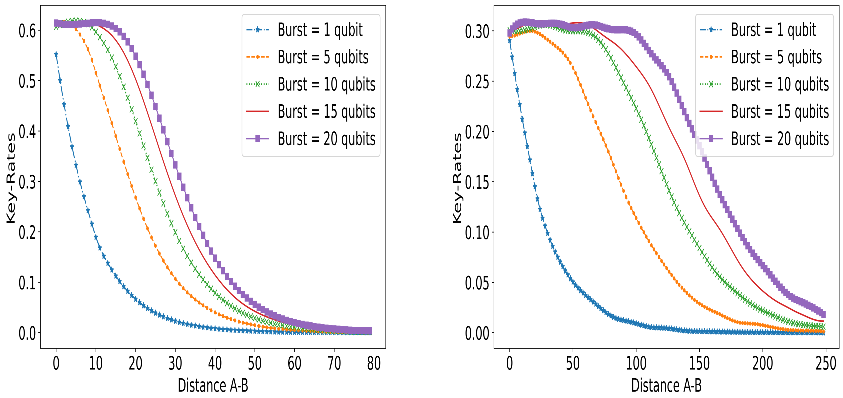
(b) E91 QKD Protocol Performance over a 3 × 3 Torus Topology.

Fig. 7: 3-Stage and E91 Protocol Performance over Torus Topology.

As we can see from figure 3f, there are multiple paths between Alice and Bob, and unlike grid topology (figure 3e), the shortest path between Alice and Bob is L itself. This increases the probability of successful transmission between Alice and Bob, and thus, we can expect a higher key rate than that of the grid topology. As shown earlier in figure 5 the key rates were observed to be higher for the 3-stage Protocol than the E91 Protocol. We see similar behavior from figure 10 that the 3-stage Protocol beats the E91 Protocol almost by 1.5 times. We also see that the stable distance for E91 is observed to be higher, as seen in the previous cases as well.

5.4 Analysing Higher Order Multi-Photon Bursts

In this section, we will analyze the higher-order multi-photon bursts and the key rates associated with them. We do not discuss the decoy-state protocol from this scenario as it requires low probabilities of multi-photon bursts. In the 3-stage protocol, we had a default burst size of 10 qubits before. As we increase the size of the multi-photon burst, we can increase the performance, but the risk of a PNS attack increases as well. Therefore, it's important to realize that higher performance comes at a cost of increased security risk. The E91 protocol does not inherently support multi-photon bursts. However, in the case of E91, we adjust the number of number of simultaneous Bell pairs shared between the quantum repeaters.



(a) Multi-Photon Burst Profile for Three-Stage Protocol over Line Topology.

(b) Multi-Photon Burst Profile for E91 over Line Topology.

Fig. 8: Comparison of Multi-Photon Burst Size Profiles for Three-stage and E91 Protocol

From figure 8a, we notice that for all of the burst sizes (except for 1-qubit), we find the key rate to be almost constant at a smaller distance. This can be associated with the fact that higher order burst size allows for a higher chance of successful transmission. We also see that the distance to which these transmissions stay constant is also associated with the above-described fact. From figure 8b, we can notice that E91 offers a larger range of stable transmission than 3-stage transmission, also seen in figures 6b and 5. We can see that for larger distances, the key rates seem to be converging to zero for both the 3-stage and E91. However, the distance at which these converge to zero varies for both the protocols and the size of the multi-photon burst used. It's evident that even if multi-photon bursts increase the range of these stable transmissions for both of these protocols, we need to explore different topologies and have multiple trusted nodes in our systems for these protocols to work efficiently.

5.5 Multi-Photon Burst and Distance Relation

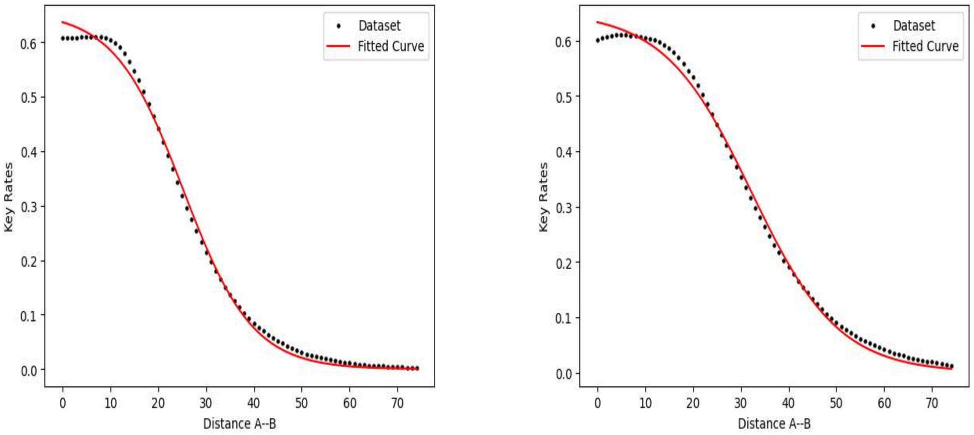
Now that we have analyzed and noticed certain trends for the curves obtained for multi-photon bursts for the 3-stage protocol, this section delves into finding a mathematical relation governing these curves with hopes of providing a predictive model for the simulations. We notice a few features from the curves,

- A stable flat-curve for smaller distances between Alice and Bob.
- A decaying curve, sort of linear, in the middle section.
- The curve converging to zero at larger distances.

Based on the above facts, we define an exponentially decaying function of the sigmoid nature as described in eq 12,

$$y = \frac{R}{(1 + e^{k(x-x_0)})}, \tag{12}$$

where, R, k, x_0 are the fitted parameters. R defines the initial constant value of key-rate, k defines the decaying rate of the curve, and x_0 is the point of the curve where key-rate $= R/2$. To test our equation of the best fit (i.e., eq 12), we do curve fitting for the line and ring topologies and present the results below in figure 9.



(a) Characteristic curve obtained for QKD Performance over a Line-topology.

(b) Characteristic curve obtained for QKD Performance over a Ring-Topology.

Fig. 9: Fitting the curve from eq 12 for Line and Ring topology for a multi-photon burst size of 10 qubits for 3-stage QKD Protocol.

Based on the values of various fitted parameters from eq 12, the following were the equations of the curves found for the above are,

$$y_{\text{line}} = \frac{0.655}{(1 + e^{0.139(x-25.303)})} \quad \text{and} \quad y_{\text{ring}} = \frac{0.652}{(1 + e^{0.109(x-32.257)})} \tag{15}$$

Right side of eq 13 describes the characteristic equation obtained for the line topology, and the left side of eq 13 describes the characteristic equation for ring topology for the 3-stage protocol. Based on our observations, we can see that the modified sigmoid function serves as a good curve fit for the equations describing the key rates changing as a function of distance between Alice and Bob. We also try to find the characteristic curves for higher-order multi-photon bursts for line topology and conduct the same analysis.

5.5.1 Multi-Photon Burst Profiles

This section explores the multi-photon burst relations for higher order bursts over line topology for the 3-stage protocol. We explore the key rates and distance relation for the following burst sizes, $b = [50, 100, 150, 1200]$. We first make the curve smooth by eliminating the polynomial noise using the SavGol filter. We then fit the curves using eq 12 and present the characteristic curves for each of them in figure 10.

One interesting observation is that for lower order burst size, we see the curve showing a better fit as they approach zero (for figure 10a), and for higher order curves (such as figure 10d) we can clearly see that the curve fit becomes better for the initial region as well. One important thing to note is that we can see the constant part of the curve increases with the increasing multi-photon burst size; therefore, we need to establish a relationship between the two quantities as well. This will be done in the next section.

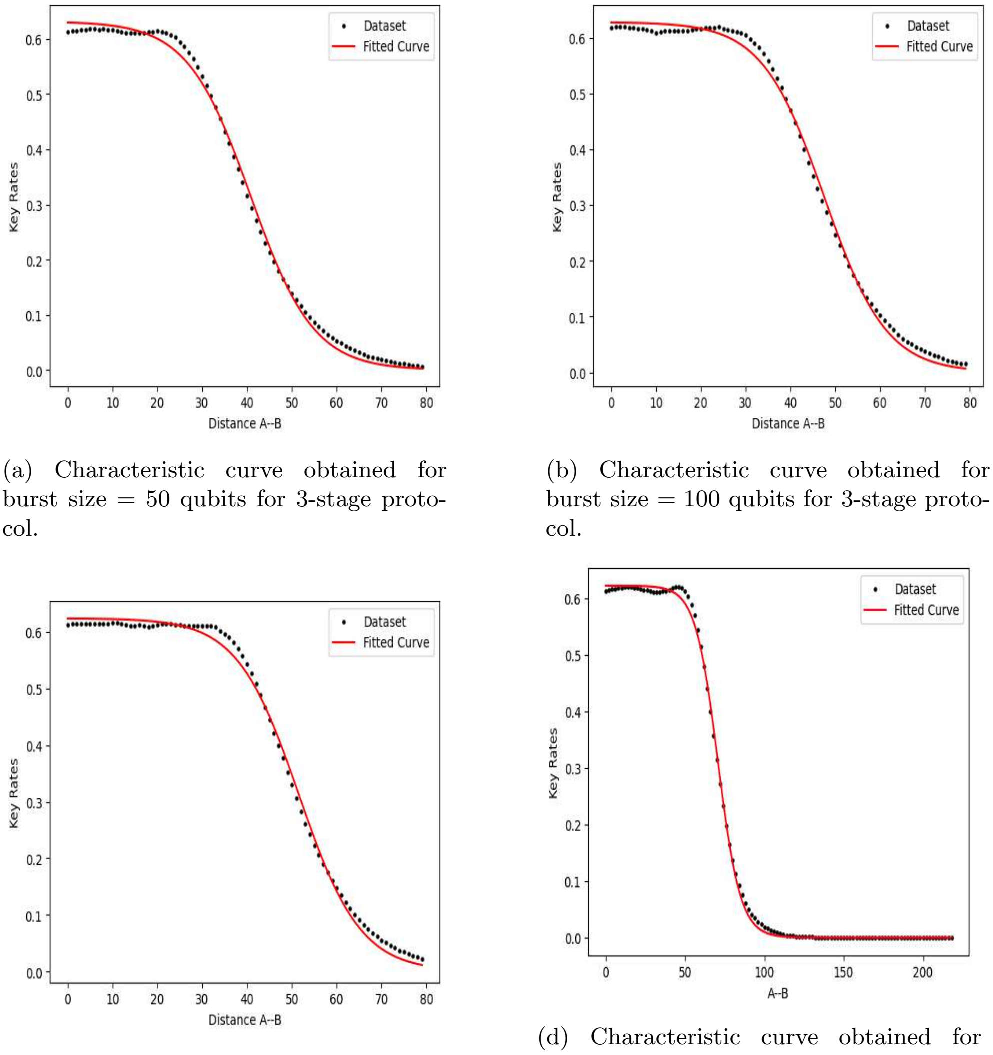
5.6 Distance of Stable Transmission and Multi-Photon Burst Size

It is evident that the multi-photon burst increases the distance of stable transmission (i.e., the distance over which key rates seem to be constant) for all of the curves that we found. To find this relation, we have to first find the “turning” point, i.e., the point where the derivative of the curve becomes negative. We do this for all of the curves obtained for burst sizes, $b = [1, 50, 100, 150, 200]$ and find the turning points for each of them. Figure 11 shows the nature of the curve obtained between the turning point and the multi-photon burst sizes associated with the simulation run.

From figure 11, we can see that a 3$^{\text{rd}}$ order polynomial fit describes the relationship very well. Therefore, we fit a third-order polynomial to the data points and find the characteristic equation for the curve. The equation of the third-order polynomial curve was found as shown in eq 16.

$$y = 0.000008x^3 - 0.003388x^2 + 0.538443x + 1.693613 \tag{16}$$

From eq 16, we can see that multi-photon burst size follows a polynomial relationship with the distance of stable transmissions. However, the burst sizes used in this calculation are of very small order. To get a general picture and a more practical burst-size relation, we increase the burst size up to a million qubits at once and try to define a more generalized relationship. Figure 12 shows the curve with distance of stable transmission and multi-photon burst size for bursts up to one million qubits at once.



(a) Characteristic curve obtained for burst size = 50 qubits for 3-stage protocol.

(b) Characteristic curve obtained for burst size = 100 qubits for 3-stage protocol.

(c) Characteristic curve obtained for burst size = 150 qubits for 3-stage protocol.

(d) Characteristic curve obtained for burst size = 1200 qubits for 3-stage protocol.

Fig. 10: Fitting the curve defined in eq 12 for line topology having higher order multi-photon bursts used for 3-stage Protocol.

Figure 12 sets a stage for a more generic relationship between the higher-order bursts and the distance of stable transmission. However, figure 12 does not give a clear indication of the possible nature of the curve that exists between the two quantity of interest due to the wide range of burst values used. Therefore, we setup a curve between log(burst_values) and the distance of stable transmission. Figure 13 gives us

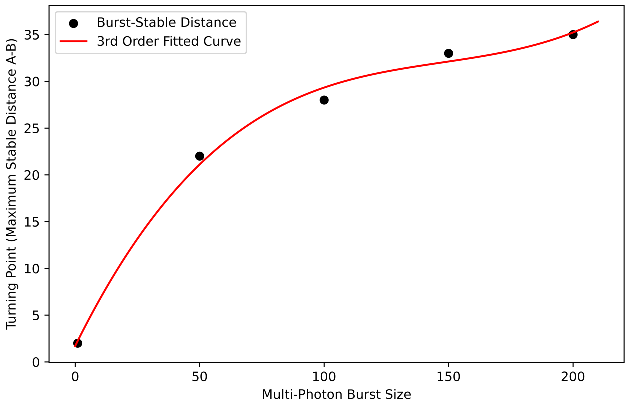


Fig. 11: Relationship between the Maximum Stable Distance (A-B) and the size of multi-photon burst used.

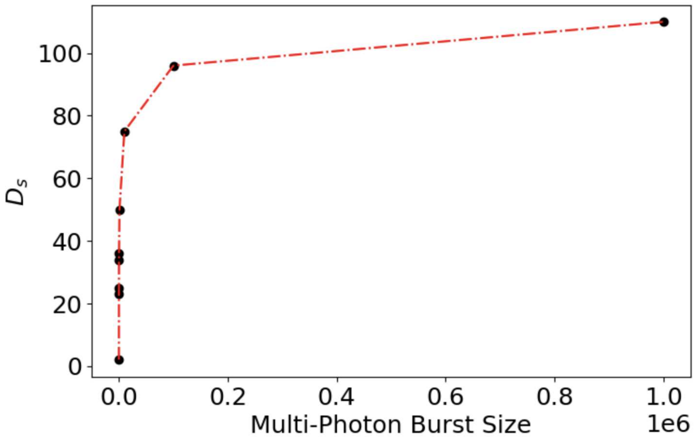


Fig. 12: Relationship between the maximum stable distance (between Alice and Bob) and the size of multi-photon burst used consisting of burst sizes up to 10^6 qubits.

a better picture for a possible relationship between the main two quantities of interest of this study, i.e., distance of stable transmission and size of multi-photon burst used.

From figure 13, we found out that the two quantities of interest share a logarithmic-3$^{\text{rd}}$ order polynomial relationship as described by eq 17.

$$D_s = -0.054x^3 + 1.228x^2 + 1.1878x + 2.0178, \tag{17}$$

where $x = \log(\text{burst\_size})$. Therefore, based on the above, we can define a generic relationship for a 3-stage protocol over a line topology between the distance of stable

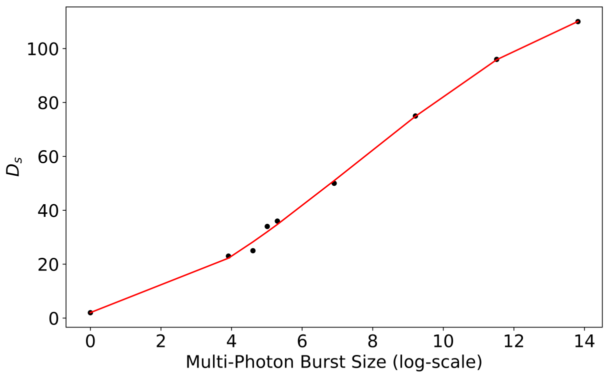


Fig. 13: Relationship between the Maximum Stable Distance (A-B) and the size of multi-photon burst used consisting of burst sizes up to 10^6 qubits.

transmission (denoted by D_s), and the size of multi-photon burst used as described in eq 18.

$$D_s = -\phi \log^3(b) + \beta \log^2(b) + \gamma \log(b) + \delta, \tag{18}$$

where, $\phi, \beta, \gamma,$ and δ are the curve-fitting parameters and b is the size of multi-photon burst used. This gives us insight into a rather counter-intuitive relationship occurring between the two quantities. For line topology with $B = 0.85$ and $D = 0.02$, and $\alpha = 0.15$, eq 17 can be used to determine the maximum distance of stable transmission for a given value of the multi-photon burst.

6 Conclusions and Future Work

Quantum networks are quickly becoming a practical reality. Several empirical works, such as the DARPA, the European, and the Tokyo quantum network, even delved into the questions of the distance between the nodes and conducting stable transmission by introducing trusted nodes and optical switches. There are several sources of errors and losses associated with the channel, and as noted earlier in eq 9, the probability of successful transmission is dependent on the attenuation coefficient and the distance between the nodes. Different optical materials have different attenuation constants, and thus, exploring different topologies to find a balance between the attenuation constant and placement of nodes is a major task. This study explored the performance of three major QKD protocols on different topologies, namely the Decoy-state, the 3-stage, and the E91 protocol.

We found that the grid topology performed comparatively better than other simpler topologies due to multiple paths and various trusted nodes contributing to the final key pool for all three protocols explored. It was also found to be more robust over time than any of the other topologies used. However, when we introduced the torus topology and studied the performance of 3-Stage and E91 Protocol, it surpassed the performance of any of the other topologies by generating significantly higher key rates. Furthermore, we established a mathematical equation that defines the changing key-rate values for increasing distance between Alice and Bob over the line topology. We also established a generic equation for the maximum possible distance for stable transmission between Alice and Bob, again for the line topology having three nodes, as this serves as the basic case for further practical developments. This serves as an important development in conceptualizing practical quantum networks, as the size of the multi-photon burst can be adjusted based on the distance between the placement of sender and receiver nodes.

As future work, after defining the relationship between the size of multi-photon burst and maximum distance of stable transmission, we need to establish a similar relationship for different topologies as well. This will further give us insight into a more in-depth multi-photon device behaviors. Another important aspect is understanding the nature of various practical problems with current protocols as most of them are based on heuristics and thus don't guarantee optimal solutions, i.e., lack efficiencies and thus, these become impractical in developing larger networks [43]. Apart from these, we need to understand various other problems involved in network engineering in the current NISQ era, i.e., a system consisting of Johnson's noise, which is due to lattice vibrations caused in the system as it's not at the absolute zero temperature. This further calls for the development of different error-correction methods that can be utilized to idealize newer forms of quantum routers that can deal with the presence of noise in the system and show higher performance [44].

In summary, this study showed the advantages of the multi-photon QKD Protocols over various topologies. This study also developed an empirical relationship relating the burst size and distances of stable transmission for the 3-stage protocol. The 3-stage protocol demonstrated the ability to transmit higher order qubit bursts, thus providing for more stable and higher key rates. While we developed the empirical relationship for the 3-stage Protocol over the line topology, the takeaway from this study will help in identifying suitable protocols for the implementation of more robust quantum networks.

Abbreviations

The following abbreviations are used at various points in the paper,

1. QKD: Quantum Key Distribution
2. DARPA-Network: Defense Advanced Research Projects Agency- Network
3. PNS: Photon-Number Splitting Attack
4. DV-Protocols: Discrete-Variable Protocols
5. CV-Protocols: Continuous-Variable Protocols
6. QBER: Quantum Bit Error Rate
7. BB84: Bennett and Brassard 1984 QKD Protocol
8. Alpha (α): Attenuation coefficient.
9. R, k, x_0: Graph-fitting parameters for multi-photon burst and distance relationship.
10. D_s: Maximum distance of stable transmission.

Declarations

Ethical Approval and Consent to participate

Not applicable

Consent for publication

Not applicable

Availability of Supporting Data

Not applicable

Competing interests

None

Authors Contributions

N.J. is the primary author of the manuscript and received intellectual inputs from A.P. and M.S. to guide the research. All authors edited the manuscript.

Funding

A.P. and M.S. are funded through NSF #2324924

References

[1] Zhang, Z., Zhuang, Q.: Distributed quantum sensing. Quantum Science and Technology **6**(4), 043001 (2021)

[2] Aslam, N., Zhou, H., Urbach, E.K., Turner, M.J., Walsworth, R.L., Lukin, M.D., Park, H.: Quantum sensors for biomedical applications. Nature Reviews Physics **5**(3), 157–169 (2023)

[3] Zhang, P., Chen, N., Shen, S., Yu, S., Wu, S., Kumar, N.: Future quantum communications and networking: A review and vision. IEEE Wireless Communications (2022)

[4] Renner, R.: Security of quantum key distribution. International Journal of Quantum Information **6**(01), 1–127 (2008)

[5] National Security Agency/Central Security Service: Quantum Key Distribution (QKD) and Quantum Cryptography QC. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/. Accessed: [16 December 2023] (2023)

[6] Yurke, B., Denker, J.S.: Quantum network theory. Journal Title **29**(3), (1984)

[7] Elliott, C.: Building the quantum network. New Journal of Physics **4**, 46–14612 (2002)

[8] Satoh, T., Nagayama, S., Suzuki, S., Matsuo, T., Hajdusek, M., Meter, R.V.: Attacking the quantum internet. IEEE Transactions on Quantum Engineering **2**, 1–17 (2021)

[9] Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J.F., Fasel, others.: The secoqc quantum key distribution network in vienna. New Journal of Physics **11**, 075001 (2009)

[10] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., others.: Field test of quantum key distribution in the tokyo qkd network. Optics Express **19**, 10387 (2011)

[11] Ribezzo, D., Zahidy, M., Vagniluca, I., Biagi, N., Francesconi, S., Occhipinti, T., Oxenløwe, L.K., Lončarić, M., Cvitić, I., Stipčević, M., Pušavec, Ž., Kaltenbaek, R., Ramšak, A., Cesa, F., Giorgetti, G., Scazza, F., Bassi, A., De Natale, P., Cataliotti, F.S., Inguscio, M., Bacco, D., Zavatta, A.: Deploying an inter-european quantum network. Advanced Quantum Technologies (2023)

[12] Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., *et al.*: Satellite-to-ground quantum key distribution. Nature

549, 43–47 (2017)

[13] Wehner, S., Elkouss, D., Hanson, R.: Quantum internet: A vision for the road ahead. Science **362**, 9288 (2018)

[14] Unruh, D.: Everlasting multi-party computation. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013, pp. 380–397. Springer, Berlin, Heidelberg (2013)

[15] Gaidash, A.A., Egorov, V.I., Gleim, A.V.: Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices. In: Journal of Physics: Conference Series, vol. 735. St.Petersburg, p. 012072 (2016). IOP Publishing

[16] Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Physical Review Letters **68**, 3121–3124 (1992)

[17] Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science **560**, 7–11 (2014)

[18] Ekert, A.K.: Quantum cryptography based on bell's theorem. Physical Review Letters **67**, 661–663 (1991)

[19] Diamanti, E., Lo, H., Qi, B., et al.: Practical challenges in quantum key distribution. npj Quantum Information **2** (2016)

[20] Sajeed, S., Chaiwongkhot, P., Huang, A., Qin, H., Egorov, V., Kozubov, A., Gaidash, A., Chistiakov, V., Vasiliev, A., Gleim, A., Makarov, V.: An approach for security evaluation and certification of a complete quantum communication system. Scientific Reports **11**(1), 5110 (2021)

[21] Verma, P.K., Rifai, E.M., Clifford, C.K.W.: Photon-number splitting attack. In: Multi-photon Quantum Secure Communication. Springer, Springer Nature Singapore Pte Ltd. (2019). Chap. 3

[22] Hensen, B., *et al.*: Experimental loophole-free violation of a bell inequality using entangled electron spins separated by 1.3 km. Nature **526**, 682 (2015)

[23] Chen, T.-Y., Jiang, X., Tang, S.-B., Zhou, L., Yuan, X., Zhou, H., Wang, J., Liu, Y., Chen, L.-K., Liu, W.-Y., Zhang, H.-F., Cui, K., Liang, H., Li, X.-G., Mao, Y., Wang, L.-J., Feng, S.-B., Chen, Q., Zhang, Q., Li, L., Liu, N.-L., Peng, C.-Z., Ma, X., Zhao, Y., Pan, J.-W.: Implementation of a 46-node quantum metropolitan area network. npj Quantum Information **7**, 134 (2021)

[24] Shenoy-Hejamadi, A., Pathak, A., Radhakrishna, S.: Quantum cryptography: Key distribution and beyond. Quanta **6**(1), 1–47 (2017)

[25] Kak, S.: A three-stage quantum cryptography protocol. Foundations of Physics

Letters **19**(3), 293–296 (2006)

[26] Thapliyal, K., Pathak, A.: Kak's three-stage protocol of secure quantum communication revisited: hitherto unknown strengths and weaknesses of the protocol. Quantum Information Processing **17**(9), 229 (2018)

[27] Chan, K.W.C., El Rifai, M., Verma, P., Kak, S., Chen, Y.: Multi-photon quantum key distribution based on double-lock encryption. In: CLEO: 2015, San Jose, California, pp. 1–3 (2015). OSA

[28] Askarani, M.F., Das, A., Davidson, J.H., Amaral, G.C., Sinclair, N., Slater, J.A., Marzban, S., Thiel, C.W., Cone, R.L., Oblak, D., Tittel, W.: Long-lived solid-state optical memory for high-rate quantum repeaters. Physical Review Letters **127**, 220502 (2021)

[29] Li, C., Zhang, S., Wu, Y.-K., Jiang, N., Pu, Y.-F., Duan, L.-M.: Multicell atomic quantum memory as a hardware-efficient quantum repeater node. PRX Quantum **2**, 040307 (2021)

[30] Dhara, P., Linke, N.M., Waks, E., Guha, S., Seshadreesan, K.P.: Multiplexed quantum repeaters based on dual-species trapped-ion systems. Physical Review A **105**, 022623 (2022)

[31] Pu, Y.-F., Zhang, S., Wu, Y.-K., Jiang, N., Chang, W., Li, C., Duan, L.-M.: Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments. Nature Photonics **15**, 374–378 (2021)

[32] Yu, Y., Ma, F., Luo, X.-Y., Jing, B., Sun, P.-F., Fang, R.-Z., Yang, C.-W., Liu, H., Zheng, M.-Y., Xie, X.-P., Zhang, W.-J., You, L.-X., Wang, Z., Chen, T.-Y., Zhang, Q., Bao, X.-H., Pan, J.-W.: Entanglement of two quantum memories via fibres over dozens of kilometres. Nature **578**, 240–245 (2020)

[33] Burr, J., Parakh, A., Subramaniam, M.: Evaluating different topologies for multi-photon quantum key distribution. In: Donkor, E., Hayduk, M., Frey, M.R., Jr., S.J.L., Myers, J.M. (eds.) Quantum Information Science, Sensing, and Computation XIV, vol. 12093, p. 1209309. SPIE, Orlando, Florida, United States (2022). International Society for Optics and Photonics

[34] Scarani, V., *et al.*: The security of practical quantum key distribution. Reviews of Modern Physics **81**, 1301 (2009)

[35] Cáceres Alvarez, L., Collao Caiconte, P.: Comparison and analysis of bb84 and e91 quantum cryptography protocols security strengths. International Journal of Modern Communication Technologies & Research **4**(9) (2016)

[36] Lim, C.C.W., Curty, M., Walenta, N., Xu, F., Zbinden, H.: Concise security bounds for practical decoy-state quantum key distribution. Physical Review A

89, 022307 (2014)

[37] Attema, T., Bosman, J.W., Neumann, N.M.P.: Optimizing the decoy-state bb84 qkd protocol parameters. Quantum Information Processing **20**, 154 (2021)

[38] Zhao, Y., Qi, B., Ma, X., Lo, H.-k., Qian, L.: Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber. In: 2006 IEEE International Symposium on Information Theory, pp. 2094–2098 (2006)

[39] Nurhadi, A.I., Syambas, N.R.: Quantum key distribution (qkd) protocols: A survey. In: 2018 4th International Conference on Wireless and Telematics (ICWT), pp. 1–5 (2018)

[40] Felix, S., Gisin, N., Stefanov, A., Zbinden, H.: Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses (2001)

[41] Amer, O., Krawec, W.O., Wang, B.: Efficient routing for quantum key distribution networks. In: 2020 IEEE International Conference on Quantum Computing and Engineering (QCE), pp. 137–147. IEEE, Denver, CO, USA (2020)

[42] Munro, W.J., Harrison, K.A., Stephens, A.M., Devitt, S.J., Nemoto, K.: From quantum multiplexing to high-performance quantum networking. Nature Photonics **4**, 792–796 (2010)

[43] Zeng, Y., Zhang, J., Liu, J., Liu, Z., Yang, Y.: Entanglement management through swapping over quantum internets. IEEE Network (2023)

[44] Shi, W., Malaney, R.: Quantum routing for emerging quantum networks. IEEE Network (2023)