

Study and Design of Efficient and Resilient Quantum Key Distribution System

A Thesis

submitted to

Indian Institute of Science Education and Research Pune

in partial fulfillment of the requirements for the

BS-MS Dual Degree Programme

by

Shivansh Malviya



Indian Institute of Science Education and Research Pune

Dr. Homi Bhabha Road,

Pashan, Pune 411008, INDIA

October 2024

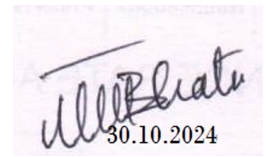
Supervisor: Prof. Vimal Bhatia

© Shivansh Malviya 2024

All rights reserved

Certificate

This is to certify that this dissertation entitled **Study and Design of Efficient and Resilient Quantum Key Distribution System** towards the partial fulfillment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research Pune represents study/work carried out by **Shivansh Malviya** under the supervision of **Prof. Vimal Bhatia**, Professor, Department of Electrical Engineering, during the academic year 2023-2024.

A handwritten signature in blue ink, appearing to read 'Vimal Bhatia', is written over a light pink rectangular stamp. The stamp also contains the date '30.10.2024' in a smaller, darker font.

Prof. Vimal Bhatia

Committee:

Prof. Vimal Bhatia

Prof. M. S. Santhanam

This thesis is dedicated to my family, whose love and support have been my anchor. It also stands as a personal reminder of the long days, late nights, and resilience it took to push through the moments when results seemed elusive.

Declaration

I hereby declare that the matter embodied in the report entitled “**Study and Design of Efficient and Resilient Quantum Key Distribution System**” is the result of the work carried out by me at the Indian Institute of Technology (IIT), Indore, under the supervision of Prof. Vimal Bhatia, and the same has not been submitted elsewhere for any other degree. Wherever others have contributed, every effort is made to indicate this clearly with due reference to the literature and acknowledgement of collaborative research and discussions.



Shivansh Malviya
20191175

Acknowledgements

I would like to express my deepest gratitude to **Prof. Vimal Bhatia**, my supervisor from the Indian Institute of Technology (IIT), Indore, for providing me with the opportunity to work on this project and for his invaluable guidance and support throughout my research journey. His mentorship has been instrumental in ensuring the successful completion of this work.

I am also sincerely thankful to my expert advisor from IISER Pune, **Prof. M.S. Santhanam**, whose expertise and advice have been of immense value. His insights and feedback helped refine my approach and broaden my perspective on the research.

I am profoundly grateful to my **parents** for their unconditional love, encouragement, and unwavering belief in me. Their support has been my greatest source of strength throughout this journey. I am deeply thankful to my friends for their constant motivation and support during challenging times.

I would like to extend my appreciation towards my friends at the **SaSg Lab** of IIT Indore for their encouragement, engaging discussions, and moments of camaraderie. Working alongside them has enriched my research experience in countless ways.

Finally, I would like to express my gratitude to **IISER Pune** for offering me the opportunity to work on my master's project and providing me with the resources and environment necessary for this research.

Contents

Certificate	1
Declaration	3
Acknowledgement	4
Abstract	8
1 Introduction	9
1.1 Background and Motivation	9
1.2 Quantum Key Distribution and Its Role in Network Security	10
1.3 Challenges in Quantum Key Distribution Systems	11
1.4 Research Objectives	12
2 Literature Review	14
2.1 Quantum Key Distribution Protocols	14
2.2 Resource Allocation in QKD Networks	14
2.3 Error Correction and Noise Management in QKD	15
2.4 System Resilience and External Eavesdroppers	15
2.5 Gaps in the Literature	16
2.6 Conclusion and Research Direction	16
3 Methodology	17
3.1 Simulation Overview	17
3.2 Network Architecture and Simulation Environment	17
3.2.1 Network Topology	17
3.2.2 QKD Protocols and Quantum Channel Simulation	17
3.3 Routing and Resource Allocation Algorithms	18
3.3.1 Routing, Wavelength, and Time-Slot Assignment	18
3.3.2 Simulated Metrics	19
3.4 Calculations, Techniques, and Tools	19
3.4.1 Quantum Bit Error Rate Calculation	19
3.4.2 Secure Key Rate	20
3.4.3 Software Environment	20
3.5 Assumptions, Limitations, and Range of Validity	20
3.5.1 Assumptions	20
3.5.2 Limitations	20
3.5.3 Range of Validity	21
3.6 Analytical Methods	21
4 System Model	22
4.1 Overview of the System Architecture	22
4.2 ODCN Design	22
4.3 QKD Protocols	23
4.4 Noise and Eavesdropping Simulation	23
4.5 Error Correction Methods	23
4.6 Routing and Resource Allocation in the ODCN	24

4.7	Performance Metrics	24
5	Results	25
5.1	Overview of Results	25
5.2	Hybrid Model	25
5.3	Fully Quantum Model	27
5.4	Classical Model	28
5.5	QBER vs. Noise Level	33
5.6	Classical BER vs. Noise Level	34
5.7	SKR vs. Noise Level	34
5.8	Quantum Key Resource Allocation (QKRA)	35
5.8.1	Network Model and Adaptive Security Levels	35
5.8.2	Adaptive Heuristics and Resource Allocation Strategy	35
5.8.3	Performance Analysis and Metrics	35
5.9	Resource Allocation Efficiency	36
5.9.1	Simulation ASLC	36
5.10	Incorrect Results	38
5.11	Discussion and Interpretation	40
6	Discussion	41
6.1	Interpretation	41
6.2	Quantum Key Distribution and Error Correction	41
6.3	Resource Allocation in the Optical Data Center Networks	41
6.4	Impact of Noise and Eavesdropping	42
7	Conclusion	43
8	Future Work	44
9	Pseudocode	45
	Bibliography	49

List of Figures

3.1	NSFNET Topology: 14 Nodes, 21 Bi-directional Links	17
3.2	The architecture of a QKD Optical Network [1]	18
3.3	Illustration of quantum key resource allocation in QKD network	19
5.1	Left: QBER vs SNR. Right: SKR/SBR vs SNR.	26
5.2	QBER vs SNR for 10 iterations	26
5.3	Input Length vs Length(top-left), Qber(top-right), Time-Taken(bottom-left), SKR(bottom-right). Eve Present. Noise = 0.03	27
5.4	Quantum Noise Model(QNM)	27
5.5	QNM: 100 MCS	28
5.6	Variation in plots for different values of eavesdropping probability	29
5.7	Over a 100 Iterations: Keys accepted/discarded	29
5.8	MCS-AWGN: 10^3 cycles, 10^3 keys, $3 * 256$ symbols	30
5.9	MCS with key length of 1000	31
5.10	For Higher SNR values: 25-35. In absence of Eve	31
5.11	In presence of Eve	32
5.12	For a full SNR Range(0-35)	32
5.13	SNR range 0-35	33
5.14	Zoomed-in view of QBER at higher SNRs	33
5.15	Plots from base paper	36
5.16	Comparision of simulation results with the base paper	37
5.17	CR Analysis	38
5.18	Comparision of the SRCR, TUR, and NSP metrics obtained for ASSL, AWSL, and SSL	38
5.19	Inaccurate results obtained	39

Abstract

This thesis investigates the implementation of a secure Quantum Key Distribution (QKD) protocol—BB84, within an Optical Data Center Network (ODCN), with emphasis on key negotiation under varying noise levels and adversarial scenarios. A Fully Classical Model, where encoding and noise were simulated using classical methods, and a Hybrid Model, which uses Qiskit SDK to simulate quantum noise and quantum-specific encoding, were developed to assess key metrics like Quantum Bit Error Rate (QBER) and Secure Key Rate (SKR). Two error-correction techniques were used: Hamming, and Cascade. Cascade was able to manage higher error rates; the QBER threshold was chosen liberally—0.25, particularly in the presence of an eavesdropper. The network's performance, measured by the Success Ratio of Connection Requests (SRCR), Time-slot Utilization Ratio (TUR) and Network Security Performance (NSP) aligned with that of the base paper. The higher noise and eavesdropping degraded the performance of key negotiation, which lowered the SKR, underscoring the system's vulnerability at high QBER values. Higher Signal-to-Noise Ratio(SNR) had low error rates and higher SKR implying the practical usability of such a system.

Chapter 1

Introduction

1.1 Background and Motivation

With the rapid development in quantum computing, it is apparent that most of the currently deployed cryptographic systems—very prominent ones like RSA and Elliptic Curve Cryptography—will soon be rendered obsolete. Quantum computers could solve some problems previously considered intractable, for example, factoring large numbers or computing discrete logarithms, using algorithms such as Shor’s Algorithm[2]. This capability threatens to undermine the security bases of classical cryptographic systems. As quantum computing continues to develop, Governments, industries, and research communities are increasingly focusing on quantum-resistant solutions to safeguard sensitive data against potential future quantum threats.

In this respect, Quantum Cryptography is one of the most promising fields for ensuring long-term security. Unlike classical cryptography, whose security relies on the hardness of mathematical problems, QKD offers information-theoretic security—that is, security based on the laws of quantum mechanics. This makes QKD systems resistant to attacks by both quantum and classical adversaries[3]. The no-cloning theorem is one of the fundamental principles guaranteeing the security of a QKD system: it claims that it is impossible to make an identical copy of an arbitrary unknown quantum state[4]. So, this guarantees that any eavesdropper (Eve) trying to interfere with any quantum communication will necessarily introduce noise in the communication, which can easily be detected by the parties, usually referred to as Alice and Bob.

The work by Bennett and Brassard, the BB84 protocol, was one of the seminal works in the area marking the birth of practical QKD. In BB84, Alice uses a quantum channel to send polarized photons to Bob. Bob measures the incoming photons in one of two randomly chosen bases, rectilinear or diagonal. Then Alice and Bob publicly compare their measurement bases to establish a shared secret key. In this way, any attempted eavesdropping during transmission will introduce detectable errors that make the key exchange secure[5].

Since the introduction of BB84, numerous other QKD protocols have been suggested, among which is the E91, based on entanglement-based key distribution[6], and Continuous Variable QKD(CV-QKD), in which continuous quantum states take the place of discrete polarization states, for example, light quadratures[7]. As secure communications systems embark on their journey into the post-quantum future, QKD holds the promise of revolutionizing sensitive data protection. However, integrating QKD into the existing infrastructures of communication, especially into large-scale networks like ODCN, is highly challenging[8][9]. The research addresses the design and implementation of resource allocation strategies that enable the efficient and resilient deployment of QKD in ODCNs.

1.2 Quantum Key Distribution and Its Role in Network Security

QKD allows two parties to establish a shared secret key that can be used for encryption, guaranteeing unconditional security as long as the protocol is properly implemented. This is in stark contrast to classical key exchange protocols, which are vulnerable to advances in computing power and algorithmic breakthroughs. The potential impact of QKD is especially significant in industries that handle highly sensitive data, such as finance, defense, healthcare, and government sectors. As these industries transition to quantum-safe solutions, there is a growing need to integrate QKD into the broader communication infrastructure, particularly ODCN.

ODCNs are the backbone of modern data communication systems. They connect servers and storage devices across large geographical distances, enabling fast and reliable data exchange. As data centers become increasingly central to global information processing, ensuring the security of the data traveling across these networks becomes a critical concern. QKD offers a powerful solution to this challenge by enabling secure key exchange over optical fiber networks. The ability of QKD to detect eavesdropping and prevent key compromise makes it an attractive choice for securing communication links in ODCNs.

However, integrating QKD into existing optical networks is not without challenges. One of the primary issues is resource allocation—specifically, how to efficiently allocate wavelengths, time slots, and network bandwidth in a way that optimally balances both security and performance. In classical optical networks, resource allocation strategies are well-developed, primarily aiming to maximize bandwidth utilization and minimize latency. However, the unique requirements of QKD—such as the need for secure quantum channels, high SKR, and low QBER—introduce new constraints that must be addressed to ensure that QKD-enabled optical networks are both efficient and resilient.[10][11]

In addition, QKD systems are affected by environmental factors, such as noise in the communication channel, signal loss, and the distance between network nodes[8]. As the communication distance increases, the rate of photon loss rises, which in turn reduces the SKR and increases the QBER. Error correction and privacy amplification techniques address these challenges by ensuring key integrity and minimizing any partial information accessible to potential eavesdroppers[12][13]. However, implementing these techniques in large-scale optical networks, where data must be transmitted over long distances, requires careful optimization to balance security and performance.

QKD can be classified into two main types: Prepare-and-Measure (P&M) QKD and Entanglement-Based QKD.

Prepare-and-Measure QKD: In this method, as used in the BB84 protocol, Alice prepares and sends quantum states (photons) in specific bases to Bob, who measures them. The security of this system relies on the fact that quantum states cannot be precisely measured or copied due to fundamental quantum mechanical principles. Any attempt to intercept the qubits will result in errors that can be detected, allowing Alice and Bob to discard the compromised key bits.[4][3]

Entanglement-Based QKD: This method, as seen in the E91[6] protocol, relies on the phenomenon of quantum entanglement, where two particles remain correlated regardless of the distance between them. If one particle is measured, the state of the other is immediately known. In this type of QKD, Alice and Bob share entangled particles, and the security is ensured by testing for Bell's inequality violations, which confirms that the system hasn't been tampered with by an eavesdropper.

The BB84 protocol operates as a P&M system, where the qubits are sent through a quantum channel and measured by the receiver in randomly chosen bases. The protocol's security is based on two key quantum principles:

Heisenberg's Uncertainty Principle: This principle asserts that it is impossible to precisely measure both the position and momentum (or any pair of conjugate variables) of a particle simultaneously[14]. In QKD, this means that an eavesdropper (Eve) cannot measure the quantum state of a photon without introducing disturbances. Any attempt by Eve to measure the qubits being transmitted will result in detectable changes in the state, thus increasing the QBER.

The No-Cloning Theorem: According to this theorem, it is impossible to create an exact copy of an unknown quantum state[4]. This prevents Eve from duplicating the quantum information and measuring it later without affecting the original transmission. As a result, any interception attempt will inevitably alter the quantum states and introduce detectable errors in the shared key.

1.3 Challenges in Quantum Key Distribution Systems

While QKD provides an unprecedented level of security, its practical deployment faces several challenges that must be overcome to achieve widespread adoption. These challenges include:

Integration with Classical Networks: One of the major challenges in deploying QKD in real-world networks is ensuring its coexistence with classical communication systems. In Wavelength Division Multiplexing (WDM) optical networks, where multiple data streams share the same fiber optic infrastructure, it is essential to manage the interference between classical and quantum channels. Classical data can introduce noise into the quantum channel, degrading the quality of the quantum key and increasing the QBER. To mitigate these issues, researchers are exploring hybrid architectures that allow QKD to operate alongside classical data without compromising the security of the quantum key[8].

Resource Allocation in QKD Networks: Efficient resource allocation is crucial to the performance of QKD-enabled networks, particularly in large-scale environments like ODCNs. Resource allocation in QKD networks involves managing both quantum and classical resources, including wavelengths, time slots, and bandwidth[15]. Traditional resource allocation techniques are not well-suited to the probabilistic nature of quantum key generation, which requires new models and algorithms to optimize the allocation of quantum resources[9]. This research explores adaptive resource allocation strategies, such as the Adaptive Strong Security Level(ASSL) and Adaptive Weak Security Level(AWSL) models, to ensure that the available resources are used efficiently while maintaining high security levels(SLs)[16].

System Resilience and Error Correction: QKD systems are susceptible to various types of errors, including errors introduced by environmental factors, such as signal attenuation and channel noise, as well as errors caused by eavesdropping attempts[8]. Error correction techniques, such as Hamming codes and Low-Density Parity-Check (LDPC) codes[13], are employed to detect and correct these errors, ensuring the integrity of the final shared key. Additionally, privacy amplification is used to reduce any partial information that may have been leaked to an eavesdropper. This work investigates the performance of these error correction techniques in QKD-enabled optical networks and evaluates their impact on key generation efficiency and security.[12]

Scalability and Performance: As QKD is integrated into larger networks, such as ODCNs,

scalability becomes a critical issue. QKD protocols must be capable of operating over long distances and across multiple nodes without significant degradation in performance. Scalability challenges include managing the increased complexity of resource allocation in multi-node networks, optimizing key distribution across geographically dispersed data centers, and ensuring that the QKD system can handle high data traffic without compromising security. The NSFNET topology is used in this research to simulate large-scale optical networks and evaluate the scalability of QKD systems under various network loads and configurations[17].

In addition to the practical challenges of implementing QKD in optical networks, QKD systems, particularly those based on the BB84 protocol, are vulnerable to several types of attack strategies. These attack strategies are designed to exploit weaknesses in the system's implementation rather than in the quantum mechanics underlying the protocol. The most common attack types in QKD systems include:

Intercept-Resend Attack: In this type of attack, Eve intercepts the qubits sent by Alice, measures them in a random basis, and resends a new set of qubits to Bob. Due to the Heisenberg Uncertainty Principle, Eve's measurements will introduce errors into the system. If Alice and Bob detect an unusually high QBER, they will know that an eavesdropper is present.[18]

Photon Number Splitting Attack: In BB84, if Alice uses a weak laser pulse rather than true single-photon sources, multiple photons may be transmitted in the same pulse. Eve can intercept one photon, measure it, and allow the remaining photons to pass through to Bob undetected. This attack can be mitigated by using decoy states, which are randomly inserted weaker pulses that allow Alice and Bob to detect whether Eve is performing a Photon Number Splitting(PNS) attack[19].

Man-in-the-Middle Attack: In this scenario, Eve positions herself between Alice and Bob, intercepting and manipulating the communication between them. While quantum principles ensure that Eve cannot eavesdrop without being detected, a man-in-the-middle attack is still a practical concern if the initial authentication between Alice and Bob is not properly secured.

By employing error correction (e.g., Cascade or Hamming codes) and privacy amplification (e.g., SHA-256 or SHA3-256), Alice and Bob can mitigate the impact of any information Eve might have gleaned during the transmission. Privacy amplification reduces the shared key's length while ensuring that Eve's knowledge of the final key is minimized to a negligible level.[20][21]

Another critical aspect of QKD security is its relationship with Shannon Entropy, a measure of the uncertainty or randomness in the system. The effectiveness of privacy amplification and error correction techniques relies on reducing Eve's knowledge about the shared key to below a threshold where it becomes statistically negligible. Shannon's entropy is key to calculating how much information needs to be discarded during these processes to ensure a secure key. In QKD, the entropy of the final key is used to estimate the amount of information Eve could have obtained during the transmission, guiding the privacy amplification process to secure the final key.[22]

1.4 Research Objectives

The overarching goal of this thesis is to explore the integration of QKD into ODCN, with a particular focus on resource allocation and system resilience. The specific research objectives include:

Objective 1: To study the resource allocation strategies that optimize the distribution of

quantum keys in QKD-enabled ODCNs. This involves simulating adaptive SL models, such as ASSL and AWSL, and evaluating their performance under various network conditions.

Objective 2: To investigate the impact of error correction and privacy amplification techniques on the efficiency and security of QKD systems. This includes evaluating the performance of SHA-256 and SHA3-256 hashing algorithms for privacy amplification and assessing the effectiveness of error correction methods, such as Hamming codes and Cascade protocols, in reducing the QBER.

Objective 3: To analyze the scalability and performance of QKD systems in large-scale optical networks. The NSFNET topology will be used to simulate multi-node networks, and key performance metrics such as SRCR, TUR, NSP, and SKR will be evaluated.

Chapter 2

Literature Review

2.1 Quantum Key Distribution Protocols

The development of QKD has revolutionized secure communication by leveraging the principles of quantum mechanics to create a secure method of key exchange. Introduced by Bennett and Brassard in 1984, the foundational BB84 QKD protocol leverages quantum properties of photons, such as polarization and superposition, to securely transmit information[5]. Its security is underpinned by the no-cloning theorem and Heisenberg’s uncertainty principle, which ensure that any attempt to eavesdrop introduces detectable disturbances in the transmission.

While BB84 remains the most widely adopted protocol, other protocols have evolved to tackle specific challenges. E91, based on quantum entanglement, offers higher SLs through shared entangled states between communicating parties[6]. Meanwhile, CV-QKD allows the use of continuous quantum states, such as the amplitude and phase of light [7], making it compatible with existing telecommunications infrastructure [23]. While these protocols offer theoretical security[3], their practical implementation is often limited by environmental factors and the need for resource-efficient allocation, particularly in large-scale networks like ODCN[9][8].

In the context of this project, the BB84 protocol forms the basis of the established quantum key protocol. The fully classical and hybrid models implemented extend this framework by simulating the process of key exchange, error introduction (through noise and external eavesdroppers), and error correction to ensure key integrity. The approach is crucial for determining the resilience of QKD in practical, noisy environments, which is a major challenge in large-scale networks like ODCNs.

2.2 Resource Allocation in QKD Networks

As QKD moves towards practical implementation in large-scale optical networks, efficient resource allocation has become a critical challenge. The integration of QKD into optical networks, particularly in WDM environments, requires the careful management of resources such as time slots and wavelengths to balance security and performance[10][15]. Efficient resource allocation ensures that quantum keys are distributed securely while minimizing delays and optimizing network throughput. In ODCNs, which support both classical and quantum traffic, effective resource allocation must account for the dynamic nature of quantum key generation, security requirements, and traffic loads.

One commonly referenced approach is Priority Queuing with SLs (PQSL), which prioritizes Connection Requests(CRs) based on their security requirements and dynamically allocates resources to optimize QKD[24].

Recent studies have focused on dynamic resource allocation strategies that adapt to varying security requirements and network loads[11][25][10]. For instance, [26] proposed a Routing and Wavelength Allocation(RWA) model for QKD-enabled optical networks, which dynamically adjusts resource allocation based on CRs and available quantum keys[25]. However, despite these advances, many current models do not fully address the scalability of QKD in large, multi-node environments, particularly in multi-core optical fiber networks.

In this project, the focus is not primarily on the design of the ODCN but rather on the quantum key protocol within the simulated network. However, resource allocation still plays a key role in determining how quantum keys are distributed across the ODCN, and the challenge is compounded by the presence of noise and external eavesdroppers. As the models incorporate error introduction and error correction, they provide insights into how the network manages and compensates for degraded key integrity.

2.3 Error Correction and Noise Management in QKD

While QKD systems are theoretically secure, practical implementations often face challenges from environmental factors and adversarial attacks[8]. Environmental noise, signal attenuation, and distance limitations can significantly degrade the SKR and increase the QBER. These challenges are particularly pronounced in free-space optical communication, where factors like atmospheric conditions and distance further limit system performance[15].

Moreover, QKD systems are vulnerable to side-channel attacks, which exploit imperfections in hardware rather than the quantum protocol itself[27] [18]. To mitigate these vulnerabilities, error correction techniques such as Hamming codes and Low-Density Parity-Check (LDPC) codes have been employed to improve the resilience of QKD networks[13]. Additionally, secret key recovery strategies [28] have been proposed to enhance the fault tolerance of QKD systems in optical networks [12][29] [30].

In this work, two error correction methods are employed:

- **Hamming Code:** This method focuses on single-bit error correction, providing a lightweight and efficient way to manage errors in the quantum key transmission process. Hamming code is well-suited for environments where error rates are low but present, offering a balance between performance and security.
- **Cascade Protocol:** The Cascade protocol is a more robust method for error correction in QKD systems. It performs iterative reconciliation between Alice and Bob's key bits, correcting multiple errors through a multi-pass process. This protocol is particularly useful in scenarios where error rates are higher, such as when noise is introduced by an eavesdropper.

2.4 System Resilience and External Eavesdroppers

An important aspect of this work is the simulation of an adversarial environment where an external eavesdropper (Eve) introduces errors into the system

In the fully classical model, noise and encoding are simulated classically, while in the hybrid model, encoding and noise addition are handled through Qiskit[31], a quantum computing framework. This allows for the simulation of a more realistic quantum communication scenario, where quantum-specific errors are introduced and corrected using quantum-native methods.

The presence of an eavesdropper is simulated by introducing discrepancies in the key bits received by Bob, which can be detected through an increase in QBER. Detecting and managing these errors is crucial for ensuring the integrity of the quantum key, particularly in the hybrid model where quantum error sources are more accurately simulated.

2.5 Gaps in the Literature

Despite advances in QKD research, several gaps remain, particularly concerning error correction and noise management in large-scale networks like ODCNs. Existing research often fails to address how noise, eavesdropping, and resource allocation interact to affect the overall performance of the quantum key protocol. Additionally, while error correction methods such as LDPC codes have shown promise, their complexity makes them less suited for practical implementation in environments with real-time constraints.

- **Scalability in Large Networks:** Although effective in smaller networks, current resource allocation strategies face scalability challenges in multi-node or multi-core environments. There is limited research on optimizing QKD in ODCN, where multiple CRs and varying SLs must be managed simultaneously[1].
- **Integration with Classical Networks:** The coexistence of QKD and classical communication within the same optical network infrastructure presents challenges, particularly in balancing SNRs and mitigating the impact of classical signals on quantum key transmission[32]. Further research is needed to develop hybrid systems that can efficiently allocate resources for both classical and quantum channels.
- **Resilience to Environmental Factors:** While error correction techniques have been developed, they often fail to fully address the impact of extreme environmental conditions, such as atmospheric disturbances in free-space QKD or fiber loss in long-distance optical networks. Improved models that take these real-world challenges into account are necessary to enhance system resilience. [33]

2.6 Conclusion and Research Direction

The section has outlined the evolution of QKD protocols, resource allocation strategies, and the resilience of QKD systems in practical settings. While significant advancements have been made, there remain critical gaps in the research, particularly in the areas of scalability, integration with classical networks, and resilience to environmental factors. This work aims to study these gaps, focusing on efficient resource allocation in QKD-enabled ODCN, with a specific emphasis on balancing security and performance across multiple nodes and CRs.

This work contributes to this body of research by:

- Simulating both classical and hybrid models to understand the impact of noise and eavesdropping on key distribution.
- Implementing error correction through Hamming and Cascade protocols, considering a practical approach to managing errors in noisy environments.
- Establishing a quantum key protocol within a simulated ODCN, exploring how these protocols interact with network design to ensure secure communication even in the presence of adversarial threats.

Chapter 3

Methodology

3.1 Simulation Overview

The objective is to optimize network performance while ensuring secure communication using QKD protocols.

Key tasks include:

- Simulating CRs across network nodes with different SLs.
- Implementing the BB84 protocol, with classical error correction, for quantum key exchange.
- Measuring key metrics such as QBER, SKR, and system performance under varying SNR conditions.
- The results are analyzed to determine the performance of resource allocation strategies in QKD-enabled ODCNs.

This was coded in two parts: 1) RA-ODCN 2) QKD-BB84

3.2 Network Architecture and Simulation Environment

3.2.1 Network Topology

Figure 3.1 shows the NSFNET topology used in this simulation, featuring 14 optical nodes, 21 bidirectional fiber links, and 30 available time slots per unidirectional link. The ODCN allows the simultaneous transmission of classical and quantum data, where classical data channels use WDM and quantum keys are transmitted through dedicated quantum channels.

ODCN: The network simulates multiple CRs, each involving source and destination pairs for data transmission. For each request, quantum keys are generated using the BB84 protocol, while data is transmitted via classical channels encrypted with those keys as shown in Figure 3.2.

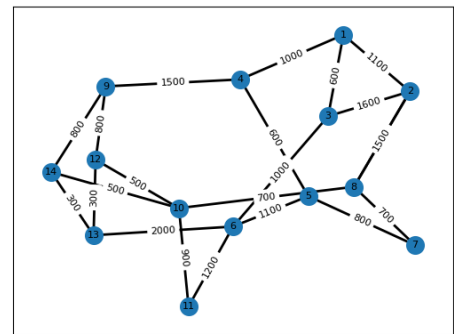


Figure 3.1: NSFNET Topology: 14 Nodes, 21 Bi-directional Links

3.2.2 QKD Protocols and Quantum Channel Simulation

The BB84 protocol is used for secure quantum key exchange. In this implementation:

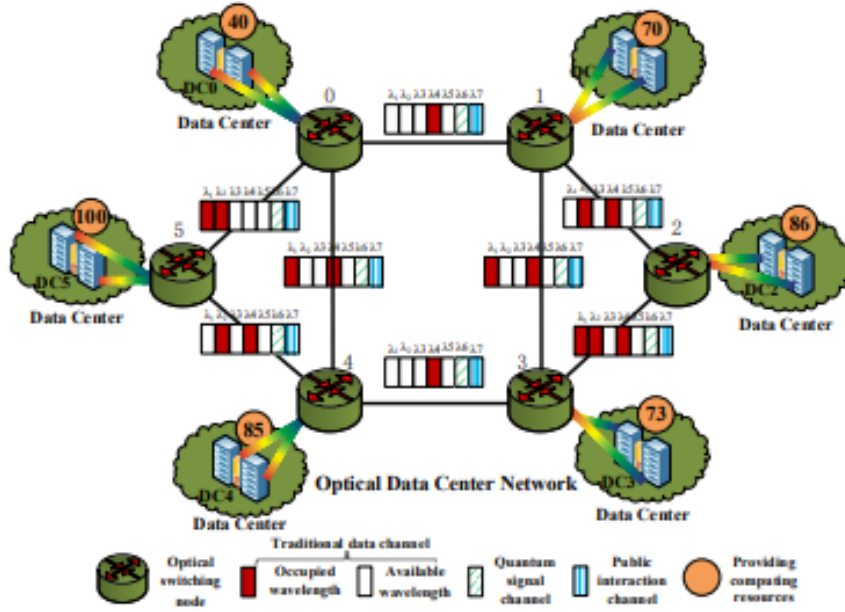


Figure 3.2: The architecture of a QKD Optical Network [1]

- **Photon Transmission:** Alice transmits randomly polarized photons—horizontal, vertical, or at 45° and 135° diagonals—to Bob via quantum channels.
- **Basis Comparison:** Bob randomly chooses measurement bases for each photon, and after transmission, Alice and Bob compare their bases over a public channel to generate the shared secret key.
- **Error Correction:** Error correction is performed using the Hamming code to address errors due to noise in the quantum channel.
- **Privacy Amplification:** After error correction, SHA-256 and SHA3-256 are applied to shorten the key and secure it from partial eavesdropping.

The performance of the QKD system is analyzed based on the QBER, which quantifies the error rate in the key transmission.

3.3 Routing and Resource Allocation Algorithms

3.3.1 Routing, Wavelength, and Time-Slot Assignment

To efficiently allocate network resources (wavelengths and time slots), routing is handled using the k-Shortest Path (k-SP) Algorithm, which calculates multiple viable routes for each CR. The selected paths ensure redundancy in case of network congestion or failure.

- **Wavelength Reservation:** Each CR is assigned a consistent traditional wavelength, as well as a special wavelength on the quantum signal channel across its transmission path, based on the SL requested.
- **Time-Slot Allocation:** Time slots are assigned in the wavelength corresponding to the SL of each CR. Higher security CRs are allotted time-slots in the wavelengths with rapid key change, ensuring synchronization between the quantum key generation and data transmission is more secure.

Time-slot allocation is subject to the constraints of continuity and consecutivity, i.e.

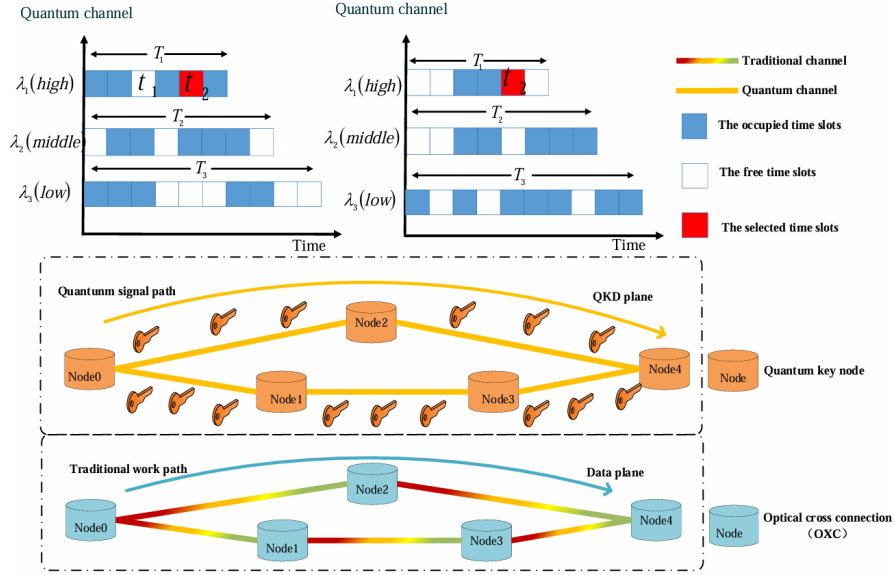


Figure 3.3: Illustration of quantum key resource allocation in QKD network

the allotted time slots must be a continuous section of required slots, and time-slot(s) at the same index must be allocated throughout the path.

Performance metrics such as the SRCR, the TUR, and the NSP are calculated to evaluate the efficiency of resource allocation which is depicted in Figure 3.3.

3.3.2 Simulated Metrics

The following performance metrics are used to evaluate the QKD network:

- **QBER:** This is calculated as the proportion of incorrectly measured bits in Bob's key compared to Alice's original key. In practice, a small fraction of sifted bits is publicly announced for Alice and Bob to gauge the error rate in that part and is then extrapolated to the entire key (Spotting).
- **SKR:** The number of secure bits exchanged per second after error correction and privacy amplification. Also represented by secure bit rate.
- **Time Taken:** Total time taken, on an average, for each iteration of the SNR range.

Monte Carlo simulations are used to generate multiple scenarios with varying CRs and SLs.

3.4 Calculations, Techniques, and Tools

3.4.1 Quantum Bit Error Rate Calculation

QBER is a critical performance metric for evaluating the security of the QKD system. It is calculated as:

$$QBER = \frac{\text{Error Count}}{\text{Total Bits}} \quad (3.1)$$

The QBER increases as the SNR decreases due to increased noise in the quantum channel in accordance with equation:

$$SNR(dB) = 10 * \log_{10}(SNR_{linear}) \quad (3.2)$$

$$BER = \frac{1}{2 * SNR_{linear}} \quad (3.3)$$

The noise was simulated by applying bit-flip/phase-flip operators with a certain probability based on the given SNR(related to noise). It is equivalent to varying the distance between nodes and applying attenuation factors to the quantum signal.

For the frequency of 1310 MHz and 1383 MHz, the attenuation factors(α) are roughly 0.34 ± 0.05 dB/km and 0.5 ± 0.05 dB/km, respectively. [34]

3.4.2 Secure Key Rate

The SKR represents the final number of secure bits available for encryption after error correction and privacy amplification. The SKR is plotted against SNR(dB) for different network conditions, showing how the signal strength and error correction affect the key generation rate.

3.4.3 Software Environment

The simulations were performed using Python, with the following libraries:

- *NumPy*: For mathematical operations.
- *SciPy*: For statistical computations.
- *Matplotlib*: For plotting results, such as QBER vs. SNR and SKR vs. SNR.
- *Qiskit*: To simulate Quantum states.
- *NetworkX*: To create Network Topologies.
- Custom Classes: Quantum key handling and networking were implemented through custom classes to simulate the BB84 protocol and error correction methods.

3.5 Assumptions, Limitations, and Range of Validity

3.5.1 Assumptions

Several key assumptions are made:

- **Static Network Topology**: The NSFNET topology remains static, without considering node failures or dynamic routing.
- **Ideal Quantum Channels**: The channels assume distance-based attenuation, but real-world fiber imperfections and other environmental factors are simplified by taking Additive White Gaussian noise(AWGN).
- **Error Models**: The quantum channel noise is modeled based on distance-dependent SNR and AWGN, with no consideration of additional physical disruptions like temperature fluctuations or hardware imperfections.

3.5.2 Limitations

- **Resource Scalability**: While the methods work well for small/medium-scale networks, scaling to larger networks might introduce new performance bottlenecks.

- **Advanced Attacks:** The simulation focuses on basic intercept-resend attack models (Eve's eavesdropping) and does not incorporate advanced side-channel or Trojan-horse attacks.

3.5.3 Range of Validity

The simulation is valid for small to medium-scale optical networks with distances of about 100 km between nodes. Extending this to larger distances may require additional noise handling techniques and higher-power quantum channels, as well as the use of Trusted Repeater Nodes (TRNs).

3.6 Analytical Methods

The results were analyzed using statistical methods, including:

- **Monte Carlo Simulations:** These were used to generate random CRs with varying security requirements to test the system under different load conditions. The BB84 protocol, including key generation till privacy amplification, also utilized the Monte-Carlo method to get statistically sound data.
- **Plotting:** *Matplotlib* was used to generate key performance plots, such as QBER vs. SNR, time-taken vs. SNR and SKR vs. SNR for the QKD part and SRCR/TUR/NSP vs. Number of CRs for the ODCN part.

Chapter 4

System Model

4.1 Overview of the System Architecture

The system under study is designed to explore QKD within a simulated ODCN, where both classical and quantum traffic are routed. The main objective is to establish a secure key negotiation protocol in a large-scale optical network capable of handling noise and eavesdropping attempts.

The SNR decreases with the distance of optical fiber travelled; signal strengths are simulated for every kilometer of fiber traversed and the same is represented by the SNR range incorporated at a frequency of 1383 MHz: at this frequency the attenuation constant has a value of 0.5 dB/km[34].

Noise is modelled in two ways:

- **Fully Classical Simulation (Model):** All processes, including encoding, noise introduction, and error correction, are simulated classically.
- **Hybrid Simulation (Model):** Encoding and noise introduction are handled using Qiskit, while error correction and other classical processes remain the same.

Both models aim to simulate the errors inflicted by the fiber during secure quantum key negotiation. Error correction is implemented in the presence of noise and adversaries.

A fully quantum simulation (Model) is also considered, but is not extensively simulated due to resource limitations.

4.2 ODCN Design

The ODCN design is adopted from the base paper[16] to simulate realistic network topology, traffic, and CRs. The network consists of:

- **Optical Switching Nodes:** These nodes route both quantum and classical traffic.
- **Quantum Signal Channels (QSC):** Dedicated wavelengths in the fiber-optic links used exclusively for QKD.
- **Traditional Data Channels (TDC):** Traditional WDM channels used for transmitting encrypted data.
- **Public Interaction Channels (PIC):** These channels are used for key negotiation, public comparison of bases, and error correction communication.

The network is designed to handle multiple CRs between various nodes, each with a specified SL.

The goal is to allocate resources—wavelengths, time slots, and quantum keys—efficiently while maintaining the security of the communication through QKD.

4.3 QKD Protocols

The BB84 protocol is employed for quantum key exchange in both models. The key generation follows the standard BB84 steps, where Alice (the sender) prepares photons in one of four polarization states (horizontal, vertical, 45° , or 135°), and Bob (the receiver) randomly chooses a basis to measure them. After transmission, Alice and Bob compare their bases via the PIC to derive the shared secret key. Alternatively, E91 protocol is explored briefly.

In the hybrid model, the photon preparation, transmission, and measurement are simulated using Qiskit, allowing for the inclusion of errors by calculating the probabilities and applying the pauli-X and pauli-Z gate. In the fully classical model, these steps are simulated through classical means, with noise and interference introduced artificially.

4.4 Noise and Eavesdropping Simulation

One of the primary goals of this project is to simulate the impact of noise and eavesdropping on the QKD process. The system introduces noise during the key negotiation phase to simulate real-world environmental factors, such as signal attenuation, fiber loss, and quantum noise. Additionally, an eavesdropper (Eve) is simulated to measure the robustness of the protocol against adversarial attacks.

- **Noise Model:** Noise is added (according to the equation 3.3) during the quantum transmission phase. In the classical model, noise is introduced manually by flipping a fraction of the bits transmitted from Alice to Bob. In the hybrid model, noise is introduced using Qiskit's Pauli operators (x -gate to mimic bit-flip error, and z -gate to mimic phase-flip error). Additionally, a fully quantum model is briefly explored, which simulates real-world quantum channel noise (e.g., depolarizing noise, phase damping) with the help of Qiskit's quantum noise model, and runs on a real quantum computer provided by IBM.
- **Eavesdropper Simulation:** Eve is modeled as an intercept-resend attacker. She intercepts the quantum transmission, measures the quantum states, and then forwards them to Bob, potentially altering the key. The presence of Eve introduces errors in the key and raises the QBER, which Alice and Bob use to detect the eavesdropping attempt.

4.5 Error Correction Methods

To handle the errors introduced by noise and eavesdropping, two error correction methods are implemented in the system:

- **Hamming Code:** This method is used in both models to correct single-bit errors in the transmitted key. The Hamming code is lightweight and suitable for scenarios where the error rate is low. However, it is prone to misidentifying an odd number of errors (greater than 1) as 1; hence introducing more errors while trying to correct it. [20]
- **Cascade Protocol:** This protocol is employed for multi-pass error correction, iteratively correcting errors over several rounds of communication between Alice and Bob. The Cascade

protocol is robust against higher error rates, making it more suitable for situations where the noise or eavesdropper's interference is significant. [21]

4.6 Routing and Resource Allocation in the ODCN

The resource allocation process within the ODCN involves the efficient distribution of wavelengths and time slots across multiple nodes and CRs. For each CR, resources are dynamically allocated based on security requirements and network load. Two key aspects are considered in the allocation:

- **Wavelength Assignment:** Each CR is assigned a dedicated (special) wavelength to ensure optimal security and avoid collisions with classical traffic.
- **Time-Slot Assignment:** Time slots are allocated continuously and sequentially to maintain the synchronization between the quantum key exchange and data transmission.

The system uses a Routing, Wavelength, and Time-slot Assignment (RWTA) algorithm to balance the needs of multiple CRs and optimize key distribution across the network. The k-SP Algorithm is used for routing, ensuring that redundant paths are available for each CR in case of network congestion or link failure.

4.7 Performance Metrics

The performance of the system is evaluated based on the following metrics:

- **QBER:** This metric measures the proportion of bits that are incorrect in Bob's key compared to Alice's original key. Higher QBER indicates the presence of noise or eavesdropping.
- **SKR:** This is the rate at which secure bits are exchanged between Alice and Bob after error correction and privacy amplification. It provides an indication of the system's efficiency under noisy conditions.
- **Key Distillation Time:** This metric tracks the time taken to generate and exchange a secure key between Alice and Bob, taking into account the time required for transmission, basis comparison, error correction, and privacy amplification.
- **Classical Bit Error Rate (BER):** Measures the error rate of classical bits in the system, particularly in the presence of noise or eavesdroppers. In cases where Eve is present, the classical BER rises to approximately 0.375.
- **SRCR:** This measures the proportion of successful CRs in the network, taking into account both quantum and classical traffic.
- **TUR:** This measures the proportion of allocated time slots (of special quantum wavelengths) to the total available time slots in the network.
- **NSP:** Tracks the total security points(chosen 1, 2, and 3 for low, medium, and high SL respectively), for CRs that were successfully provisioned with resources.

Chapter 5

Results

5.1 Overview of Results

The results obtained from the simulations provide insight into the performance of both the Fully Classical Model and the Hybrid Model (as well as the Quantum Model, albeit to a limited extent) under varying conditions of noise and eavesdropping. The key metrics analyzed are QBER, Classical BER, SKR/SBR (Secure Bit Rate, expressed either as the number of bits or the ratio of final to initial key length), and resource allocation efficiency within the ODCN. Each metric reveals critical information about the robustness and scalability of the quantum key negotiation protocols.

The efficiency within ODCN is studied by three metrics—SRCR, TUR, and NSP. There are three kinds of QBERs studied in this work:

- **Meta QBER:** This represents the QBER averaged over all the keys after sifting. This quantity will not be available in real-time—hence the prefix 'meta'. Simulation provides the luxury of accessing this information.
- **Spot QBER:** This refers to the QBER calculated by the process of spotting, that is, sampling a fraction (spotting fraction) of bits of each sifted key and calculating the QBER based on that. This quantity is experimentally available, and is the deciding factor for whether to keep the keys or not—based on the established QBER threshold.
- **Corrected QBER:** This, again, is a quantity that will not be available in real-time and is a luxury offered by the method of simulation. Here, the QBER of the keys which have been accepted (after error correction, with a QBER below the threshold) just after sifting, and before spotting, is calculated. This provides us with an idea of the error pattern of the keys which can be corrected up to a certain threshold in an environment with a certain SNR.

To ensure a comprehensive understanding, most set of results are discussed in relation to SNR, the presence of an eavesdropper, and the performance of the Hamming and Cascade error correction methods.

5.2 Hybrid Model

In figure 5.1, *QBER-All Keys* is equivalent to 'Meta-QBER', *BER-All Keys* is the error rate of all the keys (after correction and decision), *QBER-corrected keys* is equivalent to 'Corrected-QBER'. *BER-corrected keys* is the error rate of the keys (after correction) that are kept.

One-thousand Monte-Carlo cycles were implemented to obtain this curve. A trend of QBER/BER

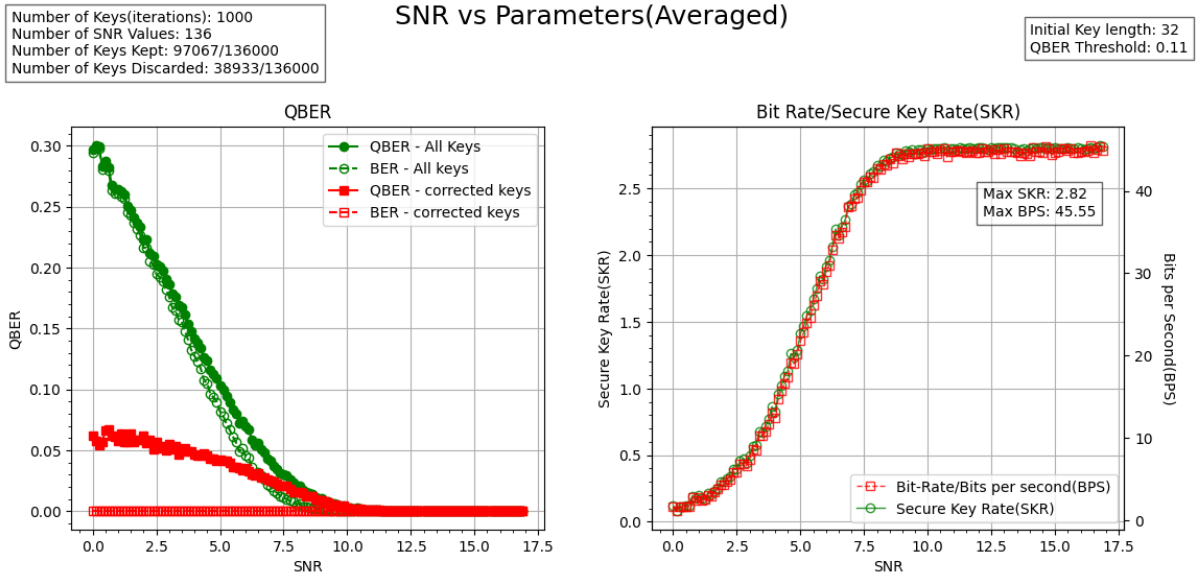


Figure 5.1: Left: QBER vs SNR. Right: SKR/SBR vs SNR.

approaching 0 as SNR increases is observed. The slight difference seen between 'QBER-All Keys' and 'BER-All Keys' indicates the rejection of keys with excessive errors and acceptance of those with relatively less errors.

'QBER-Corrected Keys' can be seen converging to 0 as well, however, it has non-zero values initially—implying effective error-correction.

The plot on the right side in figure 5.1 demonstrates that the SKR and SBR are perfectly correlated as is expected for the case with fixed initial key lengths.

Figure 5.2 shows the behaviour at low iterations. The plot indicates similar behaviour, however it is not conclusive. Upon increasing the number of which later converge into what is shown in figure 5.1. It can clearly be seen that the error rate is practically 0 for the keys that have been corrected.

The curve for *QBER-corrected Keys* reflects the fact that the keys that were chosen to be corrected had low QBER initially, compared to the other keys. Eventually all the plots converge to 0.

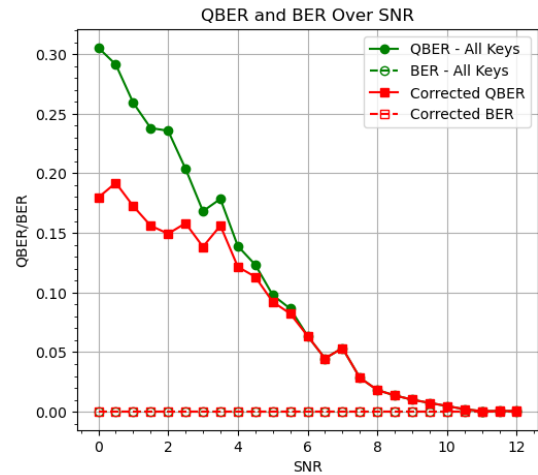


Figure 5.2: QBER vs SNR for 10 iterations

Variation with input length

The plots in figure 5.3 are plotted against the length of the input/raw key. The channel noise considered here is direct instead of SNR—noise = 0.03 representing a 3% probability of error. The threshold for declaring Eve's presence is set slightly higher to allow for more error-correcting opportunities to the error-correction techniques implemented.

The length of the distilled key(output key) scales linearly with the length of the raw key.

The increasing length also implies increasing time to process each key; hence the time taken increases and SKR decreases.

The QBER, however, remains roughly the same (at around 0.27), as there is no change in the external noise and/or the signal strength. Also to note, the spread in the QBER gets more and more streamlined as the input length increases; this is due to the fact that a larger key length allows less and less contribution by a single bit in the overall change.

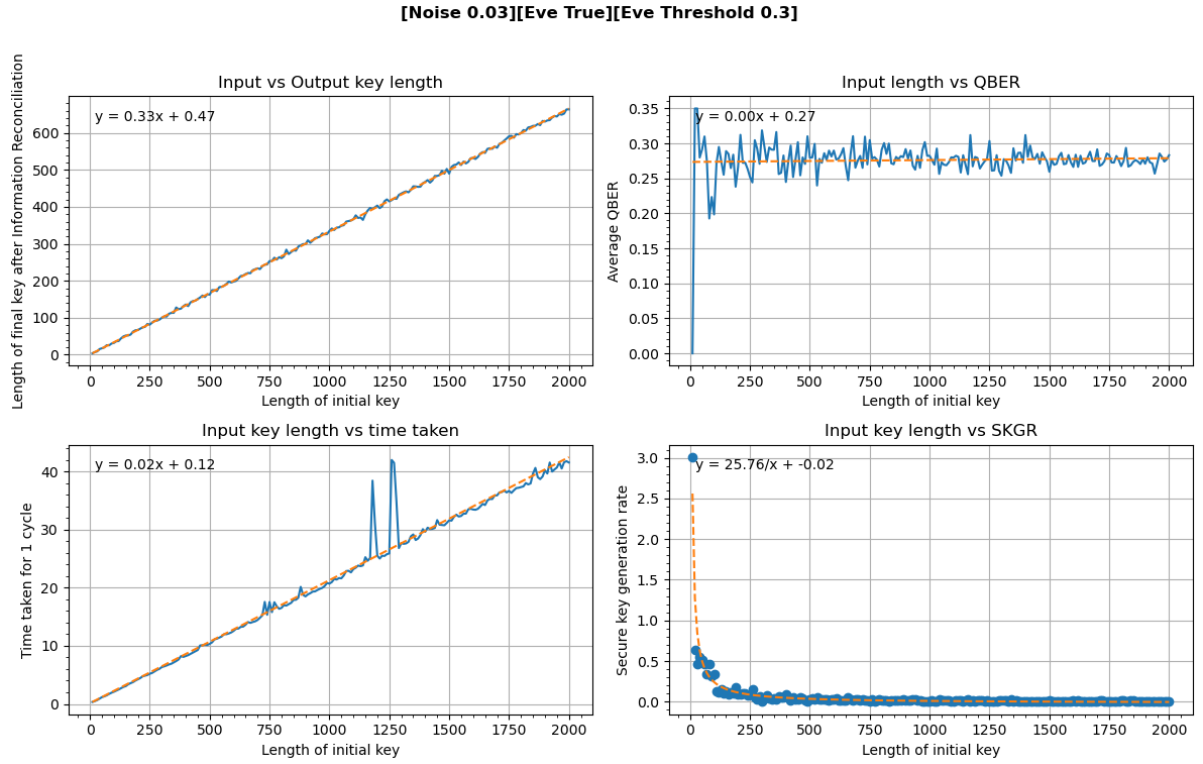


Figure 5.3: Input Length vs Length(top-left), Qber(top-right), Time-Taken(bottom-left), SKR(bottom-right). Eve Present. Noise = 0.03

5.3 Fully Quantum Model

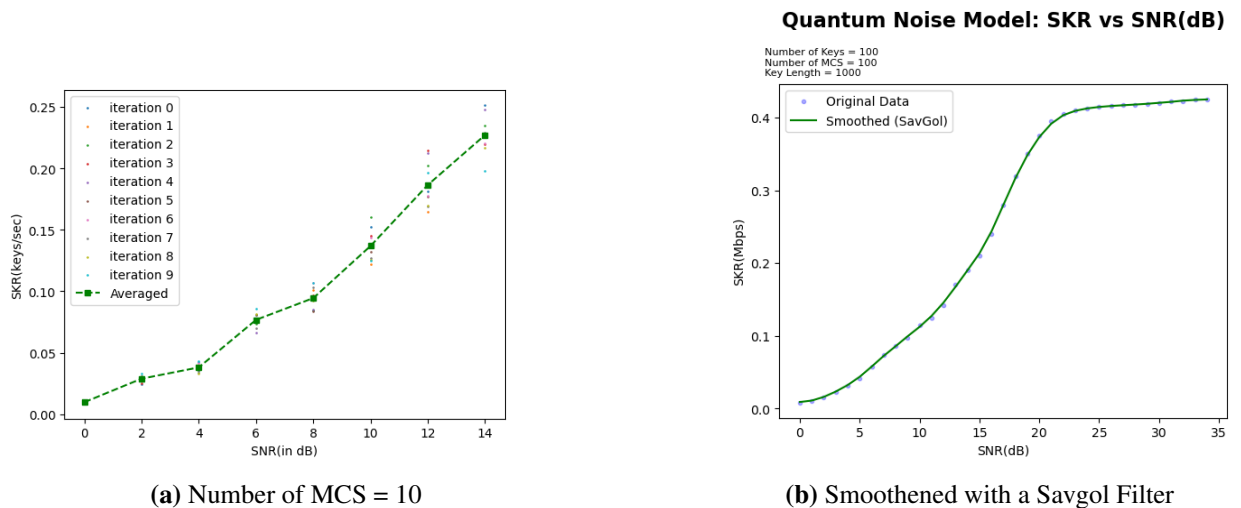


Figure 5.4: Quantum Noise Model(QNM)

The Quantum model simulates the noise along with the encoding of states using quantum simulator framework Qiskit[31]. Each key is assigned raw key-length number of 1-qubit circuits, which is then simulated on the *qasm_simulator* backend hosted by IBM, with a manually defined noise model. The noise model includes depolarization errors, amplitude damping, and phase damping to simulate classical AWGN.

Figure 5.4a is plotted with only ten MCS, and shows the steady increase in the value of SKR with increasing SNR, albeit with low values. To improve upon that, more MCS are simulated, resulting into figure 5.5, which is more statistically sound.

Figure 5.4b is the result of applying a *Savgol Filter* on the plot, which smoothens the plot a bit: reducing the effect of randomness.

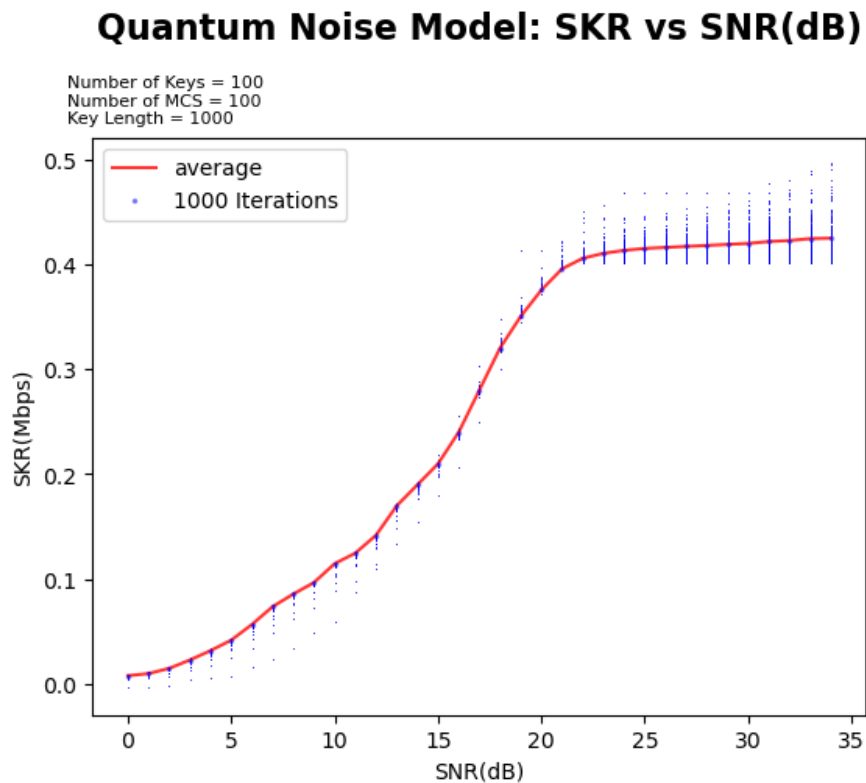


Figure 5.5: QNM: 100 MCS

Figure 5.5 appears to have reached almost the max. value of more than 400 Kbps. Multiple factors account for the specific values in the outcome, including the noise probabilities considered, types of noise incorporated, the gates/operations on which noise was applied, the computer hardware used etc.

5.4 Classical Model

Figure 5.6 represents various levels of probability of eavesdropping(λ). The metrics studied here are the averaged values of Meta-QBER, Spot-QBER, Corrected-Key-QBER, Classical-QBER, Time-Taken, Keys accepted and discarded, and SKR. It demonstrates a concrete observation of the impact that the probability of eavesdropping has on each parameter. There are no intersections/crosses between the plots, keeping them strictly bound.

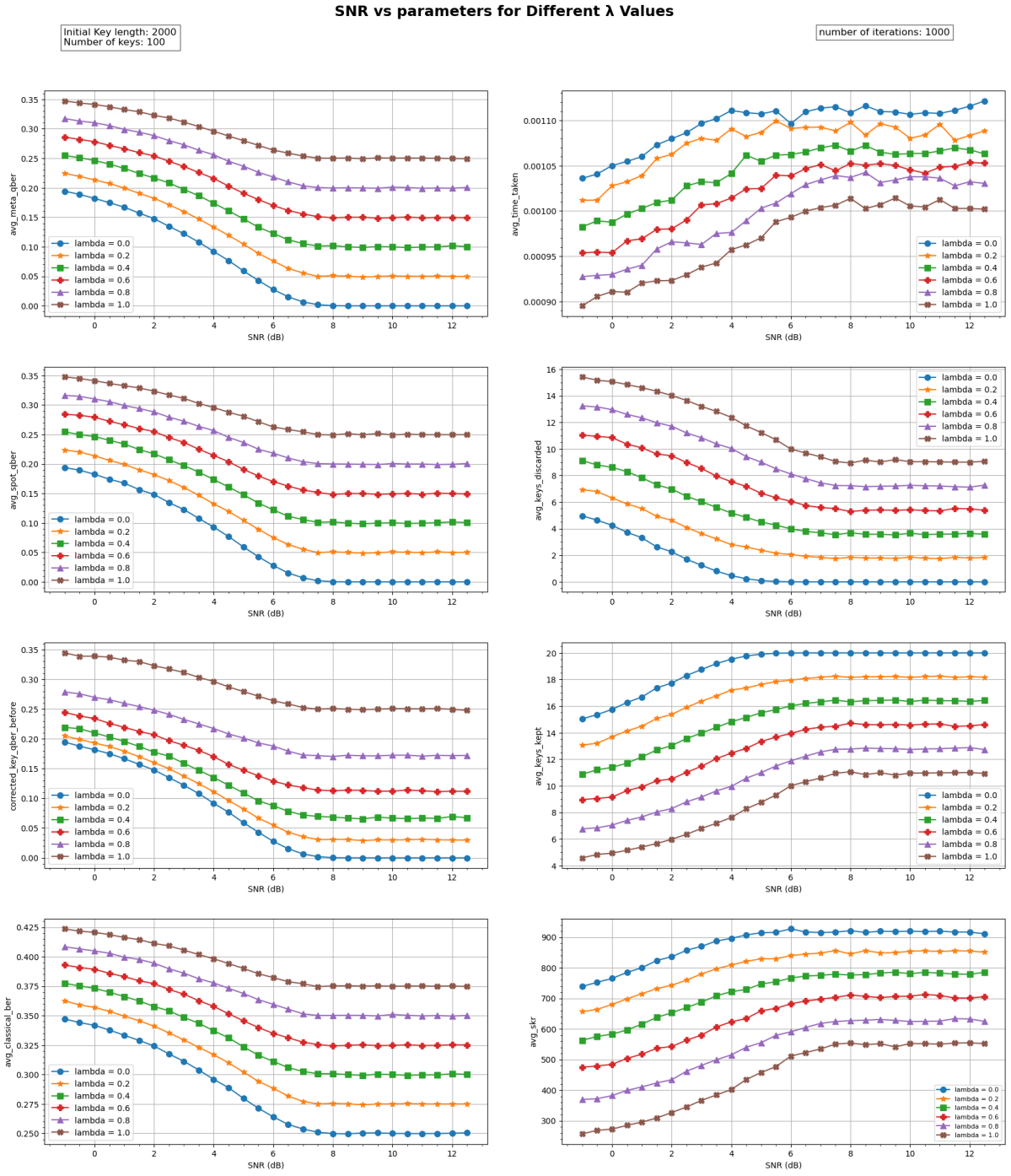


Figure 5.6: Variation in plots for different values of eavesdropping probability

Figure 5.7 shows the number of the keys kept/discarded with respect to the change in SNR. The simulation starts with less keys being kept and more being discarded for lower SNR, however, at higher SNRs the acceptance rate reaches 100%. The same behaviour continues for higher SNR.

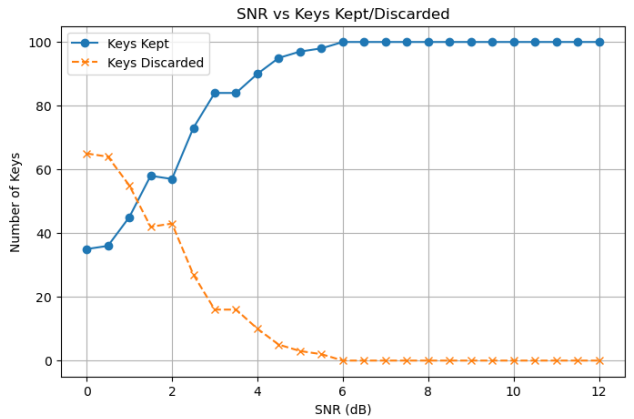


Figure 5.7: Over a 100 Iterations: Keys accepted/discarded

A larger simulation is executed in absence of Eve with 1000 MCS having 1000 keys each, with each key containing 768 symbols(key length). The SNR step size is also lowered, therefore increasing the total number of SNR values and AWGN is incorporated. Figure 5.8 is achieved with clear trends. All the QBERs decrease with increase in SNR, the Secure Bit Rate/SKR increases with increasing SNR as less and less bits are erroneous. The distilled key length is remarkably consistent with variations of less than 1%.

The Meta-QBER and the Spot-QBER approach the minimum possible statistical value of 0. The minimum statistical value for the Classical BER is 0.25(as half of the bases will mismatch; which in-turn will result into equal probabilities of giving either the correct or the flipped "classical" bit).

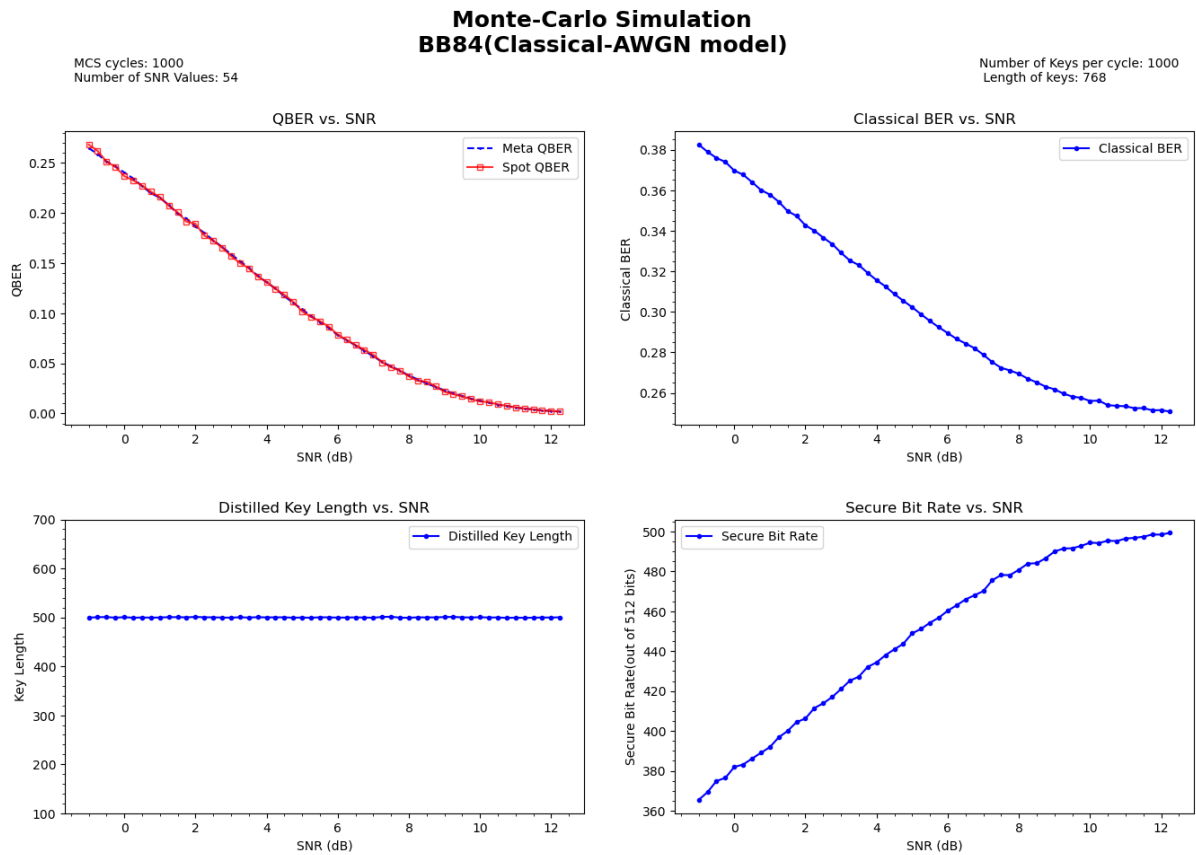


Figure 5.8: MCS-AWGN: 10^3 cycles, 10^3 keys, 3×256 symbols

To further enhance the results obtained in the simulation earlier, the key length is increased to 1000, with all the other parameters being kept constant. This improvement gives a better results that has little to no kinks in the plots as shown in 5.9.

The trends and values seen for various metrics in the simulation earlier are preserved. The plot of *key length* vs SNR is zoomed in to inspect the magnitude of change; it turned out to be ± 2.5 less than the mean of roughly 500, which is $\pm 0.5\%$.

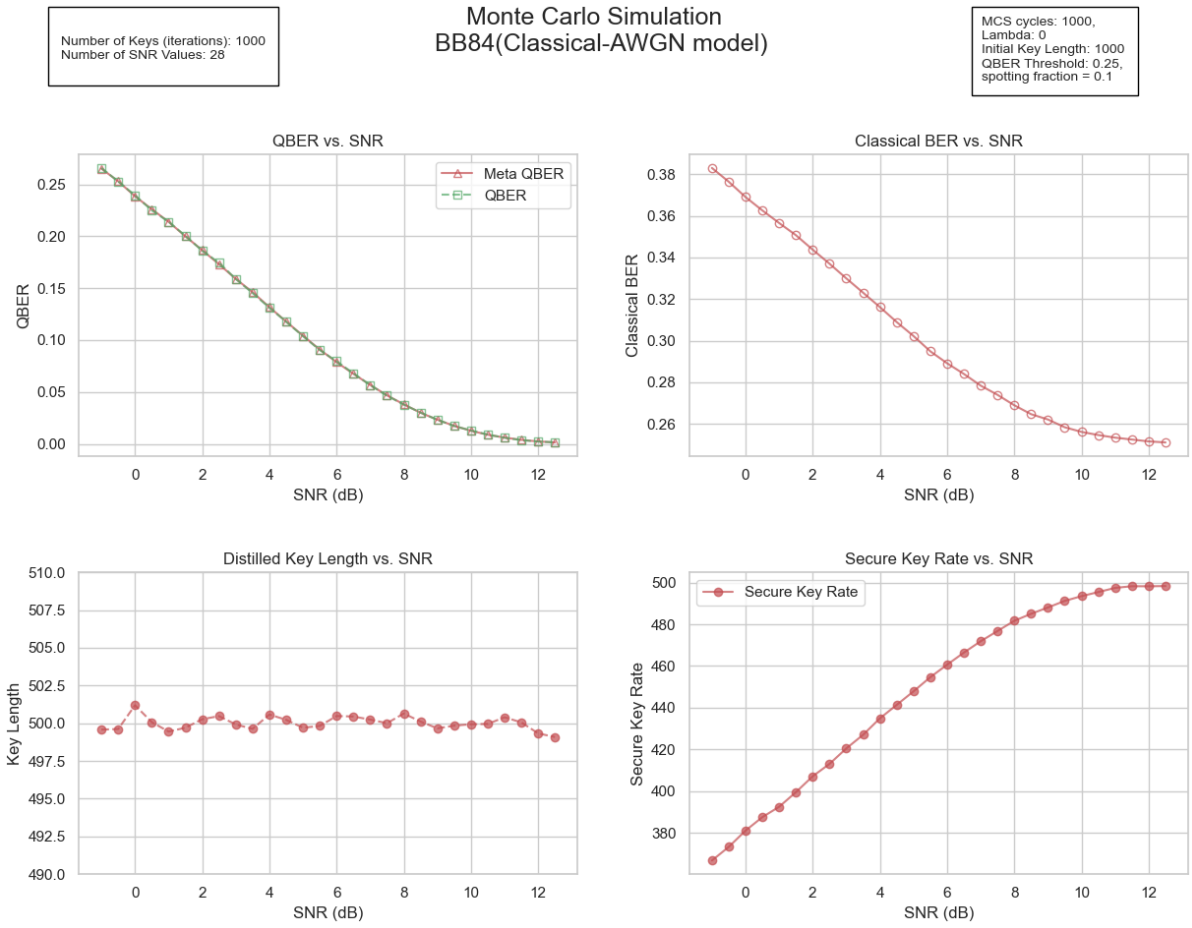


Figure 5.9: MCS with key length of 1000

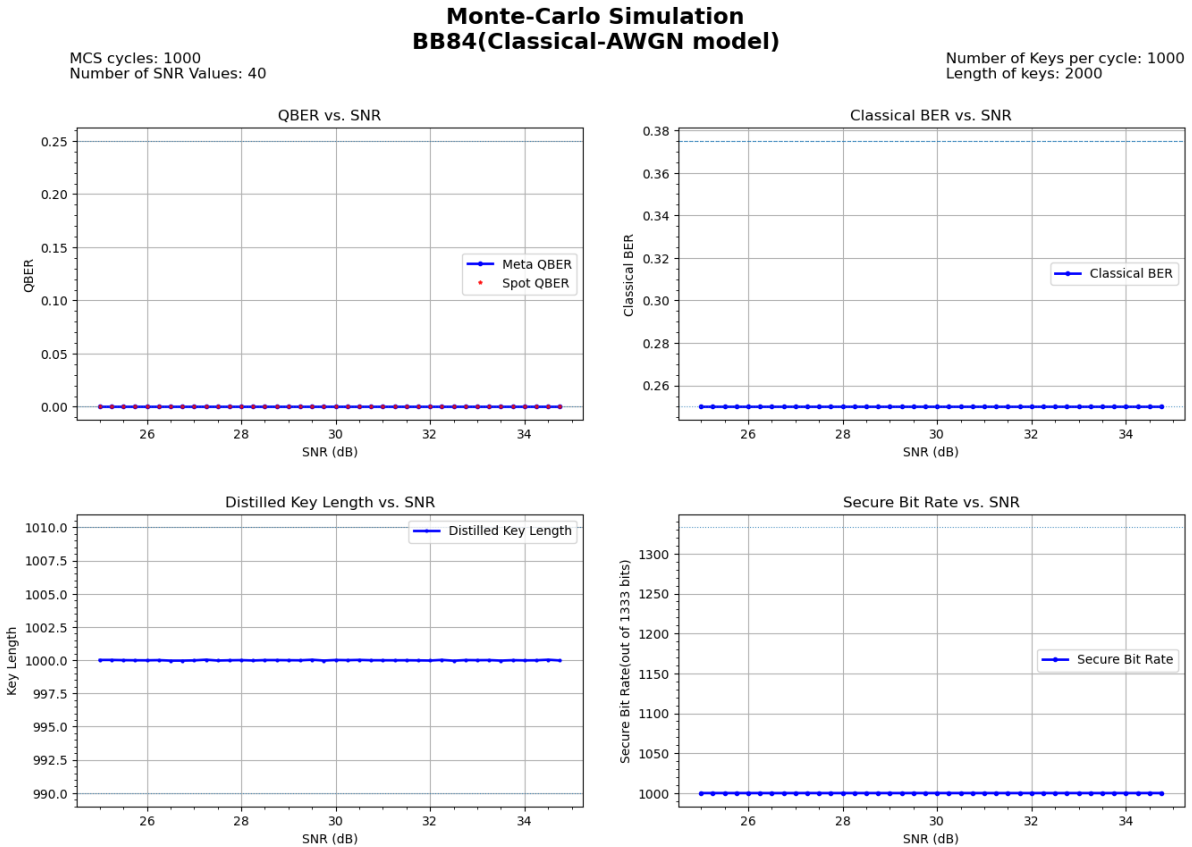
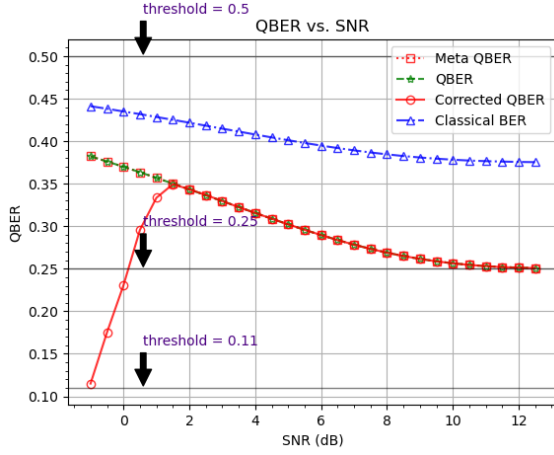
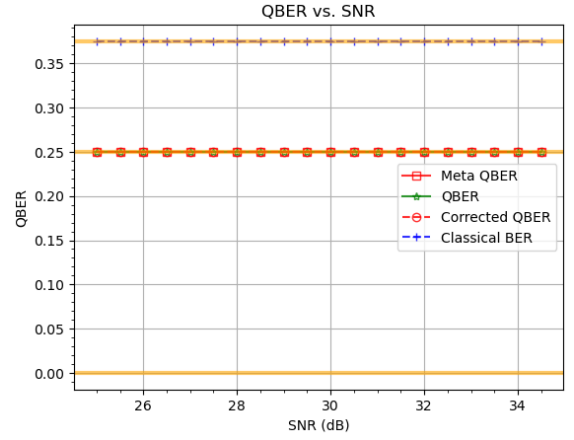


Figure 5.10: For Higher SNR values: 25-35. In absence of Eve

The SNR values of 25-30 are quite large for key lengths of the order of only a couple thousands to register any significant number of errors. Therefore, as is seen in figure 5.10 as well as in the previous results, all the parameters approach their ideal values.



(a) For lower SNR



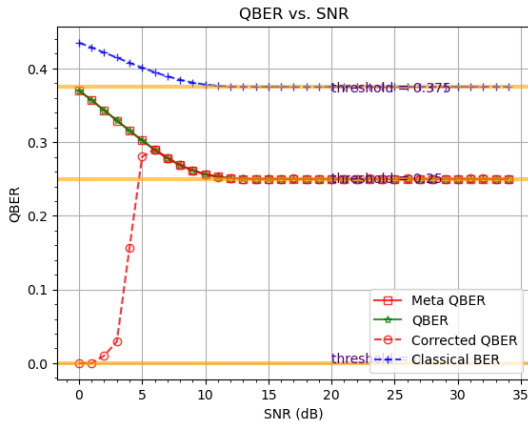
(b) For higher SNR

Figure 5.11: In presence of Eve

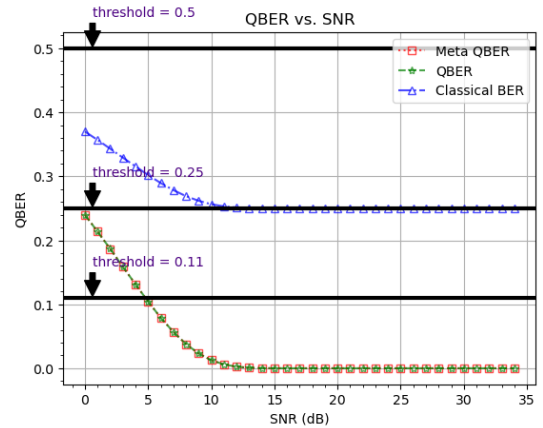
Figure 5.11a (the lower SNR region) and 5.12a (the full SNR range) show an interesting behaviour where the *Corrected QBER* (before spotting and correction) value is concerned. This is because Eve's presence causes the initial(low) SNR keys to be very erroneous, leading to most being discarded and therefore not counted in the calculation of *Corrected QBER*. This results in low number of keys being accepted—the ones whose QBERs are less than the threshold.

As the SNR increases, the number of accepted keys eventually builds up; the *Spot QBER* of more and more keys fall below the QBER threshold, which adds to the total QBER(Corrected)—increasing the QBER value; until it equals the *Spot QBER*

For the case of high SNR, in the presence of Eve (figure 5.11b, *Spot QBER* and *Meta QBER* saturate at a value of ~ 0.25 , while the *Classical BER* saturates at a value of ~ 0.375 . These values match with the theoretical values, where the presence of Eve causes only one-fourth of Alice's and Bob's bases to align.



(a) In presence of Eve



(b) In absence of Eve

Figure 5.12: For a full SNR Range(0-35)

Figure 5.12b shows the behaviour of QBER in absence of Eve. The results converge to ideal values

at higher SNRs.

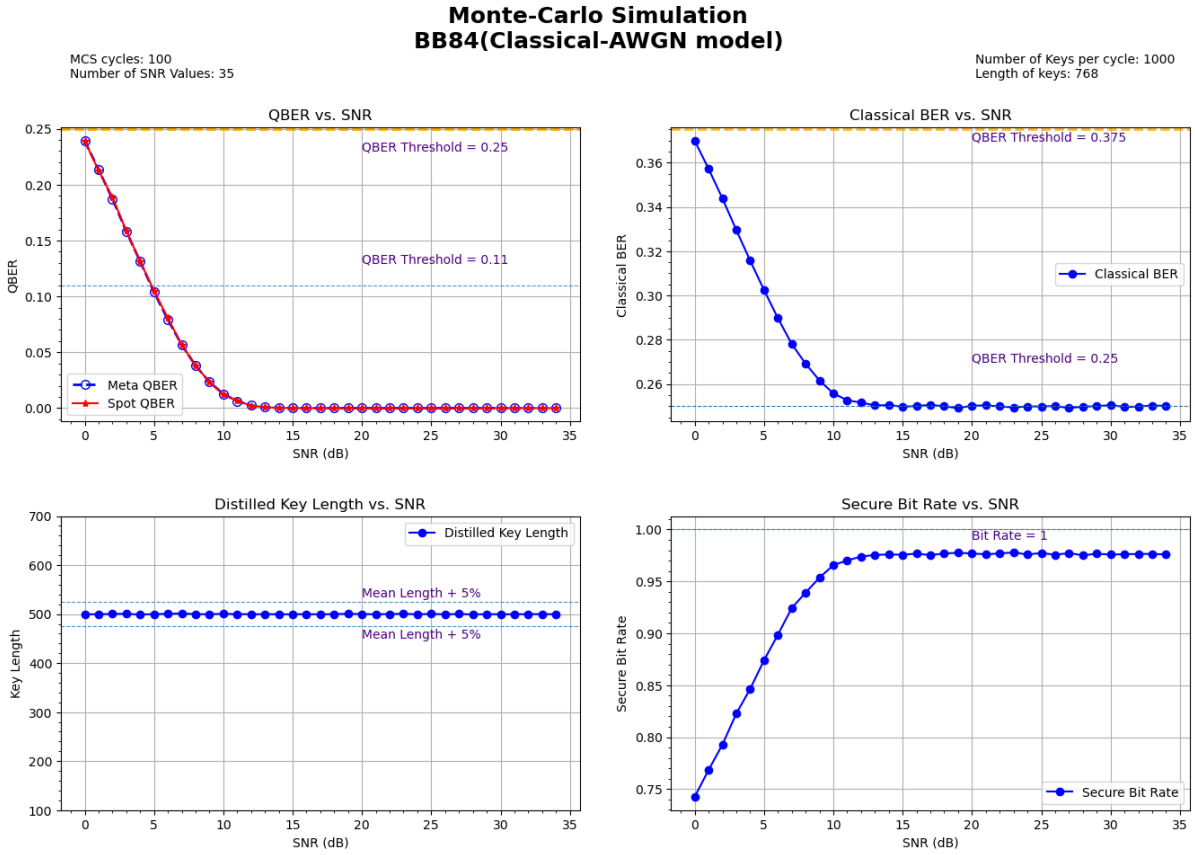


Figure 5.13: SNR range 0-35

Figure 5.13 makes it clear the trend that QBER, SKR, the time taken, and the average output length follow with respect to SNR (and therefore distance). As the SNR increases, the QBER value drops to almost 0.

Figure 5.14 shows a zoomed-in picture of the plot. It shows the marginal change that QBER value shows at higher SNRs. Overall, beyond the SNR of 12 dB, the network performs well when paired with cascade error correction technique, even in presence of Eve.

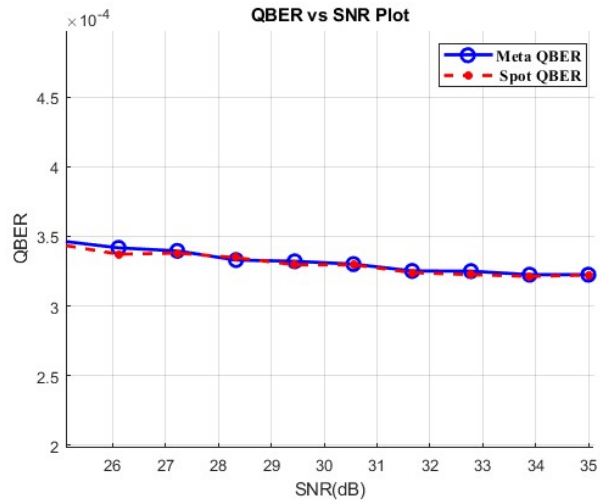


Figure 5.14: Zoomed-in view of QBER at higher SNRs

5.5 QBER vs. Noise Level

- **Analysis of the Fully Classical Model:** In the fully classical model e.g. figure 5.6, the QBER starts high under low SNR conditions and gradually decreases as the signal strength (and SNR) increases. Without an eavesdropper, the error is manageable for the Hamming error correction protocol (QBER threshold: 0.11) at a high enough SNR. However, once QBER

exceeds this threshold, the Hamming code becomes insufficient to correct the errors, leading to key rejection. Cascade algorithm comes to rescue in this situation.

- **Analysis of the Hybrid Model:** In contrast, the hybrid model—thanks to Qiskit’s noise handling—shows a slightly better tolerance to low SNR. The quantum-specific encoding(polarization states) provides more stability, but it requires a lot of quantum resources to simulate; this is quite expensive. With the implementation of Hybrid and Quantum Noise model, QBER decreases with increasing SNR, eventually converging to the same value as the classical model.
- **Analysis of Fully Quantum Model:** There are various kinds of noises available to implement in Qiskit’s noise model, such as Depolarization noise, amplitude/phase damping, readout error, quantum error, etc. To simulate the AWGN, depolarization error and amplitude/phase damping are implemented. It reflects a behaviour similar to what is observed in other cases, although with more accurate simulation.
- **Eve’s Influence:** When Eve is present, we see a dramatic increase in QBER, reaching approximately 0.25 in both models. At this level, Hamming is no longer viable, and we must rely on Cascade error correction to mitigate the errors.
- **Reflection:** This behavior aligns with what we would expect based on the literature. Similar studies[35], report comparable spikes in QBER under eavesdropping conditions. However, the hybrid model’s resilience under moderate noise suggests potential for future optimizations in practical quantum network applications.

5.6 Classical BER vs. Noise Level

- **Plot Description:** The figures depict the Classical Bit Error Rate (BER) as a function of noise. In each model, QBER and classical BER decrease as the SNR increases, but the classical BER stabilizes at a higher value under eavesdropping conditions, reaching a value of around 0.375.
- **Analysis:** The classical BER rises in tandem with noise, reaching concerning levels as soon as Eve starts intercepting. The presence of an eavesdropper leads to a spike in classical BER, consistent with expectations from intercept-resend attacks.
- **Discussion:** This trend is consistent with studies on classical and quantum channels in noisy environments, where classical BER tends to stabilize at higher values than QBER.

5.7 SKR vs. Noise Level

- **Plot Description:** The figures show the SKR for all models. SKR is a critical metric, as it represents the rate at which secure bits are exchanged between Alice and Bob after error correction.

The SKR is represented in different ways throughout the work as is suited. The SKR can be interpreted in terms of the keys negotiated per second, when the raw key length is constant.

- **Analysis:** As SNR increases, SKR predictably increases. In the classical model, SKR increases rapidly, with a notable decline when Eve is present. This is most likely due to the relatively low overhead in terms of time in case of classical model. In the hybrid model, SKR

performs better than Quantum model, but is slightly worse off than the classical model. This is anticipated due to the varying stress each model puts on the hardware and differences in physical implementations.

- **Reflection:** The rapid fall in SKR(when SNR decreases) aligns with the findings of [36], who reported that QKD systems become almost unusable when QBER surpasses certain thresholds. Our results reflect this, with SKR declining rapidly after the threshold QBER.

5.8 Quantum Key Resource Allocation (QKRA)

This section details the Quantum Key Resource Allocation (QKRA) system within an ODCN, designed to securely manage quantum key exchanges alongside efficient resource allocation. Built upon the NSFNET topology of 14 nodes and 21 bidirectional links, the ODCN model includes three distinct channels as mentioned earlier: TDC, QSC, and PIC. Each CR specifies a SL—high, medium, or low—along with source and destination nodes. The aim is to dynamically adjust SLs in response to resource availability, balancing network security with optimal resource utilization.

5.8.1 Network Model and Adaptive Security Levels

With the QKRA model, I implemented the network simulation entirely in Python, tailoring each component to enable dynamic SL adjustments and effective resource allocation for quantum-secured communications. The QSC is structured with three dedicated wavelengths, each corresponding to a specific SL with allocated time slots. By adapting existing Specific Security Level(SSL) methods to create a more flexible model, the QKRA algorithm avoids blocking requests and instead adjusts SLs according to real-time resource demands, enhancing network resilience under varying conditions.

5.8.2 Adaptive Heuristics and Resource Allocation Strategy

The adaptive heuristics that drive QKRA's resource allocation were derived from the base paper[16], but I developed the entire coding framework to bring these strategies into a fully functional simulation. A priority queue is created where CRs with higher SL are given priority and put first. Two heuristics were implemented to support adaptive SL management:

- **QKRA-ASSL** prioritizes adapting to high-SL when the resources in the requested SL are not available, and the occupancy of the higher SL is below a threshold—after all the CRs with high SL requests are dealt with.
- **QKRA-AWSL** dynamically lowers SLs when resources in the requested SLs are not available, allowing more CRs to proceed while upholding overall security standards.

The coding structure involved creating custom Python classes to model Links and CR attributes, including SLs and quantum channel requirements. For routing, I implemented the k-SP algorithm, which calculates multiple viable routes for each CR based on link weights, distances, and availability. A First-Fit(FF) allocation strategy then identifies and assigns each CR to the first path with adequate resources, ensuring rapid provisioning within high-demand environments.

5.8.3 Performance Analysis and Metrics

Through these custom-coded algorithms, I derived results based on key performance metrics:

- **SRCR:** This metric assesses the proportion of successfully provisioned CRs relative to total requests, reflecting the network's capability to handle demand without compromising SL requirements.
- **TUR:** TUR measures the efficiency of time slot use across available channels, with higher values signaling effective resource utilization.
- **NSP:** NSP evaluates how well QKRA heuristics prioritize high-security CRs while dynamically managing SLs as needed.

The coding framework I developed for QKRA successfully integrates adaptive SL adjustments, resource flexibility, and efficient routing. This portion of the work highlights how tailored algorithms can sustain secure key distribution even in high-demand quantum-secured environments, providing a robust foundation for further enhancements in adaptive heuristics and resource allocation strategies.

5.9 Resource Allocation Efficiency

- **Plot Description:** Figure 5.16 presents the performance of the system in terms of SRCR, TUR, and NSP in the ODCN.
- **SRCR:** Under moderate load, SRCR remains, but decreases rapidly with higher total requests.
- **TUR and NSP:** Both TUR and NSP follow a similar pattern, with resource utilization peaking under low-noise conditions. As noise and adversarial interference increase, the system's ability to provision resources diminishes, leading to a significant drop in TUR.
- **Reflection:** These results underscore the importance of efficient resource allocation in maintaining system performance under adverse conditions. In ODCNs, where multiple CRs compete for resources, the ability to dynamically allocate wavelengths and time slots becomes even more critical.

5.9.1 Simulation ASLC

Figure 5.15 shows the plots from the base paper. There are four plots in each subfigure, representing the proposed heuristics and the existing algorithms.

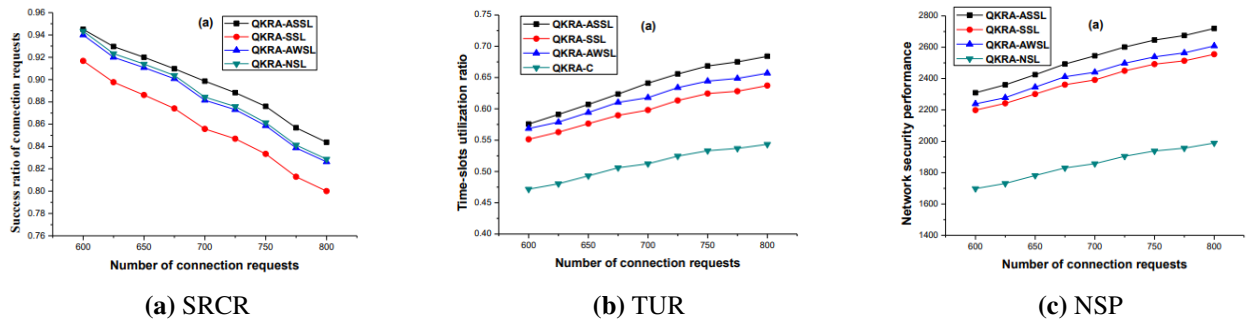


Figure 5.15: Plots from base paper

Figure 5.16 shows the comparison between the values from base paper and the values I got from simulation. The offset in the two cases could be due to non-optimal optimization of my code. The

crux of the simulation, however, is preserved—the plots follow the expected trends and the plots seem to converge at higher number of CRs, suggesting that the underlying issue has little effect when the network is under reasonable load.

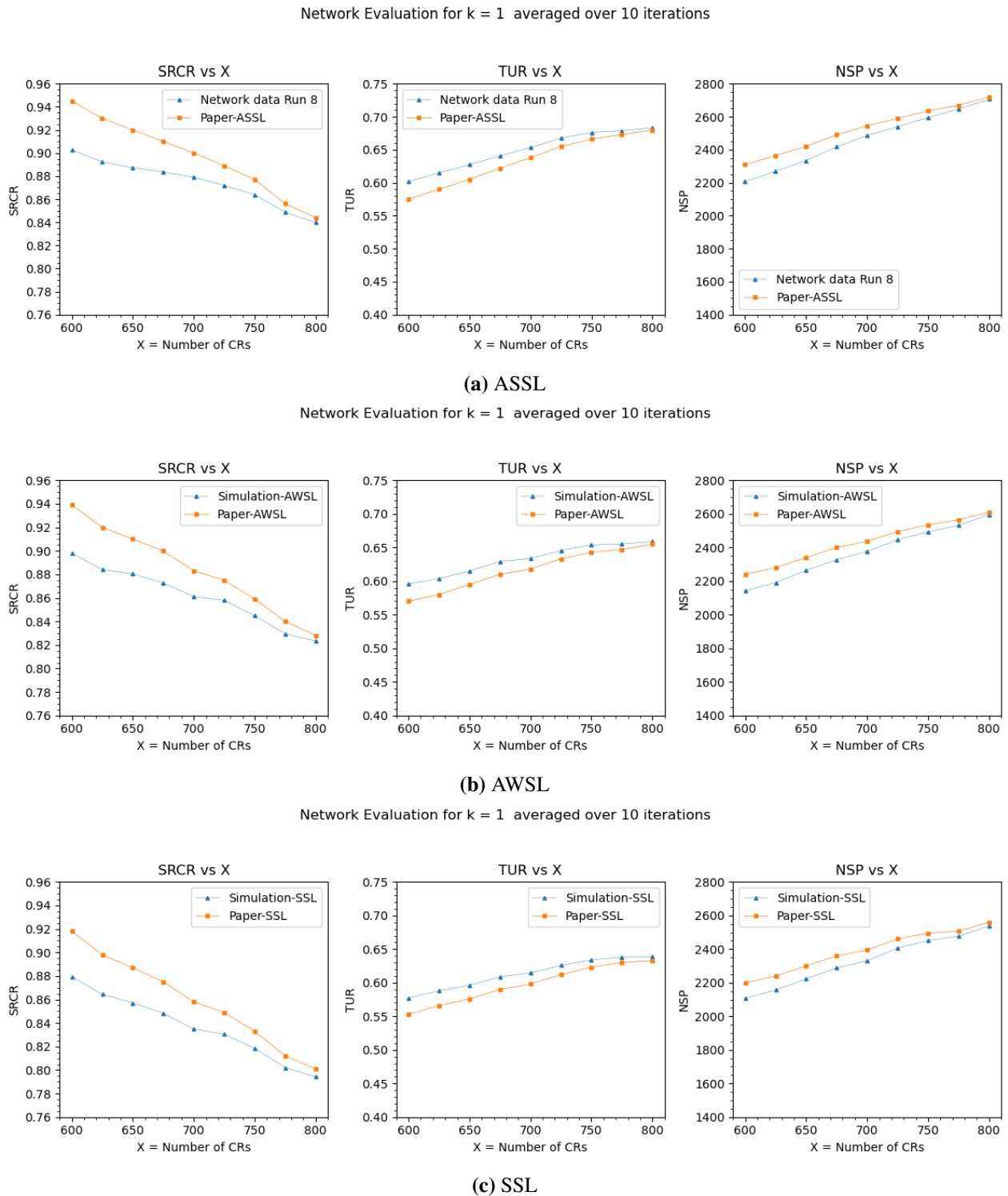


Figure 5.16: Comparison of simulation results with the base paper

Figure 5.17 shows the results of the ODCN simulation over 10 iterations. The top plot shows the count of provisioned and blocked CRs. It can be clearly seen that at the start, the count of provisioned CRs is a lot higher than that of the blocked CRs. As the number of CRs increase, the increment in the count of provisioned CRs is marginal but that of the blocked CRs is rapid—this reflects the increase in occupancy fraction, and after some value, the number of CRs getting

blocked is greater than the number of CRs getting provisioned.

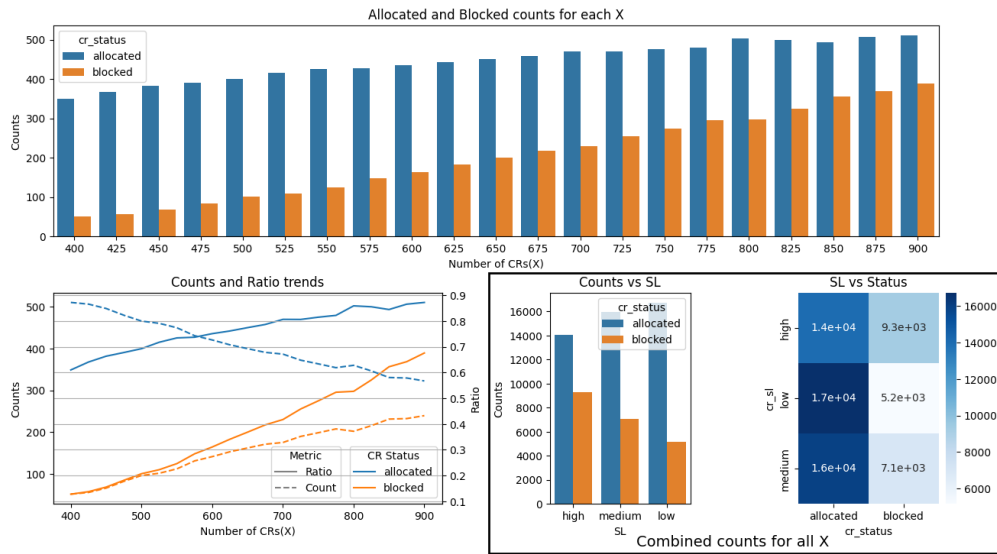


Figure 5.17: CR Analysis

The same can be inferred from the plot of the count ratio; here the plot for the ratio of blocked CRs to the total is steeper than that of the provisioned CRs.

The bar graph compares the trends between the allocation of different SLs.

5.10 Incorrect Results

Below are some of the results that were inaccurate. The reasons varied from a buggy code(wrong indexing) to logical issues. These issues were later corrected and the plots have been attached above.

Network Evaluation for QKRA : averaged over 100 iterations, $k = 1$

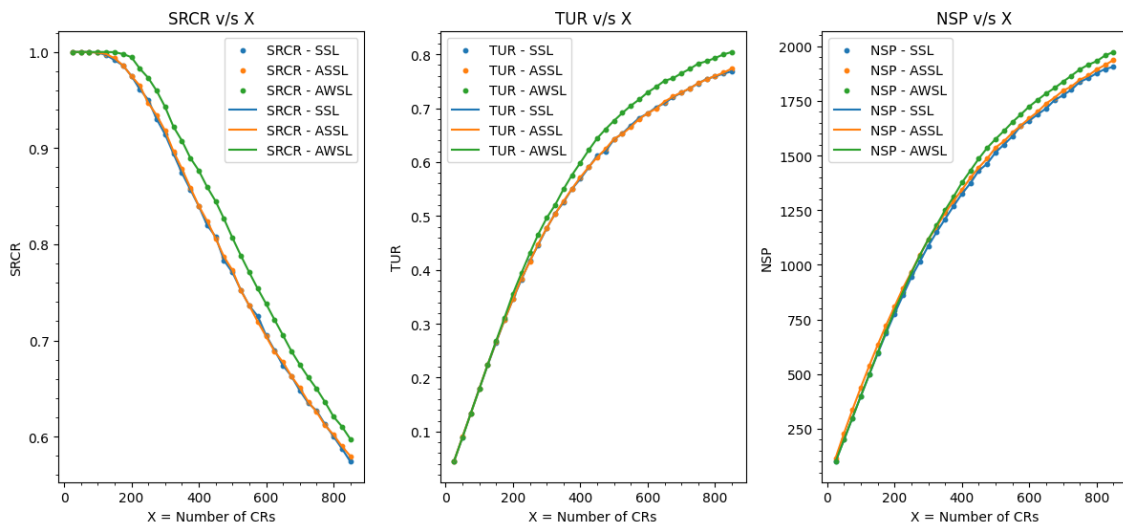
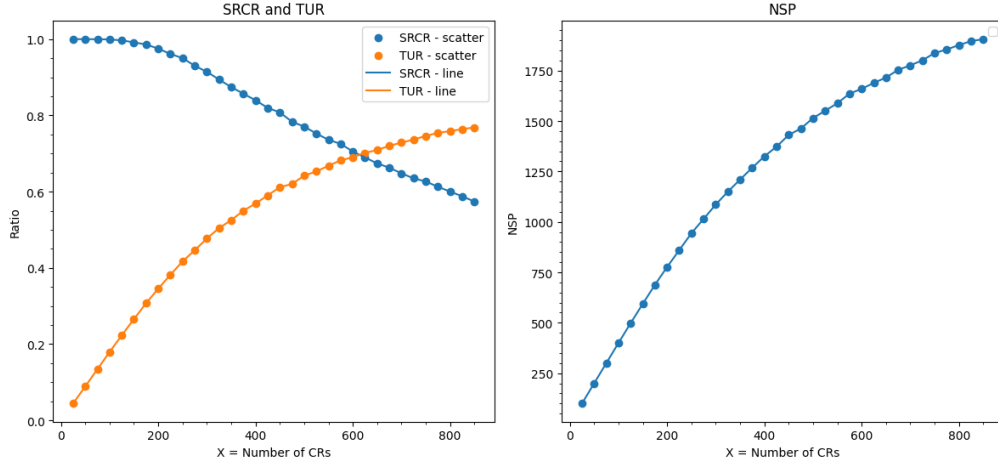


Figure 5.18: Comparison of the SRCR, TUR, and NSP metrics obtained for ASSL, ASSL, and SSL

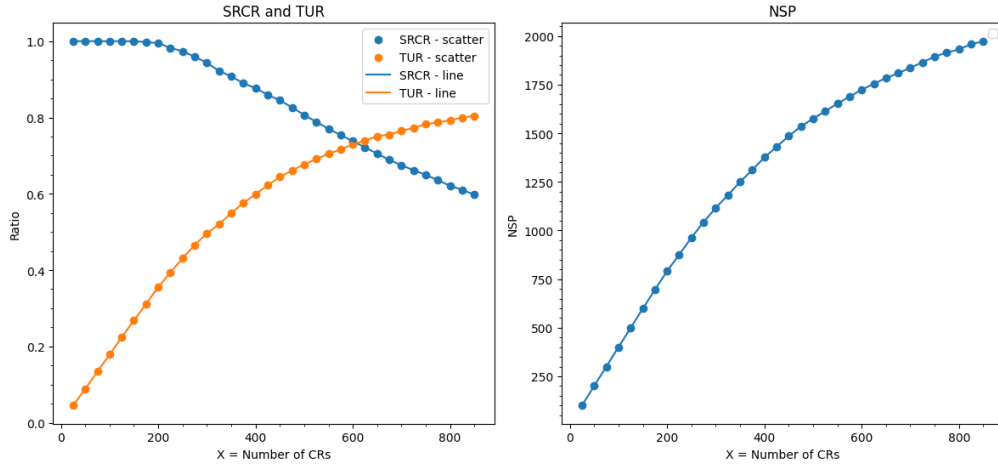
The simulation parameter in the case of figure 5.18 are: MCS = 100, $k = 1$ for X - 25 to 850.

Network Evaluation for QKRA-SSL : averaged over 100 iterations, $k = 1$



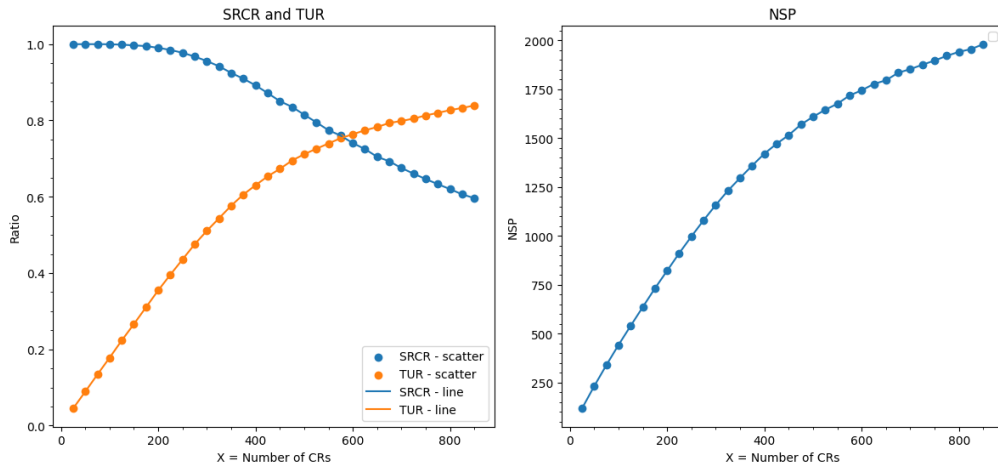
(a) SSL

Network Evaluation for QKRA-AWSL : averaged over 100 iterations, $k = 1$



(b) AWSL

Network Evaluation for QKRA-ASSL : averaged over 100 iterations, $k = 3$



(c) ASSL

Figure 5.19: Inaccurate results obtained

Figure 5.19 shows inaccurate results for individual metrics which are off by more than the allowed errors. Figure 5.18 shows the comparison between different heuristics, and as is evident, the improvements are not articulate and discernible.

5.11 Discussion and Interpretation

The results from these simulations highlight several key points:

- **Impact of Noise and Eavesdropping:** The increase in QBER and BER under high noise conditions underscores the vulnerability of both models(classical and hybrid) to environmental factors. The presence of an eavesdropper like Eve significantly compromises the key exchange process in both models.
- **Error Correction Methods:** The Hamming code proves effective for low-noise scenarios, with QBER remaining under the 0.11 threshold, as it can correct one-bit errors with certainty. However, once QBER rises above this, applying the Hamming technique further increases the QBER as it misidentifies a bit to be erroneous. Heere, Cascade becomes the preferred method for error correction, particularly when dealing with eavesdropping. The simulation confirms that Cascade(with maximum 4 passes allowed) can handle QBER values as high as 0.25, in line with the benchmarks used in other studies.
- **SKR and Resource Utilization:** The sharp decline in SKR under noisy conditions highlights the limitations of current QKD systems in maintaining high transmission rates when environmental noise or adversaries are present. This issue is compounded in ODCNs, where the success of quantum key provisioning depends on efficient resource allocation, as reflected in the SRCR and TUR metrics.

Chapter 6

Discussion

6.1 Interpretation

The plots can be categorized into 3 groups: present/absence of Eve, the error correcting code used: Hamming/cascade, the noise model used.

This research aimed to establish a secure QKD protocol within a QKD-secured ODCN. By exploring both a Fully Classical Model and a Hybrid Model, we evaluated key metrics such as QBER, Classical BER, and SKR under varying conditions of noise and eavesdropping. Furthermore, the effectiveness of Hamming and Cascade error correction methods was scrutinized to assess the resilience of the system in the face of environmental challenges.

6.2 Quantum Key Distribution and Error Correction

The QKD results revealed that both models performed as expected in low-noise environments, maintaining low QBER values. However, as noise levels increased, the system began to experience significant degradation, especially when Eve was introduced as an eavesdropper.

- **Fully Classical Model:** This model displayed predictable behavior, with QBER rising gradually with noise and sharply under adversarial conditions. The Hamming code was chosen to correct for errors when QBER was below 0.11.
- **Hybrid Model:** The hybrid model, leveraging quantum-specific operations through Qiskit, demonstrated a more accurate behaviour. Similar to the classical model, when noise exceeded a certain point or when Eve was present, QBER shot up to around 0.25, requiring the Cascade protocol for correction.

The choice of error correction methods proved crucial to maintaining secure communication. While Hamming codes were efficient in low-noise scenarios, the Cascade protocol was necessary to correct errors when QBER reached higher values. This aligns with the theoretical benchmarks found in existing research, where Cascade is known to handle QBER values up to 0.25 before key generation becomes impractical.

6.3 Resource Allocation in the Optical Data Center Networks

In addition to exploring quantum key exchange, this study simulated resource allocation in the ODCN. The system was tasked with efficiently managing both quantum and classical traffic,

dynamically allocating wavelengths and time slots to optimize network performance.

- SRCR remained high under normal conditions but began to drop as the number of CRs increased. Similarly, TUR and NSP, although increasing, were negatively impacted by a higher number of CRs(as the blocking rate increased).
- The three reserved wavelengths for QKD (with varying time slots for high, medium, and low-SLs) proved to be an efficient way to balance security needs with resource availability.

The results highlight the importance of adaptive resource allocation algorithms in maintaining network performance under adverse conditions. This corroborates with the base paper[16]. Also, the practical considerations such as the affect of environment led to a more accurate results.

6.4 Impact of Noise and Eavesdropping

The presence of noise and an eavesdropper (Eve) was shown to significantly disrupt the key negotiation process. As noise increased, the QBER reached the theoretical limit of 0.25, and SKR dropped to nearly zero in both models. The hybrid model showed a slight advantage in handling moderate noise, but this advantage diminished as adversarial conditions became more severe. However, this could be ascertained to the reliability and accuracy of the hybrid model in mimicing the actual QKD system.

- **QBER vs. BER:** The sharp rise in QBER and BER under eavesdropping conditions highlights the limitations of current error correction protocols when dealing with high noise or adversarial attacks. Eve's presence not only compromised the key integrity but also led to an observable increase in QBER and classical BER (~ 0.375), further disrupting the system's efficiency.

These results mirror findings in prior QKD research, where adversarial attacks are detected once QBER surpasses 0.25, leading to key rejection and moving on to the generation of another key. This suggests that while current error correction methods are sufficient for moderate noise, more resilient techniques are needed for higher noise conditions; more sophisticated attack detection methods might be necessary to handle advanced adversarial tactics.

Chapter 7

Conclusion

This study has successfully demonstrated the potential and challenges of implementing a secure QKD protocol within an ODCN. By simulating a fully classical model and a hybrid model, we have shown that quantum-specific approaches, while beneficial and guaranteeing the security of the key, still face significant challenges under noisy conditions or adversarial attacks.

Key Findings:

- **Error Correction:** The Hamming code is effective in low-noise environments but fails as QBER rises beyond a certain point. The Cascade protocol provides robust error correction up to QBER values of 0.25, making it the preferred choice in high-noise or adversarial settings.
- **Resource Allocation:** The ODCN performed well under moderate conditions, but as the number of CRs increased, the system struggled to maintain a high SRCR and TUR. This suggests that more adaptive resource allocation algorithms are necessary to maintain network performance when facing high traffic or noise.
- **Eavesdropping Detection:** The study confirmed that QBER is a reliable indicator of adversarial presence. When QBER exceeded 0.25, the system detected Eve's interference, and keys were rejected to preserve security. However, additional methods for detecting advanced attacks are needed.
- **Limitations:** The study relied on theoretical QBER thresholds for error correction, without direct benchmarks from real-world data. While the models accurately simulated the quantum key exchange process.

Chapter 8

Future Work

Future research should explore:

Advanced Resource Allocation: Developing more dynamic and adaptive strategies for allocating wavelengths and time slots in ODCNs based on real-time QBER and SKR values.

Sophisticated Adversarial Detection: Enhancing eavesdropping detection by incorporating more advanced attack models and machine learning algorithms to identify subtle attacks that go unnoticed with current QBER monitoring.

Realistic Noise Models: Incorporating real-world noise models into both the classical and hybrid simulations to better reflect the environmental challenges faced by quantum networks, and live network conditions to better reflect real-world challenges..

Tolerance: Future iterations of this system could focus on enhancing the hybrid model's noise tolerance and developing adaptive resource allocation algorithms that account for real-time QBER and SKR values.

Chapter 9

Pseudocode

Algorithm 1 QKD: Quantum Key Distribution Protocol

```
1: Inputs: Alice (sender: key length), Bob (receiver), SL of CR, QKD Protocol = BB84, Noise
   Level(related to SNR), Presence of Eavesdropper (Eve), and extent of presence( $\lambda$ ), spotting_fraction
2: Initialize:
3:   Define encoding bases and polarization states
4:   Initialize QKD metrics: QBER, SKR
5:   Set Privacy Amplification Algorithm = {SHA-256, SHA3-256}
6:   Define Error Correction Protocols = {Hamming, Cascade}
7:   Calculate the error rate(noise) from SNR
8: for each qubit  $i$  in the key do
9:   Alice encodes qubit  $i$  in random basis (X or +) using BB84
10:  Alice sends encoded qubit to Bob
11:  if Eve is present then
12:    Take  $\lambda$  into account
13:    Measure on Eve's end
14:  end if
15:  Apply noise model (classical or quantum) to simulate bit flips
16:  Apply noise in Qiskit using gates (e.g., X gate) for hybrid model
17:  Bob measures qubit in a random basis
18: end for
19: Step 2: Basis Comparison and Sifting
20: Publicly compare bases between Alice and Bob
21: Retain bits where bases match to create sifted key
22: Spot a fraction(spotting_fraction) of qubits
23: Step 3: Error Correction
24: if Error Correction Protocols == Hamming then
25:   Apply Hamming Code
26: else if Error Correction Protocols == Cascade then
27:   Apply Cascade Protocol
28: end if
29: Step 4: Privacy Amplification
30: Apply SHA-256 or SHA3-256 to sifted and corrected key
31: Step 5: Key Verification
32: Compare a small fraction of hashed versions of the final key
33: if keys match then
34:   Finalize the shared secret key
35: end if
36: Output: final shared secret key, updated QKD metrics (QBER, SKR) = 0
```

Algorithm 2 RA-ODCN: Resource Allocation in Optical Data Center Network

```
1: Inputs: Network Topology  $G$  (nodes, links), Security Levels  $SL = \{\text{High, Medium, Low}\}$ ,  
   Channels  $\{\text{TDC, QSC, PIC}\}$ , Connection Requests (CRs) with attributes (source, destination,  
   requested SL)  
2: Initialize:  
3:   Define dedicated wavelengths for each SL in QSC  
4:   Define time slots per wavelength for each SL  
5:   Set Heuristic =  $\{\text{QKRA-ASSL, QKRA-AWSL, QKRA-SSL}\}$   
6:   Create classes for Links and CRs to represent network resources and CR attributes  
7: for each incoming CR do  
8:   Determine CR's source and destination nodes, requested SL  
9:   Step 1: Determine k-Shortest Paths  
10:  paths = k_Shortest_Paths( $G$ , source, destination)  
11:  Step 2: Resource Allocation and SL Adjustment based on Heuristic  
12:  if Heuristic == QKRA-ASSL then  
13:    for each path in paths do  
14:      if resources available at higher than requested SL  $\geq$  half the total number of resources  
      then  
15:        Assign CR to path with the elevated SL  
16:        Mark resources as occupied  
17:        break  
18:      else if resources available at requested SL then  
19:        Assign CR to path with requested SL  
20:        Mark resources as occupied  
21:        break  
22:      else  
23:        Block CR  
24:      end if  
25:    end for  
26:  else if Heuristic == QKRA-AWSL then  
27:    for each path in paths do  
28:      if resources available at requested SL then  
29:        Assign CR to path with requested SL  
30:        Mark resources as occupied  
31:        break  
32:      else if Resources available at the next lower SL then  
33:        Adjust SL to next lower level (Medium or Low)  
34:        Assign CR to path with available resources at adjusted SL  
35:        Mark resources as occupied  
36:        break  
37:      else  
38:        Block CR  
39:      end if  
40:    end for  
41:  else if Heuristic == QKRA-SSL then  
42:    for each path in paths do  
43:      if resources available at requested SL then  
44:        Assign CR to path with requested SL  
45:        Mark resources as occupied  
46:        break  
47:      else
```



```
48:         Block CR
49:     end if
50: end for
51: end if
52: Step 3: Record Resource Utilization Metrics
53: Update SRCR, TUR, NSP
54: end for=0
```

Bibliography

- [1] W. Ma, B. Chen, L. Liu, H. Chen, W. Shao, M. Gao, J. Wu, and P.-H. Ho, "Equilibrium Allocation Approaches of Quantum Key Resources With Security Levels in QKD-Enabled Optical Data Center Networks," *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 25 660–25 672, 2022.
- [2] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.
- [3] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul 2000.
- [4] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.
- [5] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*. IEEE, 1984, pp. 175–179.
- [6] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.
- [7] T. C. Ralph, "Continuous variable quantum cryptography," *Physical Review A*, vol. 61, no. 1, p. 010303, 1999.
- [8] O. Amer, V. Garg, and W. O. Krawec, "An Introduction to Practical Quantum Key Distribution," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 30–55, 2021.
- [9] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2049–2083, 2021.
- [10] Y. Zhao, Y. Cao, W. Wang, H. Wang, X. Yu, J. Zhang, M. Tornatore, Y. Wu, Mukherjee, and Biswanath, "Resource Allocation in Optical Networks Secured by Quantum Key Distribution," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 130–137, 2018.
- [11] Y. Cao, Y. Zhao, X. Yu, and Y. Wu, "Resource assignment strategy in optical networks integrated with quantum key distribution," *Journal of Optical Communications and Networking*, vol. 9, no. 11, pp. 995–1004, 2017.
- [12] Z. Wu, H. Deng, and Y. Li, "An On-Demand Fault-Tolerant Routing Strategy for Secure Key Distribution Network," *Electronics*, vol. 13, no. 3, 2024.
- [13] G. Limei, R. Qi, J. Di, and H. Duan, "QKD iterative information reconciliation based on LDPC codes," *International Journal of Theoretical Physics*, vol. 59, pp. 1717–1729, 2020.
- [14] W. Heisenberg, "The physical content of quantum kinematics and mechanics," *Quantum theory and measurement*, pp. 62–84, 1983.
- [15] J. Lopez-Leyva, E. Garcia, E. Alvarez-Guzman, M. Ponce-Camacho, and A. Talamantes-Alvarez, *Challenges in free-space optical quantum key distribution*. Publisher Name, 2022, pp. 123–145.
- [16] C. Bowen, M. Weike, H. Bin, C. Hong, M. Jiang, S. Weidong, G. Mingyi, P. Limei, H. Pin-Han, P. Jason, and Jue, "Resource Allocation in Quantum-Key-Distribution Optical Data Center Networks," *IEEE*, 2023.
- [17] D. L. Mills and H.-W. Braun, "The NSFNET backbone network," in *Proceedings of the ACM workshop on Frontiers in computer communications technology*, 1987, pp. 191–196.
- [18] A. Biswas, A. Banerji, P. Chandravanshi, R. Kumar, and R. P. Singh, "Experimental Side Channel Analysis of BB84 QKD Source," *IEEE Journal of Quantum Electronics*, vol. 57, no. 6, pp. 1–7, 2021.

- [19] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on practical quantum cryptography,” *Physical review letters*, vol. 85, no. 6, p. 1330, 2000.
- [20] X. Zhong and G. Jin, “Application of Hamming Code Based Error Correction Algorithm in Quantum Key Distribution System,” in *2020 IEEE 3rd International Conference on Electronics Technology (ICET)*, 2020, pp. 857–861.
- [21] G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion,” in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1993, pp. 410–423.
- [22] C. E. Shannon, “A mathematical theory of communication,” *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.
- [23] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru, “Implementation of continuous-variable quantum key distribution with discrete modulation,” *Quantum Science and Technology*, vol. 2, no. 2, p. 024010, jun 2017.
- [24] K. Zhang, X. Yu, Y. Wang, Y. Li, Y. Zhao, and J. Zhang, “Service priority based cross-layer routing and resource allocation in quantum key distribution enabled optical networks (qkd-on),” in *2021 19th International Conference on Optical Communications and Networks (ICOON)*, 2021, pp. 1–3.
- [25] X. Yu, X. Ning, Q. Zhu, J. Lv, Y. Zhao, H. Zhang, and J. Zhang, “Multi-Dimensional Routing, Wavelength, and Timeslot Allocation (RWTA) in Quantum Key Distribution Optical Networks (QKD-ON),” *Applied Sciences*, vol. 11, no. 1, 2021.
- [26] X. Yu, S. Li, Y. Zhao, Y. Cao, A. Nag, and J. Zhang, “Routing, core and wavelength allocation in multi-core-fiber-based quantum-key-distribution-enabled optical networks,” *IEEE Access*, vol. 9, pp. 99 842–99 852, 2021.
- [27] P. Arteaga-Díaz, D. Cano, and V. Fernandez, “Practical Side-Channel Attack on Free-Space QKD Systems With Misaligned Sources and Countermeasures,” *IEEE Access*, vol. 10, pp. 82 697–82 705, 2022.
- [28] Y. Xu, L. Chen, and H. Zhu, “Quantum key distribution scheme with key recycling in integrated optical network,” *International Journal of Theoretical Physics*, vol. 62, no. 5, p. 103, 2023.
- [29] S. S. Gopinath, N., “Secured: quantum key distribution (SQKD) for solving side-channel attack to enhance security, based on shifting and binary conversion for securing data (SBSD) frameworks,” *Soft Comput* 27, 13365–13372, 2023.
- [30] P. Sharma, V. Bhatia, and S. Prakash, “Securing Optical Networks using Quantum-secured Blockchain: An Overview. arXiv 2021,” *arXiv preprint arXiv:2105.10663*.
- [31] A. Javadi-Abhari, M. Treinish, K. Krsulich, C. J. Wood, J. Lishman, J. Gacon, S. Martiel, P. D. Nation, L. S. Bishop, A. W. Cross, B. R. Johnson, and J. M. Gambetta, “Quantum computing with Qiskit,” 2024.
- [32] P. Mehdizadeh, M. R. Dibaj, H. Beyranvand, and F. Arpanaei, “Quantum-Classical Coexistence in Multi-Band Optical Networks: A Noise Analysis of QKD,” *IEEE Communications Letters*, vol. 28, no. 3, pp. 488–492, 2024.
- [33] Q.-H. Lu, F.-X. Wang, K. Huang, X. Wu, Z.-H. Wang, S. Wang, D.-Y. He, Z.-Q. Yin, G.-C. Guo, W. Chen, and Z.-F. Han, “Quantum Key Distribution Over a Channel with Scattering,” *Phys. Rev. Appl.*, vol. 17, p. 034045, Mar 2022.
- [34] *Optical Fiber Attenuation Specifications*.
- [35] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, “Measurement-device-independent quantum key distribution over a 404 km optical fiber,” *Physical review letters*, vol. 117, no. 19, p. 190501, 2016.
- [36] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Reviews of modern physics*, vol. 81, no. 3, pp. 1301–1350, 2009.