Multi-photon QKD for Practical Quantum Networks

Nitin Jha
Department of Computer Science
Kennesaw State University
njha1@students.kennesaw.edu

Abhishek Parakh
Department of Computer Science
Kennesaw State University
aparakh@kennesaw.edu

Mahadevan Subramaniam
Computer Science Department
University of Nebraska Omaha
msubramaniam@unomaha.edu

***Abstract*—Quantum key distribution (QKD) will most likely be an integral part of any practical quantum network 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 makes the integration of the QKD into existing classical networks, that use tens of thousands of photons per bit of transmission, difficult. Furthermore, it has been found that protocol performance varies with topology. In order to remove the reliance of QKD on single-photon emitters and increase transmission distances, it is worthwhile to explore QKD protocols that do not rely on single-photon transmissions for security, such as the 3-stage QKD protocol, which can tolerate multiple photons in each burst without information leakage. This paper compares and contrasts the 3-stage QKD protocol with conventional QKD protocols and its efficiency in different network topologies and conditions. Furthermore, we establish a mathematical relationship between achievable key rates to increase transmission distances in various topologies.**

***Index terms*—** Quantum networks, quantum key distribution, multi-photon transmissions, 3-stage protocol, network topologies.

I. Introduction

Quantum information theory has been of significant interest over recent decades, leading to advances in computing, networking, and sensing technologies [1]–[3]. Quantum networks, under specific hardware configurations, offer enhanced security for communications [4] and are seen as a vital element in the future development of the quantum internet. Despite some challenges [5], Quantum Key Distribution (QKD) remains a foundational technique for ensuring network security. Research efforts are currently directed towards developing near-ideal quantum hardware, perfecting QKD systems, and mitigating potential eavesdropping risks [6]–[8]. Practical implementations have been demonstrated through the DARPA network and other networks across Europe [9] and Tokyo [10], showing the feasibility of quantum networks. Recent developments include the deployment of a private quantum network across Europe during the 2021 G20 Summit in Trieste, featuring two sender and two receiver nodes [11]. Furthermore, from 2003 to 2016, the Chinese Academy of Sciences (CAS) developed a satellite and ground-based network, achieving secure key distribution over $7,600$ km using a decoy-state QKD transmitter onboard a low-earth-orbit satellite, which also facilitated a secure video conferencing session [12]. These advancements underscore the rapid progress in quantum technologies that are poised to support large-scale secure quantum communications [8], [13].

QKD offers unconditional security because it utilizes the principles of quantum physics, making it *future proof* against eavesdropping, unlike classical transmission methods [14]–[18]. QKD, combined with *quantum-resistant classical algorithms* and *quantum cryptography*, is expected to play a crucial role in securing future communications for applications such as smart grids and defense networks [19]. Despite its potential, QKD faces several challenges, both theoretical and practical. These include photon number splitting (PNS) attacks, hardware inconsistencies [20], [21], and vulnerabilities related to Bell inequality test *loopholes* [22]. Furthermore, practical issues with optical switches and trusted nodes limit network robustness and range, with compromised nodes posing significant security risks [23]. Current approaches aim to manage multi-photon bursts, but these methods are limited because they still discard multi-photon bursts and rely on single photons, making integration with classical networks challenging. An alternative is the use of advanced multiphoton QKD protocols, such as the 3-stage protocol, which do not depend on single photons and accommodate higher photon burst rates [24]–[26]. Recent studies have also shown potential for using the three-stage protocol in quantum secure direct communication [27], [28]. This investigation forms the core of our study. Some other experimental works show the use of multiphoton approach for several quantum communication setups. Such as, [29] proposes a modified, more efficient twin-field (TF) QKD using a sending-or-not-sending (SNS) TF-QKD, and also studies the case of two-photon emissions instead of single photon QKD. Furthermore, [30] studies coincidence measurements to monitor and selectively include multi-photon pulses (two- and three-photon events) in the key generation—rather than discarding them as in standard BB84—it is possible to boost the secure key rate by roughly 74% over line-of-sight channels without resorting to decoy states. [31] studies the effect of different noise models on quantum memory of quantum repeaters which would be central to development of large scale quantum networks. [32] reviews the progress made in field of free-space QKD networks which highlights some of the key-experimental work done in deploying free-space QKD networks. Many of the fundamental works in field of QKD are theoretical and simulation based, while some provides experimental validation to these theoretical works. In this study, we simulate quantum networks based on several practical network parameters such as attenuation coefficient, noise parameters, etc.

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. The multiphoton burst represents generating a burst of a given size, and then encoding them as a quantum state. This allows for measurements, and thus collapsing the final result into on classical bit. 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. The preprint of this paper is located at [33].

II. 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. 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"*.

The *Decoy-state* protocol enhances BB84 security by using random photon bursts to counteract PNS attacks, preventing Eve from distinguishing real from decoy transmissions [17]. Implemented using weak coherent pulses, this protocol varies the photon burst intensity and uses statistical analysis to detect intrusions [35], [36]. Post-transmission, Alice and Bob verify detection parameters over an authenticated channel to estimate and detect any attacker presence [37]. The *three-stage* protocol is a viable option for practical quantum networks and it uses a technique similar to classical *double-lock encryption* [24], [38]. In this protocol, Alice starts by encoding a key or message using orthogonal quantum states or an arbitrary state $|X\rangle$. Both Alice and Bob apply secret unitary operations, U_A and U_B, that commute ($[U_A, U_B] = 0$) [24], [38]. The three-stage protocol is shown to be multiphoton resilient. This works by encoding multiple qubits for each classical bit, and since the preparation basis is global knowledge, all qubits associated with one bit are prepared in the same global basis. This multiphoton implementation of the three-stage protocol has been shown to be a viable option for sending direct messages across the quantum channel. [39] Fig.(1) represents the working of the three-stage protocol introduced by [24]. The *E91 protocol*, unlike the BB84 and B92 protocols, is an entanglement-based protocol utilizing single-photon transmissions. In our implementation, the $E91$ protocol uses the entanglement distribution through quantum repeater nodes through the entanglement distribution. This can be interpreted as distributing multipartite entangled state across each pulse train. In post-processing, Alice and Bob keep only those coincidence events corresponding to one photon at each end; any higher-order multiphoton coincidences are treated as erasures. This makes E91 more efficient over longer distances, as quantum repeaters help in the reduction of the attenuation loss.

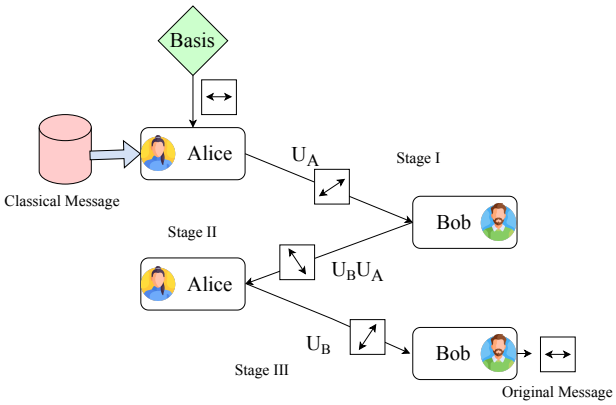


Fig. 1: Schematic diagram representing the working of the three-stage protocol.

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],

$$P(n, \mu) = \frac{\mu^n e^{-\mu}}{n!}, \tag{1}$$

where μ is the mean photon number for the photon burst. The zero, first, and second-order expansion for our photon distribution are,

$$P(0) \approx 1 - \mu + \frac{\mu^2}{2};\ P(1) \approx \mu - \mu^2;\ P(2) \approx \frac{\mu^2}{2}. \tag{5}$$

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

$$P(n \geq 2) \approx \frac{\mu}{2} + \frac{\mu^2}{4}. \tag{6}$$

The two main strategies employed by the eavesdropper to compromise the security of quantum communications are [40]:

- The first strategy involves Eve intercepting and analyzing all photons sent by Alice, and then relaying plausible states to Bob through a nearby source, carefully mimicking photon statistics. This scenario reveals that the maximum ratio of mutual information between Eve and Alice to the Quantum Bit Error Rate (QBER) reaches 6.83. Under *infinitesimal splitting*, it's shown that Eve could achieve complete informational equivalence with Alice, indicated by a mutual information score of 1.
- The second strategy involves Eve using a beamsplitter to extract a fraction λ from each pulse, simultaneously reducing photon loss by replacing the line with one of

lower loss. The mutual information between Alice and Eve in this scenario is quantified as,

$$I(A,E) = \frac{\mu}{2}(2\lambda(1-\lambda))\frac{1}{2}, \tag{7}$$

where $\mu/2$ represents the probability $P(2)$. This model predicts a maximum information gain for Eve of $\mu/8$ when $\lambda = 1/2$, correlating to a 3 dB gain.

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].

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 *torus topology* for our network simulator. Table I compares the advantages and disadvantages of the various topologies used in this study. Figure (2) shows the different topologies generated through our network simulator.

III. Network Simulation Setup

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

A. Network Communication

The connections between each of the involved nodes are achieved by simulating fiber-optic cables with transmission probability as given in equation(8).

$$P(L) = 10^{-\alpha L/10}, \tag{8}$$

where L is the fiber length in kilometers, and α is the attenuation coefficient of the fiber-optic cable used. It's evident from equation(8) that as we increase the distance between the nodes or the length of fiber required, the success of transmission would drastically decrease. For our simulation, we keep the value of $\alpha = 0.15\ km^{-1}$ unless otherwise specified. Our network simulation includes various types of nodes, with trusted nodes like Alice and Bob being crucial. These nodes attempt to connect through viable paths, storing successfully transmitted qubits in a raw key pool, $(RK)_{i,j}$, where i,j represents the node pair. The simulation also incorporates optical switches for linking nodes on a peer-to-peer basis, which, while facilitating dynamic connections, show performance deterioration. Further, we utilize the E91 Protocol to simulate quantum repeaters. Unlike classical repeaters, quantum repeaters use entanglement and entanglement swapping to extend the communication range without violating the no-cloning principle of quantum mechanics. The effectiveness of this method is shown in equation(8), illustrating that although the probability of successful transmission between each repeater is high, the overall probability from Alice to Bob remains consistent as these events are independent. To address this, we simulate redundancy by conducting five simultaneous Bell state transmissions, enhancing entanglement swapping efficiency [42]. Fig.(3) depicts the use of quantum repeaters in entanglement swapping using an external Bell pair through intermediate repeaters.

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.

B. QKD Protocol Simulation

In our QKD simulation, transmissions are completed using either quantum repeaters or direct fiber-optic cables as outlined in section II. After conducting $10^5 - 10^6$ QKD rounds, we simulate error correction factoring in a decoherence value of $D = 0.02$ from environmental noise impacting all qubits. We identify erroneous qubits, calculate the error rate Q, and perform error corrections to derive the final key pool $K_{i,j}$ between trusted nodes using equation(9):

$$K_{i,j} = R(1 - 2h(Q_{i,j})), \tag{9}$$

where $h(Q)$ is the binary entropy function and R is the raw-keyrate for the protocol run. Trusted nodes exchange key material through XOR operations. For example, node T_2 assists in securely transmitting keys between Alice and Bob as shown in equation(10:

$$K_{A,2} = (K_{A,2} \oplus K_{2,B}) \oplus K_{2,B} \tag{10}$$

The overall key rate, which has the standard units of key-bits/s, indicating the QKD protocol's efficiency, is calculated by dividing the final key pool size by the number of QKD rounds.

C. Torus Topology

In this study, we present a $3D$ topology for our network simulation along with several traditionally used topologies. Fig.(2f) shows the torus topology generated through the network simulator whereas Fig.(4) shows the schematic representation of the $2D$ representation of torus topology, highlighting the connection between the user nodes. The idea behind torus topology is a $3D$ wrapping of the connections in a traditional grid topology.

IV. Results

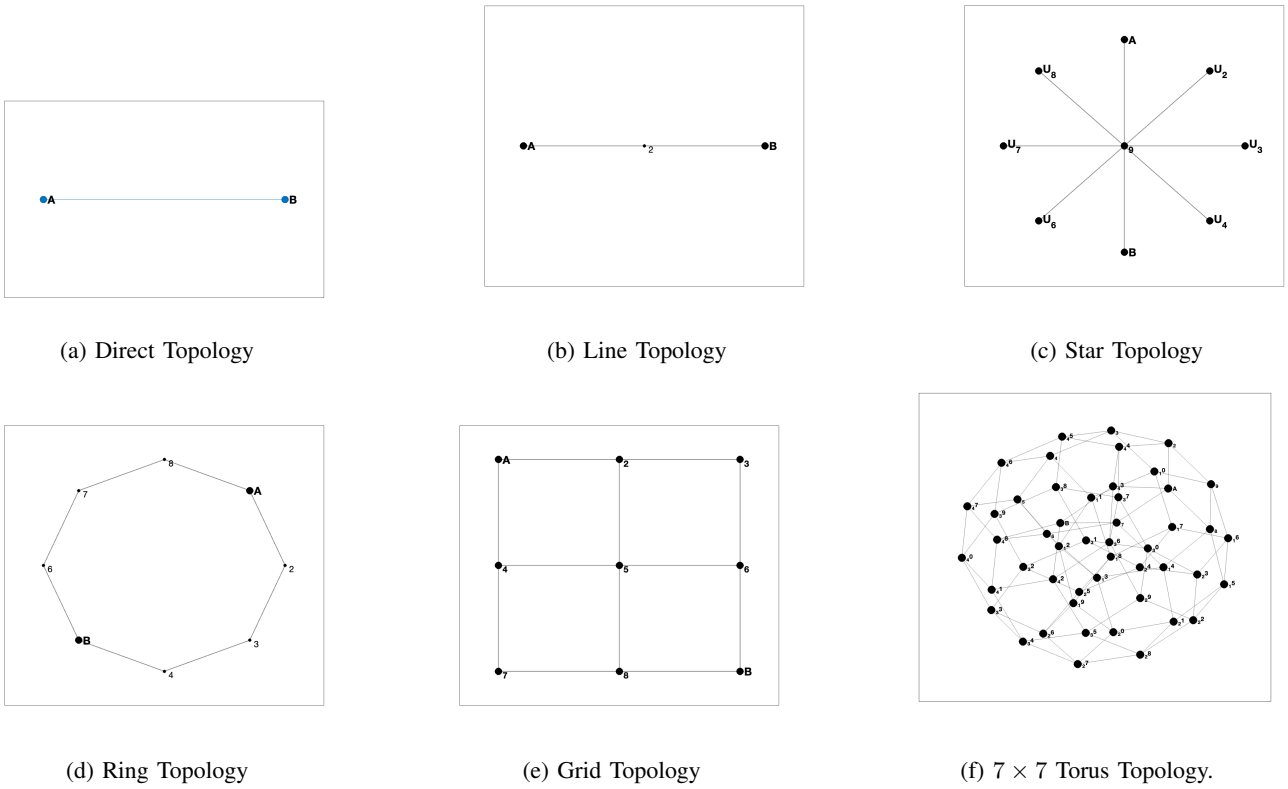
In this section, we'll go over the results obtained through our simulations for different QKD Protocols as mentioned in section II and over different Topologies.

A. Performance over Direct Topology

We first looked at the performance of different QKD protocols in direct topology because it serves as the most basic case of topology without any complexities. In this case, we simulated E91 in two cases, i.e., with and without using quantum repeaters. From Fig.(5), we can see that using quantum repeaters significantly increased the distance of stable

TABLE I: 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.



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

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

Fig. 2: Different topologies used in our QKD simulations (all of the topology profiles are generated through our simulations directly).

key rates to the case without any quantum repeaters. We see that three-stage protocol offers high key-rates for lower distances, however it reduces significantly with increasing distances. This can be associated with the fact that qubits have to travel thrice the distance than other protocols, thus attenuation loss is significantly higher. Decoy state offers the least key-rates due to vacuum bits occupying the bandwidth, and with similar attenuation, the number of effective qubits contributing to final key-rate is significantly lower. We see that E91 with repeater offers slightly lower key-rates, however it offers more stable key-rate over larger distances.

B. Performance of QKD Protocols over Different Topologies

This section explores the performance of different QKD protocols over different Topologies as described in Fig.(2). We compare the changing key rates over various distances between Alice and Bob for the 3-stage protocol, the E91 protocol, and decoy-state protocol (section II). 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 (as shown in Fig.(2e) 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

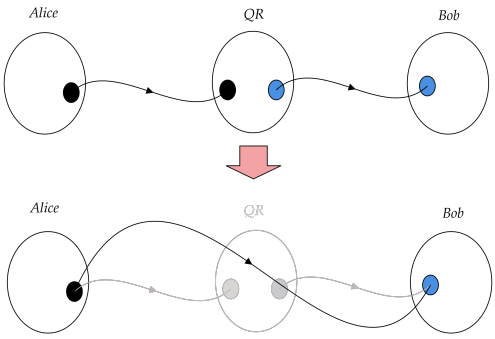


Fig. 3: Working of the quantum repeater: Starts with two sets of entangled bell-pair between Alice-QR and QR-Bob. Then, we perform an entanglement swap between the nodes to create a final entangled Bell state pair between Alice and Bob. The curly line represents an entangled pair.

TABLE II: 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. $D = 0.02$.

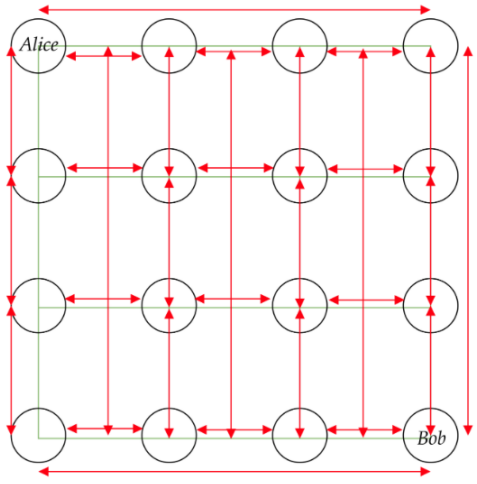


Fig. 4: Schematic representation of the Torus topology. Red lines highlights the connection logic between user nodes.

distributed each round because of the presence of multiple trusted nodes.

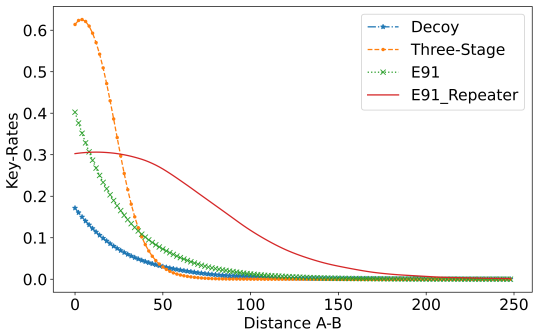


Fig. 5: Comparison of Performance of different QKD Protocols over Direct Topology.

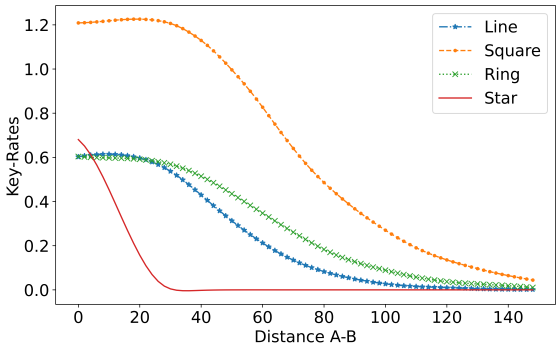
QKD Protocol Performance over Torus Topology: This section explores the performance of the 3-stage protocol and E91 protocol over our torus topology. As we can see from Fig.(2f), there are multiple paths between Alice and Bob, and unlike grid topology (Fig.(2e)), the shortest path between Alice and Bob 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 Fig.(5) the key rates were observed to be higher for the 3-stage Protocol than the E91 Protocol. We see similar behavior from Fig.(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.

C. Performance of the Decoy-State Protocol

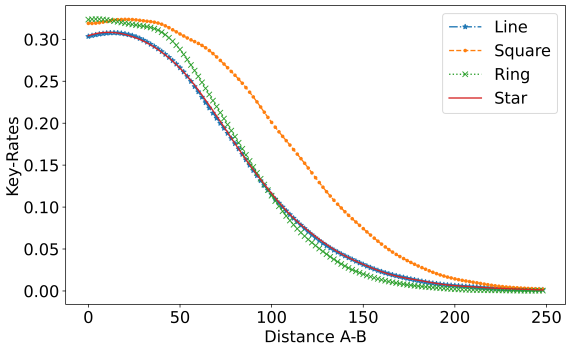
From Fig.(6c), we can see that the grid topology offers the highest key rates than the rest of the topologies due to multiple paths and multiple trusted nodes contributing to more than a single key per simulation round. The grid topology also seems to be more durable over time because the fiber segments 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 equation(8).

D. Performance of the Three-Stage Protocol

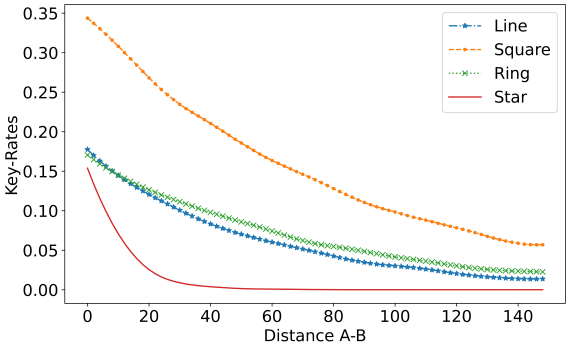
Figure 6a indicates that the grid topology consistently achieves higher key rates due to its multiple paths and trusted nodes, enhancing robustness and key pool size. Contrasting the 3-stage protocol's performance with direct and line topologies, as shown in figures Fig.(5) and Fig.(6a), the line topology exhibits slower key-rate decline over longer distances due to shorter fiber segments and a higher probability of successful transmission (equation(8). At shorter distances, line and ring topologies perform similarly, but the ring topology proves more durable at greater ranges, showing less key-rate decay.



(a) Three Stage Protocol Profile

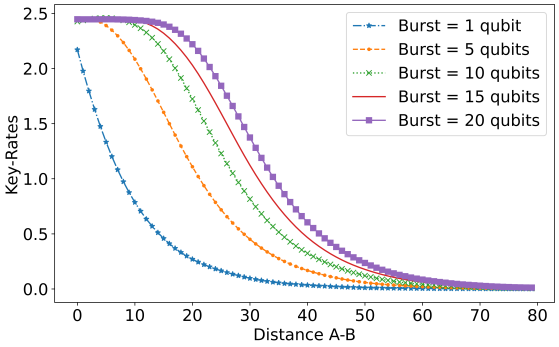


(b) E91 Protocol Profile

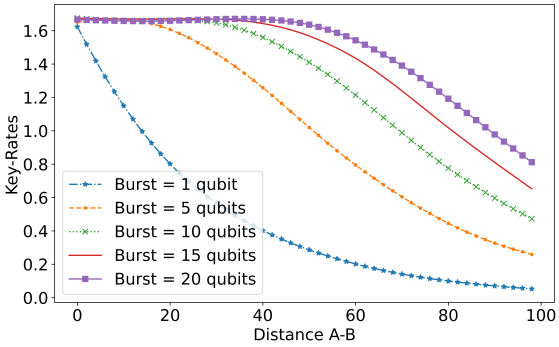


(c) Decoy-State Protocol Profile

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



(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.

Conversely, the star topology, despite starting with higher key rates, experiences rapid decay because of increased attenuation from simulating an optical switch.

E. Performance of E91 Protocol

Fig.(6b) demonstrates that while most topologies show similar performance under the E91 protocol, the grid topology shows robustness and slower key rate decay, attributed to its multiple paths and three repeaters in the shortest path. The ring topology, in contrast, achieves higher key rates at very short distances due to fewer repeaters, reducing the likelihood of entanglement swapping failures. Despite its benefits, the grid topology's advantage is offset by errors from failed quantum repeaters. Conversely, the star topology leverages a central repeater to directly connect any two nodes by creating Bell states selectively, circumventing the need for an optical switch and matching the efficiency of direct line topologies that rely on a single quantum repeater for connectivity between nodes like Alice and Bob.

F. Analysing Higher Order Multi-Photon Bursts

In this section, we explore the trade-offs between performance and security risks with larger multi-photon bursts in the 3-stage protocol, which previously utilized a default burst size of 10 qubits. While increasing burst size can enhance performance, it also raises the potential for PNS attacks. For the E91 protocol, which does not naturally support multi-photon bursts, performance adjustments involve varying the number of simultaneous Bell pairs between quantum repeaters.

Fig.(8a) demonstrates that larger burst sizes generally maintain stable key rates at shorter distances for the 3-stage protocol. Meanwhile, Fig.(8b) shows that the E91 protocol sustains longer-range stable transmissions than the 3-stage protocol, as corroborated by Figures Fig.(5) and Fig.(6b). However, both protocols see key rates diminish at extended distances, with variations depending on the burst size and protocol. These findings highlight the importance of exploring various network topologies and integrating multiple trusted nodes to enhance protocol efficacy.

G. Multi-Photon Burst and Distance Relation

This section looks into finding a mathematical relation governing these curves to define 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 converges to zero at larger distances.

We define an exponentially decaying function of the sigmoid nature as described in equation(11),

$$y = \frac{R}{(1 + e^{k(x-x_0)})}, \tag{11}$$

where, R, k, x_0 are the fitted parameters, and x is the inter-node distance between Alice and Bob (i.e., the sender and the receiver). 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 $= R/2$. We do curve fitting for the line and ring topologies and present the results below in Fig.(9).

Based on the values of various fitted parameters from equation(11), the following were the equations of the curves found for the above are,

$$y_{\text{line}} = \frac{0.655}{(1 + e^{0.139(x-25.303)})} \text{ and } y_{\text{ring}} = \frac{0.652}{(1 + e^{0.109(x-32.257)})} \tag{14}$$

equation(12) describes the characteristic equations for line and ring topology for $3-$stage protocol.

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, $b = [50, 1200]$. We first make the curve smooth by eliminating the polynomial noise using the SavGol filter. We then fit the curves using equation(11) and present the characteristic curves for each of them in Fig.(10).

For lower order burst size, we see the fit of the curve being better as key rates approaches zero (for Fig.(10a)), and for higher order curves (such as Fig.(10b)) 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.

H. Distance of Stable Transmission and Multi-Photon Burst Size

It is evident that the multi-photon burst increases the distance of stable transmission for all of the curves that we found. This is to be noted that this result can be generalized for same protocol at different multiphoton burst size. This can be done by using the following steps. To find this relation, we have to first find the *turning* point, i.e., the point where the derivative of the curve becomes negative.

From Fig.(11), we can see that a 3rd 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 equation(15).

$$y = 0.000008x^3 - 0.003388x^2 + 0.538443x + 1.693613 \tag{15}$$

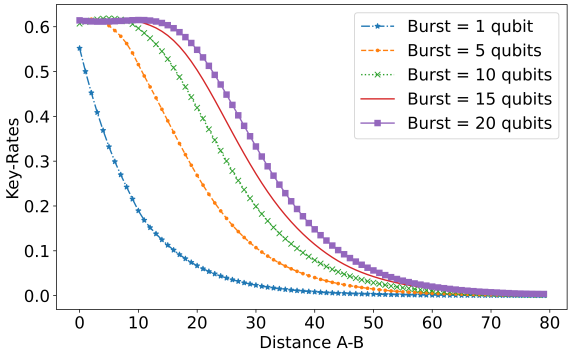
From equation(15), we can see that multi-photon burst size follows a polynomial relationship with the distance of stable transmissions. However, the burst sizes used in this calculation are of very small order. To get a general picture and a more practical burst-size relation, we increase the burst size up to a million qubits at once. Fig.(12) shows the curve with stable transmission distance and multiphoton burst size for bursts of up to one million qubits at once.

Fig.(12) gives an insight into a generic relationship between the higher-order bursts and the distance of stable transmission. We set a curve between $\log(\text{burst\_values})$ and the distance of stable transmission. Fig.(13) gives us a better picture of a possible relationship between the main two quantities of interest of this study, that is, the distance of stable transmission and the size of multiphoton burst used.

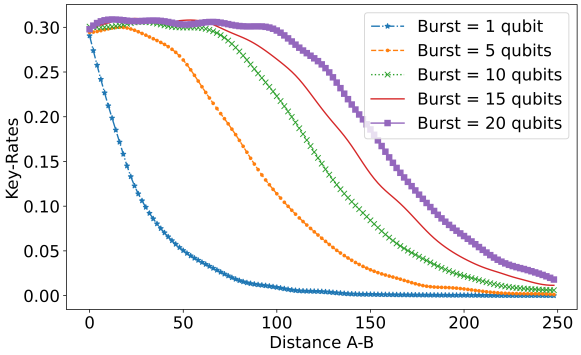
From Fig.(13), we found that the two quantities of interest share a logarithmic-3rd order polynomial relationship as described by equation(16). The model explains over 99% of the variance ($R^2 = 0.998$) and remains high after adjusting for its four parameters (adjusted $R^2 = 0.997$), showing that a cubic fit in $\log(\text{burst})$ works well. Furthermore, a confidence band of 95% also shows very less uncertainty in the fit.

$$D_s = -0.054x^3 + 1.228x^2 + 1.1878x + 2.0178, \tag{16}$$

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 transmission (denoted by D_s), and the size of multi-photon burst used as described in equation(17).

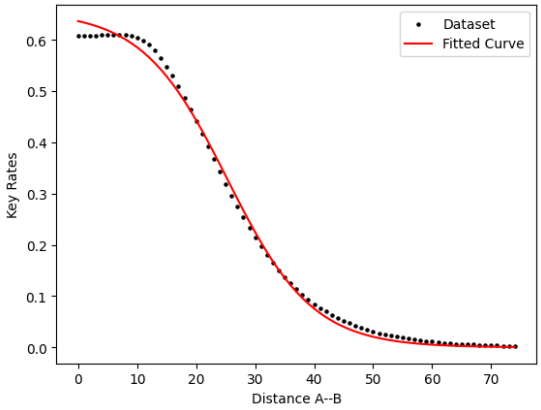


(a) Multi-Photon Burst Profile for Three-Stage Protocol over Line Topology.

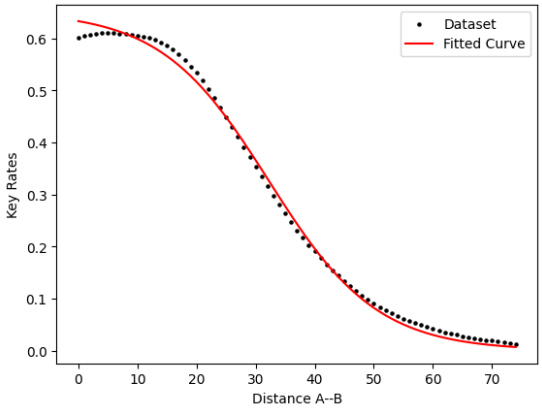


(b) Multi-Photon Burst Profile for E91 over Line Topology.

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

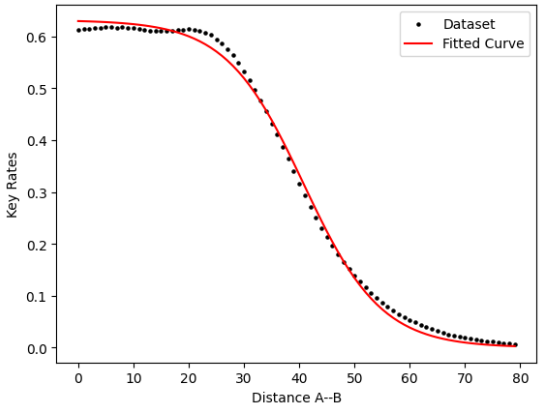


(a) Characteristic curve obtained for QKD Performance over a Line-topology.

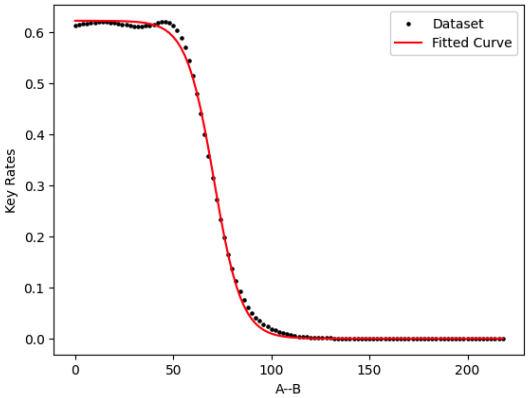


(b) Characteristic curve obtained for QKD Performance over a Ring-topology.

Fig. 9: Fitting the curve to the equation(11) for Line and Ring topology for a multi-photon burst size of 10 qubits for 3-stage QKD Protocol.



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



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

Fig. 10: Fitting the curve to the equation(11) for line topology having higher order multi-photon bursts used for 3-stage Protocol.

$$D_s = -\phi \log^3(b) + \beta \log^2(b) + \gamma \log(b) + \delta, \qquad (17)$$

where, $\phi, \beta, \gamma,$ and δ are the curve fitting parameters and b is the size of the multi-photon burst used. This gives us

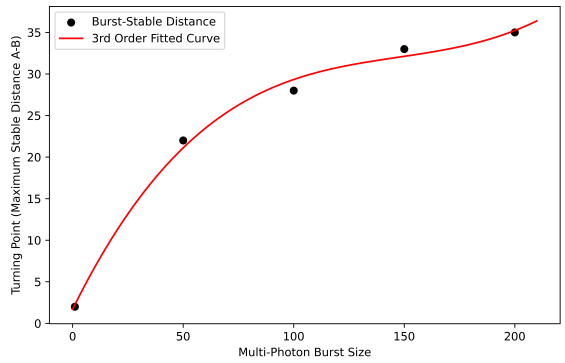


Fig. 11: Relationship between the Maximum Stable Distance (A-B) and the size of multi-photon burst used.

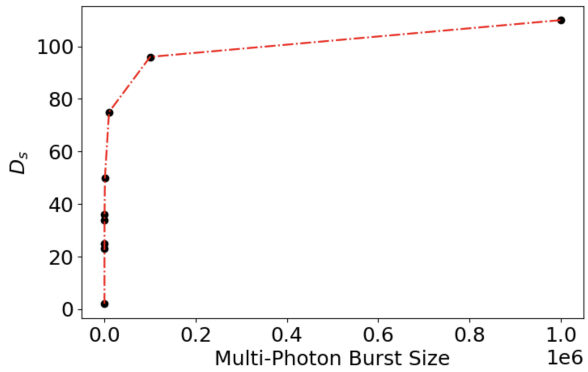


Fig. 12: Relationship between the maximum stable distance (between Alice and Bob) and the size of multi-photon burst used consisting of burst sizes up to 10^6 qubits. The dashed lines is just for visualization purposes, and to study the data-trend more effectively, we do curve fitting in log scale in next figure.

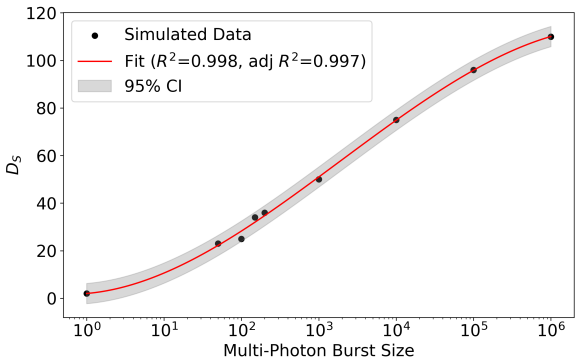


Fig. 13: Relationship between the Maximum Stable Distance (A-B) and the size of multi-photon burst used consisting of burst sizes up to 10^6 qubits (x-axis is in log scale). *CI* refers to the confidence index of the curve fitting.

insight into a rather counter-intuitive relationship occurring between the two quantities. For line topology with $B = 0.85$ and $D = 0.02$, and $\alpha = 0.15$, equation(16) can be used to determine the maximum distance of stable transmission for a given value of the multi-photon burst.

V. Conclusions and Future Work

Quantum networks are increasingly becoming viable, as evidenced by empirical studies from initiatives such as the DARPA, European, and Tokyo quantum networks. These studies have addressed issues such as the distance between nodes and the stabilization of transmissions through the use of trusted nodes and optical switches. As indicated in equation(8), the probability of successful transmission is dependent on the attenuation coefficient and the distance between the nodes, with different optical materials exhibiting variable attenuation constants. This requires exploring diverse topologies to optimize node placement and attenuation impacts. Our study evaluates the performance of three prominent QKD protocols—Decoy-state, 3-stage, and E91—across various network topologies.

Our findings indicate that the grid topology outperforms simpler configurations by leveraging multiple paths and trusted nodes, enhancing the key pool and robustness across the three explored QKD protocols. Notably, when we analyzed the torus topology with the 3-stage and E91 protocols, it yielded significantly higher key rates than any other topology. Additionally, we derived a mathematical model to quantify key-rate variations with increasing distances between Alice and Bob over the line topology. We also formulated an equation for the maximum feasible distance for stable transmission in a line topology with three nodes, laying foundational insights for practical quantum network designs. This advancement underscores the importance of tailoring the multi-photon burst size to the node separation, optimizing communication efficacy in practical quantum networks. Apart from these, the multiphoton approach studied in this work can be used in multi-carrier continuous-variable QKD (CVQKD) systems, where coherent states are multiplexed into Gaussian subcarrier channels to increase aggregate key rates and resilience against channel noise[43]. All of the results presented in this work define future frameworks for a more scalable and reliable network, laying foundation for the development of Quantum Internet[44].

As future work, we aim to establish a relationship between multi-photon burst sizes and maximum stable transmission distances across various topologies, enhancing our understanding of multi-photon device behaviors. There is also a need to address practical challenges associated with current QKD protocols, which often rely on heuristics and may not provide optimal solutions, thereby limiting their practicality for larger network development [45]. Moreover, in the NISQ era, network engineering must account for Johnson noise and other real-world phenomena, necessitating the development of advanced error-correction methods to improve quantum router performance in noisy environments [46]. A proposed solution to these problems in recent times has been quantum augmented networks. In this approach, several quantum components (such as quantum teleportation[47], QKD, quantum error correction, etc.) are strategically integrated in current classical networks to enable large-scale quantum communication [48], [49].

In summary, this study not only highlighted the advantages of multi-photon QKD protocols across different topologies but also established an empirical relationship between burst size and stable transmission distances for the 3-stage protocol. This protocol demonstrated enhanced capabilities for transmitting higher-order qubit bursts, yielding more stable and higher key rates. While the empirical relationship was specifically developed for the 3-stage protocol over the line topology, the insights gained will guide the selection of suitable protocols for crafting more robust quantum networks.

Acknowledgment

This work is sponsored by NSF award #2324924 and #2324925.

References

[1] Z. Zhang and Q. Zhuang, "Distributed quantum sensing," *Quantum Science and Technology*, vol. 6, no. 4, p. 043 001, 2021. DOI: 10.1088/2058-9565/abd4c3.

[2] N. Aslam, H. Zhou, E. K. Urbach, *et al.*, "Quantum sensors for biomedical applications," *Nature Reviews Physics*, vol. 5, no. 3, pp. 157–169, 2023. DOI: 10.1038/s42254-023-00558-3.

[3] P. Zhang, N. Chen, S. Shen, S. Yu, S. Wu, and N. Kumar, "Future quantum communications and networking: A review and vision," *IEEE Wireless Communications*, 2022. DOI: 10.1109/MWC.012.2200295.

[4] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008. DOI: 10.1142/S0219749908003256.

[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] C. Elliott, "Building the quantum network," *New Journal of Physics*, vol. 4, pp. 46.1–46.12, 2002. DOI: 10.1088/1367-2630/4/1/346.

[7] B. Yurke and J. S. Denker, "Quantum network theory," *Journal Title*, vol. 29, no. 3, Page Range, Mar. 1984. DOI: 10.1103/PhysRevA.29.1419.

[8] T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdusek, and R. V. Meter, "Attacking the quantum internet," *IEEE Transactions on Quantum Engineering*, vol. 2, pp. 1–17, 2021. DOI: 10.1109/TQE.2021.3094983.

[9] M. Peev, C. Pacher, R. Alléaume, *et al.*, "The secoqc quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, p. 075 001, 2009. DOI: 10.1088/1367-2630/11/7/075001.

[10] M. Sasaki, M. Fujiwara, H. Ishizuka, *et al.*, "Field test of quantum key distribution in the tokyo qkd network," *Optics Express*, vol. 19, p. 10 387, 2011. DOI: 10.1364/OE.19.010387.

[11] D. Ribezzo, M. Zahidy, I. Vagniluca, *et al.*, "Deploying an inter-european quantum network," *Advanced Quantum Technologies*, 2023. DOI: 10.1002/qute.202200061.

[12] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, 2017. DOI: 10.1038/nature23655.

[13] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, eaam9288, Oct. 2018. DOI: 10.1126/science.aam9288.

[14] D. Unruh, "Everlasting multi-party computation," in *Advances in Cryptology – CRYPTO 2013*, R. Canetti and J. A. Garay, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 380–397. DOI: 10.1007/978-3-642-40084-1_22.

[15] A. A. Gaidash, V. I. Egorov, and A. V. Gleim, "Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices," in *Journal of Physics: Conference Series*, IOP Publishing, vol. 735, St.Petersburg, 2016, p. 012 072. DOI: 10.1088/1742-6596/735/1/012072.

[16] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, pp. 3121–3124, May 1992. DOI: 10.1103/PhysRevLett.68.3121.

[17] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014. DOI: 10.1016/j.tcs.2014.05.025.

[18] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical Review Letters*, vol. 67, pp. 661–663, Aug. 1991. DOI: 10.1103/PhysRevLett.67.661.

[19] E. Diamanti, H. Lo, B. Qi, *et al.*, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, 2016. DOI: 10.1038/npjqi.2016.25.

[20] S. Sajeed, P. Chaiwongkhot, A. Huang, *et al.*, "An approach for security evaluation and certification of a complete quantum communication system," *Scientific Reports*, vol. 11, no. 1, p. 5110, Mar. 2021. DOI: 10.1038/s41598-021-84139-3.

[21] P. K. Verma, E. M. Rifai, and C. K. W. Clifford, "Photon-number splitting attack," in *Multi-photon quantum secure communication*, Springer Nature Singapore Pte Ltd.: Springer, 2019, ch. 3. DOI: 10.1007/978-981-10-8618-2.

[22] B. Hensen *et al.*, "Experimental loophole-free violation of a bell inequality using entangled electron spins separated by 1.3 km," *Nature*, vol. 526, p. 682, 2015. DOI: 10.1038/nature15759.

[23] T.-Y. Chen, X. Jiang, S.-B. Tang, *et al.*, "Implementation of a 46-node quantum metropolitan area network," *npj Quantum Information*, vol. 7, p. 134, Dec. 2021. DOI: 10.1038/s41534-021-00474-3.

[24] S. Kak, "A three-stage quantum cryptography protocol," *Foundations of Physics Letters*, vol. 19, no. 3, pp. 293–296, Jun. 2006. DOI: 10.1007/s10702-006-0520-9.

[25] N. Jha, A. Parakh, and M. Subramaniam, "Effect of noise and topologies on multi-photon quantum protocols," in *Quantum Computing, Communication, and Simulation IV*, SPIE, vol. 12911, 2024, pp. 148–161. DOI: 10.1117/12.3000586.

[26] A. Parakh and M. Subramaniam, "Bootstrapped qkd: Improving key rate and multi-photon resistance," in *Quantum Information Science and Technology IV*, SPIE, vol. 10803, 2018, pp. 22–27. DOI: 10.1117/12.2500438.

[27] K. Thapliyal and A. Pathak, "Kak's three-stage protocol of secure quantum communication revisited: Hitherto unknown strengths and weaknesses of the protocol," *Quantum Information Processing*, vol. 17, no. 9, p. 229, Jul. 2018. DOI: 10.1007/s11128-018-2001-z.

[28] N. Jha, A. Parakh, and M. Subramaniam, "Joint encryption and error correction for secure quantum communication," *Scientific Reports*, vol. 14, no. 1, p. 24 542, 2024. DOI: 10.1038/s41598-024-75212-8.

[29] J. Teng, Z.-Q. Yin, G.-J. Fan-Yuan, *et al.*, "Sending-or-not-sending twin-field quantum key distribution with multiphoton states," *Physical Review A*, vol. 104, no. 6, p. 062 441, 2021. DOI: 10.1103/PhysRevA.104.062441.

[30] A. Biswas, A. Banerji, N. Lal, P. Chandravanshi, R. Kumar, and R. P. Singh, "Quantum key distribution with multiphoton pulses: An advantage," *Optics Continuum*, vol. 1, no. 1, pp. 68–79, 2022. DOI: 10.1364/OPTCON.445727.

[31] A. Mihály and L. Bacsárdi, "Effects of selected noises on the quantum memory satellite based quantum repeaters," *Infocommunications Journal*, vol. 13, no. 2, pp. 19–24, 2021. DOI: 10.36244/ICJ.2021.2.3.

[32] T. Bisztray and L. Bacsardi, "The evolution of free-space quantum key distribution," *Infocommunications Journal*, vol. X, no. 1, pp. 22–30, Mar. 2018. DOI: 10.36244/ICJ.2018.1.4.

[33] N. Jha, A. Parakh, and M. Subramaniam, "Multi-photon 3-stage qkd for practical quantum networks," availavle at https://www.researchsquare.com/article/rs-3826628/v1, 2024. DOI: https://doi.org/10.21203/rs.3.rs-3826628/v1.

[34] V. Scarani *et al.*, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, p. 1301, 2009. DOI: 10.1103/RevModPhys.81.1301.

[35] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," *Physical Review A*, vol. 89, p. 022 307, Feb. 2014. DOI: 10.1103/PhysRevA.89.022307.

[36] T. Attema, J. W. Bosman, and N. M. P. Neumann, "Optimizing the decoy-state bb84 qkd protocol parameters," *Quantum Information Processing*, vol. 20, p. 154, Apr. 2021. DOI: 10.1007/s11128-021-03078-0.

[37] Y. Zhao, B. Qi, X. Ma, H.-k. Lo, and L. Qian, "Simulation and implementation of decoy state quantum key distribution over 60km telecom fiber," in *2006 IEEE International Symposium on Information Theory*, Jul. 2006, pp. 2094–2098. DOI: 10.1109/ISIT.2006.261920.

[38] J. Burr, A. Parakh, and M. Subramaniam, "Evaluating different topologies for multi-photon quantum key distribution," in *Quantum Information Science, Sensing, and Computation XIV*, E. Donkor, M. Hayduk, M. R. Frey, S. J. L. Jr., and J. M. Myers, Eds., International Society for Optics and Photonics, vol. 12093, Orlando, Florida, United States: SPIE, 2022, p. 1 209 309. DOI: 10.1117/12.2620057.

[39] S. Mandal, G. Macdonald, M. El Rifai, *et al.*, "Multi-photon implementation of three-stage quantum cryptography protocol," in *The International Conference on Information Networking 2013 (ICOIN)*, IEEE, 2013, pp. 6–11. DOI: 10.1109/ICOIN.2013.6496343.

[40] S. Felix, N. Gisin, A. Stefanov, and H. Zbinden, "Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses," version 1, Feb. 2001. DOI: 10.1080/09500340108240903.

[41] O. Amer, W. O. Krawec, and B. Wang, "Efficient routing for quantum key distribution networks," in *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Denver, CO, USA: IEEE, Oct. 2020, pp. 137–147. DOI: 10.1109/QCE49297.2020.00027.

[42] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, "From quantum multiplexing to high-performance quantum networking," *Nature Photonics*, vol. 4, pp. 792–796, Nov. 2010. DOI: 10.1038/nphoton.2010.213.

[43] L. Gyongyosi, "Multicarrier continuous-variable quantum key distribution," *Theoretical Computer Science*, vol. 816, pp. 67–95, 2020. DOI: 10.1016/j.tcs.2019.11.026.

[44] J. Burr, A. Parakh, and M. Subramaniam, "Quantum internet," *Ubiquity*, vol. 2022, no. August, pp. 1–14, 2022. DOI: 10.1145/3547493.

[45] Y. Zeng, J. Zhang, J. Liu, Z. Liu, and Y. Yang, "Entanglement management through swapping over quantum internets," *IEEE Network*, 2023. DOI: 10.1145/3626570.3626595.

[46] W. Shi and R. Malaney, "Quantum routing for emerging quantum networks," *IEEE Network*, 2023. DOI: 10.1109/MNET.2023.3317821.

[47] A. Parakh, "Quantum teleportation with one classical bit," *Scientific reports*, vol. 12, no. 1, p. 3392, 2022. DOI: 10.1038/s41598-022-06853-w.

[48] N. Jha, A. Parakh, and M. Subramaniam, "Towards a quantum-classical augmented network," in *Quantum Computing, Communication, and Simulation V*, SPIE, vol. 13391, 2025, pp. 72–86. DOI: 10.1117/12.3042150.

[49] N. Jha, A. Parakh, and M. Subramanian, "A ml based approach to quantum augmented http protocol," in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, IEEE, vol. 2, 2024, pp. 591–592. DOI: 10.1109/QCE60285.2024.10420.

Nitin Jha received his BSc. (Hons) in Physics from Ashoka University in 2023. He is pursuing his Ph.D. from Kennesaw State University (KSU). His broad research interests lie in quantum networks, secure quantum communication, and network security. He is looking at application of artificial intelligence techniques to improve the efficiency of quantum networks and building the foundations of quantum-classical hybrid networks (also known as quantum augmented networks). Nitin's research has won multiple accolades at KSU, appeared in top venues, and continues to be a part of the strategic initiative at the University.

Abhishek Parakh is a Professor of Computer Science and the Director of the Computer Science Ph.D. Program at Kennesaw State University. He received his Ph.D. in Computer Science from Oklahoma State University in 2011. He has held various academic positions, including Director of NebraskaCYBER and the Mutual of Omaha Distinguished Chair of Information Science and Technology. His research interests include quantum cryptography, cybersecurity, and trustworthy computing. He has been the principal investigator on several federally funded projects (NSF, DOD, NASA, NSA, DOS) related to quantum networks, quantum computing, post-quantum cryptography, AI driven educational technology, and cybersecurity education.

Mahadevan Subramaniam. is the Charles W. and Margre H. Durham Distinguished Professor and Chair of the Computer Science Department at the University of Nebraska Omaha (UNO). He earned his B.S. in Computer Science from BITS Pilani in 1986 and his M.S. and Ph.D. in Computer Science from SUNY Albany in 1997. His research focuses on formal methods for software engineering, particularly model checking, SMT solvers, and theorem provers, with applications in software evolution and automated repair strategies.